ID: 756302
Sample Name:
U59WtZz2Sg.exe
Cookbook: default.jbs
Time: 00:21:09
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report U59WtZz2Sg.exe 6
Overview 6
General Information 6
Detection 6
Signatures 6
Classification 6
Process Tree 6
Malware Configuration 7
Threatname: Clipboard Hijacker 7
Threatname: Djvu 7
Threatname: Vidar 8
Yara Signatures 8
PCAP (Network Traffic) 8
Dropped Files 8
Memory Dumps 9
Unpacked PEs 9
Sigma Signatures 10
Snort Signatures 10
Joe Sandbox Signatures 11
AV Detection 11
Networking 11
Spam, unwanted Advertisements and Ransom Demands 11
System Summary 11
Boot Survival 12
HIPS / PFW / Operating System Protection Evasion 12
Stealing of Sensitive Information 12
Remote Access Functionality 12
Mitre Att&ck Matrix 12
Behavior Graph 13
Screenshots 13
Thumbnails 13
Antivirus, Machine Learning and Genetic Malware Detection 14
Initial Sample 14
Dropped Files 14
Unpacked PE Files 15
Domains 16
URLs 16
Domains and IPs 16
Contacted Domains 16
Contacted URLs 16
URLs from Memory and Binaries 16
World Map of Contacted IPs 24
Public IPs 24
General Information 25
Warnings 25
Simulations 26
Behavior and APIs 26
Joe Sandbox View / Context 26
IPs 26
Domains 26
ASNs 26
JA3 Fingerprints 26
Dropped Files 26
Created / dropped Files 26
C:\ProgramData\155935024928932138495957O9 26
C:\ProgramData\283258756549760843543262 71 26
C:\ProgramData\285169655800310200354716 49 27
C:\ProgramData\500233254017371570635989 45 27
C:\ProgramData\531951220288921180464155 69 27
C:\ProgramData\698596123794895849070887 96 28
C:\SystemID\PersonalID.txt 28
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old 28
C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\4DDQNYCN\www.msn[1].xml 29
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe 29
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe:Zone.Identifier 29
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe 29
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe 30
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst 30
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst 30

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst 31
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat 31
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin 31
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst 32
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp 32
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs 32
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs 33
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx 33
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp 33
C:\Users\user\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-62FC182D-10C8.pma 34
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma 34
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 34
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log 34
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old 35
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Scripts\000003.log 35
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log 35
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old 36
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\128.png 36
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0_metadata\computed_hashes.json 36
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0_metadata\verified_contents.json 37
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\dasherSettingSchema.json 37
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\eventpage_bin_prod.js
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\manifest.json 3837
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\page_embed_script.js 38
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0_metadata\computed_hashes.json 38
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0_metadata\verified_contents.json 39
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\craw_background.js
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\craw_window.js 3939
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\css\craw_window.css
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\html\craw_window.html 39
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif 40
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\icon_128.png 40
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\icon_16.png 41
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button.png 41
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_close.png 41
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_hover.png 41
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_maximize.png 42
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_pressed.png 42
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\manifest.json 42
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\000003.log 43
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old 43
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico 43
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\ghbmnnjooekpmoecnnnilnnbdlolhkhi\000003.log 44
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log 44
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old 44
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old 45
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log 45
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old 45
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log 45
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log 46
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old 46
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\128.png 46
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\192.png 47
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\256.png 47
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\32.png 47
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\48.png 48
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\64.png 48
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\96.png 48
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest 49

Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\128.png 49
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\192.png 49
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\256.png 50
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\32.png 50
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\48.png 50
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\64.png 51
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\96.png 51
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\128.png 51
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\192.png 52
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\256.png 52
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\32.png 52
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\48.png 53
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\64.png 53
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\96.png 53
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\128.png 54
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\192.png 54
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\256.png 54
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\32.png 55
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db 55
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\heavy_ad_intervention_opt_out.db 55
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\previews_opt_out.db 56
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\000003.log 56
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000003.log 56
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old 57
C:\Users\user\AppData\Local\IconCache.db 57
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log 57
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log 57
Static File Info 58
General 58
File Icon 58
Static PE Info 58
General 58
Entrypoint Preview 59
Rich Headers 60
Data Directories 60
Sections 60
Resources 61
Imports 61
Possible Origin 61
Network Behavior 61
Snort IDS Alerts 61
Network Port Distribution 62
TCP Packets 62
UDP Packets 64
DNS Queries 64
DNS Answers 64
HTTP Request Dependency Graph 66
Statistics 66
Behavior 66
System Behavior 66
Analysis Process: U59WtZz2Sg.exePID: 5228, Parent PID: 3324 66
General 66
Analysis Process: U59WtZz2Sg.exePID: 3692, Parent PID: 5228 67
General 67
File Activities 68
File Created 68
File Written 69
Registry Activities 70
Key Value Created 70
Analysis Process: icacls.exePID: 1304, Parent PID: 3692 70
General 70
File Activities 70
File Written 70
Analysis Process: U59WtZz2Sg.exePID: 1272, Parent PID: 3692 70
General 70

Analysis Process: U59WtZz2Sg.exePID: 3184, Parent PID: 1084 71
General 71
Analysis Process: U59WtZz2Sg.exePID: 6132, Parent PID: 1272 71
General 71
File Activities 72
File Created 72
File Moved 74
File Written 93
File Read 215
Registry Activities 226
Key Value Created 226
Analysis Process: U59WtZz2Sg.exePID: 2312, Parent PID: 3184 226
General 226
File Activities 227
File Created 227
File Written 228
Analysis Process: U59WtZz2Sg.exePID: 5900, Parent PID: 3324 229
General 229
Analysis Process: build2.exePID: 1544, Parent PID: 6132 229
General 229
Analysis Process: U59WtZz2Sg.exePID: 4296, Parent PID: 5900 230
General 230
Analysis Process: build2.exePID: 5364, Parent PID: 1544 231
General 231
Analysis Process: build3.exePID: 5972, Parent PID: 6132 232
General 232
Analysis Process: schtasks.exePID: 5880, Parent PID: 5972 232
General 232
Analysis Process: conhost.exePID: 5968, Parent PID: 5880 232
General 232
Analysis Process: mstsca.exePID: 4536, Parent PID: 1084 233
General 233
Analysis Process: schtasks.exePID: 4612, Parent PID: 4536 233
General 233
Analysis Process: U59WtZz2Sg.exePID: 6096, Parent PID: 3324 233
General 234
Analysis Process: U59WtZz2Sg.exePID: 4756, Parent PID: 6096 234
General 234
Analysis Process: conhost.exePID: 4712, Parent PID: 4612 235
General 235
Analysis Process: WMIADAP.exePID: 4296, Parent PID: 2156 235
General 235
Disassembly 236

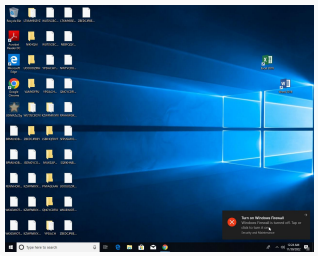
Windows Analysis Report

U59WtZz2Sg.exe

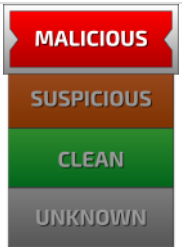
Overview

General Information

Sample Name:	U59WtZz2Sg.exe
Analysis ID:	756302
MD5:	41001fdd7879ce..
SHA1:	215964b0399da3.
SHA256:	aaef58ede9edbfc..
Tags:	exe TeamBot
Infos:	



Detection



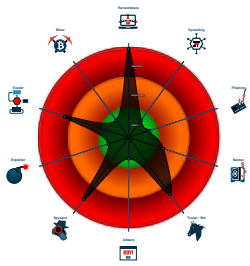
Babuk, Clipboard Hijacker, Djvu, Vidar

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found ransom note / readme
- Yara detected Babuk Ransomware
- Antivirus detection for URL or domain
- Yara detected Clipboard Hijacker
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware
- Yara detected Vidar stealer
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- U59WtZz2Sg.exe (PID: 5228 cmdline: C:\Users\user\Desktop\U59WtZz2Sg.exe MD5: 41001FDD7879CE9EDE214E92C7E492BE)
  - U59WtZz2Sg.exe (PID: 3692 cmdline: C:\Users\user\Desktop\U59WtZz2Sg.exe MD5: 41001FDD7879CE9EDE214E92C7E492BE)
    - icacls.exe (PID: 1304 cmdline: icacls "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
    - U59WtZz2Sg.exe (PID: 1272 cmdline: "C:\Users\user\Desktop\U59WtZz2Sg.exe" --Admin IsNotAutoStart IsNotTask MD5: 41001FDD7879CE9EDE214E92C7E492BE)
      - U59WtZz2Sg.exe (PID: 6132 cmdline: "C:\Users\user\Desktop\U59WtZz2Sg.exe" --Admin IsNotAutoStart IsNotTask MD5: 41001FDD7879CE9EDE214E92C7E492BE)
        - build2.exe (PID: 1544 cmdline: "C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe" MD5: B9212DED69FAE1FA1FB5D6DB46A9FB76)
          - build2.exe (PID: 5364 cmdline: "C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe" MD5: B9212DED69FAE1FA1FB5D6DB46A9FB76)
        - build3.exe (PID: 5972 cmdline: "C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe" MD5: 9EAD10C08E72AE41921191F8DB39BC16)
          - schtasks.exe (PID: 5880 cmdline: /C /create /F /sc mi nute /mo 1 /tn "Azure-Update-Task" /tr "C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe" MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 5968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- U59WtZz2Sg.exe (PID: 3184 cmdline: C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe --Task MD5: 41001FDD7879CE9EDE214E92C7E492BE)
  - U59WtZz2Sg.exe (PID: 2312 cmdline: C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe --Task MD5: 41001FDD7879CE9EDE214E92C7E492BE)
- U59WtZz2Sg.exe (PID: 5900 cmdline: "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart MD5: 41001FDD7879CE9EDE214E92C7E492BE)
  - U59WtZz2Sg.exe (PID: 4296 cmdline: "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart MD5: 41001FDD7879CE9EDE214E92C7E492BE)
  - WMIADAP.exe (PID: 4296 cmdline: wmiadap.exe /F /T /R MD5: 9783D0765F31980950445DFD40DB15DA)
- mstsca.exe (PID: 4536 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe MD5: 9EAD10C08E72AE41921191F8DB39BC16)
  - schtasks.exe (PID: 4612 cmdline: /C /create /F /sc mi nute /mo 1 /tn "Azure-Update-Task" /tr "C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe" MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- U59WtZz2Sg.exe (PID: 6096 cmdline: "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart MD5: 41001FDD7879CE9EDE214E92C7E492BE)
  - U59WtZz2Sg.exe (PID: 4756 cmdline: "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart MD5: 41001FDD7879CE9EDE214E92C7E492BE)
- **cleanup**

Malware Configuration

Threatname: Clipboard Hijacker


```
{
  "Crypto Addresses": [
    "DBbgRYaKG993LFJKCWz73PZqveWsnwRmGc",
    "3NLzE3tXwoagBrgFsjNNkPZfrESydTD8JP",
    "MBD2C8QV7RDrNtSDRe9B2iH5r7yH4iMcxk",
    "ltc1qa5lae8k7tzcw5lcjfvfs3n0nhf0z3cgrsz2dym",
    "addr1qx4jwm700r2w6fneakg0r5pkg76vu7qkt6qv7zxza3qu3w9tyahu77x5a5n8nmvs78grv3a5eeupvh5qeuyv9mzpezuq60zykl",
    "0xa6360e294DfCe4fE4Edf61b170c76770691aA111",
    "42UxohbdHGMYGPvW5Uep45Jt9Rj2WvTV958B5G5vHnawZhA4UwoD53Tafn6GRmcGdoSFUfCQN6Xm37LBZZ6qNBorFw3b6s2",
    "89SPVUAPHDLSq5pRdf8Eo6SLnKRJ8BNSYYnvPL6iJxGP4FBCBmkeV3CTSLCbk6uydxRnub4gLH6TBRycxSAQN2m1KcnhrSZ",
    "LLiNjWA9h4LxVtDigLQ79xQdGiJYC4oHis",
    "t1VQgJMcNsBHsDyu1tXmJZjDpgbm3ftmTGN",
    "bnb136ns6lfw4zs5hg4n85vdthaad7hq5m4gtkgf23",
    "Ae2tdPwUPEZDqNhACJ3ZT5NdVjkNffGAwa4Mc9N95udKWYzt1VnFngLMnPE",
    "1My2QNmVqkvN5M13xk8DWftjwC9G1F2w8Z",
    "bc1qx8vykfse9s9llguez9cuyjmy092yeqkesl2r5v"
  ]
}
```


Threatname: Djvu


```
{
  "Download URLs": [
    "http://uaery.top/dl/build2.exe",
    "http://fresherlights.com/files/1/build3.exe"
  ],
  "C2 url": "http://fresherlights.com/test1/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-5UcwRdS3ED\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@fishmail.top\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0609djfsieE",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
```

```
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz0nbtFHH+ICfx8iOU3fb||||n2XIrnrBpAvVGXvNxA5pZWItxKj+OvFrwG||/CEfnINrWfSr0K46pQ6f8hd+fO1tncP||||ns+VW+xVZVryNMzYFXUZr+uQfHpOMhRIq
9fOLGo6QD9iZN3O3Ovkgr+fNybG97Hk+||||nlZvbXnUfctQz9D6MB4KeGeFD3yqvY7hxUTQM98u1OR1zMKoS4wlqJOl2f55agMPx||||nOUQZGAVuRUMQFTjO97O||/LdPwxmS6WEFnUbS||/p9rvAaDk||/SP2E3JHXiO9+6inVHGa|
|||nIcs473QnGDkUz+O8KJNPyrFDKSLtu||/TtoT7f5iE2oS||/nQmJSQwA6eoz||/gCv||/GWMs||||ntQIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: Vidar


```
{
  "C2 url": "https://t.me/asifrazatg",
  "Botnet": "517"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x6436a:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
dump.pcap	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0x64061:$mutex_setup: 55 8B EC 83 EC 18 53 56 57 E8 F8 F4 FF FF 68 30 30 40 00 6A 00 6A 00 FF 15 40 40 40 00 FF 15 2C 40 40 00 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 40 00 • 0x640ee:$new_line_check: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0x640ee:$regex1: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0x64414:$regex2: 6A 34 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E 66 3B C1 74 19 83 F8 35 74 14 83 F8 36 74 0F 83 F8 37 74 ... • 0x644e2:$regex3: 56 8B F1 56 FF 15 20 40 40 00 83 F8 5F 0F 85 84 00 00 00 6A 38 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E ...

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif	SUSP_GIF_Anomalies	Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type	Florian Roth	
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ScreenshotOptIn.gif	SUSP_GIF_Anomalies	Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type	Florian Roth	
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.gif	SUSP_GIF_Anomalies	Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type	Florian Roth	
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif	SUSP_GIF_Anomalies	Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type	Florian Roth	
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\adm\OneDrive.adml	webshell_php_dynamic_big	PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k	Arnim Rupp	• 0x0:$php_short: <? • 0x5be6:$dynamic1: $\x9DK\xE5\xC39\xF4I($
Click to see the 6 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.378213612.0000000000627000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_STOP	Detects STOP ransomware	ditekSHen	• 0xffe88:$x1: C:\SystemID\PersonalID.txt • 0x100334:$x2: /deny *S-1-1-0:(OI)(CI)(DE,DC) • 0xffcf0:$x3: e:\doc\my work (c++)_git\encryption\ • 0x105b28:$x3: E:\Doc\My work (C++)_Git\Encryption\ • 0x1002ec:$s1: " --AutoStart • 0x100300:$s1: " --AutoStart • 0x103f48:$s2: --ForNetRes • 0x103f10:$s3: --Admin • 0x104390:$s4: %username% • 0x1044b4:$s5: ?pid= • 0x1044c0:$s6: &first=true • 0x1044d8:$s6: &first=false • 0x1003f4:$s7: delself.bat • 0x1043f8:$mutex1: {1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D} • 0x104420:$mutex2: {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} • 0x104448:$mutex3: {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}
00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0x105b28:$a: E:\Doc\My work (C++)_Git\Encryption\Release\encrypt_win_api.pdb • 0xd9ef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
Click to see the 165 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.U59WtZz2Sg.exe.3060000.0.raw.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
5.3.U59WtZz2Sg.exe.3060000.0.raw.unpack	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x1203:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
5.3.U59WtZz2Sg.exe.3060000.0.raw.unpack	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0xefa:$mutex_setup: 55 8B EC 83 EC 18 53 56 57 E8 F8 F4 FF FF 68 30 30 40 00 6A 00 6A 00 FF 15 40 40 40 00 FF 15 2C 40 40 00 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 40 00 • 0xf87:$new_line_check: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0xf87:$regex1: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0x12ad:$regex2: 6A 34 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E 66 3B C1 74 19 83 F8 35 74 14 83 F8 36 74 0F 83 F8 37 74 ... • 0x1335:$regex3: 56 8B F1 56 FF 15 20 40 40 00 83 F8 5F 0F 85 84 00 00 00 6A 38 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E ...
9.0.U59WtZz2Sg.exe.400000.2.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
5.0.U59WtZz2Sg.exe.400000.7.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
Click to see the 361 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/Filecoder.STOP Variant Public Key Download - Source IP: 222.236.49.123 - Destination IP: 192.168.2.5

Timestamp:	222.236.49.123192.168.2.580497042036335 11/30/22-00:22:18.131398
SID:	2036335
Source Port:	80
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.5 - Destination IP: 222.236.49.123

Timestamp:	192.168.2.5222.236.49.12349706802036333 11/30/22-00:22:26.085731
SID:	2036333
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.851441532023883 11/30/22-00:22:16.657289
SID:	2023883
Source Port:	51441
Destination Port:	53
Protocol:	UDP

Classtype:	Potentially Bad Traffic

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.5 - Destination IP: 222.236.49.123	
Timestamp:	192.168.2.5222.236.49.12349706802020826 11/30/22-00:22:26.085731
SID:	2020826
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.5 - Destination IP: 116.121.62.237	
Timestamp:	192.168.2.5116.121.62.23749705802020826 11/30/22-00:22:17.137850
SID:	2020826
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.5 - Destination IP: 116.121.62.237	
Timestamp:	192.168.2.5116.121.62.23749705802036333 11/30/22-00:22:17.137850
SID:	2036333
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands

- Found ransom note / readme
- Yara detected Babuk Ransomware
- Yara detected Djvu Ransomware
- Modifies existing user documents (likely ransomware behavior)
- Writes many files with high entropy
- Writes a notice file (html or txt) to demand a ransom

System Summary

- Malicious sample detected (through community Yara rule)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Clipboard Hijacker

Yara detected Vidar stealer

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Remote Access Functionality

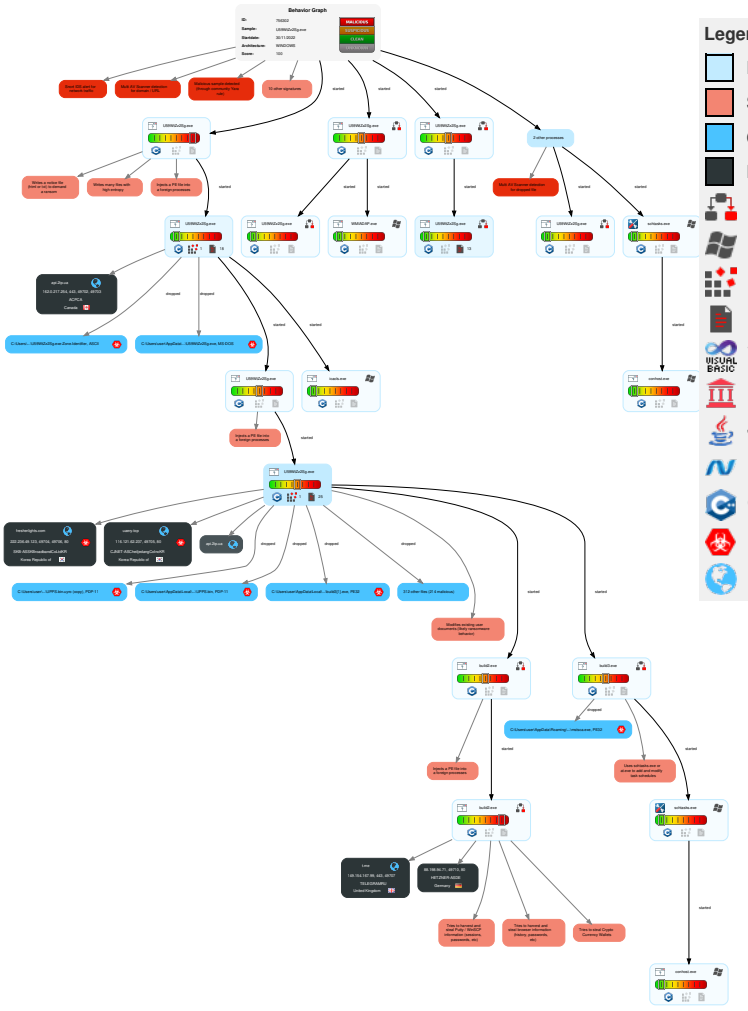
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 Scheduled Task/Job	1 Exploitation for Privilege Escalation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	2 Data Encrypted for Impact
Default Accounts	3 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	2 Obfuscated Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Services File Permissions Weakness	1 Scheduled Task/Job	2 Software Packing	1 Credentials in Registry	4 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 1 Masquerading	NTDS	5 4 System Information Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 2 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Services File Permissions Weakness	3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 2 Process Injection	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Services File Permissions Weakness	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

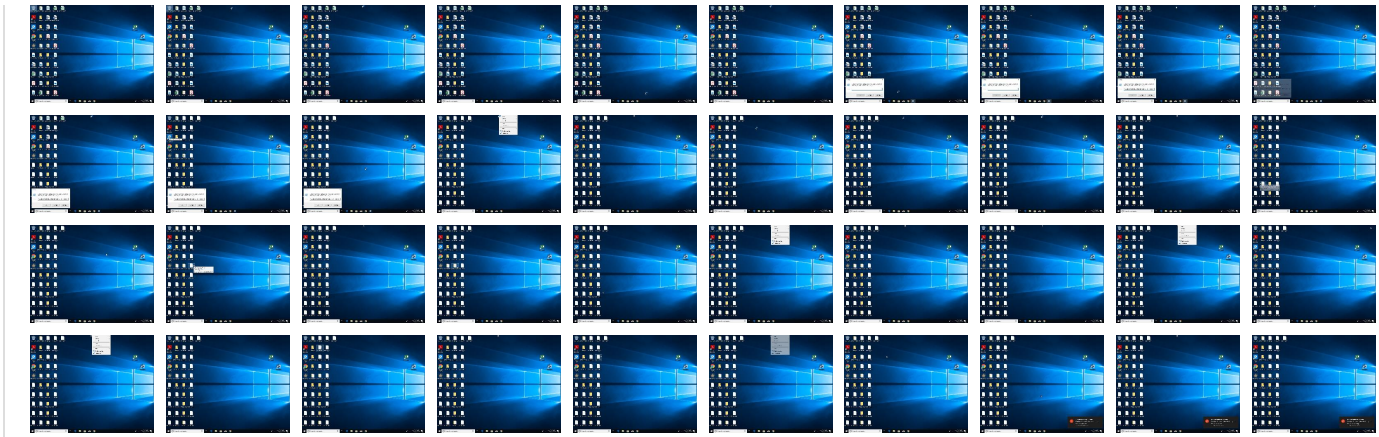
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
U59WtZz2Sg.exe	36%	Virustotal		Browse
U59WtZz2Sg.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build2[1].exe	45%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe	92%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe	92%	ReversingLabs	Win32.Trojan.ClipBanker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.U59WtZz2Sg.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.0.U59WtZz2Sg.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.U59WtZz2Sg.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.U59WtZz2Sg.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.U59WtZz2Sg.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.U59WtZz2Sg.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.0.U59WtZz2Sg.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.0.U59WtZz2Sg.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.U59WtZz2Sg.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.2.U59WtZz2Sg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.2.U59WtZz2Sg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.U59WtZz2Sg.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
6.2.U59WtZz2Sg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.2.U59WtZz2Sg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
14.0.mstsca.exe.ee0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
17.0.U59WtZz2Sg.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
14.2.mstsca.exe.ee0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
5.0.U59WtZz2Sg.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.0.U59WtZz2Sg.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.U59WtZz2Sg.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.2.U59WtZz2Sg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
17.0.U59WtZz2Sg.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
8.2.build2.exe.20d15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.U59WtZz2Sg.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.2.build3.exe.b90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
9.0.U59WtZz2Sg.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
5.0.U59WtZz2Sg.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
9.0.U59WtZz2Sg.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
11.0.build3.exe.b90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
17.0.U59WtZz2Sg.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.U59WtZz2Sg.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Domains

Source	Detection	Scanner	Label	Link
uaery.top	22%	Virustotal		Browse
fresherlights.com	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://facebook.github.io/react/docs/error-decoder.html?invariant	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	0%	URL Reputation	safe	
http://uaery.top/dl/build2.exeJ_	100%	Avira URL Cloud	malware	
http://fresherlights.com/files/1/build3.exerun	100%	Avira URL Cloud	malware	
http://https://we.tl/t-5UcwRdS3ED	0%	Avira URL Cloud	safe	
http://88.198.94.71/176356074953.zip	0%	Avira URL Cloud	safe	
http://fresherlights.com/test1/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=trueW	100%	Avira URL Cloud	malware	
http://fresherlights.com/files/1/build3.exe(	100%	Avira URL Cloud	malware	
http://https://we.tl/t-5UcwRdS3	0%	Avira URL Cloud	safe	
http://uaery.top/dl/build2.exe	100%	Avira URL Cloud	malware	
http://uaery.top/dl/build2.exe$run	100%	Avira URL Cloud	malware	
http://fresherlights.com/test1/get.php	100%	Avira URL Cloud	malware	
http://88.198.94.71/	0%	Avira URL Cloud	safe	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://fresherlights.com/files/1/build3.exe$run	100%	Avira URL Cloud	malware	
http://fresherlights.com/test1/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=true	100%	Avira URL Cloud	malware	
http://88.198.94.71/517	0%	Avira URL Cloud	safe	
http://uaery.top/dl/build2.exerunk6	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
uaery.top	116.121.62.237	true	true	• 22%, Virustotal, Browse	unknown
fresherlights.com	222.236.49.123	true	true	• 19%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false		high
api.2ip.ua	162.0.217.254	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://t.me/asifrazatg	false		high
http://uaery.top/dl/build2.exe	true	• Avira URL Cloud: malware	unknown
http://88.198.94.71/176356074953.zip	false	• Avira URL Cloud: safe	unknown
http://fresherlights.com/test1/get.php	true	• Avira URL Cloud: malware	unknown
http://88.198.94.71/	false	• Avira URL Cloud: safe	unknown
http://fresherlights.com/test1/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=true	true	• Avira URL Cloud: malware	unknown
http://88.198.94.71/517	false	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/geo.json	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mail.google.com/mail/?usp=installed_webapp	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://fresherlights.com/files/1/build3.exerun	U59WtZz2Sg.exe, 00000005.00000003.385286762.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://searchads.msn.net/.cfm?&&kp=1&	U59WtZz2Sg.exe, 00000005.00000003.497150466.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=58648497779	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.inkscape.org/)	U59WtZz2Sg.exe, 00000005.00000003.507888546.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.501922929.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.youtube.com/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mail.google.com/mail/	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	U59WtZz2Sg.exe, 00000005.00000003.421301397.000000000306C000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://docs.google.com/document/B	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mail.google.com/mail/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/	U59WtZz2Sg.exe, 00000005.00000003.545471776.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/document/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://uaery.top/dl/build2.exeJ_	U59WtZz2Sg.exe, 00000005.00000003.385404722.00000000008AD000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000002.574964169.00000000008AD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=3931852	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/AA23z1a	U59WtZz2Sg.exe, 00000005.00000003.469204147.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.449920000.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.450333989.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.468930777.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.447608292.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.446128369.0000000003060000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.471179889.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.470164900.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.459195110.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.458107166.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.471657839.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.469951048.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.446549026.0000000003060000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.454318911.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.462575287.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.445860097.0000000003060000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.470405278.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.461142803.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.467350799.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.454777697.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.460776709.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	U59WtZz2Sg.exe, 00000005.00000003.497150466.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://drive.google.com/	U59WtZz2Sg.exe, 00000005.00000003.545471776.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.msn.com/?ocid=iehp	U59WtZz2Sg.exe, 00000005.00000003.421301397.000000000306C000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mail.google.com/mail/B	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json=P	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://drive.google.com/?lfhs=2	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/about/en-us/0	U59WtZz2Sg.exe, 00000005.00000003.462575287.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.445860097.0000000003060000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.461142803.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.460215496.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.450591507.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.458323064.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsongP	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://we.tl/t-5UcwRdS3ED	U59WtZz2Sg.exe, 00000005.00000002.577338464.0000000000908000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.385599244.0000000000908000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000002.577980822.0000000002F50000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/notifications/manifest/cr_install.html	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.youtube.com/B	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.reddit.com/	U59WtZz2Sg.exe, 00000005.00000003.350865270.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.qt.io/contact-us.	U59WtZz2Sg.exe, 00000005.00000003.530047759.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528005153.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527905885.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527699347.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529404894.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528855392.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528097089.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528636685.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529863093.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529604993.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528540404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527571080.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528204840.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.youtube.com/?feature=ytca	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.ecma-international.org/ecma-262/5.1/#sec-C	U59WtZz2Sg.exe, 00000005.00000003.545871666.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	U59WtZz2Sg.exe, 00000005.00000003.545871666.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/application/x-msdownloadC:	U59WtZz2Sg.exe, 00000005.00000003.420123871.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://docs.google.com/presentation/	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.gnu.org/licenses/gpl-2.0.html.	U59WtZz2Sg.exe, 00000005.00000003.530047759.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528005153.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527905885.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527699347.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529404894.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528855392.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528097089.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528636685.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529863093.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529604993.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528540404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527571080.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528204840.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://we.tl/t-5UcwRdS3	U59WtZz2Sg.exe, 00000005.00000002.577980822.0000000002F50000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://payments.google.com/payments/v4/js/integrator.js	U59WtZz2Sg.exe, 00000005.00000003.546543404.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.gnu.org/licenses/lgpl.html.	U59WtZz2Sg.exe, 00000005.00000003.530047759.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528005153.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527905885.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527699347.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529404894.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528855392.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528097089.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528636685.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529863093.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529604993.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528540404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527571080.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528204840.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonl	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	U59WtZz2Sg.exe, 00000005.00000003.497150466.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

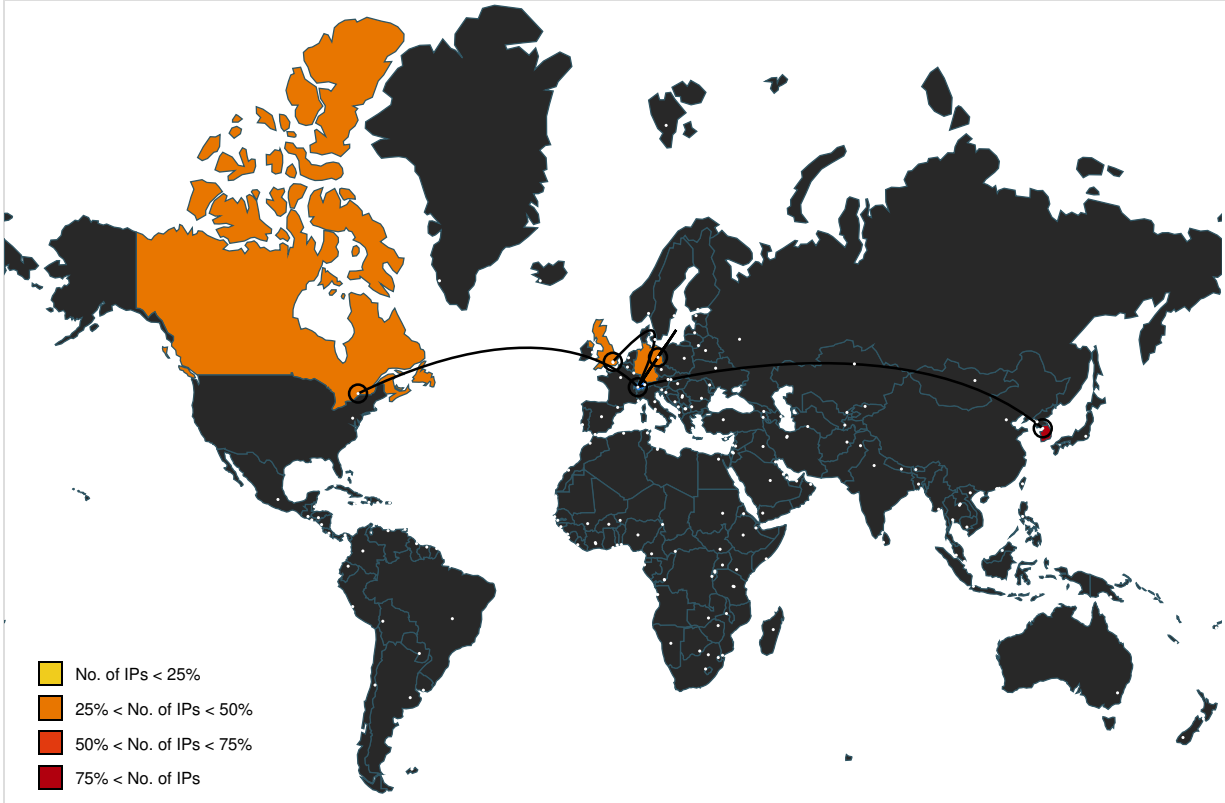
Name	Source	Malicious	Antivirus Detection	Reputation
http://fresherlights.com/files/1/build3.exe(	U59WtZz2Sg.exe, 00000005.00000003.385085396.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.522838758.0000000002FB2000.00000004.00000800.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.388272737.0000000002FB9000.00000004.00000800.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.487679398.0000000002FAA000.00000004.00000800.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.542575948.0000000002FAA000.00000004.00000800.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.488792776.0000000002FB2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/geo.jsonk	U59WtZz2Sg.exe, 00000001.00000003.306241286.000000000089F000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000001.00000003.308057042.000000000089F000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000001.00000003.306100466.000000000089F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.youtube.com/	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://uaery.top/dl/build2.exe$run	U59WtZz2Sg.exe, 00000005.00000002.574964169.00000000008AD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msn.com/	U59WtZz2Sg.exe, 00000005.00000003.421301397.000000000306C000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/spreadsheets/	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json=	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://fresherlights.com/test1/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=trueW	U59WtZz2Sg.exe, 00000005.00000003.385404722.00000000008AD000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000002.574964169.00000000008AD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/B	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd	U59WtZz2Sg.exe, 00000005.00000003.507888546.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.501922929.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json5	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp	false		high
http://aka.ms/rmssdk)	U59WtZz2Sg.exe, 00000005.00000003.450591507.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.youtube.com/	U59WtZz2Sg.exe, 00000005.00000003.351612553.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7BE6B7572D	U59WtZz2Sg.exe, 00000005.00000003.420123871.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=02Google	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.qt.io/terms-conditions.	U59WtZz2Sg.exe, 00000005.00000003.530047759.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528005153.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527905885.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527699347.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529404894.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528855392.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528097089.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528636685.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529863093.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529604993.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528540404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527571080.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528204840.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.openssl.org/)	U59WtZz2Sg.exe, 00000005.00000003.408637409.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.inkscape.org/namespaces/inkscape	U59WtZz2Sg.exe, 00000005.00000003.507888546.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.501922929.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/	U59WtZz2Sg.exe, 00000005.00000003.546543404.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/document/	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.qt.io/licensing/	U59WtZz2Sg.exe, 00000005.00000003.530047759.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528005153.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527905885.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527699347.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529404894.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528855392.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528097089.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528636685.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529863093.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.529604993.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528540404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.527571080.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.528204840.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mail.google.com/mail/installwebapp?usp=chrome_default	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://drive.google.com/drive/installwebapp?usp=chrome_default	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/static/images/favicons/favicon-16x16.png	U59WtZz2Sg.exe, 00000005.00000003.444451772.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.amazon.com/	U59WtZz2Sg.exe, 00000005.00000003.349908003.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/presentation/B	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/document/installwebapp?usp=chrome_default	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	U59WtZz2Sg.exe, 00000005.00000003.546543404.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.twitter.com/	U59WtZz2Sg.exe, 00000005.00000003.350997403.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/presentation/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/presentation/installwebapp?usp=chrome_default	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	U59WtZz2Sg.exe, 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	U59WtZz2Sg.exe, 00000000.00000002.305141359.0000000002220000.00000040.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000001.00000000.303569533.0000000000400000.00000040.00000400.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000001.00000002.309064408.0000000000400000.00000040.00000400.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000001.00000000.301786839.0000000000400000.00000040.00000400.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000003.00000002.318481347.00000000021E0000.00000040.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000004.00000002.362805036.0000000002280000.00000040.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000000.317450025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000002.564528734.0000000000400000.00000040.00000400.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://docs.google.com/spreadsheets/?usp=installed_webapp	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://docs.google.com/spreadsheets/B	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://aka.ms/sia	U59WtZz2Sg.exe, 00000005.00000003.450591507.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	U59WtZz2Sg.exe, 00000005.00000003.497150466.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://fresherlights.com/files/1/build3.exe$run	U59WtZz2Sg.exe, 00000005.00000003.385404722.00000000008AD000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000002.574964169.00000000008AD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://docs.google.com/spreadsheets/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.freetype.org	U59WtZz2Sg.exe, 00000005.00000003.408637409.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://uaery.top/dl/build2.exerunk6	U59WtZz2Sg.exe, 00000005.00000003.385286762.000000000086A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://facebook.github.io/react/docs/error-decoder.html?invariant	U59WtZz2Sg.exe, 00000005.00000003.536209004.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.536117643.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.nytimes.com/	U59WtZz2Sg.exe, 00000005.00000003.350793064.0000000003060000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://drive.google.com/:	U59WtZz2Sg.exe, 00000005.00000003.527393147.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/	U59WtZz2Sg.exe, 00000001.00000002.309333015.0000000000827000.00000004.00000020.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.385286762.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://aka.ms/rmsfaq)	U59WtZz2Sg.exe, 00000005.00000003.450591507.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gtm=	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	U59WtZz2Sg.exe, 00000005.00000003.496991699.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://aka.ms/Vh5j3k	U59WtZz2Sg.exe, 00000005.00000003.457247775.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high
http://creativecommons.org/ns#	U59WtZz2Sg.exe, 00000005.00000003.507888546.0000000000610000.00000004.00001000.00020000.00000000.sdmp, U59WtZz2Sg.exe, 00000005.00000003.501922929.0000000000610000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.121.62.237	uaery.top	Korea Republic of		9578	CJNET-ASCheiljedangCoIncKR	true
88.198.94.71	unknown	Germany		24940	HETZNER-ASDE	false
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
222.236.49.123	fresherlights.com	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756302
Start date and time:	2022-11-30 00:21:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	U59WtZz2Sg.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@32/1330@8/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.5% (good quality ratio 87.2%) • Quality average: 80.4% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:22:11	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe s>--Task
00:22:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
00:22:18	API Interceptor	1x Sleep call for process: U59WtZz2Sg.exe modified
00:22:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
00:22:28	Task Scheduler	Run new task: Azure-Update-Task path: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\155935024928932138495957O9

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3(1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*.....

C:\ProgramData\283258756549760843543262 71

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 2, database pages 36, 1st free page 10, free pages 4, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.45387870883890413
Encrypted:	false
SSDEEP:	96:iWvdU+bb3DtSOaDN6tOVjN9DLjGQLBE3u:iWvK+H3NGN6IVj3XBBE3u
MD5:	9D9851BF9104273B5AB6337A4E38A4AE
SHA1:	0FF6130A7A10B06B73DAB3687ABA6FCD4E92C2E8
SHA-256:	DBC976D79FBC0F3BA62CDEA6EFDDEEAE0ADD7EBF092B865DBB907A1D9B9DA5E1
SHA-512:	DEF485857FB1F882895122AF5ABBC502E708CA62735FF8AC855DEAEC7334D9858019D7889E90B64258EA08E634F3826B7962C29F331392670521C6EABEA0F5E8
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....&.....[5..... ....

C:\ProgramData\285169655800310200354716 49

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 2, database pages 36, 1st free page 10, free pages 4, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.45387870883890413
Encrypted:	false
SSDEEP:	96:iWvdU+bb3DtSOaDN6tOVjN9DLjGQLBE3u:iWvK+H3NGN6IVj3XBBE3u
MD5:	9D9851BF9104273B5AB6337A4E38A4AE
SHA1:	0FF6130A7A10B06B73DAB3687ABA6FCD4E92C2E8
SHA-256:	DBC976D79FBC0F3BA62CDEA6EFDDEEAE0ADD7EBF092B865DBB907A1D9B9DA5E1
SHA-512:	DEF485857FB1F882895122AF5ABBC502E708CA62735FF8AC855DEAEC7334D9858019D7889E90B64258EA08E634F3826B7962C29F331392670521C6EABEA0F5E8
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....&.....[5..... ....

C:\ProgramData\500233254017371570635989 45

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\531951220288921180464155 69

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081

Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\69859612379489584907088796

Process:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.4393511334109407
Encrypted:	false
SSDEEP:	24:TLqlj1czkwubXYFpFNYcw+6UwcYzHrSl:TyxcYwuLopFgU1YzLSl
MD5:	8C31C5487A97BBE73711C5E20600C1F6
SHA1:	D4D6B04226D8FFC894749B3963E7DB7068D6D773
SHA-256:	A1326E74262F4B37628F2E712EC077F499B113181A1E937E752D046E43F1689A
SHA-512:	394391350524B994504F4E748CCD5C3FA8EF980AED850A5A60F09250E8261AC8E300657CBB1DBF305729637BC0E1F043E57799E2A35C82EEA3825CE5C9E7051D
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\SystemID\PersonalID.txt

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.8208888513501895
Encrypted:	false
SSDEEP:	3:cRJ1x6qwZdUmnIQdOX:cHGxnti
MD5:	53BC8AA5E48C1DA5C959E645EBD3BF0B
SHA1:	1425194A71023EB54098B76F5DE96C89D06CBFA3
SHA-256:	8D177185C26DB03DA48D7944B355DAAEC9FA251A377401DE195F7520FFE84B53
SHA-512:	DEC60480AEABE911DFA29F92C37ED8A3E89342A8A34834FE96B97DEF47A3A4633897AA65D5A93033DEAD54E504B5204EC4031ACCF6D4C09C63A560BF6EA0F C30
Malicious:	false
Preview:	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS..

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	459
Entropy (8bit):	7.535586892873741
Encrypted:	false
SSDEEP:	12:vc6EeJgoT/kJTZH0g1W/9JgHFWVMtcii9a:vc6zwJTZUd6WVybD
MD5:	28C137D21FF97436D503CB1FC791D488
SHA1:	4E4A9A6311E04B3E9FFAB8C7D5C9DE744BB5DCBF
SHA-256:	26FA2C2A74B0D9A23F4157810720E784EB520D6CB3C9AA99C16593B2A91D0858
SHA-512:	2FEAA4CBB25A2DA3D6CA3FA6209AF4C5F4C55C3B2FD4A5A587A09ACDE24E57A341D705828DB900FE6F09549EB8EB24993396C1E3636B355A6C708D699ADC3 B7E
Malicious:	false

Preview:	2019/.Y...\..M..|.]..(c..h..Tu<.E...u.}.<p...H.....jm....#..^}H!..atMZ1{...|.f.,.L...i.DU.l.6...bAl.r?..J"]..P..#):"..2Q).j...r.....*.0V.%.....s..V;.z.3.'.g..v.....I...Zi(.....p].....g\j....r..7V....:.....Z.....O..W...X...-.W{h.M...e.m{...E.l.>....:.....*.H..G.@$.D.s.....j.!....Q. ~O?._..Y.&..q5.7..)C3>.M;M:.mq.....B.....[..Z....Aj.2..E_...lK6te1YGPnIbo4GcGOEP3iHx1cFF HBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\4DDQNYCN\www.msn[1].xml

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	7.2641222679610795
Encrypted:	false
SSDEEP:	6:hnMyNmQqSg4/yUY5PEgh3YMXrrZe8tYFt0mOk05OGxntHcii96Z:zNiSgoFOPEghoM7AEgt0mLCRtcii9a
MD5:	5C207E0ED495D67925B2ED17358A7AD7
SHA1:	E241A04EE6971342F9AFAFFDA97A1BA16AB89974
SHA-256:	022028B912BEB092B738681DE41CA794FE3941E30E161169272C898107950613
SHA-512:	125A098430FD7EC198CE394576C893E79404F12AD1B44A78ED46F1F56DF1B0975DDD9F278B0DE76E3970445E6B3F93474B07B3EF77B0F5E807D368F04D2C99A
Malicious:	false
Preview:	<root!.....@.."..../.Q....a.R...b...+4-qr\..[.K.....j!..(.7.:Ul$]..M.....E...uK.d.sD..6..c3.)O.[K..T<\..)Zc.*3.[.Wt.....%.--8))).....a.6..(.-.Xu.#L.....V..&.D)..}.|.LT$....}o.a..V.....U.5.S!>g..8{*|...e..T....[}..Ma..j.W..c.....{.nF.T@..3e....%.h.v.G...K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	MS-DOS executable, MZ for MS-DOS
Category:	dropped
Size (bytes):	680782
Entropy (8bit):	7.986526926520813
Encrypted:	false
SSDEEP:	12288:EEmMtgZhgT9uMA9F8GJF6y9NbgGUx0kXZPwtSRGG/t6i5l5kCYlSV:NmMtScu93d9V3U/XZPwYRGQ6i5l5k5lE
MD5:	E9FE84B69073056ECAC6B24F92F6F06B
SHA1:	7C015C421C888F822EBD97E41EC4FC0C9FFEDAFA
SHA-256:	494AC478C50EF9CBC55ED6C7D324CE84AE63FBF0809825C58C17BE91D4078CEC
SHA-512:	1FBEA24E99F888BE972110079B2F00A32E8D54F57D477B79C8E3500A1999923AA524EA5F7802EC525EB1C97BBE554D1F2EEA75F68C3DA271DC496BC207036F7E
Malicious:	**true**
Preview:	MZ...,...zz]..1..8@ .....d}(z.#}.e..N?cn.s.~.$.Y...=.K_...*N...I...x..l.8@.^W...M...(.W.;8..i..O.h...~...'...O=i..;vgC....Io..[7..sN.O.T}.B..X.._...\|V..A....(.A..l].....o..S...s..0l.3.~.N... .b.M....E.q.k.d.R..P.....I.....(?.+u.....!..;.%..Ov.....r.....;Q.o....-^.Vs..l.....g.W....q...;.b..T.3:....9...U.`.[....m.T.8.j..t..*....U.....mUrW,.P@.*>..^...=R#.>.9D.+=.Z.].rQ.7.X. /....."D'.A..Pv^.yrb...y.D...-P../7....=P.f*..;.G..V&...<<c_.UH._...)F..r.+.p.3.....Q.c..].l...j.&?OO...U.lj+.e...z....]q.....mx.DVOM..:dG.}s.9..*.....m....4.p.-%...5.~.&..VQP_.n. [...v..@(.:c~]i..d.....7....%."......cl._.....$l.G...!^.ta...H.?.)..:]S<._z.8)R..*..E....DZ&.R.z.PJWE3d..i.]...*,.GZYLv[...(.C...k(66....V...g}.;U&..&.g.....p..?T.^.Y....I.[.$...I...Y..I.....a ....b..2...IQ..E.w..N.vv..)..LN(.{...y.../.)~..v...b.g _..?..0.YyAoR.JJR..G... .Dn.w..I..a.V...W<...I..j...S...:G.N..M.k..h...)..)...]...t.[..1.=..b.I....V5.G...KE}K.....4f..

C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	264526

Entropy (8bit):	7.940912258179112
Encrypted:	false
SSDEEP:	6144:e93X+uSFbjtZ75h10z8LCPd7JkwzLs0+mKnBtt7:e93X+jJLCPNSwz5tItt7
MD5:	4CC7A6D87A0FF8F645877054501FE9E7
SHA1:	C17DDD0E5ACB6144D01F8A875FA5BA26549E37D7
SHA-256:	46514ABE0BE791F544BA44E2E6348C24174683A15DB8B53EFFA79F0DB506A795
SHA-512:	A09E1D4C4FE972E0361BD49F7F9D4F9A0D8645879F6D64013DA722A2B679AB85C4D9BC88CE9012342C325D367AE59A8EF1C50E82C372B6689FDE507185A2532
Malicious:	**true**
Preview:	MZ.....'.?.@.....Q.q_.BWF5P.c3|o....0f.A`....PzK....._).V.....|..;Y..z....b<....K..q...}..i8P..7E..S.....bv.W..\..3(%b..Cs..{;....o...w.R`.::..7Bh.Kg.;],,... .G .[..<-.....'.....PZ..... .".3e..g....ue...^...G....?.).gA&(.W.o..#Zd4(.GZ.....3.....+.oP1F.W..(-.&y.hO..GY..h...)...J.5.P.`.w|....1$.....nd.....:b...f.0.s.3..l.E.:). pmUt.....S....l....t.G.a;....1sP.O3..=.. &.O9..$.....#.l&&..T..s^N..d:.L.[.[.o..A.3.....MIt..q.f.|..-(s..D.;..q..I.CV.N.1...Ty..=L..a.....=...8K...?.C... 9N...s....M...R..I.../.E|..pJ.:.0H....(.|(%..l.....;.0....S..`c.p.:..}.....H..1.. .....c..B....j.G.1..r...d...SB..gl.{u.<.....c...r\...]c...oG.&....h7....Y.>.\x...J..e....}.?fZ...4I{...#..;.h...Q..CA..#.=..Sb..t0.....6..z7..p...1..NRS.|.<Q2.UT..f0.-:$.X.!....m.3.....+...4..MY..f. s(.6.R.Jj.Kvf.gw:."Cv...6.q.B.8.{p"[.5.^$$=.[up....RV..*.O.Fn.....\D94f.....U...fV.K..o...~....EK.:&.3k.....O.. ....0o..J.."......:'..L).{.j...v...whOo

C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	10062
Entropy (8bit):	7.984005486813951
Encrypted:	false
SSDEEP:	192:V9m073yH7khKup9kt2c7qLmPsCU5hHxmJykUEii26iLH5/:V407ClMFzh5BlJyR1j5/
MD5:	3A101335FA444CEA59A97CF434AE57D9
SHA1:	07828E3E75F853D54EF9BB67A429DE41A6BBA13B
SHA-256:	0E1326746EAEA1C2FA3990FB83F5B0974E5AC457321F3728CA5E6C8A8E98ECAB
SHA-512:	9F2EAFF8137C034D5B2F95A00EC48EB6FF24F1DFB490AA75DAFB32310648CA1603286F3478795CCAEFC729CC84B840568E0861C94B42B6CA75AAA020B9FE9E1
Malicious:	**true**
Preview:	MZ...OA.....-...g.O.q..9$.@4f...E"..0..AH....v..s.....P`w1.x'.Q....p*.}u(=N.y.)4..tj=..\..3khaA..S.+..c....d.....2?1...@_.8.1.....'.....Di.....8...O.....%# /...73.q...:..p:.R3...\.'.P .,'.x.q*y.8U.I..Yc..&....\|...."p.M....6?B.#9.ES1...0...O.?...$.%m..kn.p.,...nZF.-3..t.kkd..,e\...\...v.E...}i..c:...i...C.(....pxY.a.m..".|..*2Bo../)M).y.J./.Ax...$..a.T]}...0q.IXr.n..Ag..' .X.....[.?...T.G..H.m{M}[...e7("gD..D....%....M.."wM.$.TD.-S.HV}..y+_4s.....;...z...z.hb[.fG.vH...d.}....A.p.u<.D.C.#L..=6.K*.m.?%X$.?.!&*p`@..M..R1.S5..~.$.L{NFj.~~).<6g.... [.Z..~..R..>._.0`A.Hx...*.<....4g..H.....u8...3F.<....F.....3..>.....I....H..k.`.f-.....(.U..:..!.....dg.=-!....j..F...%z..%....C.P..BV....eF.T.]!.q|.>(..._;v.G.m.x..-../9.{.W2..w.a...sG..e..$" ..jb..h.l.....(.<..Nr.....'0ipfda.....f..zk..\|.L.k.....a.T....*....5..th.....$q@..:.../..O.9..}...\.+.....cX..8Y.E...G$.Q.....&|. Ta}..e...?.....Y.O.-.I*....~...\[..dXL/.....s.....{...}.{..*.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	1369
Entropy (8bit):	7.863573339496023
Encrypted:	false
SSDEEP:	24:VLbeYA4DODXARa+TnM/6MJjMeChPB+SXA+ixLHdhUDj857n2+9TSibD:VuJ4DODXARa+Tno6cjMe2cSXFixYe7nn
MD5:	E837F9AF72A9F997C231D71514E4B137
SHA1:	E6B40E013D7A115BDCDB653C7A7D4C5519A1B3A5
SHA-256:	82FFF461C64E101A2D749968BBF95E2F2072C697DADF1F57FF429208A31A57DE
SHA-512:	4E22F42CA238D5CD0E77E741F6F7BBEB33EA0FBB79A4A26EF2ECC26D7B08C9C436C34EF47559139AD8AA038942F82FDADD87D4A6F4CD478B2ABBA8AF192A717A
Malicious:	false
Preview:	%!Ado...S.]mD.h5...Qwc.zB.[.....;.6.!..nf4..(5..s."....v...W..<..xU...XQ.(.....J..b.X.Rg?.."....(...."h..I*..h.....F.....L....<\ T...Pea.....,f_.....2v(/.Ob_ .N....I.n...$.f.....N....\|..}...(. (..g...=*.]......Y.....&...y...8...U.....D9.R23...c.ljY4.SV..>.....vV.I...d...g04....v.....^.o...ud.... ...a.Yg.Gv<.....3.s..3 ..THY.~.f.O6.&.}L.I..M.....{...O..*p...q.b.M.....=.v...G..N.v Y.z...$.:p.[.smgl....Z.1k....:@.=.R..r.../.BBZHt.g+.'86!.cKN.)..|.."w..QUr..4r.l...Wb-<.;.d3.j.2....8n..@.=.....1...mBYf...r0{.Yh.x...V.-.w!..ig....P....3.L.*...t..En.....I.Fr.....n.0..<c. .B...r...'....ri.h.....5.....~.....NX.:...C...q.D.M.\..6...^.~..^....s.=....#...}u..<..7....G+>...I...|.O....a"p.....Z.....6.Wp.*.{|.|u.\.....)am..Q.iFNk.-.W7..:.....hZ.c[.....R.N.q....T..2 f.J%49...c.9.....K..e.m...m.....n#...{S.b...M.<..t...).3!..r&B.vS.r...W.?.@....O..]<:N..8.G;....5.m.4...#.R...2.W...D.6.j.7.....W..3)v....A..x.Q...-I_K..7DF\

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	80722
Entropy (8bit):	**7.9980796222227974**
Encrypted:	**true**
SSDEEP:	1536:clFKoAPYZVLFonlb5TwBeLTjBy4TxNvJic7dx8WJ4tTjJTyWlyEY:2APYXBzGjB70Q8dJyWcL
MD5:	CBD4463D49BD83DC35F969FEB02B6D97

SHA1:	2BF9EA7EBFA774F63CA54E9CDF1D003878ECBD32
SHA-256:	2B7095CA74E695B564A04875FC74CD590B078AFB89E7806C2F9700976E458364
SHA-512:	80A89F75374FAD67846ECDFE12FFCC86969F8310D9337B063399CD2356DBF430A543D20F3CE0987333D0B082B30DDE416597969A0D7DA4F34AC83F0AD1DA0BD2
Malicious:	**true**
Preview:	%!AdoT..N..j.,..|..(..X.1...r3y.(.&..kWZ.!.....x......?..J.....4u4;.....F.....-'...K.#..FyP.....1....:".!..|f}s....{.O..8.....K..H..?5.5].9)5l.Lpt`....;0..r.f.]WT.....T~.&.K4[x....?'..Uo>...K..\R.....}...Y.0u9.*..P...1b.p.U.....o.P.^..lJ..~.9..y..Ar.e....Z....~$Q..lU...`%..?.....5.....V..]...92...~M....Nx..%.9T.s....:..;'PD_i...{.u!..ty..P...H=.O.....S..'c.?.....K.~.).....#..&..N9I3.P...i]?...G.....].D.g....4y@...J.:..W.h._..@Q..s....<..m.IK3Q.._O....S5....0.I..Kn+.P.7.-.....O. u.;.....vY..X.....t..._Q*..5d....dg..9.....`...4.o....R._.:B....Mz.....g\|n.X3...X...w..N7A..30.D..P]..{$.t./.....-....-I..t.x.y.N%1.....q.b....R.3..*_.p...2.>..3.._..?z....O..h..K/..L5..uA...r...1Q.....I.D..gQ.....1.....dt,]2..w...,Y...b-.....aW".>G..L.w.:..w..~..].hr...G..+.....z"z1t...2...*?../..>x.-.:.(..C.oB.....tlg....Q....|....c3.w.Sn.....Br..9.fZ..I...<0../...z(.gs..i....*.I.G.`.v....X##+.....}.OU..,...nhl..Lh:.UD0

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9900
Entropy (8bit):	7.980477452728381
Encrypted:	false
SSDEEP:	192:N9+FBYRX1RWbj0MeX0rS27G1MhYWiUTI86hN1JEcAw3iwUq:OFBG1RWP0UrSDETI86JJHAO7
MD5:	4A5008A86C7059C5C09F19E3AD79BC40
SHA1:	700AF17DEF96C5E47D92EDD42417F497AC9CBEBB
SHA-256:	7112EEDE83D22D3660EB744B64BC4A591EB7AD6D9F57BE6C2EE9B02879AC8BA9
SHA-512:	F97E14F616B4ED5FFCC29674F6A1D0F89DFDACBB0EB3C237E1C842BC1FF12FB065B7F115673D715F6696D5135237D7EE674F142D47B64DF501DA9E252EC0C8F
Malicious:	false
Preview:	%!Ado.&v.}....*....{.....J?..8.....o....*...+.....KS4...r..w..pES4)....P..}b%,.?.V..F.$}.s.A..H..=Y....W..yR..T....O..1).....]xe....._Y...g....V..$....6...aE...X...u6..>.FF...!."....\.....X5}.z...i..&....~.g.FS.>B".....{J.@."...Q.T.u...|..d1..B.g.4.jR %.x4..W.3.|'..."1.....|.\...y..f.`..Z....C.o...r...oz..Z....(SNjgNMJ?...-J...q...8.%;O...M.6..S@.6..s.8.;..v....q...}..o...$....~.n.....A.....Z.z... .....)..RA..|....n.vO..l..C,1.....b.;..m..$,...@x!...l.|....X+~eX`...,.G.....%.9.s.A..>8...f..3....7>..3&.1.....L.<a.7..X._W.X.....s...B?O.qc..B._.\.z..@.....m.SU..yCV.9k.....l3.T..*.xU...W.u.v.%.A..@.A..M.T...'....V...b....l.....57R.....m=.A+..$.....i.mF. ..<B)0.\a"S.....t.....|..].)..M#D.....].EX....g...CD...%..7SJ.4.2o..)..WN...=.Bi..Y&.-.~%.N)..p.8.0?]..}...5.V..)X.....8.3AG&9..:...`..a.@...XTg.1.y.....^....ziC.p.@nH.E....9:$D...$t...1a...J..A....Z.G../[...{k.?.d.\.R..mL.....[.....".4.Z...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	252320
Entropy (8bit):	6.587558359470704
Encrypted:	false
SSDEEP:	3072:r+RmHTgdVjU9UC0Cl9t2k+ngUQUZ/WisHYr7Ah1bT562+WomP4+1:tUdZU93lYvdZuXGkhtT
MD5:	CA8E6F01DFA975EFD791171053E6B9CD
SHA1:	3BD444FD681566D1C24CC9F56930923E0228AF91
SHA-256:	27A55FD7ECB208CC4E6D5D84D2A66CECB88733B6E80C34D3275E1FF6FE1E56C4
SHA-512:	59A69068EF151D779FFBF8AD2D45661C54317A5C10479AA9BC82C046CFBE60CD2B75B5278A7BE01F45031FE6B6C7F068472C083BF08C249E67E814F2146CF7A
Malicious:	false
Preview:	Adobe...-...T..A.qO.+Js.7..f..h!.J.LJ.u.T...r.5M.g..w,.G..E.P\.X..C{..G.w.`...t..^p.{x./W[...ff...)....g.....#...r.,9/.<._....:..R..5..p.....&^1.....%.. .Lr....U..e#.{.....kI..j..9..+.....6.C.C....^.....6....yce.X.?...?j..../.BH.f."....u..NL.AX1.C..]..3..].3...".C..{d...C<g..C.uO.B.:.....A...`.!.....O....~.I..).x\a~<v\.gd.W).>x....H}....i.$%.}....~.7.....!dM|.A..5...:...^.F..'.'....<...C].KY..4.N|[.O._..".G.s.|.o)..z.qM.g.{.....Z.=.T:`..d.....Yf[....QM|..5V...U...DY.5Y.G.;-{..u0U!.L.Z.$..8!.M..6Y_.m....am.is.E^h...L.....I.q.w....1Ue1....H..q2xM...C...0q....0j..o(Q.....'.x.m..m.....Q.\...C...lj..g{t..-A....ph..#.....M.....*.,$...".[..&.46q.[.....x...\..s...g....<.p..^..6.\.jN...2.....8...I....M.%u.c.9i...,.`$F.....&{.7...X..J....rTl.(.v..8e;m.Ya..WP....,.y.23}.]..5.d^?..0...}.bm....r?1Q"...l.....4....9.2.....m.....@...Q.q.....3p.s...l.r.....[....X.&%....@....I..:.~b{.=c.K8..`v. x..{.....?...3D.S...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	32987
Entropy (8bit):	**7.995165560800251**
Encrypted:	**true**
SSDEEP:	768:l25ATIw57s956c9CRUeS3w+dzM+HfGfXaCFo+SB6xRbehYIq4/:l25nw57s956c8RUBzzM+/QXaCFo+91/E
MD5:	1C141C9FC705D03D9AD7B1ABC47332EB
SHA1:	8AD396FA56EFAA83B088FA8859B65CACB143C7DC
SHA-256:	887922E064A1A14AC29F1547AD8E6505BB40D45620FA6B7A7EAFAB85505DEA27
SHA-512:	2FAECAF5A172EE72C6F58E18C0FF73FA85E80686B25865F0588C34AEF3B628A1B892E72FE86B46CE7C87E1747BF1522053AB11A9CEC3E19FED17D0E80E4D1B29

Malicious:	**true**
Preview:	4.191si..L..z...~....Q{.."f.,...):..&...-J.K.W.......b....s..(>I...#~..G.......>.t;v.)...c}!J"(..{E+B...D.8..n.{.39..@C. ...F9..9..=...X....."...q3.7... C5..~..... u7....^..'W.._...._..>Q...)r....r.. ...a..r...2.qh ....h.........Q.bT....I.."..p..{H..}q.%.g.q9.[Ymd.5.Y.|v.P.U.?.>I...'......`.K+?-.P.. .b}N..2....o.*..._.}. .7;h"0(...7}v7.E..r... .M..M"....4;.....Ij.|.....[Gh..N..n..c.....G..S.d.dK. ......EK.Z.;..^E.o..&.. E.s._P6p`...o..f?:}.....U..:n..40.$q.o[).@,.....s..;.~v..g...R...&.x.T.E$...8.-T......kH.z^.....Mb...:.Lq..K=.Ad...qQ.....vrS...p*.3Z.....}TS..yc...L@.b.....W.n..n .*.....}.....I...C>H.I..Ew#..jV..,...^a\L.n.gX.a.tw\..:.P.QY`...._....jV.0.%@.....O...MT5.<.../.R.5..jQ.|.?.Z....f.Fr. .)-....xL...vi....F..1.E.d.c.h..Ky.....+ .=..[.u...n6(...u..9..d.....). ..`.s.....?10...-..Wo%...$.....O.x.....j.....e.CYy.....25....f.....@b...L...,Z.X..3.y..w....Z.Ge.2<.v..$i)3...O#&.....6.|....qR\...w{.....

C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	932
Entropy (8bit):	7.7630039517608225
Encrypted:	false
SSDEEP:	24:UTJRiKsDQvm43faBHl5mqt8S3CRW8qia5hRVyKLbD:UpsDQx3faBH33FD
MD5:	7A2A13EBF6E38A9D3777C4B8BDBD9C09
SHA1:	5BAB8BD2AF64DB9B222999EFDF701622EA8AD705
SHA-256:	B1AC86C34F254AFD6F0D8CE83F929680E99D54C33BB26F2EB08877A985A6D93B
SHA-512:	BC51B7A336319C02D6A0C321C91DFC51C8D1E8207A7F8D88959CE43611B0E74C515B32495F7C9DDA20FEAE87FFB146FF35D9DE818041AC4EF632BC0F0AC014F0
Malicious:	false
Preview:	CPSA.....$.....6...Ua1..$u...-.....^.;..... .Q..Xy..7...(.(..P;..*!...2c=.._...;..bI..'".v.P.?..i.}...7.p..k.iCbk2.....H..y....MU..H.YI.B.).aR..,...&L...`K.p5.I],qI.4. .i)^k.'.+..uch.f.%.....vPd. .j4.A.....K._?F6.5.R..NP.....,{x....pw`pe....._...'...x...C.....N(..IW.=...JsO.N..b..O..s\m..K.D.!i..4..B/y.%.t.j.....r..~.t..g.....;....k.e...C|-JF.....'..<...%.....i:^P8.f...5.yO..-...S...f.. ..Tp.IvV}.A7.b..k3....S_.....E=.O..<_.\d.g.....M,.e.o._.-....JI.7.....Qd)f....W.z..(...o...'....8.y.).S ..&P...x.....o.4`..n}.gu.....f..#...:Q.VM.j0..d2.I.EOp0|1.....X.i[*.B..SP.. ..(e.A.. .;..T...N..}.*.c...W.tAm.`.a.-Co|~.9...,^t.....p...'.....eA?i.RC...@..*.....z...v...dF.....?.D...D..)1....N.|..D.t.-"...$f,1..%u.p.|.N..P.j<.Nib..4..G.{..56.{..pW4Og...Y..W.g.m....W..AZ. s"Xo....U8L...L.....3...\.."K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	8526
Entropy (8bit):	7.98112083835023
Encrypted:	false
SSDEEP:	192:ycwhIZ94azNbRvjufiSXC5K6OVLdGjasC5sdM8GPB7pASvt:yc2ZmaDSZXddGyuYPB7R
MD5:	D9E8248DCCEC145A2180F79C7440D756
SHA1:	29916A837D707F6944A292D71F256D16693305EB
SHA-256:	CF0B9EE72CC7CDBC877BCD4D13052D0E610A5D6AE9911FEF23614CAEA5EFD1D1
SHA-512:	4981E6966AD07489868C438A257EF6443A4D5863D7AD2447EA50FF90DEE234B7ADC04C12ED6305CF981AFF197AFEC74291F92C36FF2F964DAC0D1279B75F6E9D
Malicious:	false
Preview:	.....Fh.f_|^.....3.T.+.....m.....^.O.>.M?.QC....1.8.IS.2.}.aU{c%!]d..`....s6....R.5..@.B.3.(sP'hHH..s.:.J..J.-U.\.....1.....ej....8.x...fc....41...P...M[0.....#.Rx..y....f\..\>.0..8.... ..K.3...X.....Dm..s.....9k.....o..%V.V..{.bs9...r..,i:..#[......T.3.....v..%@.Z..,^..".i..&0.A.x+.`...oK...4..mZ!....N..Ny..V9B..u...7.@.".&*\.7SUh&...W.`x6.c...M.O~I....*....h99..(....X. h.d#..%..d....6.jD%...C{.....=j$...J._..m...)...D:..K.^..6.....Nz%...Q...c..m..>e{( 6.....I.2..G...t.....Zq..dv@..^..#.....z;.\tN....G8o.3<.mE.T.2.A.w.)..`.W..z8...d..+%.....L..X>...+..... <x...2!..9...m7.....d=c@..1~U.i...I..<.B....O.....w..a..Rk<.....Y.h.$v,...s...@x.n.....%y9..{.....Y3...b.....gn...5.v!R.do.f8.>".d.Q.....p..j_....0.....t.Dg..m.....;.E.^...`Q..Z....@ .\.d.....q.F?. HvO..Y.'..@..<.. .t.,9.V....-xM5.k. ....v.....h8z.....*M0.n.....:....+.....Q,.8`$8F.g.-z!..c.Mg....d....d.2.`..+ ....,..@. <..@..~. ..,.

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.6705843286483366
Encrypted:	false
SSDEEP:	3072:80ud0YPeiQj5+1wl/OJPjnEVhWsyiH1DLaFahA0AnvzKDSNpnjlcig:u0KQj5+6APjEuspGAhjAnZFjSV
MD5:	47FD992FBCF903331FC866FDC10427E9
SHA1:	152108012A2D415773EABAAC5290EDD69B932BE3
SHA-256:	EAC957E5C09CFA9230F958C731FBC47BD4BCC9EAB3C1F0185A3A53FC65D7E335
SHA-512:	EA5F8103A2977DFB22B376942B2FAA0A78B1053E6D0957102A4EAAA0CBE14DBD1D3C4AFC9B8ECE991A2B30C4C85336149FBC194795B4142886FCAD5AFE6477F1
Malicious:	false

Preview:	.....t..gGBIC..#...o...g.8{....,..O..`..... t..C.....=.}7..P`....Z.G..E...=Ps.i.;.....a.o..N...(.B_]!J...O....Byef.+S|g.....t.k..f...Ze.....KG.....G.....a.:.Y~..j4T....)...T.K.P...0....M _...j.?...|....k..e.UE8..v.23../8.K....O..P..+..].%.....0(/..w..=w.e.*..3.....%.*.Y..6J....b+UC.,."...._?>...n.nc&J`.Ju.^.q...4..r....].>.....z{..=[..#L.....|.n...$oJe....T..7iO*..We.. NU;8.J.Z.i2y$]...z....Pt.N....^...oy.....g...P...."...]..^u.#`{I..k..'+GF.C..E$.0.n..W+....XX+.#.;.....n.....h.*b.x..1/..D.qq...xPd....j-!..u.$r.YV.....fXz.}..q....Z:.....{r}...*..8o..f....yT Wa.u.i...._*|.....;.H..EEY..[.U....T~]..N.d~=..%.mMp.;.e.j.I3I.A...u.f.e...v.%.y"Nm.F.G(I....&.N.....K....R?Y<..70.p....A...X.z.x..b%.U*..\.QL)O.'*..n..k.....x....!}...V4...]... .^.n.:,.....y.....7..jl..c....c....M.qq,.Q..G!...[1Tc.?./....r9.;m...-/.:0D,...F'..h..9...9.....R....I.....Ava.....?....uDw.T.....[..L....F....E...@-...^

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.6705734697462741
Encrypted:	false
SSDEEP:	6144:G5GZp4pR9jRkYhiQG3lPcsw0oRweN39aww:eGT49jRkYgXOsk2u39av
MD5:	BCA3E15713F3FEDF8CF75B5795662AFF
SHA1:	D2396F399D600CAAD14F1F28BCB79F661E99A891
SHA-256:	4E066D20B625C274ADC9E6FBD42B65E57B8698D031C1996FC135E5A15ACE14E1
SHA-512:	11D97AE7D65FE8960525442CEA47A8E666A504914969FDDFC8E158111BD3EFD58F15DBA80FE16E6AA4700793D20166B38F87053DB643FC4290389CA32218B444
Malicious:	false
Preview:	.....z.k.j.....<.r..p..NY...D..*}-.2.....y.Z...k...l.p.U....?t.....0.e..#....]T2X.d.)h....._$5...x....S.CCuPk...V.....B@.n..P.o....(.w..G.q.....N2.m_R.....8.h..F!...d..2..... y..0../.=B@.0.SI...8a...Y.B....i^Cj.b....n.....I....O..8.~.$.a....2J@F.....-n2.~.1....MH..H.5..@t..NM...61iI.A....._.)tX.....0e8<..g.c...N..w...NL.....$.r.....6..Q...].N,=.....*.Z.&....qr .....nD.2..R../Qt...i,...\..{..'.)...X.....Y.\|.....j-f.....p5Q..;.....^./../..C.y.>9....+WJe.W....[A..\|t*z5..ZS4.n..h...E.R../.4&8w.^.6..E3...$.....h.p....v3Z...PS.Z.J..6o..M].F$\....~"I.... y.v.....m.....v.s...p.<....^."...[:../...hUbo*...G.}..%x....^.%.kn....Vd#....T.....n...M.d.q2.N..=_...#(.^..I=.i..).IWttPa.....E..pL.....C!.....sb..d.aLP.(... .....n.W....!....r5P+....qXt-B. 5d.e. .%;w...D`Be.%V:.k.I*.e.0.`..1H..c.M.(.&9.d....3Zc....x..i$..v@e...}.L...l.g3.>.Z.8.r.8R].}.%.../.../Tn....2...t.5Y...h.b.....~7/L(.m.....8f.[.4.^..z]-....'..

C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3146062
Entropy (8bit):	0.6705361118460252
Encrypted:	false
SSDEEP:	3072:O4wC+rpz8dVo7lHShnZHWu92H3VEsEUK8wKGx:O4wC+rpAnqgGH3O7Ull
MD5:	C8901987DDA10AFF5F57E2B80E61BEFA
SHA1:	AF31791EF53C0F30CA0BC5B54A4FD6DA599AEA4F
SHA-256:	6740F5CACC786F9C3BAD979E3CAD476819BA119E7B3A2619D2CB56976B8EDBE0
SHA-512:	B782AD75ACB908800C3D27579CDD958FF89CEE970E6E2F5ECADBC1A9605BC9F32FA93132839A3ABD0102B2AEA5874759C08C12F3E405BDCD4E7E1400D4653 49
Malicious:	false
Preview:	.....{...XA..>F|a.!n.|..'_a,.L....<.....2..f...<....Xp]..8.J.....a..;_..Jbj.L...\...w6+....C..$[y.qb4.....N..\Hi....q....7.vwk.T...)..HQ..p`N.....sjh.,5.B...-#...&Rh.+...;.]s7Q....Y..c.f... .%.$...6..b,..B:..2...)..*....)t.D..^.f.....u../._6...g.'...H^~....>....I.h.@p..Jx.=.k.%...~2...zr.1..^yDY.....!/.G..,\d.R.&H.....L,...C.....>h....wK..q\$.DTc.....R....`)..w.....K5QS. ..6=.BY..#.N@V..4.....@.....@i.....VU.....R;.....+".'.I.e).v=....F...t./...R.r.y..e3.....[V.j..,.c.k.e.;e...]jD+u.....?.9.Pe....E...I.T-.M.e.:..[.4..>.../.8..'..E...8w.....$.f....Y..Y..i.../. c..x.w.}%./...$..7..{.....dr....lQ;y...(..U...k+.QMgB.x.~t.9Rsg.3.M..?.....v.+!.w...Z...k.....D..=yM4.....w.@.../.y..C...lE.$....g.D.%Ml\/NL6...I+.K.j.....7...{j+d....C..`....@.n...[.G+.T. .+..l..$.....(F.R3.m.y.d.3-l...)...|...Vm?(...../4Y<{..H!..+.wr...U%D ?.>....3..g9.]Q..:..:.....l.....7...x@.6...h ....]..xp.M.P..q.D-...?.".P..D2.dCV.R.;

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2323
Entropy (8bit):	7.910646689508133
Encrypted:	false
SSDEEP:	24:oqnGB0wL2yPGIIp0FiJCIhxN1DoiTsueME43ApH4pn+kXeig6aTnny8z4i03I35C:9k0WeYasYp+QxgdD4i0wicqqheBZD
MD5:	67F53C37E670F036AC5117516F249441
SHA1:	70830E9B3F1E17219BFA77CC451BF4A3632A0EE1
SHA-256:	1F6CF0BBEC0EC622854A2D77715C06EB6F9FE0B99695013BF5CA27BAA9976AB1
SHA-512:	A264816D46BBEBDAFDF494DAEBE4582BFCB0AD1C0E9E07639D6ED5389F499537DC0FEE2D4338FF945E96CD8AA528E7AF3A97EF640C7CF052F5F69CBD17738 F8B
Malicious:	false
Preview:	.{.>.....-'.Z.<l..[.....m..)+...0C.~4..+.....s...%...q.7.....i..H.d.....PN=X'.C....G..E6..2.+.!.....}j.n...2.pa.H..i.....|....+.....-d.....7..".w.s..T.lh...Ai...u...x.....UA.;....yV>m.....:{. x8.B7.-..@.+'.&.....K.....'..7...~&.w.....0=.#....2G".....>.D<.1...{wDg...R...U..tv...aV].....m.....-2...@.J..-.c..*....D=.p...m...-..U.W.s.i.,Y...w....G..'..>.Y4..Ys...K...R6..?^.. [..}.rq[-.....;..1..G...m...EY.u+....0.....&...}N.....(].B.W.[..F.C.Rg.Dv<F..Q[QK.K?./.:.@.(m.S x...z..m...q..q....)Pf/.j.{.d.}..C.;.].>.....:J.>...D"X..Ma..M...5w3.kqwk..{.Q^A.. {.JA'...#.-.8...x....e.%..E.?.v.....g...*..0...a.5V.p...?{.h.....k....7.'a.....M.Bz. .....j.C7I.?..Kh..e&..k.y...x.-.c.,3Luq.....V..j..U^.K.x$.Ppx.u.{.....<.y..lC~~..8..p.H...N..e.n .CT0..@..b...e....8.....4...`K"*d~.....E.....n..:D.`..u..k.3I.....Js#."..........y..d.S..O...Ju.&rW...Nv.H4...N...R.8.[....9e$M....+..M.K..|.RK....

C:\Users\user\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-62FC182D-10C8.pma

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	4194638
Entropy (8bit):	0.7531249128936979
Encrypted:	false
SSDEEP:	6144:mhN0OwZqvexC9fpDakU02dCMCFgEvvNjKcHfl+rvCTaHt4A:mz5wZQQmpDTU3g1lHFHoDfX
MD5:	309876A3D1246F8BC255552106DB5C5E
SHA1:	83D0272A90C0D2E26A5936CEA4E75842252F4556
SHA-256:	B0550AD95FDC88D638823A2AF1E3CCA70BD9DF14091431155E718A3535CBFE51
SHA-512:	29478349D7F8F3851DE16310C897CD5CF254C6A923E2726838A491E9E73D3DDC6A530B19456D1633DA9A30E32201858355755DC9FA58424AA18155A13116F25A
Malicious:	false
Preview:	...@.Q..W....7J...JrQ.....g....}.f...u..n|.9.....+..^?...b.b...'....!,....H7..H....ZQ.....]]].....S.1.....:.q.....=A...L...Q....-...X$.y.Lp...tBaX.D.....9b>.-s.x.^i.A\.Y&^JY..j.e^/.Z...w...X.MyT.h....-...\...(+.<.;ZX.`Z.\|....%....J.:I..-.k.W`..dS%6..i..p*..Z.h.v'}.Z.r'.\|.....oi.r....`yo`.....Q...I`S...U99....~.v...>?.$.2.d.....PJE...j..Dnf72zL.2P.N...?4..0....(x.k.W9:*.....|B..".+..-.. ...C..Z.....(...#._....7.xa...c.u .y.P4..b.yS.....D..+....j~D..O.b.+..,.b^./..$.....1=...H.E....h.}..dOh:.....U(..@'..X...,.#V.`..^\|.\|.....B.G_.1v.Sd.hWQK..M8q.'..H.....L.j..M.Il...CO.,..{..^.;_.$.....ozh...|`.u+.Y.@...R.@M.tq...$.....C..p.....{5....~N.3..!....S.....sscfL...@..'....b.P}0.A.A..`....-..'h`...|].p.k.....*8....T.J/...Zaub^..3xp..|.....5.....\.Y.....@.X....0w.z.....r.x6..7..3.x@.;.N.....|.n..1.A..".E....D..G.|./.....Z..A>r..2...J.U.L{....c...!..7SV+(.....w.....1. ..VvT.0.S?..Z..J.'.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1048910
Entropy (8bit):	1.7685960927841093
Encrypted:	false
SSDEEP:	6144:58jsVU401ZHF4hFgIoDBUV25fT8VZO/Jkre:ejsV8zl4hFg1a2BcO/Jkre
MD5:	6CFF0E55062F4F7638762AB89A00F830
SHA1:	020262E42EFF5BF456BE03756A5EE6BF759CB451
SHA-256:	F932D64DE7BFA805C6D9B7EF3A01BC6293AA2ED2D49503DBD25BE641074443F1
SHA-512:	CB576CFE9E0FDDF87665321C9993445C9B271F9108F9869B9A21BE643976A6AC4AD8ABCEA64064E41C8432EFBB2225141009254963F0CA2EB2157D20077AB31
Malicious:	false
Preview:	...@.=..'&....[.....7.s....w..;..H..@.ag....i;.F+..S.....8?..=..$\|..N...D.....A.:....G.....y.1kn.&....7....!t.pO(...8.LUu ...*.V....b....}o.S.2$Gz.....o.....P...#3....,.....|....u...M.M.h..._._..$.o!.g.dt.r}.,.. .g...d..f.i...j#.w.rH.(....1.66.W..jp.B/.X;.as+5....T.....}....G.$.V....E.h6.Q ..c...T.V.....11$...[....R{..._6...?.[56q...F6..+W..o...;.[].E.@X.....8v.....j0 .....It.~..../..-..9+V.....U.:.....\|..(..P...5.g..w+{.G.....e.4....j.3.9pE.M..%E.....n...F.\....A.8.a#.$..|..)|...t....%...O=.?;D../.F..a)..t...f(,..QBS.....y|?i....Np\...!.$bW}"U..h\|.'....ifn*m..st.b.?.b..7.....@./nWE.....DFT.C.B6....^...f..D!\.Po...Tu.Y.E.1.~$.....DQ/...u..../....~#'....m).~.TN7....^=f.5/.}^s.".Q..q-...l.qY...-2A*.....rb.5G..7..d.....*...T...<.ds.....v.....{X...2!.|.-}x.P..*G..5..d.$..q...'sr....#Y.1...x.6..[R\.f..E.5+5.+..}.....f.Q.g;..3w...y....!#>..:o.....;5}...)...(.Y.ulj.e..0.F.7.s@`N..).....Z.....a..c..{K

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	7.303489315864283
Encrypted:	false
SSDEEP:	6:z/7PzLtV4cd3pDyPXBPVkSkxBytRsIEYHCp+zId8eUJRW4T184GxntHcii96Z:LztV33pDyP/kSIBeRsIEYip+fk4T18D1
MD5:	441C1FCA3F74FE2DE63B3BF2F856CC43
SHA1:	54F384EED5902FDEB173E4341936FF5412DCB826
SHA-256:	834218AB617E671E8EDA0636576DE14427AB3072BF95348B4F42352BAAF347C9
SHA-512:	FF2966A596E06D2ED383005A770E9B902141845C2CBBD4267416C87C27927EFE3DE660CE67F674D877398131CF86531523348EE473C2776B27DBA898293FA638
Malicious:	false
Preview:	sdPC.W..Ay.9.n.#},..Mb.}..-..p.....mF..#y..Q..m...^h.... ..4.....)~1.N.-...e..a.@....8Te..@..FcIP.C....:7...Id..w...._....W}..7.Ma...X=.Z..^u..i...E..}..L.....RC..0.....g.&.ad.....E....^.#W.".|..d.tO.a.....n8Uw..L27P?p'.X.F0...._z...j1.....0.2...".Z...2U.3.Z....q. :H.K.....~..!K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	638
Entropy (8bit):	7.660745175577223

Encrypted:	false
SSDEEP:	12:qtZYsaIcZPIXzh2PFOOjkvOFTBKSOnzv7Y7bBAwGT9h+FIzapH7WiJ0W8tcii9a:+ZsIcxZInXSNA39IIzIyitCbD
MD5:	6EFEBBD8E6C10717EE635EF5310CF427
SHA1:	099C68464506259D4CAF734A11D3F9D4E08BD3C0
SHA-256:	88FAA5C8FEBB0AAF6C09182F1D0788EC0C6D0C966AC27AA6AE0BA44848756B8B
SHA-512:	AEF5C0AF89CB567E172379FA204259614F98188F8D67C5C4575D7DEBBF8302AF9FBC578B781BC8F43D2C5DB9D894C05DAE9EAC886C0EE29EB63369808AD7B8 96
Malicious:	false
Preview:	.f.5..5)4K*4.....D[..1..v.IR.6.....*.[.e?&.N.....r...?.".)....jR(..z....M.k.!...n...s....O[..,....C.....*...'....L.....P....q..h....@&B{.lg....3.m....\...q.5...|Rb.^.u..-u.'.x....t...+....L....X~;`M.... ....J.&..z...S.."1.r:..F....E..If Y..&5S9.....mgJz|./>.....>&^>j.r5.....JFh..nm..G.....c..aM...2.`U..V.8(.....QD8\^.3.4W.N..UUj9[....b.....c...Q Ka....z.tC.zg.Y...trl.....o...= ..n.9....m.S.t.s.T..< :.h.x..[.2Qo.Z.....(T....?g..v"l%3.)Y.\O.$.....P.u..>.).L.a.&A._..-..d.(...^H.?F..8Z...{.f.....`..K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36 A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	474
Entropy (8bit):	7.423889538166189
Encrypted:	false
SSDEEP:	12:PGRYCPiFk1jV5OLStxxoN1DW14Xu4WuRYtcii9a:PGRjH1peSfCN1DOigbD
MD5:	84C290D94F5097DA812D6337654B7C58
SHA1:	8BBFCE2C96B8AB008660065B78C686D01670D784
SHA-256:	7015780855B3E38E65F0B7A40FBD43C82EAB3E2FEAB1AE8CA9B7650DDBD0671E
SHA-512:	95124662EC0EF1E691CE7A7A78015B49ACB7B39442CD96CDB3F7F97EC2DBAB828D8EC71D25AC43A9E689BB51826624490E68ADD7EF517273196B446AD08E85 BC
Malicious:	false
Preview:	2020/.n.a..OIG.d. _k$.2.....3<:5.f.....jh.:.D...cO#g..&.{.XGQ.....-%...G_.~.5%F....m...t.i.D.(.>V..-.w...'...9J}Ei.B.R.yp.L.....S.....x.G...../...+Jg.Q.R...J.@.eB..B..2.....f....1..3 ...N,s.....O.-..:.[..Y4wQ..b.S.%.h/.bi.X."....o.)...m.[..[p.....#.....c....q..b%.....\|o!..).s.f.ES...X../,3^G^...QT.E..(.;\|....Y..2.....$.i....r..`...&;.%I..0.9.....Z..F...v..J(..BK6te1YGPnI bo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Scripts\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	486
Entropy (8bit):	7.458188592526049
Encrypted:	false
SSDEEP:	12:q2bfVSXzMzVSgsa1W/KDh7yG5RX2U32LHQdcKILpkZtcii9a:BzVlVSjaWwh7P5Rv3gwdy1kbbD
MD5:	BF76F471853257785278F8FA2026C00D
SHA1:	3F685A00A9C660C2B7B6C2BC65851C714CD9C481
SHA-256:	64EC4277238FB71BC64EF6D507E550384658C5C9EF3EB4E0D88A74594E635E81
SHA-512:	53E8295280A6FC96DB1AA375822C676E9AD36DA593CE9B1A5492716FB27AA7F7230E806D589A04C0E817DE6C78B5D08D2C4B7966A6AC4BEB490F0EB10B67AD 7F
Malicious:	false
Preview:	.f.5...*...V.HY.o(.....y?.....i..-..aV>Oy.v...F..k...{d.....v.y1.Ck..R.e.P.2.j.E_...4.I...3.P....X..b....a'...m.....0..~..z..;..J..#rXz...GKo..4.tP.....L1%..66L.p.-..f0...q&i.w..R....|5B.?.. >..b.....D...]..|.q.Om.....S....;;e.A...DG.....md^..1a..XA%7.....}...7..Ue..q.....Y..4.|X....y...p..>..!.....m.MG.:^.....q.F....K..kI....I..%.. }.;....Xc.l]..).....[..c. ..K6te1YGPnIbo4 GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1702
Entropy (8bit):	7.889370767975146
Encrypted:	false
SSDEEP:	48:nXXpQiWVevQdi47Gcg57d3bkSWmA7nBDL4D:JNw4QJycgtdLkSWZ7Zk
MD5:	F1213D5B6F088AD74D9EC4E601B67CF7
SHA1:	75C2514A95DE6A1448AE88BC73F59582A5B8459C
SHA-256:	D994223C66C6E10C4E716F89B3F6C407120E63C3DE2C3DD5C8366BEB9D6680AC
SHA-512:	5A8FA04B79D7397B3D912F8EA420E8AA8EBC974F443BDF7783EEAD42D7FAC525369A9E66B214F41D5DB11C176FC60B0CE5FF5E1036ECF13916ED1EFFE56670 B0

Malicious:	false
Preview:	.f.5.{[.iyX.Nz.!.p1n a=.....Q9..s.....o.*.....l...F..f...^4....K|..YfQ.*.KG~fA..-+R.Q?i..8q.$...;.b.....fS.....M.s....b...Un....M.. .d....]....0c..dR.\|^T...Y..W_....@.#.75.'.A..\.qO)6.. ..r..l..5.tn.z...R..87.6.....4L.. ...x.)....\.....W.1..f"$.....F.Gy1p.<..*...&.|({.XiH...v..gi%kI....7.....u..V5j.v..+..pz.....`P.@.3e.8l.i...%...V...`..o(.....g=....?..pN.tA.}.....e..%.%.2. ...y..X....(..^./S^n.h.3...E{w..(.O.[#.|M...QZO.*...b]NO..b,6...n....>B.>?.C.|:..P.z.....~|.....c.....r'h)..R.%Qm.:.U..._T.\x..,.....L....(._C..:Lt.P.....v.&!.c.|...n./&{2.....;F..)w. ..L.m.E8$@.....6...^*.....U=.$....V./.2...>.~...]..U.."..e30Hd.[f.3..n...\WCG$<<Fi.e..rU..V.}D.(....g....4'FBaC6..I_U{)T.E.k.....c..RT.N.. ..!..9.%.O.-.t._=wmp.x.]*#.q.....s._.. .YF....E...@.X.....D..:...T...r.2'cL.P..L9![.sG.)^.Tm.J^.uB.n:...$.....q.....\h.....{.%o.u.0...9OU.....Y+oX.....5.'..s}.L..p;....M....`*.."....?..{.@r.5Vq..C.B.....]..a,n.xF3e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	653
Entropy (8bit):	7.644608849408246
Encrypted:	false
SSDEEP:	12:Xs+UhusMCfmKHNZBGx5M4i+zmBhZSI75VovjAkf1Lv1AoLClUtcii9a:8+WusZJo5MLQCTSjJf1xAwjbD
MD5:	D65F1820AD39DCBA687424470CD84301
SHA1:	2BC1FC5D648B896E438364A3F9A14018C3969B19
SHA-256:	6E619DC3852E8EF8D4C15A3AE4530B98760878AD11866500116F33003212AC15
SHA-512:	A29A1B4413FF526CF4E2B623B4729D851370E69174009D1E3F0C697B084C9FEB859C647778BFCE79641E22780F557D1BEBCAD13E1733E3A8E774BD13E1673EC
Malicious:	false
Preview:	2020/..X...3}2.....{.}..o.....r].]H.....L...#J#V.v+.=..o....h.....H....K y.qS.I..M.x...g.....N..OHs`.?....Z.6H5.....`u...../#J.@.~E..~.....Pw>..Y..*.1:D.....,ysT.Un..\'..64t..P..5 8.+H*#....q..'s.....~b..."....."%..:....x-....-X[.C...|>..IPN!k#..HW...j.>>Vt..x@.....f....W...*.....qZ.#..& .@.....W<...g....SP.....a/g....F.R.5.....w;..0.X..Di.t5.. .K.`...7vr7.L.]7 .C.Z}.|....w.{.e..va.KJ..Q[i...zEt..]L.. .....ph..#F3f...]..?..@i.....`.....UJ.....#.%B.K.J...eR..p.`.....i.P..L../.-..d17.Z.{....z..../...f....K6te1YGPnIbo4GcGOEP3iHx1cFFHBUe guxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	5316
Entropy (8bit):	7.967877148381009
Encrypted:	false
SSDEEP:	96:vmao6sR2eeK2FS4i6GW7yHa0zq0bxdtnVBRSTY2uyxoOI7PvbRljaL+enK8O68r:+a3P//4W78bd5VfZG34Xbn0hHOX
MD5:	4A96798DD9BBFDD639D955F4915C05E2
SHA1:	D2A036F6347553B077D6877DA7428E368D7A982C
SHA-256:	B30F551FDBAF75EAD8DA9D5E8D389B38013A20F33C27E0D20D4D6610FCAA9CBF
SHA-512:	EA5C498BAC2EE80BD442FC566B4929F55F2FE2F410D7817451690930E8BD3C4D6741DD447C53628DE932FA37A77A2A4476AC1C3B39765894E6B620A484CFBEE 1
Malicious:	false
Preview:	.PNG.....X;2.4[$..B....H+...T..w....K_...-..C?..Y....(..Y/..(Z.!c.]a'..I...7....)..Y.An.....@{bV..I..vt.dh.vL6l..`.....W....&..).....,.....)W.'.#...[(.'.<x..'}.....J...$}H.....wS.h...H..... .5.Kg.....u2.K.rV-.....t/.qj.y`.X.u.....'...\..h.....Hv.<.0MMA..<.e...]...`.G.k.R..W<@..c..&..Qs.....2.....V....*...7M.]..9.....B...nh.T...3(.....W.....R.....'LY..f...C...Y6. 7...o....h. ...t=..`..H..[..h...,...g.R.M..$y;..i..^.8.o5.-...%Cv. I..AI....x\.-P.}..(3....NY.!.....7:.z.2._.....2....:..N..V.Q..+`...../....v..]....-.e..'3.9=@.K.p.f.\|.....s.....,\.f.{.F..@..T.....k.b.'..(.....L.3 0.C..2&.=..`if-.E..P%.....S.m..B..?.Kc1..r.....e.....6..iI..w.'....k.+F.4P.S....{R&J3.j.J.C.7d^...Mh5.kQ6.z.O.....)D....Q\|.-.}...X.....K.p2Q?.....U..1..E....).[k!./G..[.S.....v...p.>..- ..y.V..I!a..!x..m..2`K.....w.:.G[../.$\> C].aI-...\..OE...D...6.....q.g..._.,.....``p.k.....q...%N...]..f..e....D&..P...._B.m..-U

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0_metadata\computed_hashes.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3964
Entropy (8bit):	7.954286272790977
Encrypted:	false
SSDEEP:	96:rhJZl4rbCSFaADUEAGi/uzDhzQ2rCxr2tbdwxCInMkjf8xPJ:rh3l/SFa6iuDFQXr2tbdwxCInMkjaPJ
MD5:	0ACD1E2A3547D7B273F4DB56EFBB6769
SHA1:	6B609DA529C0891043D67310342B1403BAD94703
SHA-256:	899B7B18ED7EBB101C903E200B8F85686718A1C843B33A5A998F73539494CC7A
SHA-512:	C12228DA6327E29ECB585879C594263466540768C3848CEA77605F4DE8E635D906F98DAF0137CF7807FEFC303D91BA705B7FA8FFD52FCE2BE4A8A6C4C98DDF A
Malicious:	false

Preview:	{"fil...w....V....w^..~E0@\._..jD..0n.oq.....7.X.`%4..5cj{rg(C.`IN@.....%we=D..IB.u...|c.....I....)!....6.Us,q.."...:s....0..niN...J*=:..O.....f..ADe..nr..G+...~_4.t.d....5}.">.x/TK..7.. L0:Q....v.....s..XO8...}....5`..<..i.R.....pp..g.yV...l.....f...l..i...-....Nw.O..O..kc....r[z...**..$v.J.bo{&..!b..3U....(+.M.L>$...).....B2.,.....d....yK.7...:.)F.q]tp..2r.Y@.....!L...2..M..#.t S.4..}..W3?m.3)4...`...>v].. .6.s.....%..w)$;^.....9..!H...QK..Q..._ D..p.#2.emK.P..x.q.F...Y.m/.K.`.M.1.[.$..b.....h6...3Y...@1Gl...C.f..qJ.W}8.yA.&.q(C...Yvw.Z.=..z.O.. ..TR.>Rx..L{'Y..T....>..1=..c....\.2.j~V..\$.ND.D....U#./....Y.....Kk.....U....e)}.e^..]..(.W.D>j:.9_b.?.JlLcJ.d..s./.5#..g.....A...|.q|.....@./r...Vm....=..p...._.l.,...L...J...=.....<>.....Iz$. b.'SB.G..JV.1FCo6.c.s.K.{q\d0g..FBt..*a&k.*..q...s.R....-...'.....w.c...g.V&-..D..;.u!.XKt_.....k-..G.....k..==..z?..#...a....t.^.H.. .Q....X.....E.&.6.S.....l.c.l{.(w)+.u.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0_metadata\verified_contents.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	18624
Entropy (8bit):	7.989184679597943
Encrypted:	false
SSDEEP:	384:Zd8p+3ONR/rHcOcEUhoI/5wX2YjNV0nzuorO/4D35/z:Z+A3ONyphoI/5q2lsy0LLdz
MD5:	4BFAFE624D63B0BFF54B9B45D352E7DD
SHA1:	B57E0CB8EDC20E3E6CB3DDC2A26057BEE8F6C80F
SHA-256:	50D4B8144AE4398295E2D33CD48BAD675500F24B220BF7E73BBDEC5CD2860C52
SHA-512:	78DBACF8B3555862D139260458EAFD87FAFCAA91661913C7E0265C32321650B24FD00D96C7DB8D28DE5145ECEE7200C4C34B90EFD5E5DB9C0A1628288B1A0D A
Malicious:	false
Preview:	[{"de.Y.....yn.2.j.....Y.E!W..KOv.`4G.k...TH.[.?3..:...f....A;...."....S..+.....}..r....(.|.V.....A\..J[Gg.....k..~....a.^.....@...=.S,....>..&.....||<.It..OG.D1....FUSwn..i.9....&bL..F.D..A3. ...?.....AB...i..QP.... ~2x].(%..,~Y.....B.....M..T..;8Z8..(J....P.x..K(@.P|%..[...M({fgn.K..K...Fi4..Cq.}..3...W.....O L.....*s.+..wB.i.m..BN..KXe]....%..:.#.....I[z.5...f.."....I!.L .....E...y.T,..a..Z.....^.....A$..}...d..M.:Z./.=....TL...rO. D..kA@.p..IMN.^\.^.....(..Qg.UE6.D^.QmYr.M.M..o1. Bm%gI.-....t...f0.....*E..i...^N..X...;F....^.YA...E..../.>.. N.:^5...%[.....n..og.G..C.~B.uE.E$Y%==f....I...{....=.....I.....S...oJ...e.F.d~.z.P..$.W...b.....$..Os...t.7....!.m....!.k..P..OI.Z.)mK...n....P..O.Pp.....)...HF7-....)}..&...C.....U ..\b..=.J..R.HT.@T..c..v..LB.Gp._JK...Y...O..oB[.#".(=.d.. D...^..nq... .i...T...Va.....a.;.8..<.....JF ...z-.]b...z....{.*.W+vy..]..&d?.....,..hU~...6C.*R2..p.m.!nO..>aFcJ .r..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\dasherSettingSchema.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1188
Entropy (8bit):	7.842147316775836
Encrypted:	false
SSDEEP:	24:SwbFGedlKOk37Kq0HdJaRY+HvzXfGFaPXVLlFgRZG0SHjbD:Sw5PzkLKRaRYAOFa/boZG0+D
MD5:	6168B1540E442F82CD50A399E66832ED
SHA1:	6A2FFF698F8E47CD32E0E00CC41FC99F50C0108A
SHA-256:	B92AE5C1BBFF385F938BDDD5243A1AD80084553BD8F59B159960AF6C4B885A16
SHA-512:	E2297946DE05098E1DBD942FF48E1B8E91F94DE8B162C497B26103C1CCDC89F387DF6C3C6C4B843632EE27E60ED42E799B966F3E2E317E7CA7319C958E94A63 5
Malicious:	false
Preview:	{. "...'....\.1....0.Tqag.[. 0..s2.1..CBw/.p.dE.5...J.&..:?!..K-...?09...&.`..7'.o .t..)..^.<...y.i5\&.{..F..?(V$.x".{x.-%..... ..z-._}.<..Y.yC.J.x.~.t.k.2>....~..|.I{)k`A.}K...Xh...y.cU%vs ..=b..Q.....K...Zy.....}.T.#.z.p.,.v.'..Q?hli...;...^IWQ...(.1..j...)....r].....V:...7....]..S...y#.A.E.....8e^.(..Z.....@'..R...7.H..s.(C.`..>e.b.+h.o..Y.....w.g9"X;`#.]..Gb....t..{*-..K..L ..\....s.9.....A....LP..w.!.f...w...qe...P.]..7...k.G....6w]*.R'b...:k..G...k.d..UV...,j..#U9.b.....h.C.6.x..5.Q.F.=,..../';K..m.L..*..?..U.#.B.....c..8h.=....U....r....|.....5W.....2<.V5..c. [.. .B..5..S.v.x3..9i<h.T^a7...S`.....+oTx(.k.G.V.bG..(..I2..d....w...N.B.....8..-.....z,.I.`u.....j..N.)...:....$$..v.Q...}.$.L...u.Z.P.-..?.(..b..b..C:..m."...K.:~.$E.q.5.5n..w..z~..}XC- w....mJ..6..h}..m....Z.Hk.o...+f..U.....s.P....?E...W..J.....2..v..^...wX.....k.&.Xi..O..I..T...',..*D[%...7O.W_....J}...J|..S9..5....cXn3.....-e.P.nR..(@n.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\eventpage_bin_prod.js

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	68133
Entropy (8bit):	**7.997517400133588**
Encrypted:	**true**
SSDEEP:	1536:oT1F+fopSNCMnLDmHhYVtaplkK4zOjPQHHDJzabOpXSfGSW:QDQcM2WGkaPMzaI1
MD5:	E27A2F1357B342B33F51DACA171646CE
SHA1:	FACED8EF8226E9A1D8F0F671E80175064D42FA93
SHA-256:	E26533D0A3457140D9C10DE74F8757A9FF6BA17B56F350613AE8DD867A62D0CE
SHA-512:	8A5A893D62758F1714959D1A8F2DC7547643BC4CABC51C915F7676AFAC0D1DA5E1C507B06B5DD414019C52C4D3770E6BDB6314BCEF803AAADD9C185867E80 AC
Malicious:	**true**

Preview:	/*.. .....Y.[.L/!....6-.Y..C..e..rzc"..1...M..3...4=..+w]id]J..../.W.c...W3...#..i....#....).2b..o...9m.._.|P[..g.6..W.?.w...!..e[.RA.z.3.....>..?b..P..jQw....._$R(.~.....~...a....-...E.'..p....2".$-.a>[.`.E.. .dM..E..vB...X...B.....Y..h.w.....Oc..{r.@.z.@..a.+Q...*r'.J.....0[.w9$.\|...[./z...>....#m`..a.....k_o]!@.Q@....+.7G...9...5..9.[.1&1.?qB^}.R.9v\....:w.....q.!..s.L{..] ..24.e...U..-..yk.J+...S8...:[oj..z*\|..08..]g*y.D./...'"g.f....}.O.%..{.;8..0.....N....1.....$&.xV...j}..T#t.R.)..:G.mf.PBtUM.T..cdU.. ..g.....fR.O.HNP.ncQ...3t).....S...$..3...n \:..F.Ei._.5.N.E]i(.xw.....Nt....x.7P.p2..E.Z.A....Fi.....c.$V.N..h..a....*#.....#..V.....=...C.i'.FL.RL1{...^IE..^.^.F!2,.7.....Ri.c.....HQ...K*..(T.UH.OJ5.....X..^..G.Nb/.? aH.)...)b..?.>3Go]..)...r..}..W....b.i..]...K.....a...\pX.....vE.L...G...Z.KJ.\.....x%.^.Y..@7X..FK-Xo.I....5..m..G..)0."O;.:..g..kI.#CvH....P..M..V.k$...$...as.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\manifest.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1854
Entropy (8bit):	7.889303549505147
Encrypted:	false
SSDEEP:	48:QH7Whxm1zIIScDL3lKYzWfz2pP/IIIIMZO1kTdGc32u4FpD:S2x7PcDL3QYzWfz2dQfOSGc31S
MD5:	567AC0DA19B1A4D6E7DB7BAF2CBCA628
SHA1:	68BB1A58F78E57BEA156405F6EA1DFCD87EFB56C
SHA-256:	98AE1F3665CFAE05FD91467371BB2EAEBD4823C553298C74F14C8012F39625AA
SHA-512:	873C0946D8160A97E68EA047425F31FA609C970E4DB576983D56A6890E6224096DEEE108ECF16D0FD26CA184C31ECD18811A626A864D6A6EF70E8F30D042B60
Malicious:	false
Preview:	{.. ....C.z._.e).}Q._.w.|..i..|.3....\q.<.Ho.[y.q.c.:....i.I;yV.....i.........;U....:...2+.7..!...._b_CQ.i....9m....[..sJ...V....h.<..z..P.aV.7...Y..c..+...m...a.H.p..H..M5...S..+^.Dhr....RJL2.W.s.. .v..]Tjz.....qo..W...o.u..9....0@~....f....SoZ.n...5..2RHB...'.h.$)i6Pn..'...,~..;...b....-...[5..x\._.....X<]z...>[.V.....AHbix....dU.L.B..Ja.....N._N....I...4.....8..F.Qn.X.r..y0....EI...C....I. HE."..^.....8...~.#./.MB:?D..t...FO..G.....ye..,.....i*hy}$".N.....D.....'...k.Y./iK.}AM...=.|VZ.z...u..n(.0.....U..&.....:..i.$YZJ-..n.?..e.\|.....,..:n..3U.i.C....MR.^.@...E.....&p.W... ..Qw.,d...C\\..NS3e.!..;..K.u4n...L..ng\f...\|e@..U'...$...nv.yG.A7W^Y@].A-..-...*....q.....I\8...R..n.)vI...z..y.f....S.nn..Yt.....".{.1...ZU....^..#e....kd..V.v.W.._&.'.. ..../.EU.....C. ..1...m.=.w.6.F.).XJ.DN.v.@Y]....y..5;.N...].+..g~y...`zI}&nn..3.....8.U.^0.....k.cx.a.9\7...'F..&x...4t.{...K?.nb.R.h..v&}.....C8=.gx} .....).EQ..OC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.14.0_0\page_embed_script.js

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	581
Entropy (8bit):	7.584789203489974
Encrypted:	false
SSDEEP:	12:22VLGIBoOmT80XF3On0ovUfB2VCEoAyIrdifcMtcii9a:22VLVo7cn0yUfBA5GybD
MD5:	EB94EBC7F5E1EAA42B45C8181C800BC5
SHA1:	B4AC8B1B9A11A99E42FC93367792EFE5CB11D5E2
SHA-256:	0AEC796A20AFE074AD5538FA3087961B9F337F5B4601124C252B9759B29CB78D
SHA-512:	213DEB98235EDE3B1BF11AD37299AD14270BD9263D9727F47E70D47D6C1FB6CF55FA0C729F01435E856D398C7C4C75AB154F4FF8186EEBC13D901C23E5565A 8
Malicious:	false
Preview:	(func...X...J.....VT.x.....4.`...7IOsm..W.$K.1.qP.....O.....nJ]b3j. .....I...hJ.*._...O=...R.r.j^K.=..7b....D f.....5...PO.6.....v...i_.G...-..V}.....C.u.!.....F.a..[.O...\|%.u.<..p S.xhDP.P..2.....y....$.J.....j...ie.....1>5{W^.r.T..>P..`...)./.D..."X....m...KMn.0>H.@(".o...i..j..R;..9.'.....3;6;.8..9.k...h.k..4. .6u.?Ow..2..+.ok.T..y..B}..|...kPA.|....$mwR.... {..'.LcM. ..T....I..D....TB`..0...}%..4.xa..-.V..!!...B..?.jiL..N.Wm.9.8}.3...r?.Q|.<&..'.xh...kK6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82- 0EC5B14B4DF5}

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0_metadata\comput
ed_hashes.json**

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	18272
Entropy (8bit):	7.988372191864928
Encrypted:	false
SSDEEP:	384:ouf3pF9XuvI/KNyPkzxWXjTouoZxE6Wq/ncGIupNw/I:ouhF9XC7OTouoDM+2YE
MD5:	B6677C22EADBEB8CFA11F8F555030DBB
SHA1:	45000524D0E332CAF55293A49466B0C4BAD48E24
SHA-256:	D1C4AA2BE081C3B607AFB11F663F8FA8B2C036D0EE850B4E1C1397A348D895A5
SHA-512:	DA4C0ECF78359C3BB99FB882697954907DE715517A5A710762E7EF6BF0434B20AA75BCA6097FC9BA08DEE7471ED543D1FDFDA314AA3DE4F6B92C2ABE2F63B3 FE
Malicious:	false
Preview:	{"fil...H....vt..,.....R..##q..B.%..5...8...Ti2.....>At.[..V.B.^"p.\...m.T..I.m....g.Wjn.X..)..q`.D...6.t.c.~t.cP.B.....`.[...cNzSO.3Bx...G..BB*`4....>&.y.o.O..?3.A.+v.*.....2..".L... .3Y..Vi..z.D.;.I.K..6...2+.....\.[5...U.]....L.t<.+....u..H.....X...u.4h.X.C.(...F..^.....e3nX.e.#e..1.....N.*%.t0.....6....iM..'Q..&....v.IXzr.{..Nn%.6....`y.O.: .k......x..4.{.zc2..F...P....#.k..t ..6.Y...."...TU.]].;.....(..%....I]cX.....L.<G...I.....`.....g.....%..k.D|;kw.....}.U_...B...N.U..`.9....dR]8. .._.V@^w....ZK.j.}F8.onAF.?...,)..$.....u.*....JH....-.a.wQ.Ry.?.6~v.:.. #"9LI...@,.Z.z.....$b.O^CruA<..8I.....aZ=.&....KDI.cW....p..C.}.HO...c.....6.s+K.....Y8.t.DL.g.....3.y@....vGl.c,..9.....[+:d....Ob..q.A.....X.l...r4.....:.-.I.}.1..L....K. |m%>9t..z...K5../...S1M..h...d.....R....J..{o.ni..=.."..A>.ik..g1gmV.P.{.V#\.[.B..c..-!.....i..K..RA..c.Z..\.L08.....aW.wT..lz.+e..a.x..J...O...&.....>.2..w8...o..1.>.}...9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0_metadata\verified_contents.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	8114
Entropy (8bit):	7.980653056438372
Encrypted:	false
SSDEEP:	192:vVTVHpx/YkZEIDcGq9MSTG8Sasxs6goSiuO52WIWMWU5lFw7xDthxV:vV5HpxhZjhqNGqKs6xWWN9lFw9Dtd
MD5:	A30BCD80EC177489F7A48C31B47E0C86
SHA1:	F2F77813542B3A7745F4683519804A99B10591D4
SHA-256:	F05AF7E7440C7CFFE55B8526D4857570DA1699EBEE377D5D908C47EBC59990DC
SHA-512:	7A218632B7BF5AC1828A4DBB986CA5B611C4AE2CC54CAA7C2C5ABA2FF03BD42257F5F3F50ABB2B31BA2553E7A2942E40BA95B24DBCCD486E2ABA33FC32FE6573
Malicious:	false
Preview:	[{"de-..4...f%.O.E.C.i.....s_m..~..vl?...0.$.....-.....".F..."...y..~.T..V...E..]..o....3}+.t...-(.-e..e...gn..!.`&.B."(... \|wB..5..)Qc.f.k^?EwF...0.z.J...^..T ..O..vH....r.6..`..Ji.u.....S.. ...H.Bb..Yg..q~o.s.f.Z[.1.n...&."......+..4.`AX7~.M\|....a.7../.....}E...,#3.xe(...U+....V...E..S...K...].5!oh..j.....r.T...7m..vD/.Y.....c.y.../.Nu.V..6..$.]P....b.`Ux1w.e..%...0V.]Q.. <U....t4D...0.z../..ijZ+....}.y..R...R_...yR._.th....RF...W22...>..?&.}*...TD.....4#)>....uN.d_v.74o....T."+.cqh.+....G.;.,!..i"....Y{...`..('k...b7...'.|...C..j....E..B.k&....-A5..7...r.._a.. .....v..&....-..ma.'....2K..c.r5..;=V.s...'....6..[j....w.&.}.....C,.~..H...p~..D.}g....WA#\8..^.w.....U..S..$..$.D6.....$...v..E.eoi..$.g.;C..*.=.YI.....5.....C)*_.I'..@@n.....{: .\&..}.m..$.....T.1Z.z..h.....1*#.*.k..w...E_.&I...M.....!.P7..s.....?..&.-"@.1(r B&.j[...-...}.....J1..!L....R..\lT.fzLh...v.....O.....o.h1.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\craw_background.js

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1125962
Entropy (8bit):	5.998288747102356
Encrypted:	false
SSDEEP:	6144:WyDmKqbt+4vu6sX/O8jXZrp03tPgAhcDnR5eTjnZV4VGLPEz1019sZMbPzWab3/v:nkb3w/fg3OAhcl5eTjlGb
MD5:	6D0D31423A01A0DD34981ECDF29D16C3
SHA1:	F213E10A62FFA68E9168E71318270D95B6303B95
SHA-256:	3D1B4B0E0CA0B6387B27C499BAFBBD7525526CDDDACB41B6BB49084D13199241
SHA-512:	4C1ED1F248BD5F991B0083C4E736DB204BF55515C60837244E01436F4B94B1069F3CD606B5EF19D0B4E429759136C2563FCD3ACB56687BBBB602A6FE66C73D6
Malicious:	false
Preview:	var d.c..j.f....]g.N<S:M.N.S.....2..Z.J.:.v.....(v...>\B...../....,iy!!.S..0.O.....{.."N..vy@..(...D.f.Cs;.....M...t^y.....Fg..i.\.7...~A.-.P.i....k.A2Y..NX.q.!.....Z....h..k..T.r1U.:..cs9+..4:8A.. ..e..j[.(..t.............x.].S.]9.>.!..p3;().sO#m...&.y#&....44rO....|.....%..6....m..@.....uT._7.<..y+.{?&..N..D...t..>2.URK.....~.....s...G..q..a.S/."s....^...9.dr.f....p.#.r.{=.....I:.o.u|.Q.E. .w}#.0..v..x.....P.N../..V.*0.T.."...i.P...Y..[.}.2.gb.vt..]..a...; ....V.<.I.N_/j.....-.*.f..*.....N...`6.D`.\.. {R..l[AK/<..{.Y.q..m.\..W..o)Q..F.&....).....D'.u.....G.)%.).%\,,..QZ....TQ ..+*V....."..0...."..I.1M.u.|...E..>.SS...R(...x'.....l.....L{!....j$..!..v.X=`.w.I..My.{y.t..P.....vBLLI...G.Zf.....0E.....( ?{.....=#....8P..=...vS..:.S..._..fNwoN"3..>.Z`_.....?...{..2.../ ....Gi.....g*...Y|.."F..*.....a|^..<.3.o.+.U.t[..q..q[.a.g..a...Z...*Ng.1.?.H...-4.u.WWg.U.....)P0}..X..FU.#.E7.7...,+..8...}..3.H.y.o.Yd..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\craw_window.js

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	266127
Entropy (8bit):	7.47589802519111
Encrypted:	false
SSDEEP:	6144:6/PR8t+E2di5xZh8/i+jNxcINsOVmhYw0mHno:6XiVmcW6yZ57w0J
MD5:	5407256EB12516505B740CFBE11C97B9
SHA1:	F5104DAE23F1AB5CF1B4709C9BB1B049C6F6A9A4
SHA-256:	F1E06E47E0BC6270AFA0530CBA6F6C2C1507828066C2FAE30BF33E006AF755AB
SHA-512:	54B31133A52376A85B781FD52C5050492CA5588226251DE35FBAA716C997042ED711B7D64C826FB63CEF084BA736FB43C4A747AF03A32DC3EF695B222837C54C
Malicious:	false
Preview:	var a.=%>C.TZo.!.....h..3=....Ap....q.K.u.....vkl/.....oa.n.=....9+].>Z'..&.....p...}. .E.....t.....ND.T.....[.*A.....C.L!...L*VZ...Hj..}...~..)*r."z...X...u.].....A...zg.i....s ..... 7.`Y..3|.....3...^...b..G..Z.i\...p..0Fk#...c%...Wca...+...[.0iJw..E.f.t.r...]^.rN....U.VX.@..C..y..(..YUO.k.Z..y..|.uW....am.V.MAQ.D..h#.....#.!v .B...c.....zt.h@.i1.....S....Z.=C N:.&.%AL...N.4..8.]}.....=.....U..'.f.<bR.+#....p.U...../.x.....y.i(w..l'....;..`.<H.....'..>..[^.{_..zW<.9.<....}1...9..M..=N@1.....@...j.q...%.H.....i.[*u2#..W..[.=.!...Y..T....a.....:.{ .w..l.l7.#..,=)..U.#.4.....E^..h..n|BJ.7.a.....m.5oV.ws..8..naW...oau...k...m....\H....lh.@.Z.Q.=l.l..>./."...rU...6.^.]..>.5Ti..`.0..[.|#....=.:*Ym0...=.Z.o7[H..B.G...D..r..4%.>".....f.=ul- ...O.Z7..?...!#.o...Q..8V...c...$..%!.l.... ..R..M..g...1.d.....ft.....QM.....m?...EM.M..}.l.....l=.g..e0+O.y3.).,....6n$`./....2(@.#.H..3#..3+,.^...Pv....Ye.....w.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\css\craw_window.css

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2075
Entropy (8bit):	7.902006258175799
Encrypted:	false
SSDEEP:	48:JuMgGhqPhAOpiVXDcDQTeit6or3TWvlzsfq9HhkwD:Ju+sPCOScQTpJjO08Ss
MD5:	9DB2C16697AD65C8E052C76977EF3C49
SHA1:	80D89AAD59A259E57A125A9A880A1D077E26C74C
SHA-256:	746D2D4467BD945F6267B80C735453E707CE743436FED82C191FDC6D24E4B242
SHA-512:	700C36ED89492DA9B26E364875E0F26BEEB8E07DF2525ED797BF6693931EBDF94CB34650F7D3AB0B738984E7F51A2699F899DC4E5EA9BDF3D92E7BE4AF397F9B
Malicious:	false
Preview:	html,.+....\.Gj.]..nB..W\.Iq*..dc....x].KHZ...).W&\\>e...&.f..F..Pr.....T.......Y...@.3.;..*.S.>&u.0.C2:......}.V9..7..u...gA.........P.........bc16M.X.'....`7...mx.l...]...,.v[....{.....g?.l.r.(;.F*.. ....a..V.)..OP.`#..(9..".N.....t.D>..33.l0..:u).B..v..w%w...O.g.U..n..U...9m-.!.ASH5x.....2..'.N'z..u.x.r..b.Px.t.....U...z....]..Re.C..{{.,..-.7..%?...w!z8k..e...x..'.....Ut7.*.....0:...g..... 5.J...m.1..a.9.k..&0 ..&....].o.|..^.E.$..!W.\i_.....<>..%f...3.4.d4.....v..^9....!...-=.KT$.....c.?zn9{TG.....).MQ..V>.....s.h!..k5<..q..\.E.....v.9'.....m..F.%;...4#...=....c(.s..E ..fm..1..r\JYF.....T.TdF.C..}....@.s/.....4b...Lu.a.....26D.74....h.GHT..0.z%.o+#9..X.....~....R(R....].yU.a..an.=.....L\.U....>...w.../h%...b.zs....V../....k...Se..S...T..!j..d0..\.r.'J.\ 7.S.....F(}..yl6..h..].aj.#{. ..l-.....=..N..:|.t.....[.C.b.....zO....S....;.w..tz....-)-8..7..~...V.....8-.-..y~%..K.SY....D..... `.....d....}pG..Hh./.s.N.(....i...n...M..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\html\craw_window.html

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1144
Entropy (8bit):	7.820022209000287
Encrypted:	false
SSDEEP:	24:fMP4lMa/aGDwQICGYbh1itpB94UjdO1FyMwmxFPzraYvgiZA+fPGTubD:fMP4lMaHwBCGYN1itf94UwSM5fra5+3L
MD5:	4156FBCC4BDB8D6001CE129E1BF41F45
SHA1:	8FF17B23BAD87C5BF1323AAC0641231C99BB0F7F
SHA-256:	B17068A064677D4E916490BAA6CD8ED01177F3BC3AF4121D8C5D326DEC11D3FB
SHA-512:	705C1EF3F753DDA49D4A2E23CCCBF8DB721980ED39F8594D63D143C755E4646C756525246376EAFE9B5CD3DC5531B259E6C15D8979C3B5566BA01529572DCA4
Malicious:	false
Preview:	<!DOC.....5W9i.v.5.G..../..w&5!.....P..Y...9e.`.....vl.3.[PzW..l..v.4..|.68DoNU$...r.pr.Qz.f.=.....t...;...Y..kV.vK@.....&.&.....[...k`.UBT...y.q...G.)..D.....'e's..[.0.sO!...i& F...x.. ..?o'.$gJ.x..K#.(0oR.SR&.Ji5..V..&.C...'Fg....B.....B!.....u\..iYF8>.|i.;.....a..R..g./;...i+..O...n8.XE.T)..rE3..f.Z..K. 8.+...h.....G..p#P:...Yd.h...M^.....k|.lt....RBH..q9...I. i...X.g3&7.....~..]%w7. .v..d#&?lU.u.....^b..P...B.7...c....m.$xh.vu.8k...rv..W.....pq*9.N....O.C...\|vi.....o..0..}.....mE....>.@..C...m..5....%f;...@.'W..IK.JeZ.*R.....v.....F..p.A.%.L. .....-H...P2(...E*S.m....1H...:.K.0.W.$.Z..k.%.@....).A|.:a....bz.l[5.X..T.....$.....r..}4#.ut.....-..0....B.`...E.Y.iL..$..ou..c.o.....?..../P.'...,t.3;.(...+.].0-~.h..jx<4...._.j....2. >.b5bb..G3..U.h...z.....N.A-!..#.4F.....V.....M~wQ_A.F6..(.8.....A..9c.+<.....%3_.Mo.....5.m..s.&.x.0\...n.2.!.....A8._^.., "..cxG3...lw.....).m.....]l..q....`XZ?.5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	GIF image data 6044 x 14818
Category:	dropped
Size (bytes):	70698
Entropy (8bit):	**7.997219341190102**
Encrypted:	**true**
SSDEEP:	1536:XlPH99Brar/W9RBCrR/EQfr3mjrYvl/tKJLK:XlPH99Ba7iCrfr3mjrwlV
MD5:	7077BE1F1D4EDD26CD87CBC060619775
SHA1:	72411E2E4EAB51177ACAEE7D893C18FB375E35CE
SHA-256:	925133B4B1FED2077BC96D18C16F9A83DC9998BEA0BAA3CFD334623B2B3C7831
SHA-512:	EFD09946F4D5099AC19324181047EC1EF5966E4237C3D613AFB2351EE79AA214638C99B500E16BC1B2F9BFB8CEF83812BB1F0CC07941A71152E0238E6F816DD
Malicious:	**true**
Yara Hits:	• Rule: SUSP_GIF_Anomalies, Description: Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type, Source: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif, Author: Florian Roth • Rule: SUSP_GIF_Anomalies, Description: Detects files with GIF headers and format anomalies - which means that this image could be an obfuscated file of a different type, Source: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\flapper.gif, Author: Florian Roth
Preview:	GIF89....9N.z....go..j.'.=.4.6^..d....w.....c.a..H....!.,...rbs....na...3*:.i..6..P.O..._....j..eJ}.\.B..f..y..T4$...5".Vw.....b.0.....q.s..7]......H:.....ms.@...ie(8.....<?_.....W.xp..u#g.)b.. s.....]B....."6.D.....Y.....YP'r.LZj.....P.X.JZ5.u\|..:3.$.....I..:a{.X*....T.o.H.4.....s.Y..>/..:..4|.;M.$wK..E}T...G.(..r.B.IE..&.Yh..T..W.}.,I=u..%f1...$b .r.PSr.& :*..zs.D/...=....H..... .:y..N>.&.t....EA..J.....~{.F(.-S..+o.bk^..x.@...u._.f..a.&.E.K.....O7.h..`R.I..$fWJ$b....1/..5./.rEC...j.*,.Z.#rO....s..C..c.....Y`.....f...a.m5...d.V.P.`.r...#ldG...|.k..yO...D.....o.H..i!-C..qz...t....0F2m.H...K.h....}..FY5....sa.....I..33.+Te.G.x.+tm.....w...}...GQ...0..* &...p?.u...fW.9Y..>.....".."..;...}.....2..~..J.....9G.....=..X..tt.b.C.C/..-..)..v....6b...r6.....pI *...q.Q.....3...[.m.7kG../'z,Z..|.u....b].....q.....6....Z.....V#M%O...K4.E.....`gi...[.^.h-...0R..>..+.../>.Ve8za...W.^.....s....6.=....]U$g6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\icon_128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	4698
Entropy (8bit):	7.966727909149362
Encrypted:	false
SSDEEP:	96:T26hmF488ywaha/33EtZeMIwB1nVlhJu1pLI4TSEDcQee2CYkZhbEJ:i6A288yxha/30lWpLIkXDcQ9TU
MD5:	681A1A6107959ABC285771F8A4BD0AD8
SHA1:	636B31B18539D9E0F0AA0F726900756D688F5A80
SHA-256:	2A602C20FD9BBB99B178AD34BEE427CCE051165696DD1A0611AEE13DF06B765F
SHA-512:	593CAD49BE0BF4FFD5CBAC5407A5AFC0393967123A18E987D2CB46B13CF63E67C4AA538573F85BA62301782330B71565E0B8A5AD7FE1363F613316A4E1F7DE59
Malicious:	false
Preview:	.PNG.. .._.i.Q.N..].uH`0.{...?...8.9..M++.%%.....Fc..#z)..9m$.[f.J.+.q.....a.Z\.}*.f\..a.q ."...vs.....A..R*!...-.`.[z.X...w..B.F..>..e[....:x.....\|,....bz&n5..z.4qiyM.}..?....\|.v...v.....+#..;.. "..a.R._s..Y.qFtt.PJi#...IcK.A\.~....)f.L.....-.C.-..)3[...p ..q.....wh.....Q1....lU..%.I.oE.m<B>.....".=,.2.^...H.B.k.....%JD....b.3.h..)....q.-j..9^..k...R.(..$.D?..Q.....`.V'fA6::... p...2.....t..kq/.}.j.....L.AZ;..L.;.>..h....Z..b.i.r.r_.Y.r06...Jw.....eN.....6>]t..>..z.*uM....5JZ....1. S<.z@W.....zG...t.....b...4mb`...0qY...w....=N3....L.f.:.....,D.....\...V...K.0..^\... .n#k..l..k.....C....r....U.....G..3..l.(....O.m...K....N..l<B....m.....wU..:.W.3,...l.K.C.o....3..fT..%.@9E..:...p..?..-..tD..8<...5..&..S.....Q.....3.d.v&....ag.-,.a...x8.(....QW=.....2q.,r... ...n.....<.HW.[..0..Z^tZ.....RJ.`{.].y.V...._.....~.....F7./V...S...5..."...9....A.#.T.:l...?..?..U..N.0....C1.d....v.....:..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\icon_16.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	892
Entropy (8bit):	7.750400889144331
Encrypted:	false
SSDEEP:	12:5NQyT2N/MF5B3uz2DgxcQwGj8Oqe4KZ3Z9VL/htY4zC0jGufym91sXtcii9a:5NQySMzBLDgxzwVA/hJ7KuP94bD
MD5:	FCCA21383E32AE882613E311BF9847D2
SHA1:	E4FAE2494B03AC4E0B62542E0D147A2DE123E016
SHA-256:	38B66CBA03F6BBFA2D003381ACF1FFB32B26AE3C93CD9BB237A3FB6D582D7C64
SHA-512:	B49CD7D420C8D2DD14EEC773BC9316551F1CA915566D0CF19CAE2C6F62B1A5CC3C8484457EDBDE664A2DA6FDD3F60EB492CE3FA28CDA1AE7BD723054F501471
Malicious:	false
Preview:	.PNG....3.....gBT3Y../.....3.Y..@k&W...M;6L|!.@.....1>..9...v..i.=.Q.*....:.x).:g.u..b.w.nS.n.%nR`..+..\T..2Z.."....XL#5.I.....v.ZN@....-8.0S*.e...ls/.o.....>c.D...I.. d...H .8E.H._(."..!..\.u.._.3#.V...Q.....p..J.Ko.iu9..].....C.g.2...ZW.g|.(I.O...\./...j..:e...N.....%.....D{..+.*....".j.D.....$..6....0.....b.....%MD..=..?+W*e...-B0'...i....L.....D..b1...J. G.*Z.....74`o..\..7....[...pRD3..}.....{..n.....{7R&.).:..}!...]....Sc..Q)0...I...8eK.....~....%.%..kX.....+..d...k.o..0..h..[....#....2f.....f....t...;.j...s`....r..E2.of...N..qF..RA....I..Z..}.&.3...^..q< .8...H....."....Q..v..Y.....0.'...&M...F8j.....R8\|t..f.....v7a#.....4.q..L.t.UvO.dS.....GIK..]..z..{2J6YI.*.ifA...j..u>...B.....1.I...Iyg...._..2.d...$.F.k.?.a...K6te1YGPnIbo4GcGO EP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	494
Entropy (8bit):	7.556076015557796
Encrypted:	false
SSDEEP:	12:hXluR6V8mqe+RdlChOCJ9GtwqcSg6Ytcii9a:hVuRT2J6YhbD
MD5:	ADA95D12C2E30664EB78D28E4290896B
SHA1:	B9071BFD7618B5675EE2132E44229FA28EF79080
SHA-256:	D1BF4FBBAC5EACBD62FB24D586CA94244CBC9F55FBF34A95319F7EC6F4BAE646
SHA-512:	A5B7BDF2AECCAEDF0BE9C2872B4A0ED3CDF0AC458C9F08FCA8BCC95D23AD6A9B7F05C347BACE92CD2187EB5C7B0A5715C7942192D535CD914C349F701907B382
Malicious:	false
Preview:	.PNG..>....kZ.c...D}.....d%...u.....d_.h-.>....k..KKf...9J....d.....{...C.,2u....2..&r...Z..3i.jw].....^..g..y4*..2....V..:e.....fm...m..Y...D.?/K.I.RoY.%..P{..a....p..]...d..d.6._!.x{... ...zC@R..:...!.D.Y.....|..1..x ..5-S.oq~.... m.@K.!f...:.c.....~R....z.....xI?.{Jv..3.t.ph.....".(J..N....2. ....A2.8.b..9F.|h.=....c@&V..R.....n..`g.=3(N6.u.}.4.n....4.C...;"..A... .....sA..^K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_close.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	586
Entropy (8bit):	7.623566174270631
Encrypted:	false
SSDEEP:	12:QcPhnPIO43AKrS9WS662qkaAZ3dCW174NTNc5hlInmYtcii9a:H5wO0AZWSVrk3ZNH8PUn5ubD
MD5:	379D1160E5E7C08E10E5419E6A7B9ED9
SHA1:	EA4546380F25CE9A35E15C893D9C1F42D47D0869
SHA-256:	59B52EBF64ED9D14D12F2B7B6F7B53557BEDC3EAB23441B11675D305E5E2C4F6
SHA-512:	65ACC3C74650AC157839E6E436163735F470D92FCA76833622D45B34DAEC1B37F7B88AC16B71A746A63C8A12DCD943911956F9A9958FE36474257831B6750CAD
Malicious:	false
Preview:	.PNG.Y.{.A..7..O.XO.:..@%a..3.....V)...c.....H.....}.....".....i.=.3.QT.L..j.xL...a..;.....1%..!.h_{.p.....5..K...e..gO;`.B....IMeF...L-^G.sU.LT+s".o/5...f$....Z.q.W.. ..Xw..x.O...e.5..|...-.0P...VM.....L5.f5.|...h....9..:k`ce."wt.....ll.t\|$HE.q.~...?.9..4....F.8.)R. .u.._D....X....jRp....;.)..s.+...F,)....IZ.....&.j.dY.j.F.b..5.....S.~5@g..+.P..(..O... ...Js.....4..y.U.Y).c]..B..G.....g#..0.2$x....HR.i.L..%;...F-.)'...{.....X.+j%..#..y.5K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_hover.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	494
Entropy (8bit):	7.569284839241023
Encrypted:	false
SSDEEP:	12:53W9wQdUiVQkcE5VqoNpAEbknVKGACsh5ZtpQ/5WA7tcii9a:5D7rkceAE8VZmtpwRbD
MD5:	E32E584CB5FF0681CDC7951DDBA2156A
SHA1:	85BEBFAA853EC03D8815AC6BC2C88AE87F6641CE
SHA-256:	11FCD2C3D0E855F5C193A7328FA9401787EAD66A9ACF73FDFA2BFC03C6DF3EF8
SHA-512:	0DDE4BBDC04B1229411D8C9363027FCB536282E49F5C7A2343075DEAEEC2A0F5A6AA8CA0AB7B0ADB61D06B56CA393CD610692BC48AE441350169BDDB22525 2F
Malicious:	false
Preview:	.PNG.J#. I...&.6.E.....m...J.M{I.^.e....:..4....4R.@y.....?-.....<..I^.I_.n....i[...\.W.....C..|.2t...so...t:....]....2..2.D#....U.5%...../..a....YZ..u7=.Vlx.*..{.s...L.(.Q.....8.|..C.....L....yz; (.....6..'y.J}.sH..r..LC..R..(+...5..Q=.....C.~..c...@.&\7..b...x.S.KnS.s.J..jt..}....u<.n.3.U.9.s.fN].N..;....p.|4X..j"5oNTnj}..{.....{.Wb)...=..<.O...M.S.....,.F....+,...<..K6te1YGPnIbo 4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_maximize.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	500
Entropy (8bit):	7.500044316862127
Encrypted:	false
SSDEEP:	12:pMDIDw+xhWt6AjLzl476bon0fVgNLM+ffktcii9a:+xAoaHlju0fVWnibD
MD5:	C046DD7596063A2836D7BF21F97BC81A
SHA1:	0E0754ECF63490BABC08813566C2958B317306D7
SHA-256:	01E83C07D457785BFB45B7D2FF692A52CE2DE49D4ABAF901A200EF834994C083
SHA-512:	BEBCFC6150349890D84D19C199BF30567A2F567871CA2321CDF86BF574CE036EBF575156FA4DF419379433C18FD4142C0D5D13B79221B06A90F9BD886743D051E
Malicious:	false
Preview:	.PNG.ed.?....r.jQ..@;..mR....i...ZCB.$...\3.+.#.J...6.E.Z=....uw...J..r.V..6Y.....z.....u../.Nk...K.t...m.....I.(',;d....U...2.....H.G..z.&..P..!.r..D..(J..P..m.9....n....S..A.3..7L.CR.. *.=...lm..g..W.CD...i.J.,.x$.j.}.@.....Y.....Q...G6...tA.vz..../T.....}.....!.Q....W.....c...C.4Ow.,.....G...|...[.z.8.p.....;..B&uq.9K0...B.n.q.....Cgf`7.P..Y.....0.gQ.Y.....YWK .G....94.R9..K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\images\topbar_floating_button_pressed.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	494

Entropy (8bit):	7.532809623869233
Encrypted:	false
SSDEEP:	12:Fcj7s0Nn01viJ2BT7rP/Xfy4C06sOl3Fyu1Bg6Utcii9a:Jo016J2BbKFBr351Bg6abD
MD5:	138B24E077811A0BE5742A422F8111B2
SHA1:	05819D745D39C5C2784533F87F889F5872A08DCC
SHA-256:	EBC22F7B6527961A4D562C1E519D92066DC68EF76FAB697F2BF1D62640018D50
SHA-512:	8131AAFBF70524F043A8734594E170DE8D782F404DC6DB93C06528397A2C8C3B6F55A76F81D8B1457034629C8294A6A5640A3E3B5AA235CFB66570E586682913
Malicious:	false
Preview:	.PNG...:.A.....b...Z..[....$...%./.WIn.0nu.y....K..A.....hh...c..g.d...HQ...{.....@..i.^a.'6._U.=..9w..6.>..jG....b...1.{.....v(BT.W...A..9.q:F.%E...R.m....].w&....2.E.rx-..?=...v..W[i...r .....k.. .+5...G.....m...f.j...5S1.!..&.Ev..1..u..'./.-I.,....uSm...u.....=ie.#qo{..J.....Vt...3.....#....\.z2.xxm.....}...C..`....0r9.]..(.yL.....`....^.,.qE5...|.b...!.=..B.%.I.z{R...i..f.. .*.K 6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_0\manifest.json

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	7.879357612605069
Encrypted:	false
SSDEEP:	48:9iqZ1tGILufNOJWmSrxRRjH1q2wl1hyGD:9N1tGIL0OMRNHUnMe
MD5:	FE30824C53235CF8F59708C63A2FA9CF
SHA1:	BC8C2F726E78115EB3F06531778E96E47275505E
SHA-256:	1B4B668FAB37B8D7E2416F5EF7DD49B6009D07FC66F9F7F93609CBAB1C356C52
SHA-512:	F7D36C48D3695AF8B36EBCADE0158603E3C0DAAD05F7D44B6DB099F37F508BE8638CAA1FAD3530F24F52D8A1CC4136006A731429D221F070E222C16AF6DC17 5
Malicious:	false
Preview:	{.. .Uy`.....C..Y...'..4..[.P.....{*....Dy...*.8..F.N...>....K...}.....;gA.....`.{.W...&..m|S...<t...gg....I...w^.`..S.xt...$\....D.<..!.....2.k.Bg....M.v..e...xf..)!...\|.E.D.-..=.2w.)..H. :..."TG...C0.[..D).bE.\|.....w...W...c.6..s....%U.I.....U.W..6.....I%.!..e..\|.....I.../.....[1=..)Q.[.Y..C.%r..%...Vk2.h....v.1.=.[M.R...U.o.....~....)..@..."."Z...LFjp{.....*z.N...? ~vg7D...J.....GL.(J....3.KSF-A.o.S..q...7@h.<.O...u.CC.1"X.....Y9t.....uy.....j.J...>k.\."{....EqF3...<..V.f.E.LW..]4.....*.....YVC...Q....M%.T.*Y.C....4{..(.MRc.S.5e.q."..... ..P...1..p.....a...~4..V...T..J./-.#.P...a.@j...y....z,.7/..\|CG.oO...L...O....1.93...Tx.q....b6]m...@cN....g..E.f...}v.....NE.....;Q.C!..\H....:D.>.8..D8.)..f.8G;...GD.....9.....a`.;,...<. <.N.r"..h.B.3..T=X..Ye.yn\|...MI..8...+...../.9..2w]...s...fM..7....3.!....g.i_.. !."..e...C..#....^....Pw.tv.. [.-&$q....u\c$...Y....1..;.vO..&.T.h.B#.....EX\....8..M#..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	790
Entropy (8bit):	7.721692403108043
Encrypted:	false
SSDEEP:	12:YQrzZhQVGWyVRq8MwfY+7lNeH8yUhm6LbbxweWbcrPlOrifsevZG96m6eRtcii9a:BiVXyhVFMSbUAhSKkllbD
MD5:	45F40B35269E9DE090071F2A810910E2
SHA1:	99193D534E46A2DA9CD0513FEF0449BF25D02274
SHA-256:	9DF72869D0C9CEB7928BE950CDB85C357ECC4796F746F57B4A8A8614702B87B5
SHA-512:	AC0BFEF0B844053AEC688D976A875FD29B09F0050E55D7069F19CFA36D0CF19E3B313E091568809B12F8F670453EC4402A618A9B68D4340092AB75EDE9F53D83
Malicious:	false
Preview:	....0.....J.].F.V.A...3N.....k-.....y..mBj-=...v1N.u...@t...0al?.X.....=..]...[.P:....on..X..t.....-^.+..m.....-.I.U.0.....B.....a..(0(B<.\....5.:.I.y%.A../S..T.,....O. ...B.&h.g^..K.&./..".#....?.. {F.Y.%.....Ts....t8.q.v.2wx9.m....<.....V....._.....z.:...O.{.q....s..}Z..S.P.XH.@P.G.x.R.y.I.@...ezy..?.....SE.....L.]r.....=.4..h9/..ob..Pa...}...Fd4.."....".Y.$..J..@..U.V`.....f .....~m.....o,.]j..K=..mCr*.;b9.Y.`W,.5E3.....".(.....;...P.v)7..h..."....z.o.....z.t.r!QxdV.O*A.P.s..n.T.....z...8.<..j....C.qj...c.....X.].a.UE.o....Y...K]...0|D....jX_I...P[.T...I... M..*Q.9.#B..B2&j..uo.....g.....D.,.n.....:.OPZ/=;.....M-g....gS%K.K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	479
Entropy (8bit):	7.49435643814914
Encrypted:	false
SSDEEP:	12:ZAoHvPIrYNcfWqNrKzLByHZlxNWMCR7KShYtcii9a:ZRHvPI4FqAzLBFDWM27ZubD
MD5:	886655B844028B4AD845EEF0FAAAFE49
SHA1:	B29E72B3E92491624D86EC4686A6AC18DCC12E44
SHA-256:	DE156EFDB056536AB8463E3B4A8A87BC83B51E166727EB6CBAE7703ECAABAADD
SHA-512:	5FB14B4AC7CD03627904844DF3EAB54AAF9FD584DC88E0B1994A36E20295EB30A83A53922978212D197A4CF355432D2BC07D8269A0888321E0903DF712E0925A

Malicious:	false
Preview:	2020/...Gi/`..~.....^..nN.@]...I....!.*...k....]..zI.P....I>...]m4..nA..Y=V}p.mgI.....R?..U..aM..T}.?]..K..t...3..b 6."....i.....&.....Q.<.../...9>.k.i8...pa.....r..m9..(...H~...F..&C..w*.>7..j.-...e..?GO.._.G...[.H.*M..;.\.w..[.{Wx0...}..(..d.S.K..pb.....%-.c6._.e.DlO...f..i...P..Q.y.F..Sv..j.9,F}-?].m.....\..jzuYkG...a~L#.w.q.f_...1.....R.U..Y..%.kg.p.....U./l..K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	192624
Entropy (8bit):	**7.998719632140624**
Encrypted:	**true**
SSDEEP:	3072:csoxBSmDJl5qfzXcmQMpa9XhtR1U04LO6cDtpcAQp2AhM:cscB7/IfzsmQQqxt3U0I1p2Ay
MD5:	95F322EBF9F052D7180FB8BCE1ECD7FC
SHA1:	B920FDFB929E2F42DC059EC9265C754ADD6F4844
SHA-256:	B67FE7F481975352A1BC5D176E810103DE70B65EE2F06A3BCCC777DE2EA73308
SHA-512:	D727B73FB07226B7AE490A050C0F3DBC719DB611F36F9A31546B450414C7571FBBE7A88D3F8E20B9A3A7C1FAF86B978A818E5C2535C68F473DF536A063AAE016
Malicious:	**true**
Preview:	.....;...V....Ea%...%.....\..B2Nt...n.Oz."R.).0.^.>.....n..,..yGh!../..28..6.W.....-...=.J.....2.A...i.J.?5.....xJ..:...&.sL.t....H.K<9...M(vK0u.8.....8...k.<....\.>.V.q..sx.f...b~I.8Wi.....p.fh'.l).....r.(..AZ.....w.....d.z. K.mI?c.fK.~y..."..hB.~.I7...lS.....c]....q.....ys:f.W....[l.u&..3...z.s.v."..d.yV...J.....t.v%.mE.-..U..}.~#|..0...../(1...m...z..9.~M...r.....B)v...<..%.a...j.....3i..n...<H...0.."JWv;.9...-T.....y]."..n.....Z.}..p%.I(._t..j/..'.@.....kY...D-..u.S..#.)b.Kn..y..S.|.....^..8.....h....V...L..4.s.j.q.....t..5.a._.....'t<(.....E-.@.....e~...<.S...dyuB.,...).S..\2...#...[.=.5. .P.|.<.5#.....E.Iq0C.....zc..^.L..8..@!.}...u.^.....V...f..5z.o.....A.a.?p.3`1.A./(EmL.:..B.....&.+E....d....3.C.F...[.@.....U../.B.\@...Y..x.3`.....58....`....n:...B}.dyw.H.....F+%...e..u|.....=.s."..A.../x86.0..&.H....t..X]*t...~.y..O..<.J....+....,..npZ..@....i.>G...,..vl..Q.-.8.Ni.7.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\ghbmnnjooekpmoecnnnilnnbdlolhkhi\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	383
Entropy (8bit):	7.367298346834235
Encrypted:	false
SSDEEP:	6:w4+Tp4PNsepMgxjAvIaQMapLFqRHEiwIeQCA4LCbuMu93yTIF+/AbGxntHcii96Z:XKDgxAxapL85Eibe4bs9g2lUtcii9a
MD5:	A83705C98AA5A768702B4B5D2725DC52
SHA1:	EB8C1831BB1F86318EAD3516119C5EF7E108B803
SHA-256:	8F34B684AEC8BB2414E5AE551B6568F1D130A0CFB48096EB37803C8B3C8CC6CC
SHA-512:	A936DAEEC13A291EEE5F02BBA138EA64EF11392AAA992C357BC518D457F0B2C15395EA44C332CA6C1B52D90DD1615859C1A9EBEF666DFA48F9F5D6C5313A2820
Malicious:	false
Preview:	.X.%*..+z...W....Y.....].J.(.F....E1...'].5_....HKmju.%...O..\...V.Q.RR.7...@...}.Bv.?s.W.....q..z-..g..`c....g..X$S.....E.W..j.s{C.V9..(.. I&&..J.Y.i.U.T..f.^.....<Y.N.;..bh.q....r.6...g-..r$..3:.2MJ.....&...].Y....m.KM.Y#....#.....Uj.M@.G.%..}..8.,...Q...pJ.XH.ru$.A1.o7;..L.....V...1.P.\K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	6043
Entropy (8bit):	7.967638543256387
Encrypted:	false
SSDEEP:	96:WXJo1jPeUEfncstvj/1utpU+dqzRekhLqvy8B0tC+Eiphr:WXu1jNE0stvj9eUBeOqvBB0U+xpN
MD5:	315A900159D15247A821FFB092262040
SHA1:	7FB1436E13B2C615C8655A11D0CF6FE60356208A
SHA-256:	B66971E77F00C5892EA5EA78714073641D3709345BC80D6207C4731832E5B129
SHA-512:	C9E9D6F3390048CA39EF0AA5FDB56E05F6584CD9D904341EAEC8464479EF0ECF7A6C2DCF87692D9F4E2BC9CC4C54486AD4E8AC2CEB5ED80AADD66B282BCB6546
Malicious:	false
Preview:	.d.....I.....w.W.-..uzC.*...8..$.j..2:..).Ih}oi..R.d.d.{..t.9.T<'....DT..Ih.d.,.=.\.B....<..&....#.O%:.vF=a.>.'...}..ho...Q..T....."..R]W%..Izw.x.0...(nsUR>....u..z.5..F..3....L..D.Z..s...3r\.#..U"".3'c_...PkF.j...#.Z$...\&*y.w..p.+....3.:..Y.&y;..a...s.Y...Q;.]"RK...h6..vR5.....T.....w..H.A...S.i.0..0W.1.U...?.....>I.....\.L.[.E==.nV....x..Fm...O.B.B....@D..'..\.....r.W4...`..k.N....p.#...O.....D1O..I.~.N.D..."..>..\ ..<.@m.;>O...9(..5/...7...7T.p..y..I....F!J..2.....X/.Lf|.k..?.....H.s.Q....'..m.].*....>.3.[i..d.i[.m+..6...6..:.b\..I}!yS....Y*s.....i.@.I..8.[....U...5aWY6....m...Z`c...o.....U...h....?..2..L6N...8.....!L4p..?_....5<.)...3:'...i.+q..Hv.!...9.....|ig.($. U~..x{.w..{...J..n.st.i.>...D....U...\.Z&,..?...".v'.L..Hk:.w. 2j').G0L.|.....ReL...0.....T..H.r.....R.:.....^.nhr{.S....qV.rw.%.....TP.S.)A.#.....%I@.22y_J.6..Zj....~...Q[..Js?.gS..s.;..t.'..(C....k..f%..<.y....e..D.9 ,....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	668
Entropy (8bit):	7.670059090967736
Encrypted:	false
SSDEEP:	12:tzjNIYLLPQu8kxyUnCqttUBy8eoXPOgAC/QCwzoCKT0Medtcii9a:5jiuHxHnxieMzpFe/bD
MD5:	787D387633F69DF21E1FF8672CB91F82
SHA1:	09CF4A6A2D9D74AF2928CFC6B91E16324E2A98CF
SHA-256:	E58806AAD055CA35E5AA247BD40D10A7BA1FF752AB28E936D0A94AD59A86A9B2
SHA-512:	3D09EF0157A1EFCC4751EE4EF4ED214DC4458BE6C93688745A2434E0B446B3D57CE07600C46DB43B3F7C2D33C242E78168ECA63DFDD4F737CC1ADF56B879D2D
Malicious:	false
Preview:	2020/~E...3...s#...#.....k.f.....{.....GV=:...V.uV.w..E.s.....QN..rw.....v.U._.T~U~.Rs..M3.....c.Q8.h1...~.2..?.I..K.....?....k....u.P..2#<..e.....^.k.....>.:=.fd.G.).j.n.1.....;. .H.@k>'.....g...$.....u)6.....w#..0. ...x.H(.}.. ..dy.N{*. +W{0..x.....;{..q....].6.'..8..rh_.*..e....T.....zjA.e....1..B....r.%....3\|.)...*r.....]>..-...[...#.....P.7N...PO..\.....n..z.. ..@).q:....V._]...b}.G....>.....%...%..hF.Jz.....".."...4O.v.....?..Q...z..o..K_.....BV....m+.N/.(74...t .*...V..?O...4....$.....A.o.n.....ZG..^....>..'.o...Y..m.....Y..z...K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	667
Entropy (8bit):	7.674052990054767
Encrypted:	false
SSDEEP:	12:PQvyLn44OvIIYlvAnkZfM89Qwk2vc7KDzcTBnZbW8KStcii9a:POIvOaJ6kxBfk2eeQTBZPKsbD
MD5:	1C88A5A637F13C1C5EB13005037EEBCB
SHA1:	4902CF73A0BF0F59C325A91D348D5D9BF763E599
SHA-256:	26DB325F56E60D907D0CB764A4966D286C6EB5A7A16BF789951A3E138D6EC0C3
SHA-512:	582F07774D7BFA561BE64C93A575C51228FCB3AB60A52721D79758E7EFD84AD343633E893EC34D034A3CB5A72A9629F2FC97974B5125C0221B83F30BEE619D6
Malicious:	false
Preview:	2020/.....<(.....%.....;].>LX.,N.....v./.f..P..w....T...#.-..n.@l56...f..M.C....v..Z..=..J..J5.b..'...b...._7..A..d.z..!#h[9p.UYe#3&h..y&.....N..W....\.....^.....t.].....h.....?...D..k." .frK..u].....X...*..W*..1.=...K.4.N[.....o.....4>....y[7.es;!_....bn...A...I.d....LIR../...../....y...F.....o...Y.....p._.M%.5...a.v*.n.]x).....=...L.2~'.....m6.o..O...</.d.....87...H.*. .....5.....{.p.x.....5..N.....gm.....*.H.4.`P.....R.W.s..O.(h...A.l]kc..=.....Q]... ..!..{.g...N.I..f.IV...#.,.~.....yj..0...$..!.']*K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	769
Entropy (8bit):	7.697798423732244
Encrypted:	false
SSDEEP:	24:bK13lvscKBmRTjNvjNK29ZfpPhwJre/pJTp/bD:bK1RcKBMhvjYkh5z/pJT1D
MD5:	E34F5B56C6DEEA610347ED1816F667D8
SHA1:	542DF7E39A4D501123A5654297DF2D243170A3A7
SHA-256:	0CF0523FC019B5804F4A744C7087DFA9430FA72898DC10AA27A6B414D38E2CBC
SHA-512:	09047AF632D8F425CC55A457561FED9DE9D98BC1D8900AD75231ECE91E69DF464F0CCC24DE2223173E78737F34A030D8C3BA9A7BF5CC751F6B50EA548F30D93
Malicious:	false
Preview:	*...#.?"..!."8.^..&..A,.X..y'@.....1X..>."..N....0..l)...?....QZ.&:P..&.....Hh.w_!7.....V.....3.eb0V.c>....M.....c.{..l,[.....N..*.=R.M..Hx...;0.....1...e.6.C....Wg~NK.....v...lb....? .y.<^.....=.#.0...D.j..+...E<d...M..[....d.x.IW.D...y..|....E...x...i.....w..'..H....\gcW.W'}.....e4v..b.l|p..t.....M- ..\.:-*....o..^..^6x.S..m.I."..L.J.....o..D.b...$.*..y...r...~*@../V&...< ...'.Vt.P..U.k..nR.G!.=.....Z....3...^.%...*..~...U5.3.a;..n?..!.E.XD...a}.....;...G.....n....Bs.\|.5...Oka[..Y.N}K....p.T...q.7...y]..qe...=..t..e`..y.....\|)$X..S...uf..k.`...W....%.O.....yF.D..:]U.. .....a.wV.bl...e.zv&I*..9....$..@U.5*.....|j=...jMY.MbK6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	653

Entropy (8bit):	7.638873793462919
Encrypted:	false
SSDEEP:	12:bY3LJQIFCJ7LB4nuX8Ig3Om7mZinuLU+r4BUBP/TBPidEKtcii9a:ktjCJPOus57ugcLRB8bD
MD5:	3F9394F679ECFA767C6ADA465666E773
SHA1:	1FA448A8E3B9610582030691851CB8E3801A1161
SHA-256:	8DE591AEA32A3FD0DB36A55F7C974AFBCEB39A3CB393115F9B08054FFF9F58FE
SHA-512:	6B8710F4CE0F65792E9A5D8586B4B277BCA98D1DA7881C078EA3291B6C993B024ED0616B3B3C87920A7E4EFFD28FF981721C5079FBE99ECDDFC8A028FD1E2D07
Malicious:	false
Preview:	2020/e..BUP4.>....P....5h.#[....d..@h...P.]./..D..5...r^..Iz.2.%.).....V.fsK.p...?.....N-..g.T...?4s...oO}.&-...@.....|.3...P.!...../l.....E?.R.+.9.....!...!.{y2".(^.X.#.d[E.Q.].:..B.. &.x...^..k.....e.}.]N....I.....u6d.P.V.CU.O.]...v.m.b.....<+..i..<....X...q...~.E.....k...G..c.2...Hv..d....Gy..c.T?.[6.5..!..Arx..+.,.}.`.....&.....j.....\....i`.b,.{...n....Y..u.].I.T.Fj..v.%...g.. ....F ..=.....Ke...@.0s8s.N....A.h%.).K.....C2.:.[.+.....q...yw..#A..._....V.(.2.n.K..&..3MW..4..c3....A.N..nW.\..Z..f....c..N....\ZxGT....t.....K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	7.396614774215386
Encrypted:	false
SSDEEP:	6:9Zzk3waD0GZx5zoAIEhza+Pgjao6MozxMvqzGLEsf4gCWe0grqbRAliGxntHciik:9ZlfD0GZLiv4TukqzGLggC107ADtciik
MD5:	C8C19ADAF44C9A870BC9A702ECF7A598
SHA1:	931F03138C765063E2BA953BCB660042925BFADC
SHA-256:	7C822056DC7E2F30336CE08C33CE7DB971DC491906DDD427748B19BA2893DABC
SHA-512:	F84024A02694825EC7A125C1F95EA7AD334933FAC7972148E02BE855E33747FFFF1D475C974C4313C0B6BE162B4AC1323ED715E03ECE2A7756524E60FF36D56F
Malicious:	false
Preview:	.On.!..aS.....+..KF..3..W..PH.....A.*..=.....i0d..._.o.....{.m....OM..Z.....P.....0.....h...O.d...7'..;...\h.....,".PL.....Qv}..v_.1lO....%.....Y.|.!.. .....3..]....m...>^...=.Sn.:<... ..q.....0..S.yq.{#o0.[N...-.._"...7..Y....?h.....L.~Nw..Vj..J....q.....q)K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	9100
Entropy (8bit):	7.978760662505691
Encrypted:	false
SSDEEP:	192:ldUf+3OeC43EkGeC3PCgpxfTzZMZncDV29tOkvQctSgfRh0RqeL3s:fbv3tLmPCuxeGQ9vQctSU0Rb3s
MD5:	BEE09D2C0576FF772EB3F8DDA2BE7F79
SHA1:	CF6D7BC6645E5188E9450BE879AC600045D23156
SHA-256:	238DB7F954832886CB2DA1732BC0F9EE326967B48D501853E79EC3D186834475
SHA-512:	0673CE214D58599C158B859653C00F6C97656F344CD08DA45006D75284AD4ED2699AA8F936369E2E0BD01B0F395B8A2D04372E7222D42A51CA1E7EDF01E2261(
Malicious:	false
Preview:	...n'.[W.Ee.NM..C.....W<.m..z.5...Z...nW.U.Q}..K.#K....R;..=..I.%z...3.....=q..[.x>)@.?4....4.@KSA./.).....7.uO...1.m`.1R...Y....=H.....4...G..*aV.._.d.....X....t.P....b.y....a. "h..sE.HhSr.(...e.`...H.90..4....\...e.(abN9.Vm....9.j....._Y...;K..1.,...E....Qh.JP..I.....po.....<-..3..+...W..i.....'H....s.;V4..*..;X..7vzar.a..]..$.q...@a...Oj.....L.*@....U .R..3b/'.n..Ue....e.p....=0.X,b.A.....z....4\'*.....y.,....IZP.06.e.....Z...Z=...N9.uuB..Mb ,.....!WX.s.....f._..1.\....U....`T.....<..a.....z.d.F...-..)..]../.-K.,...=Li...xv.....J5..$...S['.?... .... .2..J..0.sP.C...%6'.w<.~..>.....].%.(.....\....z.Z.....@.}...I..@.....NB.....#.e.....$..u.p..Za.3..w...k....E...HKy..-^.....8'Se.....pM.Yr\|y.(.....tj.....kT....!*'T"...JW....'..Pi..Q.I.f. ...6..q-k..).....D7...k.k.g^X*..9.w.b$xE9..fFH.q3L.PY5.a....j.p.9.....T.|5N....9f.@g..X..q..._.M^..+;...\..%..r..=ga...@....0.....I./%?.4.)uk....t.p.....W:..*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	660
Entropy (8bit):	7.649127992846428
Encrypted:	false
SSDEEP:	12:1pe9LdO7bwSyBM9gX0bMDcFd/Twa2XcVgtWrPy9kQj1CSnxt7dtcii9a:zo8FNY0bzFVNy9t0WLj1VtrbD
MD5:	1078CFFE322A5F483EF2BC4949198A45
SHA1:	C7E346949ED582BC6F85570F1D40F5E6EDBF58C7
SHA-256:	FE62732702AC3E1AB321AB394F75DCC99E6C61104298652E400D5F31A8458E2C
SHA-512:	07653149E57ECF4596449C0654198B412AA525487319C38601DE4369DCF23AC57990E1B7A54EB5C21E86E8BBC12026559C39D48BBDBE5C14D93B0E50CD8C490

Malicious:	false
Preview:	2020/..-]..1...n..f=i...&....2.. ..)..........R<GJ..M...0.....^..Q...g.?u.{>c...m.C.n.a_.z....m[!..).5.Y.m./..6.....Es".R?C.{$.C9..x.....)MA(.i.).g.._V..)...b."...30p..EzI.....iG..:..3...."Yq .....G.j.x.Kd.!G.....c.$.d...c...8...3(.D`..n..-....^...*..".r.....=?..a.4..Cox....H.`.hc%.`...+...6.h..|..f.....-%A...P|.....xr.\,.....-1..;...40E...l3M.^.<.3..D..._O.P.".}-.X..._.4..?K.I:%[. J.\..p.....|5....).1O=/.....b..S..*.K.....p...>..U..BEg..ve...<.f.....>=.m....Qh:.....c...(..K..a..@6.B.9V+&..h..B.#.....Jo...C...Ws.[.....g.K6te1YGPnIbo4GcGOE P3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	8296
Entropy (8bit):	7.978450396782321
Encrypted:	false
SSDEEP:	192:9Z3Ey6dvKDeck+HpaYNenBeC+jj8Rnjy97fExX4xCi+La9p:zzeSskeBeNH8Itfw4Ei+cp
MD5:	5CDB1CE4644F150FB732C6E740F8A88C
SHA1:	949CBC452066C1C0050F6B7512B021E77ABD39AB
SHA-256:	071D986F16B321D2C5BD9675014FA2D69BE2B1A1A2062C556E39093953E7FC48
SHA-512:	731BE0B952D2FCD8D14175937E09760251D819F33DAC54E483DD3C0C2BCDAFA5E250E8EF9CEFEDB92835DA5C7A7A3B05DD995A669560E50E80B9547A66E1B53
Malicious:	false
Preview:	.PNG....._..J.k.U.....*P`t...[....Q....P.m....\w....?....zv.</G...D...}.HW.W....@.\_.!E.....SJ.Zv....(.'=n.....:3..J..g....c...6~.K.I.u.4..|.j...>.E1.....4E.FE.T.#...g.'(.eP:Z6...m. ..>...A.....}..v.xLCCB.5..Rq.V[..o.."=.....c.'....18@..D.....-..~..hpT.>s.fU.."..v..\....IW.*.U...`.v.....(|..i...I.FIEI.....7}.'....g.O.%W!0].....n.L..E..s.....f.*..K`]....C...oD.....(.....W i.....#...z..qo..'.uS....*5do.^q..s.....jp....R....F....c...98...}[{..b..n.....w..K.....\_...v...}.[.O^./5#.[U.....5~\.K.I^.q.5m.[#..9.D.3o.R.b.&T.._.....b.....dh..S.!Z.d...(.R.).5M..\ ./?....A.Y..r~h.....h.2.8.....a!`]?6.]h.Y.....bDRF..f..XV..v.t.7...dH.c.....S'.\l.....+.>.....q.....{....M.....h..".3c..bt.i..|.....d(MY..G..|.....S.....y#.x.....0Bp.Ia...R..(..&m.e... =C...}z|...(....3z;.....Y.B.!.`.\4.:O.f.$S.C%,..uW}...7.Hw...C0N..sk:../...Pq....z.....'.....Y6\,8..9..wAZ"~..(....!.....T..K.T.*..g..6....K.q..WT'A.....8]..p

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\192.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	6023
Entropy (8bit):	7.972857180537423
Encrypted:	false
SSDEEP:	96:5KquxkBkMBMlbVkHJtw2NNhkBRjW18Dci3v/U4+pT2SxRMHM3E3c14vo3JztO8y:5buyBkfkhNNeoyncT2SDuM0s1HJztO3
MD5:	0E23B318DFE7EB2FB7BD908B34BF1DFA
SHA1:	5567653AF56A118ACE91693E5D57CC04B27D5F2C
SHA-256:	D59BCE2C217BFEE2025ED724287643A1A50C72DA7D9CD7A65166CF938B42D8C1
SHA-512:	7571463FA5F34AEF0947C6C628818798C276A59F9A1DF5828EACD47CAB2024549D3B683815B220F342ADD7D2B69C8A618DE4B7E594F28E8A286CEE09FECB056
Malicious:	false
Preview:	.PNG.x.y.....(..(...a...Q..t2...}.H..K..,H..#.H...}.....%..:.Z.R.H^.g...1.....r|.."....wu....p.)....R.H ....M..?.L...D<$.._ZP.!...(..4}..$3*.$.$?..C.rZ..+..b..t.+..;w..T/R%.]...`...C.5.. B.I.I...8X,.`..vA...H.~d.....S.j.t..GH....N..'..c.....K..*.?!t.B..r...Q.....`V%o.....Ee....U.....n...M!8..,gcFntY=...%....u(..i....-/...,w..o.$d.\l...{.. ....N.....q.....|...D.h.1.Y.J.nT..... ...o.....mq.....F....$.'.`.1..Z...].8.{....j..4u/.n.....o.i.....\|...2....{&.n.J..\l.A..5A.X.`F2m..vP.\|aRd.....2CJ.V...%oJ4.i..&P)]7.9.Y.;.{..i..NN.L.f..n-.5<)..k.sUzk...o../zb.Y.S..,".7..'8 )F.....9...:S.~....'...o{36.....UeE,...\|.p.Q.....zl.?.M.Z..mU"..t#B"...\.2.....R.....;...f...]tM`..*.hV~.j.3_-.....M...^.I...n...J../._..*.....F.....c.....@.MN..E.x.N5....5....~..o#..U... .nZ....Z..gB.@...$.....^...[.....r..|."..../3.y..4r%..I .[...:.b.w.&..J....7...^w....I..oH..g2.g.....b#...m.`fde.....)..IyP.....?.e.....I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\256.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	19928
Entropy (8bit):	**7.990946717067047**
Encrypted:	**true**
SSDEEP:	384:YHCVYPMVU2f8ZCi5sfptG8iJlrW17KD5CHrbH0xx3b:YHoYPMmTceIDiPrW9+5CLz0/L
MD5:	76B0AECCA79009E4B27CECE4B44AB567
SHA1:	0C9ED9B16BD4E8686D090BF52546E8B41AACCBF2
SHA-256:	FB360917F19EAD9C4239C90A0768E9CCF331B450BD2A06EC82D6E63E8A79E851
SHA-512:	9CABB97542D2E6348E6218E4A3ED8EAEA252E710D9E7AECF51A2F8A78A859708029C6251344B0CAEBF671A77D4AD9698B81EDB986F52F1597E712ECF1C9844EE

Malicious:	**true**
Preview:	.PNG..w.*..6OC..1...J8..HA...vR.k_..=JA.....x+..s.~.]2..y?o^..?{,7.?.W`-.y....._.+...h.yi...\zQ.].3y..2F..K...-Q..h....%..aZ.%..K..I...S.^.Q..8..'.O.+X....._o.....:.I..N.zgG .r6W.....3^.B^...!...U.2^x'.....R.Br9M0#.dzp )...F[.o.Kq.,]...r.e^S..9./xL..R`.{!.....}....N"._-ug..H.T.....:w.cT...\.aV.}.k"...t.V....R...v...^.-Q.R...3u@3...l]....E,.s.....~.v.v...~".[#. ..O..M.!:.....}.<X.M..t.~.3.<a.b..x<5.T..+.nl.....s.Y..i..y.(.MC2.0.?....._.lmj.:.P.K.Q.v....j....uh.B..._8.....?.%.!.0;.:.....a/(...xpK!....,..m.a.=8...T.B..(.....=.....g.A...Ao x&HtgU.W..e...T..k..Lp.....S%....O?9.x.....s..T..^..Si~.Wn.....b3.'8. ..|`l`..7.@K..#.V.h....c....+Q..%\.....E...$_.....pm..8.....EV0.e~.X.V.;.}<.._6v#,* .h-.....T_.....I.4.,.f s._V./.xn....TG..R.7.UY....<.b.~.D...{.....~...<.Y..3..[.bQ.6....?....5~7. .....=.G.k;s<u.....d.....i)I.;.....q.T...N...s.l....C..FoO.....0t.9t.....g..%.....v.cgY..}....=.r?....j.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\32.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2150
Entropy (8bit):	7.894838455997438
Encrypted:	false
SSDEEP:	48:gyzOkNT79cUjtZbSAug7ApNxpUrKGlC86yu82mnIOHkDQmD:gojj3SAug7KNxpU2W6uN+
MD5:	0368FC44052EBE5766887EDFE863921C
SHA1:	77A16CFEEF768A66D5F5EA8B1A2D8051BB71B1D7
SHA-256:	9E88388BFC6EA72A0EB4CEF2D7500C217F9D2ED4854C502497C800281922F398
SHA-512:	312EF3542B657361C4989C5BF354B45B1B358397BD311BB198389A04DD01E053328EAE987364C901E06A8DF0C6A381DB08FE83C95048409E2DC57E0647C70422
Malicious:	false
Preview:	.PNG....s.....k.xm6Hty..b....O...'*..It.?~H..~...k.SZ..n.-.A.....G..z.M.X.;.Z.c=....Bc[.%.R.u.D8.s.q$.zJ^".h`.....&]...y..<D..6...j..G..H.W.....v.%..h...qK3.....h]yR.$F.k.}#..F_ .BO:5.Mav.r.-.....&3GT..F%.S+Y...KM...b,hG..<~.E...|..2l.>..px...P.....D.....|.....er....-..6.fg.~r.Hv.Z.*....n:...e.q...$2.z.W .01...G...:`..ks...A..{.JF].T.?..0.Gk.....i\..F..6FE4u..... ....Nv...%...u..o.6.nH..6...t...l..k8h(...E+...L.&1..q.....YA.....PFQ.QM..i...jj.... .A.T.st.Z...E&..t..X`.Y.;.....p...N.%.k$.u.{}....7x...,GID8E}.o\....p....J.Z.0y.CN9.UW...,..j_=.hn..~ .|.F.a..^G.N:MP.3U...;v.o.7.D.r.H7.Y.S.....<...f.Tg...*;...>...C.....i..8n|..-..|..<.P.D...X...+S.....f.z..P.T#.{..W;...w.....`...-a.....b.....rf.>..0...:....xB....3~....C.1]....w>.....L..2(" `.k..sE.w...*...8u.....n{.9+.j..*..C.F.$P.....Y^^.&..V.kH..e.....y-..*...&%B.C:+...n..x.....<.....n@pK.L.L.....5...2U9.[N..:QA.....RI.s?.....[...]n...u.."]y@.P.....^..&..L..`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\48.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3201
Entropy (8bit):	7.937383274033901
Encrypted:	false
SSDEEP:	96:AHqMJ+TJ5NSuXhpJbVjA2L57G2Qkf34i0nICkuaJ:fFNxRH5jAa79NIi1
MD5:	0E9DB0540EC9F914C573E49C1D3D57B6
SHA1:	2F798EA473C15FC9C5E2DBBE771CB65A8E13D162
SHA-256:	143DCDA4CE752BF6B8DA0189A87265C9DB65B8690938C166916F4C47575247CC
SHA-512:	434EE983B9F0A2BD918FAD8BD11DF5EFCE297E91762011F52933BC3B3472E2277727BD9CF7CA123E755B64243D20D6281B30355298B608F2A75DA3E2FF8FD6C
Malicious:	false
Preview:	.PNG.~..1....E.2(.....#.2j.....-.K..lV.%..X*.(...E.a..?.....D.x..S."H3..R....a.pS.!.Z^.....t..&..>.u.X....B..o.D@...g....j.'....la.p.d....lh....@.T.|.#..w..e...e>.e..5hd.v.i*#..fi<V{!...q ...9...+Kp&....].....g...[.&.e.$...2....NS.....7.0.3[.qj.E...X.P..; .....T....5...g..u).,.M9N/V..J...}D.....A....a.m.)N.H.j.@:.^.....C.....J...;`..1[hK>..:e.6.2.....]+...bk..F.e7%(....._d_Z.F... ..~..^E8.?....7%..`R..bv..$.0.P.....{.R...[...Y.)Z.O. ?..?.'...kqP.7..).....#.].HT#.=S..O.0../.....*.....0..b..i.3.F>..:.....o..H*B.G..U%.TFa%.$.m.w..YP` .+...S...K:.|.r,.....r...U5.M. !@.Om...RA.4..m.4X..+....._l.....V.7...K.J6m....8Zn..:q...6..H..7.;#.....+.w.....wxp~....t.2..y...GP$HaC3RS..r..!_.....0[.g..A.3...u.....:...J.0SI...bm..<_..A.....c...).4...(..M..ne ,.....(.j.?...%.f....Bo.....7...?.U..+...^mR..F.....h]...I.....GI}..^F.../.c..]..FK.u~.7.i).K~.*z..B...}oF./3...b.....8A]._...r.....K.)v..u...G.#.,.W....$.Y.9f.B1B%..~S...X

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\64.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	4170
Entropy (8bit):	7.956316605559718
Encrypted:	false
SSDEEP:	96:Ehc03GYR4fYRY9csjT57qlyQNPe8dbVSrZ6mWU:EbGEYCsvolyQNvdB66mt
MD5:	9735BC839F2401673CF7A2A685F842EE
SHA1:	069AA691CD58F018D890AE15D4491B106846F170
SHA-256:	3F66D4999B26095E50327C47D83AE8F7AE8C82011414AEB11AD970E5F8ED876C
SHA-512:	4EECED280E93B26C9FF19F54DC6F43696F1901497CF527D6917CFAF102D47EEBA79C7E1684109B526958BAA79673F10CF46EA48C69372CA5E0531D38A27053A
Malicious:	false

Preview:	.PNG..*.....3.JC..t.Y.....x.-..J..[=.I..D.+S.. ..'\,H%.......J..i 1X.....p.....+.....8[Vc..N..7_..<.....[.h.G..x.a....._O..g.....7,...mn....-..K....Y..N..K.*.YmuZ.%E)...T.I...Z.(aG..F..=...}. ...G.+.z...8s"=.c....e.....E....."1...!.nu.0..I..sU*....n8.f...&...eW.....o.. 6Mc..m...d.e...<..-...R...3..Y....1..*...v64m..}..@..N...'..@.YR.%...P.2?....MT.@\....!.[v..m..t..J.#C...0j..& .C.....Q.^......w.. ....t.K..r.i....H@i..y>cl\}d.=.=.f.1v[.....a..s?..I..<?..m..;.&>.I...p...+mV...,....I?..:..Yk....Z".t.v..r...Aw..9P...j.G.{@...]..).J}O./.^MjfK9.CR..\I.....t..PY.....L..#.. &|;..N...@....v.....n..p..Y.XuZ[.1..8].....&...)..._...eK.Ev..ZGP...7.!B..D3XO.E&...(e.....bb.._E.....8..o.7..A.H.S..}..aDrSA.....PFZ....cY..c.#r._..E.H,K...&.Q..6.....-.....>..M.a %.Nt.,..I.I...2..C...2....q.....4..H.....n....aH.....A..;I..>.....K...W.B .zv.^.V..@m5...?..SNk..L....1.,.rr.j"..Bs/..R.e..y.(J.v.3.ZY...w[$y..?DP.K...,..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\aghbiahbpaijignceidepookljebhfak\Icons\96.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	6103
Entropy (8bit):	7.972218538034077
Encrypted:	false
SSDEEP:	96:z69egiySOjzOo4xYbqf+AISYT1dqNjvtPvszXHH9WjpQDOUP6ivEvsA4ibJcRkCT:W9NxSwzOo46G2AIVHYvtPv4nUjCDOUym
MD5:	7F6A14C1DC76DB709D26FF225487A0CE
SHA1:	A1DF7067495572CFFBA4E173DBFF4042A0B279A0
SHA-256:	CEE50B5D8E6F0134B4497B55944BD878800C6BCCE22B67194A5F5F97217F0030
SHA-512:	37D164D542C62BD809D97CB14D80AD09ACA6DB8EEFA60472CC2B3E03735E6BA77D62195CC719C6AB44D53E8972C4D10ED0A57C9ECF20151D94ABE9C2D62C8A9
Malicious:	false
Preview:	.PNG....gq0.(Bp:h.]...;..A..y4...V..1.8`..q.iWu.S,..c.b..xO..d.wO,.....z..."........X^..g[.{.q.S_.Xru....3M.\]8.>.OP.=4...g....s....t..9..wH*..DU.bf.....@.I..0..Z?h.I...I..Z.........9..43q ...o.9....Z..3`.....x.+|O..k..[k..^.A...aGAQOm.....e.q:.fXC....h....]..x..$.pF3....._Y..n.e.8..3..j.[.....m.....I.i$....(...#.e...m..6.....KO...)...Br.2.7...Fy.....h..F3.V.=.....Y..UM,t..tT.w... ...B.._O..+...5..%.O|.t.?e.....f..V.*.....H.}<.....Cf...Q.....%.ZIC.) ..@.rj.]E.....,..Dy3L7.....nF..6.@...v{.m.?.I.*D@dp..jH#o.y.=.....>M.....X.F.P.....cY..!.!t(|.JX.....>= .#..T..... Y.~.-9P.7..5A..3... {.'.c.....Dw.x6..;....h..MeK.X9/wG...':.up..\...h.p.....3..v ..r.[....OjA.H...Z./....W..6C_.....Q>.V....K....a...8...Jc..[.....0....W..3..U. ....C...hH.....]..d|C.=..F.....*...#2..(.u.#..I..$.t.t<.. ..1..].v.+j..\.$.7.P.<..O.....e0..u0{.vf.$...J.=.....Gm...*;g..V....a.&..7;.o.b CP+....^.>Y=.+.%.U..o....E.T..._`.."

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	10398
Entropy (8bit):	7.981961379286768
Encrypted:	false
SSDEEP:	192:ONk2KJ7iy+9rI266cVt0cE68a/tqvMj7uWywkYxbbXMH2GmrrHeGk:iM7U0266M58iHkcX9H6
MD5:	6EF88F1B510917DFBBBC8D902BA3C80B
SHA1:	63093781DAAF91D41483A984839BDCE12BB5F764
SHA-256:	9A247E335C18D9ECB437C51ACA2A78ED74851642D067A6BE3602AF9116A8FC6D
SHA-512:	2875E21AE33455F2BF2B062ADB639C28D9FC875AED0D7A23807B4B5214FF4A7BF6199F45CEDCBE1F08FC2D1E7B3FF0EEA13827BCCA9CB78B79C0F86294021E87
Malicious:	false
Preview:	.PNG.T]...u.W..$.:.....m..;.q..h.....b..p'.n..o.<..]{....9..}\..3[.....R5.F.....O.fWdR.....:j$....2..-@..,zTP.Hs.....O.E:.Wz..eT....8.....j....%...h|..xg..&./...<N.L.=....4=.:s.....d.b ..w.3.w.....{/.1.+5..'.h.*B[..PJ.....|...2z;d..6Q.&.....#zz.E...8.....#).N..v..w..;nB.m.....B.w.w..8....T...._I...B....~.....+.....t.-...|hr.k...n'hS.T.U0.br(.N....ZQ..IO.%...w....O.....`. ...y...\N..Sa.....h./.Qbv....:f...^.,%I1k..,.....4\.[{.....h!i0.h..x.)....D..[W(6^X.n...>.7....H.um_..&<6).Z._.3.....-.2...M.la.....K..L.T.k."J..OZQi<f.P..s...".hx..."."+..Z...Q.}#....2.{.[H..... {..B.2D.:...."...6\7%Yn";X.....q`3e.2....W../../..?.'..r1='.....4...+..!.?..*.....l...d.e.....8*Z.....F..t...._*u.....>xn\.(d..g.....+.q.2@ .c.6.R..E... ...Y.....CG.....Y..7!.b8.....e..k%} @T..#...h...U..._._...#....]^..(..w1....Xd.>.3o5]."......-F.sQ.....r!.PT/...8.B..Z.....y%..U...tz.....N5..6..\l.=.\^~.Q.....>..9....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\192.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	7289
Entropy (8bit):	7.976007936767282
Encrypted:	false
SSDEEP:	192:TncOpjJ34U4gqMCbTQy5rcDvfnwEA4fodE/NbEpOQMAMBIdMI:TnJLrbkbT1xaouoqNgF8Wd5
MD5:	F076A3B2F42CBEA6F27DBACDF7422778
SHA1:	657A8A22FC3FF100F9E9CD2FF8DC854847FFEC34
SHA-256:	F690CB7A8CB07948F2939F7B25820EE585B6ECD599FEFED3F301884578E9B952
SHA-512:	69FB4EF7B08D2361BAE352D29CC023F491741ACB9ECF4189152EA2490C69BDEB47902654CF051E2F3CD8EF61F784ACC87ADF1DFEC51B9A41B0568D212B57DE04

Malicious:	false
Preview:	.PNG....eK0.;f[..o..Q.5-#k.....R0...IPk..f.e..*.Ub.@f.|a.UN.Df...C...Wd...K... sD.)I.....<.8..><,.&Fu...h.b..B.:..*.....$.[fl.....05L-.g3..\8..ZTGJ.*.(.Z.G.k...uQ._i....G.".#G.7..v{.2...>. ..t.Cv....T...+..$.....2..Y..6.........s>...jN.....3.m...R.'..Y[.c...l.F..d...OWA...I...6-.f.x.K.....w.....E..&w"Y.....e~.pO...GI*.-...X....<.=.RG.M...2wS.7>.h.lp...@!*i...5.y'..6.e..k....{R.+|j .*Q....<V...x.....0.z'..7..!L..."....KT....Y..i.Q.4Ew.~V.%T.....O....ls...M:,...]e0..7... U.}.....C'..F?O.....>.Z....R.).SVp.....-.....j...K!F. ._.1?.y..gV[Jk.p..j8_Q...$.....a...nJ..,5 .T!.N.....y...t?i.NZ.J.e.)Sj...y(....M.XB.... S.QI1.o#-"=..v.W..5g2.-%.3.p,.j.....}M..u.....+....E. ..b..6r.....d...<.X...SL.."m..1d{pl.r..v..lO..rTj.hsK@C:`.}....w6...}....*k..E..v ..RN.N..$...K.%..w....v..;^.....o..\./..]...>...W...?kAb..\....>.,.v5B..!.....h>J.)..._.y.....J..G#.r.ji. '...;]..~<.+m....3.,Et..Y...S..,...T.s...h[.\=$:..-.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\256.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	25673
Entropy (8bit):	**7.9939633129255085**
Encrypted:	**true**
SSDEEP:	768:3U+l/mWGhtxiV7eSsS60SAmxe5B9m5fLuK1VC3Z88eMK:3UO/fGh7ioSDilSK1VC3deh
MD5:	F9D097A93E0D84C55B28E3E406827376
SHA1:	4D53B3C1A278BE4E516023B152443E3A4573D83C
SHA-256:	4458046279D68BC861963B6BE374EA087E3CA7B9AB0884151EBEBDD7DA44DC53
SHA-512:	298D09841C25F0BC1C863FE6C25788D7DC1F12E74C7C459300823C5E4A62DB18538D6EE8AE2CAF79F49FA7094247213B721720C73B4E9AA6233099EBEABA2B25
Malicious:	**true**
Preview:	.PNG.j..$.....\|.t.p.L..).O.aQ)....f.....Y.....E...:..Y)1.%q=f..n.$..|.K.9E..7.R3l.w.el....q..v.(....x...$,@.....cS..u.4..[.+..7.V\|.i.w.m.l.....gz.K.]..R....E.t.7ke.B&Nh..9B.....J.=...4. u..]\|..X..Lvf.m.}..dA.l..=..9.....<....S6.Y.K...._.....@._h'i.....'U...Na.....c#`....6....LQ@e.7..3%q.(..u..A..W.....U.OC....3...\N.....v..9`[....pl.S.hq'O4.....fX...Tw}n.4J6. "].'....GP...3.4.....;@'(..J.....,[i-..nL....,e....E.Y....;....NI.....P....M...xF.R9.T..w.k.G.j.Cr.. BZ#[c.{.6n.\.X.....>..".z..+..4Q..5.....+\|...t.#JA..A... :.....=.].g..`X..0.!...kP.G..vv x.zi(..9 .jGT.E(]i.j:.m..F....g...>..!?...T.).g...>...../.,...\|Z...(.c.rY.v.d.....^'CH.`.O...Qh.j)..U..s.$.e.^..V Dlq.[V...e.....k.....2{B.CH.8.z.1...:.p*>...<}@.....3..%.=w.....Gu.....!.#. Z..S...g..d2.0,.|..%..a.:.....2.....5.>..0E.%.D.5..^..0.:.L.f..a.....~.-...5&....YJ)..?..3....Z....J...1...P.v..0Kc.Z....v..JNBjk.8.....C..j@..PP|={$[].

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\32.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1823
Entropy (8bit):	7.8743531472906465
Encrypted:	false
SSDEEP:	48:Q0ULZgmln7g5RcJEQUw6hPHY+0W3zFSx3AYMm90/eY/Mifqe4OgD:1aZxciEQUwEl3zF2AYF0HMbe6
MD5:	4A3EEFC211932FE5039B61B9DE3585CA
SHA1:	6E07009C5BA7A53B37401068D33E316990DD56D8
SHA-256:	FAD4B8217B83675E773089AE59D284797308A608655E5D469EB1956AA11F5C5E
SHA-512:	A12D8E21F32D3229309F6E8C3259B02C26F5517CA8C8D39E3ED66E10ABB38CF31D7D898BEE55589A5BC01B77CD2AA3DFD8D35B6107530AD66F752EA5381F607
Malicious:	false
Preview:	.PNG.vS)4Cb.... .....@-].8..C5.....;?..(w_F9.=$..<.z..I....Z.....).{.B.#.]~.\|...J.1.....jw.[..@v[S..W....o..7D....$...N....W."#s...mJ.A.....#AG...f...S.jj.....X.%L{v=....I.F..^ST.9... .!3..Je..*1../.....;.0.g0g.L*...o.G.....$:{"xA.Bi./..1.....(P.....6.jsH.i.."....[].....*\|..s..y.....`.I2o..e.\|.....<....w...W2...E+~....Z.s.;.tV.0=....{..I....5H...V3..W..vb..N.....BY.y}.XGU...g.^ `;.....\..Z...1..}.s=o'g.#....z.^]..+&.....!..Ev1. 4....86.....:R..".}7..nz.....j6sUg..L.L.j..,c..Am..>.r~O(h4.}...+....R.<C.7...P.3%.5..P?..'....X.Kw#.4...\|..o5.]. ..&U._@Z6.Ug.....,...K.. .@`...Xj.....@\.............=C.b*jX.....5.b.S...qA~[.)..Ba.#T.%...s'..D^6.O.....!p.0.Q:.'.....ZD.1yL...T..,.59o...D.CCa.3.H.D.z.Z....U....0S.7.o....[.....pJc..u..c;.1f...xb.Q.+...W&. .:M.8u.B'..h.{....z...1.x:....."...D.n."-m.....D@.w.d?m.".y.`)...!..]....uY=.....J".I.[....~...I..k..T.*}_..? .....oq....t.....s,....HPf..4@t.....q...$XPX..V...i..$..1.?.e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\48.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2747
Entropy (8bit):	7.934144817292472
Encrypted:	false
SSDEEP:	48:02sTX5ny606/szFEKHgJh2u3OAEMyqsGM2ngOM+SJlaXczzyYFkuwD:0o8LWufOcnCJlHKYts
MD5:	B2C6ECE3FED803C21815DEDA4AC424B2
SHA1:	F4F6C3F4E78ED5691A07DB923336C64C1D3FE293
SHA-256:	8E5B57F7A36B67E2A1F05EA0ED270A0436AF5510BCCC0F8C4DCD2CC070790CE3

SHA-512:	02BF61BEC4E307943DFFE1F245D83DA4286F4EEECC724D093EFFB17A18628642B8033831C46531171ED89EC4F218CA717F1EB318E9528ED0FFBC5AD5F01DF0 1
Malicious:	false
Preview:	.PNG....x.....B.....8R..5p.3.I..H1.NL.R;.<.I.b.f..i....p.'.....2.Pu....<ig....AP._n8b...R.sY.s.....R.A.1..u...g...R.....83.9.0.m..~m.[|.RE].....1.=.u=..K.z@.....~Mz.t..=.O..... .....@..4o...c....~...7..1.6B..N..6R..f6..B'f..Kca.m.....h].4*,.'JM..Dx.....k.ljhg.(D.m.....rz...4..g...H.....:3].t...N\...z..o.ga.....F.....d.tm.Y..)fO!R....I7.I..C..=*...c..^....W.I.?..e..... .Y..Rp.N{.t...[...{..Ua.....>..96...:e..Z...^....pX.5].%.....L.(V.n..5t....`...`..k*Wbk .X.L..^^}.3.,3...*G.....&..... ....[.....I...2J6...$.../../..w.{..n..=.....R.z.]...S!.D....BC.n.O.PSh. ..4zO.\.....I...~../.2...B%....>{.Y-..+.....I..w....6.....].S..:Zi1.ru_..u.....w'|sGI.....:..nY..;O..P.v.=..;.HR@.?1w.....p..Br.STe.WB....&.wha|.#K.A3H..!..#.{.....K;.p..Oe.....}. C_.U.\>'.....W...U...8.... .....I.a..^....@...J..d.ch#)....(.k...Z..v..R.....g..[..:;.b.n.....2J.|..p..>...T..<'....'..3..;b|..XXV...Q..|.+H.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\64.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	4111
Entropy (8bit):	7.949936786165925
Encrypted:	false
SSDEEP:	96:tUEAd8PfwLG0hFjfpBpUWinOVsinMnQPXwj3+WzgIs:tUDmwy0hxB6lEuQPXwjuWzUs
MD5:	B506C030F5FDB0F2F82015154DC85B28
SHA1:	6437DB3E933FB57B3E0AC61E9250C924239D5803
SHA-256:	8A2EE33073057A42F4575F5FBB2A0E06884F4C1E512B75CAD1803365BBE05977
SHA-512:	D3F0A3435BD5ED031B29F8F0C9C884C4CDEAC90C0599F81165F8EFD27A20055C1816F7C5B1FFF1BF993F646CCBEFF235EF9E6B6B098EBEDDD9A51D46134C7 EF
Malicious:	false
Preview:	.PNG.J..#...6&n..3.e....T.....TC.Z..aW./6b.H.....S..q....SIL.....m.|...;z.C.b...bV.k...n=.7.....).U.._.m...%.f..Hk.pH."4..5.!.....H.D.\K..Y....tR.. Y... .5.....<.Cs.....+... im.._Xfd.2..=X..R...U!r1.v...s..>m...}../....y.....[.....+/t.5.YZ7..t.Q...~...t...J..s.|U...B...../...`...q0.s;G...M.pK.X.....m....G...s.}..E...d9a.q.....A...."Xf..#.d...8.$=e6..Q_.Y..#.....w..` .U..<tL4.....~l.[.!.g.Y.....#....3..Yk_..n(...d4..%jI.I../LJ.q0.s.8I...Q..C..-S.[.....k.RXl..p..W+t[..p...qf....e.OG.z..R.a..8.F.a..?.D..`8..a[T\.e.{b.S..b....2..L*..#Z..&....U.....8._TTB.. .\|.....,DQ\....$w2V.U!w..t..Z.L..E...1S.He;kVU.5F>U0.....H.)....84....?..T...c}.jzt..O.K..H.....d. }....u9.M.p..)d....wW:..Gd.. ..g....oHD..{.'...w.6.'.N.ki}w.....vo..u..+...OE....R. .'.~.9...7.`..}.....f}g.$.....SB..T.Qqp.....GFg..W.|..0../.....;...F.6..a....&.....*.\..... ..H..!...+.....3...d.O.C#Hh~.....J...E.n.)._.*.xr.j.0.*CI.d._.30.4.....R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\agimnkijcaahngcdmfeangaknmldooml\Icons\96.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	7049
Entropy (8bit):	7.970794535964921
Encrypted:	false
SSDEEP:	192:thGcywKrx3iL10o6qo5suhn2V301Jnyn3fn7h:tlcWra0o6qyYV38+9
MD5:	0E214E2B74A4EABAF7ACD0EFC7E2E99A
SHA1:	3315E6BE97B49A0AAD6174F95BA5F97601EF815C
SHA-256:	6B447CC6AD4A09D4F24E5ED4A60FC57F2ED33F09A48458CBF0A1C5D90D202615
SHA-512:	A4593C4FEAED7E3F870AC8C6AA40CA96C802583950E1347D13DE598C99561504DCA104C093D026E734168266EC9C8D1FF82D88B63C5BD7A61FC827B7427223F
Malicious:	false
Preview:	.PNG.Y.q:.D?[k.~..y.i.E.....vT.....Ce.....m[.F=.w....r.`.O...G..h..y.%.C....q.....!#E...0..(t|-.... Z.....E...F...;)...^^.\..9!x..z?z.>.h..L.)."^4.5....1..H.b.....7Ts%.....-..{0.Bd= ..eZ^....k...%...F3]..-...6.]...x..{hD...-g..+.0dl...`i w.5H....O<7y..f.25B.NP..a.....S./../.?,,^zLE.'T....c.....@.)8i.....^.....2.....n\4...>.V*.I.JQ..v....Q.2...b..E.+..v...)...M...#CJgIX. t.e.n..-e.;.w.....L.P.A..8.....U"_.SfS.v.Z..}...W.85.NT3..p.r..L....i....'.....%....{Y.\...zB.<...c%FYs..7...v.1..."...64..W.....W7..vm.=..U.!&N..,].pXD?a.fy..._....\.[.....vw7.%qb Y9..6B..tE;..6...r.,;4."I.&..k..T..|..J7.....]...\T.j.E.c.k...B..n..!.).`.sU.4.b'.f.....%].M.....]...|.xT...8.|....$.f..`...B0nX.....F.....'.^^ ...U..i..(*9..*..W.-..})..6k.m.i...2...1.@..s..J. dO.8o..a.pE..2.'.]...0o..e.+...l.{....e.C.]r2,....A.}=Ig.....3....y.g\|.W...].6fX;:D.....!.w...E$.n=.. Q.....h.Q.....>.....9..c9...7...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2642
Entropy (8bit):	7.929673355975747
Encrypted:	false
SSDEEP:	48:utNv0wu6VFCPJUOK3AHEm1jxWnAY9+raZ7a2R1rp69AfXGSudCEM2bcNh3b4QD:utFA6vCPqpiEM8nAY9qUaSrZfsAEMVrd
MD5:	CEF6DFCEB828F5D98A6A17EAD46AEC0E
SHA1:	280F1B285D68E01BC88773C849C2AA24A5FDAB52
SHA-256:	801702444DA5CC6663EA96C913A0B1D924689645DF07FC452455797F91E5C829

SHA-512:	72DA1C1978CC718DFA8BE01F5E7D17DA08CDF0DA96770BBAE8624ECD1EBEC95C73A10FABF83BEB4CC0DF19DDBC435F11736D66CCDE6352824F56B33DF990 75CB
Malicious:	false
Preview:	.PNG.G..)X>.}..M.YW.I6..L,.x)...u*.....[.,....-1^P...$.|.D"t..A.U.B..U[.>...Y.I.}a.....h.....K|..o.t.....h.r....."........~J.[....Mr5..P.^k....$M..T...(.L.....\...c.....D.D^..1b.\.].&.c9..ao.8o 4.....#.^.F(*]+Jq.<g[P....}..~.....K....b.vq.....8.9...qg.$.N....?...VU...).....u.$-(.....Dh..L..!.;...g4i%..rB.5.6.o.YM.. .d.S..dp....Bq.....<x.._...5....8.}.-.K.S.t#.%.'^.....+;c@.7...v...-t3 .B.....X..e.....8.....0.$.C.q,...@.h.C.....o^.qv }.j..:.b.?....O.:.g.h#n.>P4.fL.f. .I..:I7p.:..iQ@...$...4..(.i..|VP.Iz.$..|....T..(.t.]C..X..T,^..O..E.....*<.....rS.v(...[.s...&.*.y..d....F...0 . .....,n`..>E....?&.V.TE%n....g}8LK((.q#....WIV.....b..D....5.;...Ra..RP^.....v.'i....E..>.V.Uw..U._7..B.BF@Q.....y.M....M.wk}.....r.%.q..Ret.8g..^.%.....r...r..&.K...w...e.lu....: .v...j....~..*#..2.1oc...`1..P....$.*d..U. &..m.a...N.BE..B.p.].)q..\..y<.np..L.B.....^....]..3R.~..@.T.?.....0.....`3.....4-Y.zMSu..E.. ...[U.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\192.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1629
Entropy (8bit):	7.8810524179433505
Encrypted:	false
SSDEEP:	24:UTrQyjqYsHIoujiJnAfCLmS6jMXRzXEIYqh8Oi2pbrzf7RyVxloQ267XWfNWKCZ4:W+nHDtmqlBLdOTHzdm7hJKEXsD
MD5:	895F05F6274C8D747CE2A1E6F090B0DC
SHA1:	C06B51C3D3FD61AD6E8EEAD96BB5D6F2CD54D955
SHA-256:	EA4DFAFDCED9ED2D1954089A43D70ED21621DCD53AB4D503B567853AAA5F7969
SHA-512:	EBEB199F550D50496A632DB6CD0F5DCAE0DF11D4E90125736CC9EAD999799F1BEE5370A15DE95D38C7359720799B9B0964B6E6D66779FBC2EE823D0B0A1842 0
Malicious:	false
Preview:	.PNG.u.F.-%....Q.s...(..fq=.2v....Y3..7.....V..s.A....a,....'.i.C.>e<.....0-..'>.V..r..j.....N.<.@-&G..0..GV.W...K.....b.....sZ..T...rO.q1M..u.Sk..<....jpD.3..5.o.y..[.H...Wdl..9s..W.. ..o.....z...I..X..u.Do. B.....;ZK&.....!>....7S.Y0.B~...m\.}.B.....h..h_..|..E.....p..D....7....pi..*0K@.1.n.7...p.....;.....<:.lu..@..}.1.....].....a.cA.@tsM..,d.....vb.4.... ..K..Z[%...m.6:..!g;dD...9...Q`.a'....|'i..7V.E.T.6wD..pY.....u|...>....1..Q....Rao.|.X.+.W}.....I.. ..|:.p.....B.....,..O...N.E.R.^h.P.c\..0.&t.....N..z.....Z&.f....v..1.....).[..T@ ..\.ci.yx...4.....9..#.X....#t-4..rO...r.P.@.M..p.M./2~/.-.4%.W.,PL....<S.!>.<.9U..h...^.=.T3..{. .i..b.sH....q.AY>.<,Q..m.....)0Ur.y..#. .g .H.~6.+T.@%$.....f.....?U.^."T....x.*..... .$S.-...)9.a7...K@.....5.....sd...$.;....k...!m.s.i1~D..a..6...O..}.qU8n...q....2..^.v.....]...t.....'PP.B..)z.h4s...v.....X.6.`..u.....Y....M

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\256.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	5525
Entropy (8bit):	7.964038854719876
Encrypted:	false
SSDEEP:	96:Ql//uFUHLwX4NsYqbfhPhlBBTymXsPnCob5z279jyyQlPtx1+AFek0fvoY78A9:Ql/MwiuqDh5gMs/CobRA9jyyQltz+zfV
MD5:	CF8471670A85CEAA1EFCECB31DE41D0E
SHA1:	A30959D5F6F0BBE0B04F8DF3859F1BEA595B3976
SHA-256:	71DEF8A1064DB9694B64DF4A3F376CD6CEEC08C9B556343FE4475E8A5BAAE310
SHA-512:	7BA1E02C352E8C9FC6A91DCB1A32EB5A728FA5AA5D394FB1895CD9396C0058412FA60558E08E512CAB5A6C65086337FA8BFBCDC2B55536E5794B23BD4FE770 15
Malicious:	false
Preview:	.PNG....'...v=..$.....^..=.i.....~.VQ7.....rx...-\....G.5.....=..v.e...|.`...Bo9..H..u.....R@@r.]>.....:\.,.....V.....W.c..N....7Q..^&.....C...b'/,....t...v...:r...B.r...\....>.....C:.S.. .KW.B..._.....M+.t.../.4%.....8h.7.V#;r.i...s.....N.DA.....WE..m.XPR1.Z9"...8...i.A....t..@..+.}....Z>....XB.#SnJ..p.W..t..q..!..b3}Oe.....g.{-...,..fqi.6..]n.+eiyj.2.....$L{>xlw\....v ~k..$....x.S.....l"...|...x+w.....2...[..)..Fs...2.....q.w.....?.+..3....<T&!K.a....W.xu..._s.D...2...P#.@...8.Ki.....:*..)..j.&.6....H.....w.....d.r,v.0.f.d.E.s..?_W.....>3...U.?.`..m..8. gt<.....p..w..c..(..#..`.....T...N.6.`6...r..$11..B.. f...`...L.U.o.;..7r~.C<.V..).....eb\QN....D.HG..z.....h.[.B.v..,s...$.....^.t.....=.+.....w.!.cZ.G.uj.i.;*a..!/.$.b..0..).t.4%{.... (|)..\._.D.#s.i6&.....Q..... I..%.8.GEY..u0.n..A....jC....."..8..$jG-..b...Qh6..n..4#.3.9.a..'.>.._.C.....a(_.Z>#.C...y.<._:.^.`{...Y...1. ...G..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\32.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1359
Entropy (8bit):	7.8470436207124825
Encrypted:	false
SSDEEP:	24:34jg4ya3uZ4SoRMdBPxF66JuUI1r9fxuky1sr61R6HfvRPV/3kic/bD:oGpd46ny9ZE13vyf8iAD
MD5:	F6C2C81B701113F1097E321E53DB4B5D
SHA1:	1BC7FF4B8C96DB62538990028310A71F25FD39AB

SHA-256:	89E26944E9427F10E049385C5FB9EFC56EAFE46E076479AE2DACCEB047199D69
SHA-512:	CD157D489D3C4B500453DF713011730C0130A111CC70CFB902176A46590F33EC7A7C5461B4BD3A422A62148D22403E0DC81CA5315DB10406B28B17EC73D9141
Malicious:	false
Preview:	.PNG.(.....T9/c.`.,Ih@.... A.Wj....gV.k.....|1.Q}../.>p9\.n?1..x..Z..D...=...U.9}f...d.E\...@4d...(..i..7.*1...!...u.....!j.XTG..8.b.nXh&.IjX}'...B7C.R...K.... Q.N.$./V...Z.`..^b\C.=.k .....3TK_..a..J..s.L..\|...M.A.4.. WA.....,..m.^...A...Gj..i..uB..t.'.i.Our2...9.4..3.....d.=v.h...Fc...Jl..0'..S.,B..>...c..`..B.]..MNr\|...Z...Z....].^#ub...D..T..`.....\.^,.[.*".K2`ey8... ..M*..z..jg...r.x].....#.1.....7f.D.....s...C..&A...\3..b.[.px&&q.X.T...h;z.}G1..}T.....HM.f.#.@. .....U;o".....u..0.U.}.oF...q.....1'd...\o....,...$ !4JK...*..??.S.d..n..v.M..$..*.o?....kO..b ...[.P'...2..).sc8...8C#]..jD.`...K...t..=.8:....9.PK..]..:_..I...Z....0.....aO..-.B..i.K...D....8...!.....=.i....xk....2.[.....?E..&.D3VZ..C..h..m.{.u....=..j-...DWx:....=..|a..;dg*Xn"c.`.r.qh.L{- .!Mf.f!...;>3....Q .e.y\k.7..1....A...4.....q.....w*.-.....Z.:.e....>.#l.....I..U..v3...!...MJ...i....`F,.`.V.HU...].r....8.f.=.../.._P_.....I.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\48.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1703
Entropy (8bit):	7.871106632070574
Encrypted:	false
SSDEEP:	24:NJszrPPHWBkW8GPzvt+KA/t7+i1hHunwiMC27KMz32TjDbCHpLIgBHSEK8zPYfSl:9k7GPZ+KY7X1hqeC2WMij3KLnS0wSdD
MD5:	C59825685457BAF192B83432BD3F3827
SHA1:	DEFD4F3E8C73E2AB23D32C7CF45C8AF748665B00
SHA-256:	075D4DAB7BD727F16AEB40E7167373C9C686A5ECF82642D7F56AC5B056AF2573
SHA-512:	CDCAB46305E62F0754D740A7A824C56D384843BAA1CB205076FBE72A5F199641A3666A62C8DEFC6A23F7D9331998BED12548A63DF33E08AD70BA25BACB1D09A
Malicious:	false
Preview:	.PNG..{.s.gh5.#e.\..x.]...f9i;...`C#...F..-J..Cc.....R......5\`~%.$N..y.L.-T....d.....!.....E..]. ...P..;e.I._..&_.E^..\|h...s...\|.b..5.t<.P.....Zur...PP..."....Q...A.b.q..../D...lt..F...E$!..$+.. (P8..l`.)$k.I_.X.)Ow.\.....Wx..`f...\W...kB+.5.!>./..2.(...g/...R.....:`....<.f...p.Qf....h.'x...[.D...U.~zzf.4...&...>.....|O87...'-R_.m.L..."..d.D...2<.%..u+cF.....8t..]x.....N.a.$...2...z.. ..4.....N...~..../...rg.B.f..m.iz....DZH.5.....`....6....._:s.> C...../UY.[/x-4....,y..h..#.....V..O../v.V..`...`%..J\.....*.X.h.T.@M.....`.*.F...np.a.....1....pn...m.>...(r:)....'...J.c.sGY.P..M.. [y. `*.....kp.....$.....`.v..n.(.v../y..E..1..RI...u.] .....+.O.....d..T..F.*f.O!x.#.|.g..@NM.0r.-..y....c=...C.....P..D...<^....t'l,.=.)..a,...+.2v..d.]..m..KZ_.....P.N...gyN.K.U.s.U..... .....o`.-...V....5.fv?....?._...a..j\."7.B...':....#.@..5_..)1.b.7.j.w..]7.-.n..f...g...j...?vG..-.b..+...E....0c-....n..F.b?W...ptJcj.eP.....=.h.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\64.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1848
Entropy (8bit):	7.881089842830607
Encrypted:	false
SSDEEP:	48:8KWxQRf+mUI5lE4uNsVxBoOODnTMzMrYigb4xID:8AX37b9V/oXnvKb4u
MD5:	26CD041711BDF929BBF18DA2FA7F4695
SHA1:	440F7D4EEEB257C44CE8037CEF2521F1F98E61FF
SHA-256:	061FF6624594410DDC63E874A972F7DA37EA153B17A2555D9A813961781E0C3F
SHA-512:	F6C9C67DF8AE96FB49063335579DA6E8DDD3E10BE06F859C15D346EA249B623C46D4A2CB9665A609309D6291D34AE5883FE0416C72288186EFDA9C36F2E3DB5A
Malicious:	false
Preview:	.PNG..h4...K..M$.G...[G.\|....F...a..WLr....gh....~.-.....2.i%..k.H.P.....IX/.t.?...WAx..N.E...&jZ'...EPQ....o.H..S.v....M..gd...B..]......f.....s...dP+.....?...<.q]2.+..X..P.1xi..*6.Z_. .\#.\pq@D.(..d..K.q...IS.g(..d.0...K.s....!4a.Y..8.4@...2o/..(..:{.@..$.U..%..U2 ...-.*...;.4..r.~..M(.-_.K."F.Y.....%....I.<..=B..@:.uq7..aqC..Sy(.2u[kj$Fi.B,....e.....U.R...~.....0..#... ....#.]..9.Wt...k. .c.~.....T.....).W...x'...U.....BE.m.A)=.....;y..U...h_.:e...V.j...X.).....JH1\|.i.i...G...V.V..:X$.9.^.g.b`.....EV.{$,.f.G.Q#$BJr.|m]H...i.TT.o...../.R..R..T..O.....5....=...?-.. ...".N.S4.n...f...5..DS.....=.~.f._.^~,oTF..L[!P/.`l......b0....H.).{Rq0^....I."...1.....+N./ ..KE.2..."..@eU. ,.....Z.E...R.&..m.#...+..a.....@../sG.<.(.....Y.$.....]....=l...l..Pe.i....(.k.. ..R'.X.>Ll$.). .....P..p.....aW.N....S.rIt...7.1B.~#..).4..G.L`.I..2.'i....w.P. q..A?...*`A.F...b6.*.....{.H.....I."..u2..h.][.n.....d.2{..2...H.,...Z..c.$|{o].

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fhihpiojkbmbpdjeoajapmgkhlnakfjf\Icons\96.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	2181
Entropy (8bit):	7.912922003197393
Encrypted:	false
SSDEEP:	48:OBSsJhKADsIPrD95C1GXg3akOpbCD3D22TD:Ovo0C1Xa2D3Dn
MD5:	6E345210FC2D34B97F06FC9DB777695F
SHA1:	4D2F770C6539DAD0A55EE681C7596FD92C6ACF4F

SHA-256:	E58880706CD80706535EF7E1E0240A8027BD7F89E444C7B0963150DD1EB367E6
SHA-512:	453AB1B6BE975D75CA6844DFED54D75BF68C7C179E9816BBEC935E7D18D1CAB730966CCB16C63E88E7214820DFCD707AC3AED54DB90C45E7C0F05CC70922A6BE
Malicious:	false
Preview:	.PNG..g1. .o.....].OL..)....0.D...,..~.&..E..%...s)"<.....'...K.].C.?f..a.....v...B.2N.nh.({.....LN^{..fQ...].+|M.....M...WK.q1./x.h..ZY.K7.....8..`.. ..&.Q.$..^X.s..^W2..J.i.?G...ftVz.. .@...U.>..e...r.U~.i.kq.0.0.,E.+0..G...zc..!..e.4..7...Ez..f.....21&..B..x...nH>.-..Nw6.)..}iT....:.=.\. .R..?.\|...j.6;Y.K;A..F.S.!@`.%@M.e.w...'....fe..uT,T..{x\|..k.}.e .4.f..f+.} ....O.....w.S....)..`....,7R6.... ..:v#`X.S..J?X@Z...+]..t>".,Hl..A..-c..Rj.."....?.].cR!...L...7.&.....GhJ..Z.$y.'.....4",..v.....`..Q.z.T2.....vl..l.H...w..'.....K..M.q..E.$...2E....% .4q.i.H..,.YI...w..n.{6.Z..K./.-....h.yl.....5...#*.}.....}.|.Nj.N3.w..3...L.g..\!#.@...;x...Me..y)..6..cs....qP..h...P...@..iD.;..aO....1(}...c/6.o:.....n....ue.....C...*..V?....c..* ..b.E..ae11.>.....T(-...|...Fq...'g.g.d]!z{.6.f..;....y.5"...MN..t..6.X...u...\..Q.6<.....z.`.rw.....Z;9..:l.....@.4N..A....[.....k~..M...N.....Q&(...ux..7O....a...~<.*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\128.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	5710
Entropy (8bit):	7.965591297004057
Encrypted:	false
SSDEEP:	96:UzTyqHomlHl+9iC0YSHciIt3b7CTdAkJRpRHqf60xTRb4KA9qpELguwICx:UvBs9Ltz3b7sCkJJHqxTR0KSVLY
MD5:	E1426FCB7CAD78606D359D9B8269B580
SHA1:	2B4CB315540E14A5C001ACF06F8782380C8830C9
SHA-256:	0FBDB9F0BD2B72FE9F808D2AE56D95C865B5370BB78A2DBAEEC57A73CB54E92B
SHA-512:	A5D3FA5FD3890CD689C2C11DA625E8D0A1763F7154DC0F30B9065A71CDB89088C2038C1E617A3DB36AFDB61031AB30465D72A8B83B234B4B6082C36ED26F6D2
Malicious:	false
Preview:	.PNG.;..x..W3....(.....c;. ...M.L.u...M.*.'.....c..!./{...vR..M!..B..'..4..`...ZkSkh.cF.....dA..n=.....t.....!.4..EqY'.^y.....F.....].`....!..B.f..4f.W^r.....Y~.`."..&...Z...+v....^..G ....2 ....Jy.}..a..."..Q&h.~...%..!.....F..$..j.....5lZ]=[r@.....'..@5..@....4v.}. ,..?..Q...I....j.s.L..u....+)^.....D.V .s....?z:.`D..\g..'.%F...P.;.....u.f..g .....[..?.nD2.?.....{..Se..Mmv.u...-.T. .....?..$.y'.....E]q.c.e_v.[4.i..X.fz.....=.V..#^.Gn....j...QA..x..H'Yq..f..efom.e.....F.OT...Y"<v.....$..3R...l}....:m4yp..}..=-.....V.'.u..#.ou.. >.(....;W..Y..?..ZA.<....`..L.}...=.. .F.o..RT.....~.....}....>2..XJ0..:.^.1....%..B.OU...Y~.....w.6WOK...KW.:..^..7ED.....y1_.....T.....I..XP...6o.).....Yfk:.#P....5`c.|."...2.Q.I.\LD...-...q{K-.q...x...m"|..\..X.....(.(ij.....(... ....I.H..j..s.HSg.=.)T.."m..k..aGi....h....b.....66.R~...RE%b]..Y.U.G...3n5..O.../H...K.....O.4.Qy1.*8`m...VQ...5E...0. .p.o.W.).....R.*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\192.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	3253
Entropy (8bit):	7.940311078925311
Encrypted:	false
SSDEEP:	96:PHCAO1WGsP+l35p3X5mIF8MI61mh8nqmWHbH6lQagZ:/CAO1KU5mIiMdWjagZ
MD5:	1923661F5B1A73C6E89D0837CF3EB028
SHA1:	255FC273BB1308D65F18B416FA3A59342D605170
SHA-256:	E024E96CA2D4F34B799BA46BC53C73D8BF4F4C032476559C25ED14FC765BA096
SHA-512:	FA6AF046B2D62177074C216544B6701BAA721C7E39A651116ABD0E088E2CEABCFF09D3270C86EFB31FB18BCDFE4376B7E224DB94D7F899A2993397E51155336D
Malicious:	false
Preview:	.PNG.....V.....(..o...{...$...v.....v.].8p]iHm..F.{...i....(.Z}....."..&7M..Y....e.'.+.j.iB..9.C..TXjKT&.7.<.YS...}a8..y*.../..++...p..R..0.. ...}..S..T..C&..-.G3..R...t.6.....D.<.....I.o!..X .6..I..u3_'.....8....u.KLO..-..:.H..Pc$.h.....(Z....drm..y...L..0Q..qF..i[..S...&9..s..'@..^u..P;...EM...@..$#]&d.....3.8..F..Y..N.`.hTz.tm..Q.[.....N.a..=...,..+3.j.}.2..u\|.K.....Y...B)a.T.I.&.k.W..GJ...8V...*.?.n.....#.U..+...r..W...4.Tt.O.Ks5o.e..K...^..Ch..?_e..s.U"../.....T/W?..!.)..S...p5..0..ma.....<.6.:....0..M\|.F.t,N..}....-Bz/..1s.X....$...D.q..+.*.|Q...L. , .K...].G.{....5..c9....=...P.C..E.o.a....@.f..k....5...E.....a0.+}...E...;?..P.....]YB.N.<mh..@.....`7....t..lQ0.k7..R.....lv.t.q+]Y.nAT.....{u..r....6...,.....j.`f...J...T*.S..:....#5ik/K....l.... .D.8kL.\;g..9..-..DR\3:.[.....{|.m..I.q....D.+.-'.j/mQ....H..7"w.....V=2..0.Q.i....A.".oA...k..[.u5...g....f.._.....0..../.Oo.r.@.....]S}.6..j~.....8...eU.z..)j

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\256.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	12565
Entropy (8bit):	7.98577116595789
Encrypted:	false
SSDEEP:	192:tnaT8L7F+ZqehTslgzLm/FKEqfEzaTq2gWiCuoStvMCxQo9j8PDQIGovmzu0kCxi:8TFsV4JqaTqbpCuNECLEMev0KCUaSl/7
MD5:	DE208AFF6F5CFF3510A414EC7862ED8D

SHA1:	FBFE9188009EDF556DF5531B5A5EB4882B3FD038
SHA-256:	BEF9B1BB0ADC79F4A388536C577EE2FE9076FCCCB6134FF1D270C2BD0E998EE0
SHA-512:	6728CEA5F10DFB0E9FFBB1D252517101161 77E5CC3696452B86EBC67CD4BE613E01940C1342ACD36AD4AFC7FA41AE953D4B42255846A200CD98B5697C641C0F
Malicious:	false
Preview:	.PNG.....<.<.D >.....,....g.0.n.p.<E/.{.3...,.F..XD.....*..B.d....}.*D.v...2JT..ZU..27.,}[...W...w.....Y.....h.....:.2.....N...q#W..I"..G.~.S?@.....p.zp1"..!(a..`..p.eE\uZJ.....T?!.,I.. ..GV9Sa.9F(S..(.>....q..1...c.....xkA....w.....9..r7L|y.~.F....Bgt._.M..cL...5M.....gK2G.....,I%!..\..r...r.5nq..#;x?.p9..d.8.1A.C....".....~..&...u.....]..... c.8..Lq.Si.....> w.djGt};T.<.A.'I..L....n.,Q.....r..Ed:n@. ..c....5...]./..j.S..r..a_Ro...`.vg...[F....-.>...jU.Q....2.9....-n+=.?a...L.3.WL.?!..Pq...7...l.t._....D.....b.e[.)..._../..[.B..H.n..2....8.. .Nb.S`..T\.W.a5*[{.wt....V.E.~.J. .C....\....y{..W.,e\.....5.D...vL..ul..a..='9..Q.....<....*.....$s.O`..G..zL...`..>.....8...T:O.W.uI.I{..O/O.=/[.<...(NkE..VX.U/o.d.H.J...\B.`IV..H... .]..@.z..s..A.6IJ.....}.D....#.... .....^._.n[]n...M.N.(..8...F2.....Yt\|....C..Fx....e6.v..5$...p%.S...^..x.CwamE.....R..K.c...*f..^0.^....vKT(..dk..3...7.2..n..S.....L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjjmmmlfnkbppncabfkddbjimcfncm\Icons\32.png

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	modified
Size (bytes):	1892
Entropy (8bit):	7.899129168187769
Encrypted:	false
SSDEEP:	24:HQDBQOL4wjo78FLBJ9qb/qWK1zXF+pwdP2myKC/M9CDD9C6wbLm+7EDbDV/gkbD:HQDBD48vJeSWuLw4y7DM6SLhERguD
MD5:	C949FF5D28256F640D6B8A1CE55E7682
SHA1:	197D72C48FC584C65FFFD2D1DA83D42284C91920
SHA-256:	69A2E91E1F25251D058AC3653B102C2BD98F438A8CBDD974E6E154A62C5C09E5
SHA-512:	7307EEC444F718E6F2404770AB7D18B722758AC9A9A3ED1FD05D998586F3644BB78C647FDCCE121BEF96CC3573289160B326C68252581DCE1EBA6394A2404A6
Malicious:	false
Preview:	.PNG....x.{.+..%..W.9..0:.*h./.'.....r"..._....U+X4t.....7..Ed^.1..im.....Aa...k2....A.].5t.q.xLa..Z'..&.tx.s...H;..Wh.....-../.8`>.:QBT.....aXG.....fgm..$..`..h^F.^H.@.#.8Z..k.0 X....j.{.o../....C/....D...A.....4...L.....Cx...,_..}..}..H~.f;.|[/+.];....J0)9..[..P...=.u.'E..oh....;.n^.].2.`.i.r2v.....(..b..../..c.`..^..T.e...- M..;".VX.U`#>O...*x3... .....H...].R../k.1....K...Mu %.Q.K..z.....&.2.....|,.N...I.....M.*.Dh.mS.Q*B]Dg..v^.8.:..L..]D...r..3.uA^.\...mX..j..F}T..._.....mU....cU....`|%..x.I1.`.....+d;..R_..]".b.R2N6W....6NNW.G...S}q.}.....y=..%)A:.6.- b~aC%t.....2...b..:S.N6.o.....b-.dL.r.G.z@e.hj..;..N.?...%o....(=....&-.....k.....2.-..Z..h..g.&.I._.+e.).-?Hyv.....t3.;-R...s.&M.6~...'".&;..NmC.....g.Vo.{s..;,..H.J..2..s2.w9'.'}.a .Tg.g.+..G....r8(<NA..N....1J...(.<U....!k.>.z;..={..K..C..t.HvX%IK.`...r...|.0.....d9.0.4.c/....p../....v.S..9..Hq./."....Ycq\.!.^.f....d@._..O.}}..L1.g.....P.fm.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	29006
Entropy (8bit):	**7.991880391735602**
Encrypted:	**true**
SSDEEP:	768:qqdVVFhH8RewqoC2rn+xgB0YUhM7U4WYQ5G:5QRQ2630WFG
MD5:	748B6BDC6485525FB0CF69600F6D7F78
SHA1:	3824D24C2CB20786E9C488191208B4FC397907A6
SHA-256:	43638BEFA8B0B05D089F7A8FDE78F3CB68E4F627F2BAD87380E45A16525D9CEF
SHA-512:	4444BD5178F5471B40EA91BCE473C796122E556EB735A706A094E4F538DF09EFF1CE1BA92C60DA6F1E704D73B93C16689B4065D6F039A5706B0F616F391D5183
Malicious:	**true**
Preview:	SQLit&.....'...|..P..O..SA..... w../.,-.3a...Q.,0y{....OG..H.*1..$d...P.1....F.H;#.dB.,b>.E.%.(.#LG.)|..j.x=8.rG>&..hU....G..Y.Z.&.g.9_..&W...r.m..F.Sk..>x.....Sg.R.i..YL..iNX ...O..X..c..-..y@)Vu.....x.....k.%...?Zl\.!.....}.>..T....f\..Y@@.....I..@}.}.^..QbX....V8@).!zN.2...|RS.pn..~y.al.aJ.P/.....'+.-.....x..L.....:...n.Tt../...)=e7..N..{.>.lqg.)P!.....Ql...l. ..&^... Ru..#."..].`..\.:/"<40w.....b.;.,..w.....`K\5...r~1.....=d...c..0.'.6.L.V.v.....J..)n.....5T.../EF.a{.d[uE.v...4s.7.-x.K64.n./...y'=v,...6#">...e.....K.]..... ..%7..w.....r.lj J,.7!..._.b`L.{.+...s.%..O.{Q...y"....f.fZ..@.z...n..rRr..gTW<.P.....| |.t...5..p.e}<.4.:q....-.....e....8=.e.2...../5...MV.e..\..oO..X.<.E..2.^l...*...V1].W...w.....Q.r.s....X.....x.Jx...5{.3..1n.. .....c9.>\.>..`.tC...Z.C,4n{N..W.no...L...K.]M.B..b.9..1.....q]&....5i.%+Q..j.....Qo.....<.o,..l.....ua+XB....>.tx.v...a.V."P*.....}..:.GN...L.4=...HG... +v].z|...7w.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\heavy_ad_intervention_opt_out.db

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	16718
Entropy (8bit):	7.988537338661867
Encrypted:	false
SSDEEP:	384:PCSB8OI5cCk4j2atfBM4RbWGISQX1DXEIHPcRY68hhlyqFj7S9:PjbIFk94JM4RbcvX1DXExcpoDlFj70
MD5:	FF28AB9157240A6D13A91D0CF9D44792
SHA1:	CDE40184515C3EF577C2C146E016E0CF8F3BDF3B
SHA-256:	DEC9B6611067CBE43BB7111973DE6B4BCA32C6F786785EE60DFD1B99C2F0B534
SHA-512:	8A28364D1819BB0F17E4F14B4917DCC274C2E2DEC0B99E1A224E36A3E438728125B24FACCDEF82E1EE1B21E42BA30502EBFA4ACA3C7615C64A8DDFB6C8E99D0F

Malicious:	false
Preview:	SQLit/N.....<+.{P.D>...EB.K..U...rY.dv>... ..2...8..<...61{e..h*.....L..>U...y....I.....`>....E...0}.V^.nEYy..x.....4J....+.7....H..z8.....'..N.X.g...+u..F.....I..$.7.H.(M;..e..D.s.....7.=.....x...%..6.fQ...%{.kT.9.6<.D.5..>k.s4.*'.B.@..N..[.."d....~....\>0..B.W.....5.zf...}...."*..^.5q.x?r..A.J.....z..b.#...UePjHu...N.d...d.....|..L.}(..9...|....x....Y@.P]....@..3...Z5Z.'&<.>'".<.....O.2.v8.l."^..v"...;.....,..6..|...+z....3.>..{9b...L`7.5M.e.S.....m.g...../Q.4..'VM_.....y.-Jp..)^.{.{...C=.uf{.=.Md.WF.O....|6{`I..^..h.0.~aH.IB..?..M.h..H....\xLK.?X9.a.g..@O...j ..L.....O.0...@..9&..'..K.I....=f...?F..o..+,m0..4.....;.I.....H.d..\.....w(....Nn....(.....>.....p.iFZM....#.RAi.2.S'...]......4.x<.&.s'.s.....8W.'...|.].+P.LQ..G...~..18...DBG..H..X'.M....X.i l.4.0x...:.TZI).....3.!MVUO... .-...I..?.j..z5.U...;...`.....J...(.<...6.....].t%.....:..C.0.@.,vR.:{+.<<.6.+....Wx.C.H..:.wG..RS..../.2m.B...Dy9.74]...J..2....[G...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\previews_opt_out.db

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	16718
Entropy (8bit):	7.988298566665822
Encrypted:	false
SSDEEP:	384:ywhA+fttrQ99vnyrFj9UyUNTDrda/RIvyljhdhcd:yWjfttrunkqR1IQ6hu
MD5:	A45C3F65662C028B528036AC28018945
SHA1:	38EB93C44ECB77B41BED640BE81C3D03CA89607D
SHA-256:	091B328625B8CC28991F0045A85AEA67D5E76548DAFC0492B15FB83B64FA7915
SHA-512:	03B28486A159FAA25D12A2EF9F099582BE4426B8DCA8C96C24EAD56183B1A76BB922C86FC3D4BF15A4C71DB17EF310CDF370206A9292DFD7142603FE46988E9C
Malicious:	false
Preview:	SQLit[j..x3}...d....^...$).=j}N.Bq%X...\| .A4.....}.....&S...\|.....t..{%&=..q...e...-7..rZ.....7A...-.n....!..f...b..z.....Q...m....w.....i...ucy.Q....S.n>...'BZw....Hvr.$.Q..s.....Sl&e.a..& v?....*-.]:.&_.b....+.b.7C.....k...J.[....G",;!.CI..o..q .D...6$.S..O..]..*r.....p8...V@Ia...s.!K.Y.dP.R....%].S._KH"`.)..0.Xr...Hg.+.\|...<.9.5...].D.....re..A..v...,.c...!.f...C.n.....=.U.8.4ci ..}a...c.!B.a...9)[+@y.3n.<.-#&W.z..d..Xaf;U.r..{.2.....$..E..5N.....~g...x.....:,.....8...83.UX..3%]C.....);.%dR..8.eWhH.."....E.o.....a...}.y.'.I....c..$.....I&..[..*j..%..T.."..*.V. ..A.. p...rj5..O.I.....W..=.6[.#t.....u.c.r;.. .Q.)..b.U.....0.I.>.....#L..{$(.....k#..~O....dN. ...p.b....cc.J.....t....&.e..'"Ep.../.s{..1...<Y.. .j...T.I...-..g...`..R.....TG.D..(.1..m.r.x..Bqy3...[.[.* (..@.....iE....._P{.\....-..}...b....N+X.....z..w....=.:k.m..O...../#...g..m.....0.....L;.9)s.w.....'.1..A..<....1zkwB...@... &.o`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1066
Entropy (8bit):	7.807638670941954
Encrypted:	false
SSDEEP:	24:lOiESxmQwYSC7t0wZizVM55JskEfsXsUbD:l1xm9Y1ZiCHJsdOpD
MD5:	F581A0EB2AAB13EF0BA5F9CB9F84214A
SHA1:	167EE7953A0AE12DFDB413AD510309C5E3190EC5
SHA-256:	EF6D539BDAA2E04C3F97D0D70864860A2D41ED27BB8BC8EA4480162FD12F9610
SHA-512:	11A60F308F2E801E3C130191BD49C97F6C98F031F463A36BD076A1E033B97D7A7A97E41D3EE517C7AC1504F4FD1D0EF7A543715FADBE657B903D28D400A7FD10
Malicious:	false
Preview:	A..r....$.;.f...[.L....DEB.G.D..x..t..r..N.+K..N.....J...V*...C.....2.;HB..yu.K.1O..u.0g,..~..~.6~.cH>.X..U..$.%..dS7...2.I...i.K..Z#%0./.."0..A.A...|....p..%.h...b...kJW..I.(..<..x,A.04.a. ...Fg..vc.$.....a.J"><2..o.._..R..s.... p...?g..Qa.._.....\|.U..h5h./....>.J.y.Z.~.p..Y.....n.-P.S@.U 4.<?.....>.<T.kJ..w-..j...O.@....."...d.<.e%.....k.GG.._.....W.J..../2Or.U..... ,.IX.f.....J.N{.;..0g...e..$....D..0.;.bn%woW.....G..v.R.....C.n..x._..[....a..[.8._2..h.....g'..a..w..c....V...>..}.x+^...5X..[.....^^.....,*.I.....(I..*U...xZR...p..C.....{..D&.6%1....u ca..&i...4.d.I..p../Z..'W.s.{=.....V..,.^..S./..y.qM.|..%{}.....Ph.4`X.]>n..../>..~..[.\r.&'.....)..z.%7...`S....i.z..{...z...V....#...L.f.r...=...57.....V....]..-..R0..A...C...!}.Yc..>.q|.N...)HL.._.< .vP.....3&..G9.U..PZUC..T.6.....W^...]YF=,{...]E.)i.I.x..C.Q]c.m..a.....'.....I.....*.^.....hn}."...#.\..Y..Q.7t.6'Z...p;Q....|...K..b.g.....]....E.....;K6te1YGPnIbo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000003.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	1061
Entropy (8bit):	7.7843666279256665
Encrypted:	false
SSDEEP:	24:esIRm/KUhH4RKwIC1//YH95PkfSNCsqDjs7XTubD:etRmieYRZv/aLsfDsowgD
MD5:	DC7CECB780FA46F49F3E3658461D7DF6
SHA1:	95C09F59D78049ED1E4D6B0F06873CE393313D46
SHA-256:	B1633335E2A16B7ED94D5A7F617B6F038E100675882FE87E50C2FB88B1629754
SHA-512:	CCF4C1FA6AD7D83D3ED69623556C1443D89E0AA34FA1D21C93A4339109ABDA2137F2EA2AD3BEC24B4194FD4A863DAC9897842224CF646D78505A64CA4CCCC94
Malicious:	false

Preview:	.DO&.h....qN.B..n.....V+$.0u..D.U..,..&..DX1..v..4.2.....:..v_....(J..[.].h..t...U.z)T l..Ud.X.Q..3.M....f.2]..8y.....R...h:.7$..D...X.....S.....Z...*..O.....;..+3.M.....GSX....N....Tl..f.a..Wml..."....l.]..c....E.....z>...[."...:.:..3)'v..d..~T....w.....-...N....US.....ue.-.z....o.0l...K..eL.....s.h....$P. .e.}.....|W.h+[TY..bs.9dZ.....a._.'.["A.YV...c...S.....;..`.cGv...h+.....6.Y..jk..|F.[..~..@./Q.VY...;...o.O..."..B...:....S_'.4:l.b...;..no..;.v>.P.f.....zJC.:.YZ<...:.<.Vx.H.....p\Pk..)..7...f.7.|.....#"0..)....k.%g...V..U.sV...`.,.7y.....[CZ&.^...tH^ .-.....;{!..d.jV4S+...<..2.3#X ..@.\.T.l...!.....;.!LG..I.97....;.e1".f.P.%)I.....T..#..L5...hpM....q..u...\.MK.n.q...0..[T9..Q>..:\...n..6q.....&....}..#.7..."..H2..;...d=M.7.B..0..n.NVM.x,6.gt.....guO.....1.....i..Z..Q ..1....%c.6Q..%.F....}....>.....~>..6~.@QOF7..E.D..]Mn.@.....].n.....!.Z....T.l..[.3U.N.S..aK6te1YGPnIbo4GcGO

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	483
Entropy (8bit):	7.481380602966872
Encrypted:	false
SSDEEP:	12:o9sitj9dyW0stawMtYcz8nh1ntyQzgVV8STYtcii9a:GsitjzXLawM8nTvgVV8fbD
MD5:	DCCC373C50642EB3CFD515D6FCED268A
SHA1:	70F52AD0EE7190FC464B63D57FFE59A9EC46FBC1
SHA-256:	E273869A30365B3646B6132746D33C10C8803E1DF096426159F1986C5AB4E1FC
SHA-512:	EC403BA6DB351F2FF1F0FBCF56F07DA3ACEA8B69B3B6481BA691CEB019FAD4DA95B8586530C97151680E46C8AAE4183D5CE798F5511837E3F39194D83FD4FC60
Malicious:	false
Preview:	2020/$n\|j.j.....d....bo..80.....<$y]..s....0.3.n..s`..i...&.Nze.5j 8.0..&.jT.q.....'...]3....Y.z.....k.YkWK@!..WJ[....5.....v^.-...t.@..:_IH..r..SY T2.%.!|rW.KvU.v..L.....4.;[..v.[.)..Z.....}:.he..lfi.oE...oFc.x..H~hAr..Y.drx.c..(.G.D.Jw..:;..;L6..3..l..|.....\[.<heJ.....k2.e.Q.....\-.....}:G.v+.4A.....2.Hg..=.RxB...e.,q..U..z.]F....3.Y.'.....o..)s.... ..} .-.Z..{x,K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\IconCache.db

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	18296
Entropy (8bit):	7.988657311597812
Encrypted:	false
SSDEEP:	384:9Qk4Kqfac/W+6cfC0RupGnDCpswxKRtocMppx/Q+n/Ufj:9PxqCjcqquyDqtYRtocMpt8fj
MD5:	1687E79B59F47F0E5786C181DA45FBB7
SHA1:	D8B4BB4F2B9E492E85BD8FC99780F0D4375D8027
SHA-256:	64F8B5DF1B8FAF64E58E10F89823818E338A066D623AB3C15CE126912A61F207
SHA-512:	FE22A926D788128C4D6ED0DF73B6B380E966F2E6E489762A9DBE61F6052577FC0BDDAA42A21F332DE351607B0FC336572F0E7823A88EFB1B657AC505947A95BD
Malicious:	false
Preview:	H...W.,...U..?..G[d)..>1....CC./..I..H.,_.=..O......&p.x.....'1.....mW..*.j...1..#?....W..X7.^.....B|C.#{.+(..b....u.`..~W..!p.S]q...H..y..k...9..I..w$..IF...0.U..Q...1..,.Bn..hS...0.f..!..q.iy...g".rH'.D....rG@5..N..+.-.3...u]...G"....C.eW.%....0D.x2!.\.Z.W.....!j=....zT..2.I^a...../..Ug..G...KrH....v9..J..rr..i.....Ne.':.%.0.....}.Q..{:..j.....Ku.....\h.PO.E....@ep..t.EZ...._.<.n.az:Wsn..K.]8.._N....c<AgY...2.L.m..V..."<.'...O..6#....#...B..;vMa...iE...[.....o@.m..{t....`.3..2.R.O^...S3{>.....Q.s..e...4.3../....H.=..G..{....I..".\...[....?..S.G.K.f.z.o^..e.PX.Dh...._.....E....t...inJA....W<*p....# }...+.].].....i.vq.w`P]M..".o6..W1.l[...*pedR..j..q..G.p.g.h.k.P..V..=8..'.N....@8/.....D.ld.R.n..C.C.1#.?nx..b+...Nz.*...$..n.....hL<.%.W."...N.....q..f..A.[.....:7...o. ...*.....@;.{.....G..K....19p1...Gu.....Wk.&YP.D....n.....8...2M....p..|v.T.s....r._.@y6X..f.....o3.&.....AY.KL.-.f:S].$E.\.

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	7.548926528026075
Encrypted:	false
SSDEEP:	12:QlKPH/PMFrm/ZskGhJkbjW5okNUaEHv0yQWgAldtcii9a:Lsm/ZecZaUgApbD
MD5:	05D38523CAFBEBE6EBB274416DBE166C
SHA1:	F9A81D70F04E2B94CA832775F4707B735F788C29
SHA-256:	32C8CBC6523373ECFE8A17EBF04D8F8FC1C183D8E42D55C1662A5CB61D9DE080
SHA-512:	50685788E076A9BF6CA547C0132161A0941C47B45D8A870878C61916A7A90D7EF6AAD0AE6B923B4359012D1F5A763DC14F988E0C8BE6A9A5DCEA62AAD294B53
Malicious:	false
Preview:	1,"fu ..a:.....=M"l..%./r.M.!(qB.\E..*...-.A\..+6U.....r.*U.b.tN...1....^.%D.V....=Be.....p.0z..S....#.....=b..P/...[.f,".j.N"...O.+.JF...BV.....W!..5".W..P..._Anc...)..J.-..|.....7a.<FL4.....4.s.1R...x&B.d.v#`u!.....^.....*..d..&.l..S.).gi4...Q.8\...A..V...*.?Y.....2c|ns%.O..q.^..".0?k.J..".9.....ESZ.14.nH...b..>40...>.\p.w..S.l..^#.>K.=@.....{%...y.(.f....#.)...i#y.^!;../..b_.>.fMC...d..[..9=.37....L...O$.S.K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log

Process:	C:\Users\user\Desktop\U59WtZz2Sg.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	7.360185954216639
Encrypted:	false
SSDEEP:	6:QujwMI4q7mi8OWyAM2Wrb9kuyBUv8e7KZVeo80Z06vXMICJ8VkDGxntHcii96Z:Qkwrtmi8jmrb9zyBhbH3/h8Io8Btciik
MD5:	D11CA32ADD269F8DF99258B64CAC5BD7
SHA1:	A8B55C036EFFEB52DBB764CA5E936A98A321A241
SHA-256:	0FAC78C28DF0465A2864AA6FA988BF3DF5338C200696B098064D234F8469CC04
SHA-512:	F8C6EC5D21822D7512C2611286235D07EC67FE8A58129E56DCFB161F88D8620F00760620DE383CB6A2392677F4EEBAB12D6FE6285F86F9BE84230031450E6A5A
Malicious:	false
Preview:	1,"fu..`.......).Y...LiC.U|}..O.W....6y.`!...D.!M...n).*t..y=....D$.N.....o.2.#.>O..j...U...[i~.X&.J.Ns.D><.....=0+.....g..`..pr.[.N...:\0f.....t..Cw....;.m+.k.....x....,.....l...F....,..%.c.x.. .@..n..O..Q}...n.c6%..y.A.s5RtS...i(o.Zq..^../:..w..<N~.d<..>.&NK6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.904357034984543
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	U59WtZz2Sg.exe
File size:	680448
MD5:	41001fdd7879ce9ede214e92c7e492be
SHA1:	215964b0399da37b41b7f420806a72feb72a7c28
SHA256:	aaef58ede9edbfc0cbbdd3dc7abfa9ae0f977ed1b33af4f5d7665123187801d1
SHA512:	1d125890b19e323fd3a67b3b2575c97df72f4f8b7f13d5e1d3e010063b88cc40a6f55d25513ada752992434f0b1d350152798381d43cb2ec591020c85eec44d9
SSDEEP:	12288:Q2lMqUe8G9qSkYuZpeKF8GJF6y9NbgGUx0kXZPwtSRGG/t6i5l5kCYlS:Q2K98cT3d9V3U/XZPwYRGQ6i5l5k5l
TLSH:	CEE423217A90D073C887557079228662773F757328FE8C87BF5198E51EB22C67A1A38F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I.....4.I.+...$.I.+...].I..]2.2.I.5.H...I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L.....Ib.....

File Icon

Icon Hash:	d4b4b0e0e0eaf0c0

Static PE Info

General

Entrypoint:	0x404c97
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6249E282 [Sun Apr 3 18:08:02 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5

Subsystem Version Minor:	0
Import Hash:	2ac0f7085258eff31142b9f87cb0f218

Entrypoint Preview
Instruction
call 00007F3200A3565Ch
jmp 00007F3200A2F83Dh
sub eax, 000003A4h
je 00007F3200A2F9E4h
sub eax, 04h
je 00007F3200A2F9D9h
sub eax, 0Dh
je 00007F3200A2F9CEh
dec eax
je 00007F3200A2F9C5h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007F3200A30BCEh
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 004A33A8h
add esp, 0Ch
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl
inc eax
dec edi
jne 00007F3200A2F9B9h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]

Instruction
mov byte ptr [eax], dl
inc eax
dec esi
jne 00007F3200A2F9B9h
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [004A3FB0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [00401170h]
mov edi, 00000100h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a9c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x3050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2cd8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x23c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x107d4	0x10800	False	0.5117039535984849	data	6.09735691865179	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x12000	0xc5c68	0x92400	False	0.9938334668803419	data	7.994721199860208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xd8000	0x3050	0x3200	False	0.629140625	data	5.666597605339273	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
JEBOPOZUSUHARAFA	0xda430	0x55f	ASCII text, with very long lines (1375), with no line terminators	Raeto-Romance	Switzerland
RT_ICON	0xd82b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0xd8978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0xd8ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0xd9f88	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0xdab78	0x2d8	data	Raeto-Romance	Switzerland
RT_STRING	0xdae50	0x1fc	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0xda990	0xa0	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0xda3f0	0x3e	data	Raeto-Romance	Switzerland
RT_VERSION	0xdaa30	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	OpenMutexW, GetConsoleAliasExesLengthA, CopyFileExA, ReadConsoleOutputCharacterW, CompareStringW, SetVolumeLabelA, FillConsoleOutputAttribute, GetConsoleTitleA, QueryDosDeviceW, EnumCalendarInfoExA, GetProcessPriorityBoost, IsProcessInJob, AddConsoleAliasW, CreateFileW, SetMailslotInfo, GetWindowsDirectoryW, GetModuleHandleA, GlobalLock, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerA, GetVersionExA, SearchPathA, MoveFileExW, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, LocalAlloc, GetBinaryTypeA, GetCPInfoExW, WriteConsoleOutputA, GetCommandLineA, EnumDateFormatsW, CancelTimerQueueTimer, GetHandleInformation, FindResourceA, CreateJobObjectA, FindFirstVolumeA, GlobalFlags, CreateNamedPipeW, InterlockedIncrement, CloseHandle, CopyFileW, GetComputerNameExA, GetShortPathNameA, FlushFileBuffers, GetLogicalDriveStringsW, InterlockedCompareExchange, EnumCalendarInfoW, GetConsoleAliasExesLengthW, InterlockedExchange, GetNamedPipeHandleStateW, GetModuleHandleW, GetCurrentActCtx, GenerateConsoleCtrlEvent, MoveFileW, AddAtomA, SetThreadPriority, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointW, VirtualAlloc, _hread, EnumResourceLanguagesW, ClearCommBreak, QueryMemoryResourceNotification, GlobalFindAtomA, HeapWalk, SetFilePointer, GetTickCount, EnumSystemCodePagesW, VerifyVersionInfoA, LoadLibraryW, CreateFileA, GetLastError, WideCharToMultiByte, HeapReAlloc, HeapAlloc, HeapFree, UnhandledExceptionFilter, SetUnhandledExceptionFilter, DeleteFileA, GetStartupInfoA, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, HeapCreate, VirtualFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, GetConsoleCP, GetConsoleMode, RtlUnwind, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, HeapSize, ReadFile
GDI32.dll	GetCharWidthA, GetCharABCWidthsA
WINHTTP.dll	WinHttpSetOption

Possible Origin

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
222.236.49.123192.168.2.580497042036335 11/30/22-00:22:18.131398	TCP	2036335	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download	80	49704	222.236.49.123	192.168.2.5
192.168.2.5222.236.49.12349706802036333 11/30/22-00:22:26.085731	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49706	80	192.168.2.5	222.236.49.123

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8.8514415 32023883 11/30/22-00:22:16.657289	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51441	53	192.168.2.5	8.8.8.8
192.168.2.5222.236.49.12 349706802020826 11/30/22-00:22:26.085731	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49706	80	192.168.2.5	222.236.49.123
192.168.2.5116.121.62.23 749705802020826 11/30/22-00:22:17.137850	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49705	80	192.168.2.5	116.121.62.237
192.168.2.5116.121.62.23 749705802036333 11/30/22-00:22:17.137850	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49705	80	192.168.2.5	116.121.62.237

Network Port Distribution

Total Packets: 54

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:22:09.435889959 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.435945988 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.436464071 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.469263077 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.469322920 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.546952009 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.547126055 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.898497105 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.898566008 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.899504900 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.899597883 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.902540922 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.902566910 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.943552017 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.943653107 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:09.943658113 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:09.943805933 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:10.054886103 CET	49702	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:10.054929018 CET	443	49702	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.200620890 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.200680017 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.200789928 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.245260000 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.245289087 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.312412024 CET	443	49703	162.0.217.254	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:22:16.312542915 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.346792936 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.346860886 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.347371101 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.347579002 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.350308895 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.350330114 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.396068096 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.396161079 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.396238089 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.455621004 CET	49703	443	192.168.2.5	162.0.217.254
Nov 30, 2022 00:22:16.455662966 CET	443	49703	162.0.217.254	192.168.2.5
Nov 30, 2022 00:22:16.704987049 CET	49704	80	192.168.2.5	222.236.49.123
Nov 30, 2022 00:22:16.841957092 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:16.997359991 CET	80	49704	222.236.49.123	192.168.2.5
Nov 30, 2022 00:22:16.997529984 CET	49704	80	192.168.2.5	222.236.49.123
Nov 30, 2022 00:22:17.013473988 CET	49704	80	192.168.2.5	222.236.49.123
Nov 30, 2022 00:22:17.136807919 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:17.137012005 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:17.137850046 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:17.506212950 CET	80	49704	222.236.49.123	192.168.2.5
Nov 30, 2022 00:22:17.635873079 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.131397963 CET	80	49704	222.236.49.123	192.168.2.5
Nov 30, 2022 00:22:18.131433964 CET	80	49704	222.236.49.123	192.168.2.5
Nov 30, 2022 00:22:18.131561995 CET	49704	80	192.168.2.5	222.236.49.123
Nov 30, 2022 00:22:18.131875038 CET	49704	80	192.168.2.5	222.236.49.123
Nov 30, 2022 00:22:18.425659895 CET	80	49704	222.236.49.123	192.168.2.5
Nov 30, 2022 00:22:18.428991079 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.429039001 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.429260015 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:18.725884914 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.725986004 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.726016998 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:18.726057053 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.726106882 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:18.726135015 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:18.726202011 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:18.726202011 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.020948887 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021039009 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021250963 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.021750927 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021878004 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021920919 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021985054 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.021986008 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.022032976 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.022056103 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.022083998 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.022130966 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.022201061 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.316337109 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.316379070 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.316396952 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.316416025 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.316667080 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.316667080 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.316993952 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317049980 CET	80	49705	116.121.62.237	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:22:19.317094088 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317120075 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317167997 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317214966 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317276001 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317364931 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317444086 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317487955 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317508936 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317549944 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317610025 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317665100 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.317768097 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317805052 CET	80	49705	116.121.62.237	192.168.2.5
Nov 30, 2022 00:22:19.317894936 CET	49705	80	192.168.2.5	116.121.62.237
Nov 30, 2022 00:22:19.612457991 CET	80	49705	116.121.62.237	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:22:09.378216028 CET	61893	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:09.401011944 CET	53	61893	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:16.162992954 CET	60649	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:16.184927940 CET	53	60649	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:16.657289028 CET	51441	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:16.671861887 CET	49177	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:16.689538002 CET	53	49177	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:16.839822054 CET	53	51441	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:30.252228975 CET	49724	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:30.271348953 CET	53	49724	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:30.948734999 CET	61452	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:30.970451117 CET	53	61452	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:34.384795904 CET	65323	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:34.407268047 CET	53	65323	8.8.8.8	192.168.2.5
Nov 30, 2022 00:22:41.460248947 CET	51484	53	192.168.2.5	8.8.8.8
Nov 30, 2022 00:22:41.477461100 CET	53	51484	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:22:09.378216028 CET	192.168.2.5	8.8.8.8	0xe9d1	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.162992954 CET	192.168.2.5	8.8.8.8	0xa0fd	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.657289028 CET	192.168.2.5	8.8.8.8	0xf43	Standard query (0)	uaery.top	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.671861887 CET	192.168.2.5	8.8.8.8	0x31ae	Standard query (0)	fresherlights.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:30.252228975 CET	192.168.2.5	8.8.8.8	0xcf1c	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:30.948734999 CET	192.168.2.5	8.8.8.8	0x49a3	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:34.384795904 CET	192.168.2.5	8.8.8.8	0xcd11	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:41.460248947 CET	192.168.2.5	8.8.8.8	0x5cf6	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:22:09.401011944 CET	8.8.8.8	192.168.2.5	0xe9d1	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.184927940 CET	8.8.8.8	192.168.2.5	0xa0fd	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		222.236.49.123	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		46.195.100.42	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		210.182.29.70	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		195.158.3.162	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.689538002 CET	8.8.8.8	192.168.2.5	0x31ae	No error (0)	fresherlights.com		211.119.84.112	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		116.121.62.237	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		175.119.10.231	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		190.117.75.91	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		190.219.54.242	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		181.94.48.228	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		222.236.49.124	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:16.839822054 CET	8.8.8.8	192.168.2.5	0xf43	No error (0)	uaery.top		195.158.3.162	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:30.271348953 CET	8.8.8.8	192.168.2.5	0xcf1c	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:30.970451117 CET	8.8.8.8	192.168.2.5	0x49a3	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:22:34.407268047 CET	8.8.8.8	192.168.2.5	0xcd11	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false

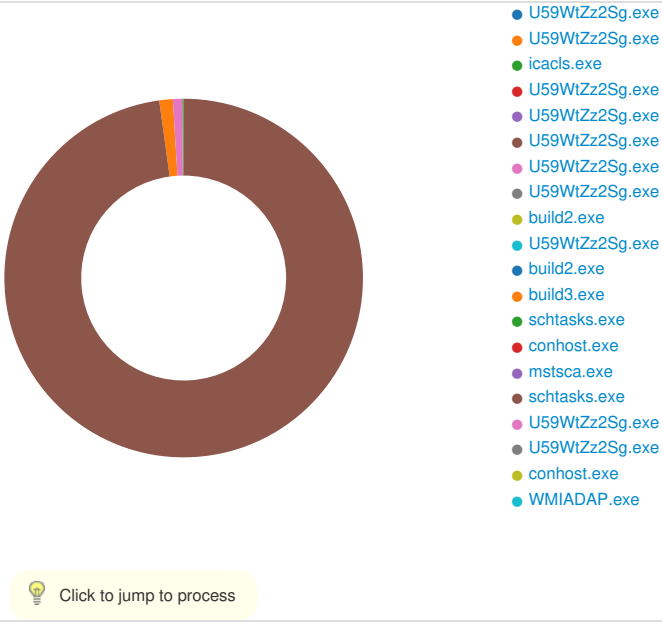
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:22:41.477461100 CET	8.8.8.8	192.168.2.5	0x5cf6	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.2ip.ua
- t.me
- fresherlights.com
- uaery.top
- 88.198.94.71

Statistics

Behavior



System Behavior

Analysis Process: U59WtZz2Sg.exe PID: 5228, Parent PID: 3324

General

Target ID:	0
Start time:	00:22:04
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000000.00000002.305141359.0000000002220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000000.00000002.305141359.0000000002220000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.304747895.000000000218B000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: U59WtZz2Sg.exe PID: **3692**, Parent PID: **5228**

General

Target ID:	1
Start time:	00:22:07
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.303569533.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.303569533.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.303569533.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.303569533.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.302933053.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.302933053.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.302933053.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.302933053.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.301522504.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000002.309064408.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000002.309064408.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000002.309064408.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000002.309064408.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.303182079.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.303182079.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.303182079.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.303182079.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.302301176.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.302301176.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.302301176.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.302301176.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.301786839.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.301786839.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.301786839.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.301786839.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	411F94	CreateDirectoryW
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	412052	CopyFileW
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	412052	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\geo[1].json	0	500	7b 22 69 70 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 39 22 2c 22 63 6f 75 6e 74 72 79 5f 63 6f 64 65 22 3a 22 43 48 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 5f 72 75 73 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 33 38 5c 75 30 34 34 66 22 2c 22 63 6f 75 6e 74 72 79 5f 75 61 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 35 36 5c 75 30 34 34 66 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 75 72 69 63 68 22 2c 22 72 65 67 69 6f 6e 5f 72 75 73 22 3a 22 5c 75 30 34 32 36 5c 75 30 34 34 65 5c 75 30	{"ip":"102.129.143.49","country_code":"CH","country":"Switzerland","country_rus":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0438\u044f","country_ua":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0456\u044f","region":"Zurich","region_rus":"\u0426\u044e\u0	success or wait	1	40CFD3	InternetReadFile
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe	0	262144	4d 5a fd 00 03 2c 04 fd 08 7a 7a 5d fd fd 31 fd 15 38 40 20 fd fd fd fd 02 64 7d 28 7a 13 23 7d 1a 65 fd fd 4e 3f 63 6e fd 73 fd 7e fd 24 fd 59 10 fd fd 3d fd 4b 5f 12 fd fd 2a 4e fd fd fd 49 fd 06 22 78 fd fd 6c fd 38 40 fd 5e 57 fd fd fd 4d fd fd fd 28 fd 57 79 3b 38 fd 06 69 08 fd 4f 0b 68 fd fd 12 7e fd 13 fd 27 19 fd 0e 4f 3d 69 11 fd 3b 76 67 43 fd fd 2e fd 49 6f fd fd 5b 37 fd fd 73 4e fd 4f fd 54 7d fd 42 03 fd 58 fd fd 5f fd fd fd 7c 56 fd fd 41 fd fd fd 0f 28 12 41 fd fd 6c 5d 00 fd 19 fd fd 6f fd fd 53 fd fd fd 73 fd fd 30 6c fd 33 fd 7e fd 4e fd fd 19 fd 62 fd 4d fd fd 1d fd 45 fd 71 fd 6b 08 64 fd 52 95 fd 50 fd fd fd fd fd 05 49 fd f2 0d fd fd 2e fd 28 3f 08 2b 75 40 fd fd fd 01 17 15 fd fd fd fd fd fd 08 21	MZ,zz]18@ d}(z#}eN?cns~$Y=K_*NIxl8@^WM(W;8iOh~'O=i;vgC.Io[7sNOT}BX_|VA(AI]oSs0l3~NbMEqkdRPI.(?+u!	success or wait	3	412052	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	412052	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SysHelper	expand unicode	"C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart	success or wait	1	4120F9	RegSetValueExW

Analysis Process: icacls.exe PID: **1304**, Parent PID: **3692**

General

Target ID:	2
Start time:	00:22:10
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0x1190000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	84			invalid handle	1	1191B0A	WriteFile
unknown	unknown	59			invalid handle	1	1191B0A	WriteFile

Analysis Process: U59WtZz2Sg.exe PID: **1272**, Parent PID: **3692**

General

Target ID:	3
Start time:	00:22:11
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U59WtZz2Sg.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000003.00000002.318350093.00000000020FB000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000003.00000002.318481347.00000000021E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000003.00000002.318481347.00000000021E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: U59WtZz2Sg.exe PID: **3184**, Parent PID: **1084**

General	
Target ID:	4
Start time:	00:22:11
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe --Task
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000004.00000002.362805036.0000000002280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000004.00000002.362805036.0000000002280000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.348844154.000000000210E000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: U59WtZz2Sg.exe PID: **6132**, Parent PID: **1272**

General	
Target ID:	5
Start time:	00:22:12
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\U59WtZz2Sg.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000000.317450025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000000.317450025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000000.317450025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.317450025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000002.564528734.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000002.564528734.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000002.564528734.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000002.564528734.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000000.314511925.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000000.314511925.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000000.314511925.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.314511925.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000000.315044936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000000.315044936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000000.315044936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.315044936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: 00000005.00000003.362157229.0000000003060000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000005.00000003.362157229.0000000003060000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000005.00000003.362157229.0000000003060000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000000.317037787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000000.317037787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000000.317037787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.317037787.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.314284082.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000000.313991274.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41DDE2	CreateDirectoryA
C:\Users\user\AppData\Local\bowsakkdestx.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	43B911	CreateFileW
C:\SystemID	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C951	CreateDirectoryW
C:\SystemID\PersonalID.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	43B911	CreateFileW
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41E28E	CreateFileA
C:_readme.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40F12B	CreateFileW
C:\Users\user_readme.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40F12B	CreateFileW
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41E28E	CreateFileA

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	C:\Users\user\Cookies\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	C:\Users\user\Cookies\deprecated.cookie.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BPMLNOBVSB.jpg	C:\Users\user\Desktop\BPMLNOBVSB.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	C:\Users\user\Desktop\BPMLNOBVSB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\FENIVHOIKN.png	C:\Users\user\Desktop\FENIVHOIKN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\JSDNGYCOWY.mp3	C:\Users\user\Desktop\JSDNGYCOWY.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI.docx	C:\Users\user\Desktop\KZWFNRXYKI.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI.png	C:\Users\user\Desktop\KZWFNRXYKI.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	C:\Users\user\Desktop\KZWFNRXYKI.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ.docx	C:\Users\user\Desktop\LTKMYBSEYZ.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS.png	C:\Users\user\Desktop\NEBFQQYWPS.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	C:\Users\user\Desktop\NWTVCDUMOB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	C:\Users\user\Desktop\QNCYCDFIJJ.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\RAYHIWGKDI.pdf	C:\Users\user\Desktop\RAYHIWGKDI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SFPUSAFIOL.mp3	C:\Users\user\Desktop\SFPUSAFIOL.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\SQRKHNBNYN.png	C:\Users\user\Desktop\SQRKHNBNYN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\UOOJJOZIRH.jpg	C:\Users\user\Desktop\UOOJJOZIRH.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WKXEWIOTXI.jpg	C:\Users\user\Desktop\WKXEWIOTXI.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WKXEWIOTXI.mp3	C:\Users\user\Desktop\WKXEWIOTXI.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WKXEWIOTXI.pdf	C:\Users\user\Desktop\WKXEWIOTXI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX.docx	C:\Users\user\Desktop\WUTJSCBCFX.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX.pdf	C:\Users\user\Desktop\WUTJSCBCFX.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW.docx	C:\Users\user\Desktop\YPSIACHYXW.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW.jpg	C:\Users\user\Desktop\YPSIACHYXW.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	C:\Users\user\Desktop\ZBEDCJPBEY.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	C:\Users\user\Desktop\ZBEDCJPBEY.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BPMLNOBVSB.jpg	C:\Users\user\Documents\BPMLNOBVSB.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\BPMLNOBVSB.xlsx	C:\Users\user\Documents\BPMLNOBVSB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\FENIVHOIKN.png	C:\Users\user\Documents\FENIVHOIKN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\JSDNGYCOWY.mp3	C:\Users\user\Documents\JSDNGYCOWY.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI.docx	C:\Users\user\Documents\KZWFNRXYKI.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI.png	C:\Users\user\Documents\KZWFNRXYKI.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI.xlsx	C:\Users\user\Documents\KZWFNRXYKI.xlsx.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ.docx	C:\Users\user\Documents\LTKMYBSEYZ.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS.png	C:\Users\user\Documents\NEBFQQYWPS.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\NWTVCDUMOB.xlsx	C:\Users\user\Documents\NWTVCDUMOB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\QNCYCDFIJJ.mp3	C:\Users\user\Documents\QNCYCDFIJJ.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\RAYHIWGKDI.pdf	C:\Users\user\Documents\RAYHIWGKDI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SFPUSAFIOL.mp3	C:\Users\user\Documents\SFPUSAFIOL.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\SQRKHNBNYN.png	C:\Users\user\Documents\SQRKHNBNYN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\UOOJJOZIRH.jpg	C:\Users\user\Documents\UOOJJOZIRH.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WKXEWIOTXI.jpg	C:\Users\user\Documents\WKXEWIOTXI.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WKXEWIOTXI.mp3	C:\Users\user\Documents\WKXEWIOTXI.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WKXEWIOTXI.pdf	C:\Users\user\Documents\WKXEWIOTXI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX.docx	C:\Users\user\Documents\WUTJSCBCFX.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX.pdf	C:\Users\user\Documents\WUTJSCBCFX.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW.docx	C:\Users\user\Documents\YPSIACHYXW.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW.jpg	C:\Users\user\Documents\YPSIACHYXW.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\ZBEDCJPBEY.pdf	C:\Users\user\Documents\ZBEDCJPBEY.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	C:\Users\user\Documents\ZBEDCJPBEY.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\BPMLNOBVSB.jpg	C:\Users\user\Downloads\BPMLNOBVSB.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	C:\Users\user\Downloads\BPMLNOBVSB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\FENIVHOIKN.png	C:\Users\user\Downloads\FENIVHOIKN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\JSDNGYCOWY.mp3	C:\Users\user\Downloads\JSDNGYCOWY.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\KZWFNRXYKI.docx	C:\Users\user\Downloads\KZWFNRXYKI.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\KZWFNRXYKI.png	C:\Users\user\Downloads\KZWFNRXYKI.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	C:\Users\user\Downloads\KZWFNRXYKI.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\LTKMYBSEYZ.docx	C:\Users\user\Downloads\LTKMYBSEYZ.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\NEBFQQYWPS.png	C:\Users\user\Downloads\NEBFQQYWPS.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	C:\Users\user\Downloads\NWTVCDUMOB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	C:\Users\user\Downloads\QNCYCDFIJJ.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\RAYHIWGKDI.pdf	C:\Users\user\Downloads\RAYHIWGKDI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\SFPUSAFIOL.mp3	C:\Users\user\Downloads\SFPUSAFIOL.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\SQRKHNBNYN.png	C:\Users\user\Downloads\SQRKHNBNYN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\UOOJJOZIRH.jpg	C:\Users\user\Downloads\UOOJJOZIRH.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\WKXEWIOTXI.jpg	C:\Users\user\Downloads\WKXEWIOTXI.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\WKXEWIOTXI.mp3	C:\Users\user\Downloads\WKXEWIOTXI.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\WKXEWIOTXI.pdf	C:\Users\user\Downloads\WKXEWIOTXI.pdf.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WUTJSCBCFX.docx	C:\Users\user\Downloads\WUTJSCBCFX.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\WUTJSCBCFX.pdf	C:\Users\user\Downloads\WUTJSCBCFX.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\YPSIACHYXW.docx	C:\Users\user\Downloads\YPSIACHYXW.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\YPSIACHYXW.jpg	C:\Users\user\Downloads\YPSIACHYXW.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	C:\Users\user\Downloads\ZBEDCJPBEY.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	C:\Users\user\Downloads\ZBEDCJPBEY.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Amazon.url	C:\Users\user\Favorites\Amazon.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Bing.url	C:\Users\user\Favorites\Bing.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Facebook.url	C:\Users\user\Favorites\Facebook.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Google.url	C:\Users\user\Favorites\Google.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Live.url	C:\Users\user\Favorites\Live.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\NYTimes.url	C:\Users\user\Favorites\NYTimes.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Reddit.url	C:\Users\user\Favorites\Reddit.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Twitter.url	C:\Users\user\Favorites\Twitter.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Wikipedia.url	C:\Users\user\Favorites\Wikipedia.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Favorites\Youtube.url	C:\Users\user\Favorites\Youtube.url.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\bowsakkdestx.txt	C:\Users\user\Local Settings\bowsakkdestx.txt.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\IconCache.db	C:\Users\user\Local Settings\IconCache.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	C:\Users\user\SendTo\Bluetooth File Transfer.LNK.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget	C:\Users\user\SendTo\Compressed (zipped) Folder.ZFSendToTarget.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	C:\Users\user\SendTo\Desktop (create shortcut).DeskLink.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Documents.mydocs	C:\Users\user\SendTo\Documents.mydocs.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail	C:\Users\user\SendTo\Mail Recipient.MAPIMail.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\DNTException\container.dat	C:\Users\user\Cookies\DNTException\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\ESE\container.dat	C:\Users\user\Cookies\ESE\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3	C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg	C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\BPMLNOBVSB.jpg	C:\Users\user\Documents\WUTJSCBCFX\BPMLNOBVSB.jpg.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\FENIVHOIKN.png	C:\Users\user\Documents\WUTJSCBCFX\FENIVHOIKN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\KZWFNRXYKI.xlsx	C:\Users\user\Documents\WUTJSCBCFX\KZWFNRXYKI.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\WKXEWIOTXI.mp3	C:\Users\user\Documents\WUTJSCBCFX\WKXEWIOTXI.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\WUTJSCBCFX.docx	C:\Users\user\Documents\WUTJSCBCFX\WUTJSCBCFX.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\WUTJSCBCFX\ZBEDCJPBEY.pdf	C:\Users\user\Documents\WUTJSCBCFX\ZBEDCJPBEY.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW\RAYHIWGKDI.pdf	C:\Users\user\Documents\YPSIACHYXW\RAYHIWGKDI.pdf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW\SFPUSAFIOL.mp3	C:\Users\user\Documents\YPSIACHYXW\SFPUSAFIOL.mp3.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW\SQRKHNBNYN.png	C:\Users\user\Documents\YPSIACHYXW\SQRKHNBNYN.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW\WKXEWIOTXI.jpg	C:\Users\user\Documents\YPSIACHYXW\WKXEWIOTXI.jpg.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\YPSIACHYXW\YPSIACHYXW.docx	C:\Users\user\Documents\YPSIACHYXW\YPSIACHYXW.docx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\Documents\YPSIACHYXW\ZBEDCJPBEY.xlsx	C:\Users\user\Documents\YPSIACHYXW\ZBEDCJPBEY.xlsx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe	C:\Users\user\Local Settings\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	C:\Users\user\Local Settings\ConnectedDevicesPlatform\CDPGlobalSettings.cdp.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\AdobeARM.log	C:\Users\user\Local Settings\Temp\AdobeARM.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\chrome_installer.log	C:\Users\user\Local Settings\Temp\chrome_installer.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	C:\Users\user\Local Settings\Temp\JavaDeployReg.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\SetupExe(2020072310200717D0).log	C:\Users\user\Local Settings\Temp\SetupExe(2020072310200717D0).log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\tmpCDDA.tmp	C:\Users\user\Local Settings\Temp\tmpCDDA.tmp.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\{72C857CF-E54C-4041-A4DB-FE40A1ED71CD} - OProcSessId.dat	C:\Users\user\Local Settings\Temp\{72C857CF-E54C-4041-A4DB-FE40A1ED71CD} - OProcSessId.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl	C:\Users\user\Application Data\Microsoft\Office\MSO1033.acl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm	C:\Users\user\Application Data\Microsoft\Templates\Normal.dotm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Low\ESE\container.dat	C:\Users\user\Cookies\Low\ESE\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	C:\Users\user\Local Settings\Adobe\Color\ACECache11.lst.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	C:\Users\user\Local Settings\Comms\UnistoreDB\USS.jcp.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	C:\Users\user\Local Settings\Comms\UnistoreDB\USSres00001.jrs.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	C:\Users\user\Local Settings\Comms\UnistoreDB\USSres00002.jrs.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	C:\Users\user\Local Settings\Comms\UnistoreDB\USStmp.jtx.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\container.dat	C:\Users\user\Local Settings\History\History.IE5\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\ngen.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0_32\ngen.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	C:\Users\user\Local Settings\Microsoft\Internet Explorer\brndlog.txt.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	C:\Users\user\Local Settings\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	C:\Users\user\Local Settings\Microsoft\Internet Explorer\ie4uinit-UserConfig.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	C:\Users\user\Local Settings\Microsoft\Internet Explorer\MSIMGSIZ.DAT.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	C:\Users\user\Local Settings\Microsoft\PenWorkspace\DiscoverCacheData.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\CR_4BAC1.tmp\setup.exe	C:\Users\user\Local Settings\Temp\CR_4BAC1.tmp\setup.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\DismHost.exe	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\DismHost.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\container.dat	C:\Users\user\Local Settings\Temporary Internet Files\Content.IE5\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	C:\Users\user\Local Settings\Temporary Internet Files\Low\MSIMGSIZ.DAT.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	C:\Users\user\Local Settings\Temporary Internet Files\Low\SmartScreenCache.dat.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	C:\Users\user\Application Data\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\CHICAGO.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\GB.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\GostName.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\GostTitle.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl	C:\Users\user\Application Data\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl	C:\Users\user\Application Data\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\ISO690.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\ISO690Nmerical.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl	C:\Users\user\Application Data\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\SIST02.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL	C:\Users\user\Application Data\Microsoft\Bibliography\Style\TURABIAN.XSL.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	C:\Users\user\Application Data\Microsoft\Office\Recent\index.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK	C:\Users\user\Application Data\Microsoft\Office\Recent\Templates.LNK.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.acl	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.acl.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.dic	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.dic.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Spelling\en-US\default.exc	C:\Users\user\Application Data\Microsoft\Spelling\en-US\default.exc.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	C:\Users\user\Application Data\Microsoft\Windows\Libraries\CameraRoll.library-ms.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	C:\Users\user\Application Data\Microsoft\Windows\Libraries\Documents.library-ms.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	C:\Users\user\Application Data\Microsoft\Windows\Libraries\Music.library-ms.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	C:\Users\user\Application Data\Microsoft\Windows\Libraries\Pictures.library-ms.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	C:\Users\user\Application Data\Microsoft\Windows\Libraries\Videos.library-ms.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	C:\Users\user\Local Settings\Adobe\Acrobat\DC\AdobeCMapFnt19.lst.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	C:\Users\user\Local Settings\Adobe\Acrobat\DC\AdobeSysFnt19.lst.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	C:\Users\user\Local Settings\Adobe\Acrobat\DC\IconCacheRdr65536.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	C:\Users\user\Local Settings\Adobe\Acrobat\DC\UserCache.bin.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe	C:\Users\user\Local Settings\Application Data\Application Data\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Comms\Unistore\data\AggregateCache.uca	C:\Users\user\Local Settings\Comms\Unistore\data\AggregateCache.uca.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\chrome_shutdown_ms.txt	C:\Users\user\Local Settings\Google\Chrome\User Data\chrome_shutdown_ms.txt.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	C:\Users\user\Local Settings\Google\Chrome\User Data\CrashpadMetrics-active.pma.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\persisted_first_party_sets.json	C:\Users\user\Local Settings\Google\Chrome\User Data\persisted_first_party_sets.json.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022081620220817\container.dat	C:\Users\user\Local Settings\History\History.IE5\MSHist012022081620220817\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History\Low\History.IE5\container.dat	C:\Users\user\Local Settings\History\Low\History.IE5\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log	C:\Users\user\Local Settings\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	C:\Users\user\Local Settings\Microsoft\Internet Explorer\DomainSuggestions\en-US.1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\DOMStore\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\EmieSiteList\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\EmieUserList\container.dat	C:\Users\user\Local Settings\Microsoft\Internet Explorer\EmieUserList\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	C:\Users\user\Local Settings\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	C:\Users\user\Local Settings\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	C:\Users\user\Local Settings\Microsoft\Internet Explorer\VersionManager\versionlist.xml.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\alertIcon.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\alertIcon.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppBlue.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AppBlue.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorBlue.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AppErrorBlue.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorWhite.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AppErrorWhite.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppWhite.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AppWhite.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.gif	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.gif.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.png.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppBlue.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppBlue.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppWhite.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppWhite.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Error.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\Error.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ErrorPage.html	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\ErrorPage.html.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileCoAuth.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\FileCoAuth.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncConfig.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\FileSyncConfig.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncHelper.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\FileSyncHelper.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMHeroToast.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\KFMHeroToast.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMLockedFileToast.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\KFMLockedFileToast.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMScanExclusionToast.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\KFMScanExclusionToast.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\LoadingPage.html	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\LoadingPage.html.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDrive.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.VisualElementsManifest.xml	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDrive.VisualElementsManifest.xml.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveLogo.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDriveLogo.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveSetup.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDriveSetup.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveStandaloneUpdater.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDriveStandaloneUpdater.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveUpdaterService.exe	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\OneDriveUpdaterService.exe.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaCritical.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\QuotaCritical.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaError.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\QuotaError.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaNearing.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\QuotaNearing.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Resources.pri	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\Resources.pri.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\SaveApplicationEventLogs.wsf	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\SaveApplicationEventLogs.wsf.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ScreenshotOptIn.gif	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\ScreenshotOptIn.gif.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\TestSharePage.html	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\TestSharePage.html.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ThirdPartyNotices.txt	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\ThirdPartyNotices.txt.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\vaultIntro.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\vaultIntro.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Warning.png	C:\Users\user\Local Settings\Microsoft\OneDrive\19.086.0502.0006\Warning.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	C:\Users\user\Local Settings\Microsoft\OneDrive\setup\ECSConfig.json.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	C:\Users\user\Local Settings\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Vault\UserProfileRoaming\Latest.dat	C:\Users\user\Local Settings\Microsoft\Vault\UserProfileRoaming\Latest.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	C:\Users\user\Local Settings\Microsoft\Windows\1033\StructuredQuerySchema.bin.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\microsoft-skydrive-desktop_16_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\microsoft-skydrive-desktop_16_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_11_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_11_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_27_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_27_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_37_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_37_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_9_0.png	C:\Users\user\Local Settings\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_9_0.png.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\AppCache\container.dat	C:\Users\user\Local Settings\Microsoft\Windows\AppCache\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\cversions.1.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\cversions.3.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{0A0496DA-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{0A0496DA-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000a.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000a.db.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000b.db	C:\Users\user\Local Settings\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000b.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\ExplorerStartupLog.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_1280.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_1920.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_2560.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_768.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_96.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_custom_stream.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_exif.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_sr.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_wide.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\iconcache_wide_alternate.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_1280.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1920.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_1920.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_2560.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_2560.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_768.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_768.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_custom_stream.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_custom_stream.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_exif.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_exif.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_sr.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_wide.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide_alternate.db	C:\Users\user\Local Settings\Microsoft\Windows\Explorer\thumbcache_wide_alternate.db.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\IECompatCache\container.dat	C:\Users\user\Local Settings\Microsoft\Windows\IECompatCache\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\IECompatUaCache\container.dat	C:\Users\user\Local Settings\Microsoft\Windows\IECompatUaCache\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\IEDownloadHistory\container.dat	C:\Users\user\Local Settings\Microsoft\Windows\IEDownloadHistory\container.dat.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Shell\DefaultLayouts.xml	C:\Users\user\Local Settings\Microsoft\Windows\Shell\DefaultLayouts.xml.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\UPPS\UPPS.bin	C:\Users\user\Local Settings\Microsoft\Windows\UPPS\UPPS.bin.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V01.chk	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V01.chk.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V0100009.log	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V0100009.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V010000A.log	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V010000A.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V010000B.log	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V010000B.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V01res00001.jrs	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V01res00001.jrs.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V01res00002.jrs	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V01res00002.jrs.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log	C:\Users\user\Local Settings\Microsoft\Windows\WebCache\V01tmp.log.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_00.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_00.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_01.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_01.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_02.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_02.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_03.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_03.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_04.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_04.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_05.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_05.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_06.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_06.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_07.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_07.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Microsoft\Windows Live\Bici_08.sqm	C:\Users\user\Local Settings\Microsoft\Windows Live\Bici_08.sqm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DNTException\container.dat	C:\Users\user\Local Settings\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DNTException\container.dat.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\1527c705-839a-4832-9118-54d4Bd6a0c89_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\1527c705-839a-4832-9118-54d4Bd6a0c89_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\1527c705-839a-4832-9118-54d4Bd6a0c89_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\1527c705-839a-4832-9118-54d4Bd6a0c89_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\E2A4F912-2574-4A75-9BB0-0D023378592B_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\E2A4F912-2574-4A75-9BB0-0D023378592B_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\E2A4F912-2574-4A75-9BB0-0D023378592B_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\E2A4F912-2574-4A75-9BB0-0D023378592B_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\InputApp_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AsyncTextService_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.AsyncTextService_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.AsyncTextService_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.AsyncTextService_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.BingWeather_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.CredDialogHost_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.CredDialogHost_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.CredDialogHost_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.CredDialogHost_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.ECApp_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.ECApp_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.ECApp_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.ECApp_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.GetHelp_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.GetHelp_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.GetHelp_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.GetHelp_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Getstarted_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Getstarted_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Getstarted_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Getstarted_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\HasRegisteredAsDefaultApp.setting	C:\Users\user\Local Settings\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\HasRegisteredAsDefaultApp.setting.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\MessagingBackgroundTaskLog.etl	C:\Users\user\Local Settings\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\MessagingBackgroundTaskLog.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\TransportIdList.setting	C:\Users\user\Local Settings\Packages\Microsoft.Messaging_8wekyb3d8bbwe\LocalCache\TransportIdList.setting.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Messaging_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Messaging_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Messaging_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Messaging_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Microsoft3DViewer_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Microsoft3DViewer_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Microsoft3DViewer_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Microsoft3DViewer_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MSPaint_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.MSPaint_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.MSPaint_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.MSPaint_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.OneConnect_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.OneConnect_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.OneConnect_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.OneConnect_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.People_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.People_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.People_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.People_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.PPIProjection_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.PPIProjection_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.PPIProjection_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.PPIProjection_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Print3D_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Print3D_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Print3D_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Print3D_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.StorePurchaseApp_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.StorePurchaseApp_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.StorePurchaseApp_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.StorePurchaseApp_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Wallet_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Wallet_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Wallet_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Wallet_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WebMediaExtensions_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WebMediaExtensions_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WebMediaExtensions_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WebMediaExtensions_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.Win32WebViewHost_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Win32WebViewHost_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Win32WebViewHost_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Win32WebViewHost_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CapturePicker_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CapturePicker_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CapturePicker_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CapturePicker_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\TempState\CortanaUnifiedTileModelCache.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\TempState\CortanaUnifiedTileModelCache.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.HolographicFirstRun_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.HolographicFirstRun_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.HolographicFirstRun_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.HolographicFirstRun_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.OOBENetworkCaptivePortal_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.OOBENetworkCaptivePortal_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.OOBENetworkCaptivePortal_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.OOBENetworkCaptivePortal_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.OOBENetworkConnectionFlow_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.OOBENetworkConnectionFlow_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.OOBENetworkConnectionFlow_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.OOBENetworkConnectionFlow_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ParentalControls_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ParentalControls_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ParentalControls_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ParentalControls_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite-shm	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite-shm.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite-wal	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite-wal.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\PhotosAppTracing_startedInBGMode.etl	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\PhotosAppTracing_startedInBGMode.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.PinningConfirmationDialog_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.PinningConfirmationDialog_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.PinningConfirmationDialog_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.PinningConfirmationDialog_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\TempState\StartUnifiedTileModelCache.dat	C:\Users\user\Local Settings\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\TempState\StartUnifiedTileModelCache.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.WindowsAlarms_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCalculator_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCalculator_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCalculator_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCalculator_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog.etl	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog_Old.etl	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog_Old.etl.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxStore.hxd	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxStore.hxd.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsMaps_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsMaps_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsMaps_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsMaps_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Xbox.TCUI_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.Xbox.TCUI_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.Xbox.TCUI_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.Xbox.TCUI_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.XboxApp_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxGameOverlay_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\Microsoft.XboxIdentityProvider_8wekyb3d8bbwe\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\Windows.CBSPreview_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Windows.CBSPreview_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Windows.CBSPreview_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Windows.CBSPreview_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG1	C:\Users\user\Local Settings\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG1.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG2	C:\Users\user\Local Settings\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\Settings\settings.dat.LOG2.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\roaming.lock	C:\Users\user\Local Settings\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\roaming.lock.uyro	success or wait	1	41127D	MoveFileW
C:\Users\user\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat	C:\Users\user\Local Settings\Packages\Windows.PrintDialog_cw5n1h2txyewy\Settings\settings.dat.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\AppxProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\AppxProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\AssocProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\AssocProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\CbsProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\CbsProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\CompatProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\CompatProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DismCore.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DismCore.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DismProv.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DismProv.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DmiProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\DmiProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\FfuProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\FfuProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\FolderProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\FolderProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\GenericProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\GenericProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\IBSProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\IBSProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\ImagingProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\ImagingProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\IntlProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\IntlProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\LogProvider.dll.mui	C:\Users\user\Local Settings\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\en-US\LogProvider.dll.mui.uyro	success or wait	1	4116DC	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\geo[1].json	0	500	7b 22 69 70 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 39 22 2c 22 63 6f 75 6e 74 72 79 5f 63 6f 64 65 22 3a 22 43 48 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 5f 72 75 73 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 33 38 5c 75 30 34 34 66 22 2c 22 63 6f 75 6e 74 72 79 5f 75 61 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 35 36 5c 75 30 34 34 66 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 75 72 69 63 68 22 2c 22 72 65 67 69 6f 6e 5f 72 75 73 22 3a 22 5c 75 30 34 32 36 5c 75 30 34 34 65 5c 75 30	{"ip":"102.129.143.49","country_code":"CH","country":"Switzerland","country_rus":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0438\u044f","country_ua":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0456\u044f","region":"Zurich","region_rus":"\u0426\u044e\u0	success or wait	1	40CFD3	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	46			invalid handle	1	42E51E	WriteFile
unknown	unknown	2			invalid handle	1	42E51E	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\get[1].htm	0	562	7b 22 70 75 62 6c 69 63 5f 6b 65 79 22 3a 22 2d 2d 2d 2d 2d 42 45 47 49 4e 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 2d 5c 5c 6e 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 41 51 45 41 34 4a 55 50 58 68 63 4f 70 39 56 5c 2f 45 39 6c 78 5a 73 45 4b 5c 5c 6e 51 65 30 4c 55 52 37 46 78 49 58 39 2b 32 57 5c 2f 58 32 6e 47 65 52 59 79 35 64 36 5c 2f 78 6b 75 54 77 49 39 4c 44 75 42 75 55 4e 59 4c 4c 70 6b 38 41 70 53 66 67 4c 37 72 72 45 33 64 4d 61 75 31 5c 5c 6e 53 79 6f 4a 46 37 32 6d 7a 64 6e 76 76 36 53 61 42 59 58 72 49 4a 4e 7a 38 47 62 50 36 7a 6a 69 6f 6f 4e 38 4d 6d 64 33 67 53 66 6d 59 58 46 41 2b 38 45 56 6a 51 37 4d 53 36 68 6a 44 6d 59 63	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4JUPXhcOp9V\/E9lxZsEK\\nQe0LUR7FxIX9+2W\/X2nGeRYy5d6\/xkuTwI9LDuBuUNYLLpk8ApSfgL7rrE3dMau1\\nSyoJF72mzdnvv6SaBYXrlJNz8GbP6zjiooN8Mmd3gSfmYXFA+8EVjQ7MS6hjDmYc	success or wait	1	41E975	InternetReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	0	562	7b 22 70 75 62 fd 0d fd 03 5a fd 4d 0b fd 58 fd 5d 72 26 69 59 18 44 fd fd 15 29 7b 38 74 27 fd fd 44 fd fd 0d 5b 23 fd fd 6d fd 3c 57 fd 33 fd fd fd 63 fd 09 37 30 fd fd 4a 00 41 28 71 74 fd fd fd 7f 72 52 68 fd fd 7f 0f 37 09 69 03 7f fd 0a fd 1f 6a 36 fd fd 07 0e fd fd fd 0c fd 3d fd 5f fd 07 fd 15 fd fd 1e fd fd 20 fd fd 20 6c db 34 fd fd 1f fd fd fd 04 44 09 39 5a fd 5e fd 6c fd fd fd fd 57 54 fd 6e 0c 32 79 7c 5a 1d fd fd 74 fd 5d 77 5e fd 4c 5f fd 4f 5c fd fd fd fd fd 59 4e 55 fd 0a 50 c6 7b 49 07 5e fd fd fd fd 0b fd fd 66 fd af 1c fd fd fd 15 23 68 fd 49 60 0f fd 58 75 62 fd 27 0d 42 3b fd fd 63 68 11 44 03 fd 2e 6a 22 3c fd fd 1d fd 28 7a 7f 71 32 5b 2c fd 57 52 fd 7e 58 0e 28 20 c5 7c 3e fd fd 40 35	{"pubZMX]&iYD){8t'D[#m<W3c70JA(qtrRh7ij6=_l4D9Z^lWTn2y|Zt]w^L_O\YNUP{I^f#hl`Xub'B;chD.j(zq2[,WR~X(|>@5	success or wait	1	42E51E	WriteFile
C:\SystemID\PersonalID.txt	0	42	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53 0d 0a	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	42E51E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe	0	10240	4d 5a fd 00 03 77 16 fd 04 27 ce 3f 17 40 fd fd 09 fd fd fd 51 fd 71 5f fd 42 57 46 35 50 fd 63 33 7c 6f fd 7f 0a fd 30 66 fd 41 60 fd fd bf fd 50 7a 4b 02 b6 1a fd fd 5f 29 19 56 fd 10 10 fd fd 7c fd fd 3b 59 fd fd 7a 26 0b fd fd 62 3c fd 16 fd fd 4b fd fd 71 93 fd fd 7d fd 2e 69 38 50 fd 05 37 45 0b fd 53 fd fd 04 fd fd 1e 62 76 fd 57 fd 06 5c 0d fd 33 28 25 62 fd fd 43 73 fd 1c 7b 3b fd fd 0f 06 6f fd fd 19 77 fd 52 60 76 3a 3a fd 2e 37 42 68 0d 4b 67 fd 3b 5d fd 2c fd 06 fd 20 fd 47 20 fd 5b 60 fd 3c 2d fd fd fd a2 fd fd 27 18 fd 75 fd fd 50 5a fd fd 1c fd fd fd 22 1d 33 65 fd fd 67 fd 19 fd 31 75 65 fd 0c 0f 5e fd fd fd 47 fd fd fd fd 3f fd 29 fd 67 41 26 28 03 57 fd 6f fd fd 23 5a 64 34 28 0d 47 5a	MZ'?@Qq_BWF5Pc3|o0fA`PzK_)V|;Yzb<Kq}i8P7ESbvW\3(%bCs{;owR`::.7BhKg;], G [<-'PZ"3egue^G?)gA&(Wo#Zd4(GZ	success or wait	26	41E301	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build2[1].exe	20480	10240	fd fd 59 fd 46 5c 3d fd 22 40 00 74 07 50 fd 70 fd fd fd 59 6a 0d fd fd 10 00 00 59 fd 65 fd 00 fd 7e 68 fd fd 74 1a 57 fd 15 68 11 40 00 fd fd 75 0f fd fd 58 fd 43 00 74 07 57 fd 43 fd fd fd 59 fd 45 fd fd fd fd fd fd 57 00 00 00 6a 0c fd 10 00 00 59 fd 45 fd 01 00 00 00 fd 7e 6c fd fd 74 23 57 fd fd fd fd fd 59 3b 3d 60 fd 43 00 74 14 fd fd fd fd 43 00 74 0c fd 3f 00 75 07 57 fd fd fd fd fd 59 fd 45 fd fd fd fd fd fd 1e 00 00 00 56 fd fd fd fd fd 59 fd 7b 0b 00 00 fd 04 00 fd 75 08 6a 0d fd 0f 00 00 59 cb 75 08 6a 0c fd 78 0f 00 00 59 cb fd 56 57 fd 30 1c 40 00 56 fd 15 fd 10 40 00 fd fd 75 07 56 fd fd 1f 00 00 59 fd fd fd fd 0f fd 5e 01 00 00 fd 35 fd 10 40 00 68 7c 1c 40 00 57 fd fd 68 70 1c 40 00 57 fd fd 05 47 00 fd fd 68 64 1c 40 00 57	YF\="@tPpYjYe~htWh@uXCtWCYEWjYE~lt#WY;=`CtCt?uWYEVY{ujYujxYVW0@V@uVY^5@h|@Whp@WGhd@W	success or wait	19	41E2CD	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:_readme.txt	0	1115	41 54 54 45 4e 54 49 4f 4e 21 0d 0a 0d 0a 44 6f 6e 27 74 20 77 6f 72 72 79 2c 20 79 6f 75 20 63 61 6e 20 72 65 74 75 72 6e 20 61 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 21 0d 0a 41 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 20 6c 69 6b 65 20 70 69 63 74 75 72 65 73 2c 20 64 61 74 61 62 61 73 65 73 2c 20 64 6f 63 75 6d 65 6e 74 73 20 61 6e 64 20 6f 74 68 65 72 20 69 6d 70 6f 72 74 61 6e 74 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 20 77 69 74 68 20 73 74 72 6f 6e 67 65 73 74 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6e 64 20 75 6e 69 71 75 65 20 6b 65 79 2e 0d 0a 54 68 65 20 6f 6e 6c 79 20 6d 65 74 68 6f 64 20 6f 66 20 72 65 63 6f 76 65 72 69 6e 67 20 66 69 6c 65 73 20 69 73 20 74 6f 20 70 75 72 63 68 61 73 65 20 64 65 63 72 79 70 74 20 74 6f 6f 6c 20 61 6e 64 20	ATTENTION!Don't worry, you can return all your files!All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.The only method of recovering files is to purchase decrypt tool and	success or wait	1	40F1A7	WriteFile
C:\Users\user_readme.txt	0	1115	41 54 54 45 4e 54 49 4f 4e 21 0d 0a 0d 0a 44 6f 6e 27 74 20 77 6f 72 72 79 2c 20 79 6f 75 20 63 61 6e 20 72 65 74 75 72 6e 20 61 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 21 0d 0a 41 6c 6c 20 79 6f 75 72 20 66 69 6c 65 73 20 6c 69 6b 65 20 70 69 63 74 75 72 65 73 2c 20 64 61 74 61 62 61 73 65 73 2c 20 64 6f 63 75 6d 65 6e 74 73 20 61 6e 64 20 6f 74 68 65 72 20 69 6d 70 6f 72 74 61 6e 74 20 61 72 65 20 65 6e 63 72 79 70 74 65 64 20 77 69 74 68 20 73 74 72 6f 6e 67 65 73 74 20 65 6e 63 72 79 70 74 69 6f 6e 20 61 6e 64 20 75 6e 69 71 75 65 20 6b 65 79 2e 0d 0a 54 68 65 20 6f 6e 6c 79 20 6d 65 74 68 6f 64 20 6f 66 20 72 65 63 6f 76 65 72 69 6e 67 20 66 69 6c 65 73 20 69 73 20 74 6f 20 70 75 72 63 68 61 73 65 20 64 65 63 72 79 70 74 20 74 6f 6f 6c 20 61 6e 64 20	ATTENTION!Don't worry, you can return all your files!All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.The only method of recovering files is to purchase decrypt tool and	success or wait	1	40F1A7	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	5	86	fd fd 21 fd 22 53 fd 01 fd fd fd 4b fd 61 fd 59 29 fd fd 75 6b 02 05 fd 72 fd fd 22 7d fd 36 fd 4e 03 fd 1d 18 fd 27 fd 12 fd fd 42 fd 7d 51 fd fd 20 fd fd fd 18 fd fd 6b 15 fd 92 5b 62 fd 69 fd 72 fd 58 02 fd fd 74 fd 25 5f 28 fd ae 66 26 57 27	!"SKaY)ukr"}6N'B}Q k[birXt%_(f&W'	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	91	256	1b 14 fd fd 06 bd 77 fd 40 7c fd fd 3b fd 1f 1e 1b 2c fd fd fd fd 3f 62 fd 70 fd fd fd 0c 1b fd 6a fd 09 16 fd fd 29 0f 0d 45 fd 5c fd 0f 5c 17 fd 39 fd 56 fd fd 3a fd 67 fd 2b 47 fd fd fd fd fd 5e fd 5d 2d 15 58 fd 04 6e fd 70 fd 67 fd 18 fd fd fd 6e 4a 27 17 1c fd 7c fd fd fd fd 34 60 5c fd 1e 07 fd 49 fd fd 73 0c fd fd 3d 59 fd fd 45 11 fd fd fd 3d fd 18 16 fd 5a 5e fd 1e 04 fd 26 00 fd fd fd 18 1a fd fd fd fd 36 fd fd fd fd 0b 0d fd fd fd 4d fd fd 41 1c 4b fd 4b fd fd fd fd 62 fd 77 0b fd 52 fd fd 0a 04 fd fd 26 fd 18 e0 67 0f fd 4f 61 4e fd fd 0a 10 fd 7a 37 fd 13 fd fd 1b 59 fd fd 4b fd 11 72 fd 51 fd 5e fd 45 44 01 fd fd fd fd fd 19 1f fd 3c 05 4e 65 78 2e fd 05 65 2a fd fd fd 54 fd fd fd fd 74 fd fd	w@|;,?bpj}E\\9V:g+G^]-Xnpgn'|4 `\l=YE=Z^&6MAKKbR&gOaNz7YKrQ^ED<ex.e*Tt	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	347	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	387	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.jpg	5	1021	fd 19 28 69 fd fd fd 43 42 fd fd 23 89 7c 68 5f fd 49 4e 15 fd 7a fd fd fd 28 02 40 75 68 fd fd 10 1a 30 0e 4f 63 fd 58 30 57 78 fd 5a 3b fd 5d 25 4a 19 43 4f 1a 08 fd 08 fd 0d fd 62 73 65 fd 1b 25 7d fd fd 72 06 fd fd 6d fd 45 07 fd 3a 6e 41 30 6f fd 15 35 3e 6a 70 fd 1b fd 70 fd fd fd fd fd 71 fd fd 0c 24 78 01 fd fd 71 2f 65 19 5e fd fd 2f fd fd 49 fd 6c fd 6d 3a fd 24 fd 5f 13 52 f3 fd 47 fd 1b fd 5e 00 3a fd fd 39 fd 0c 7e 0b fd 6d 63 fd fd fd 5f fd f6 fd 77 09 39 7e 5b fd 1a 07 fd 0b fd 66 fd 0a 44 3f 1c 2b 13 32 fd fd fd 4f fd fd 28 18 fd 25 fd 0c 7e 13 70 fd fd 69 61 47 53 6d 32 fd 6e fd fd fd fd fd 7c 23 4e fd fd fd fd 0d fd fd 02 fd 21 18 15 63 40 fd 0d fc fd 01 fd fd fd 47 30 52 fd fd fd 5d fd 29 fd fd 13 fd 09 14 45	(iCB#|h_INz(@uh0OcX0WxZ;]%JCObse%}rmE:nA0o5>jppq$xq/e^/II:$_RG^:9~mc_w9~[fD?+2O(%~piaGSm2n|#N!cG0R])E	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BPMLNOBVSB.jpg	1026	256	25 fd fd fd 51 69 fd fd 11 fd 28 0d fd fd 51 68 55 fd 7f 4f fd 47 fd 3e 6f 14 fd fd 72 fd fd 48 7d fd 7d 17 fd fd 7c fd fd fd fd 70 e3 fd 10 68 35 44 fd fd 07 57 fd fd fd 7e 05 fd 49 36 17 3b fd 04 47 6c fd fd 57 fd fd 39 8f fd 13 0a 68 fd 46 fd 1f fd fd fd 0c 63 fd fd fd fd 74 2e fd fd 8a fd fd fd 7c 69 74 42 fd 05 1a 38 58 fd 6a fd fd 5e fd 0a 46 0c 0e 00 fd 2a 00 eb fd fd fd 79 fd 53 fd 21 fd fd 22 7a fd 4b 3b fd 1c fd 2a 3b fd 25 28 fd fd fd fd 4b 9e 50 47 4c fd fd 07 7b fd 40 69 fd 01 78 0d 95 fd 79 60 fd 21 fd fd 6e fd 44 fd 05 10 fd 12 46 69 fd 51 36 07 3b fd 33 77 fd fd fd fd 35 5a 0e 0e 2e 6a c4 fd 15 69 fd 0c 02 fd 59 fd fd fd 38 fd fd 77 fd 02 52 40 0d d9 2e fd 5a 11 fd 3b fd fd fd fd	%Qi(QhUOG>rH}}|p5DW ~I6GlW9hFct .|itB8Xj^F*yS!"zK;*;% (KGL{@ixy `!nDFiQ6;3w5Z.jiY8wR@. Z;	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	5	1021	20 fd 52 fd 6e fd 35 73 fd 22 fd 68 fd fd fd 24 fd 09 fd fd 09 5e fd 0c fd 97 fd fd 1e 5a 4e fd 74 fd 24 51 3d fd fd fd 3d 66 fd fd fd 44 13 fd fd 66 0e 36 fd fd fd fd 3b 3c 24 04 71 22 fd 12 fd 44 71 fd 00 fd 0c 60 fd 77 25 fd fd 4d 74 16 fd 6e 23 fd fd 23 5e 08 35 fd 10 5a fd f8 fd fd 4a 77 fd 30 fd fd 0f fd fd fd fd fd fd fd fd 52 fd 31 fd fd fd fd 55 fd fd 60 55 40 73 35 fd 1b 1c 2d 0e fd fd 4b fd 1e 1d 76 7a fd 1b fd 22 fd 33 1b 3f fd fd 31 fd fd 49 11 a5 40 fd 39 4f 42 fd 5b 5d fd 7f 58 fd fd fd fd 46 38 3d 1a 6a fd 40 55 3b fd 0b 7e 21 fd 67 34 70 fd 71 3f 0c 4b fd fd fd 16 36 2d 17 fd 03 5f 34 2e 58 fd 79 ac 46 37 fd fd 01 78 fd 70 fd fd 4e 2b 15 b0 60 4a 0c 5f 1b fd 52 fd 4a 33 05 fd fd 0d 07 fd 22 fd c1 fd fd fd 55 7a	Rn5s"h^ZNtQ==fDf6; <$q"Dq`w% Mtn##^5ZJw0R1U`U@s5 -Kvz"3?1I@9 OB[]XF8=j@U;~!g4pq?K- _4.XyF7xpN+`J_RJ3"Uz	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	1026	256	19 fd fd 7d 32 4c 75 fd 42 11 fd 19 45 2e fd fd fd 29 fd 19 4e fd 4d 17 fd fd fd 19 fd fd fd 37 59 fd 19 fd 47 fd 25 1f 73 1e fd 53 20 fd 1b fd fd fd 79 17 05 1e fd fd fd fd 73 3d fd fd fd 09 fd fd 69 4b 29 6d 71 fd 93 59 4d 2b fd fd 28 fd fd fd fd d4 55 2d 55 fd 05 08 63 fd 61 fd fd fd 19 fd fd 1d 4a fd fd 23 fd 7c 57 fd fd 26 2f 2c fd fd fd fd 00 fd 51 fd 7e fd fd 77 fd 00 fd 02 0a 25 6c fd fd fd fd 2b fd fd 2a fd 45 15 5d fd fd 20 7e fd 1e fd 64 51 d1 fd 7b 46 fd fd fd fd 2c fd 11 77 fd fd 50 fd 32 6c fd 24 2c 33 fd 55 05 41 fd 20 01 61 33 fd 25 40 6d 29 fd 09 fd 3c 49 21 3f fd fd fd cc 16 35 fd fd 54 fd fd fd fd 30 fd 68 57 fd fd 32 72 49 fd 61 fd fd fd 4d 11 33 fd 41 fd 24 5b 5c 6a fd 3a 40 37 fd 62 39 fd 3e fd	}2LuB.)NM7YG%sSys=iK)mqYM+(U-Uca#|W&/,Q~w%l+E]~dQ{F,wP2l$,3UAa3%@m)<l!?5T0h2rIaM3A$[\j:@7b9>	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\FENIVHOIKN.png	5	1021	60 fd 32 1f e7 73 59 fd 35 fd fd 5e fd fd 35 55 fd fd 02 fd 5d fd fd fd 72 15 fd fd 42 04 fd fd 1e 33 74 fd fd 40 6e fd fd 5d 02 11 fd 15 fd 70 55 fd fd fd 00 24 fd 70 0e fd 43 fd 5c fd 15 14 5d fd 11 57 fd fd fd fd fd fd 06 15 fd 63 ad 33 fd fd fd 51 74 fd 71 0d 62 7c 0c fd fd fd 25 4c fd 26 fd 57 37 fd 14 fd 0f fd 6b fd fd fd 6f fd 24 28 fd 63 fd fd 00 10 fd 00 41 6a fd fd fd 70 33 fd fd 57 fd 45 5a fd 32 fd fd 32 fd fd 6c fd fd 13 fd fd fd fd fd 4a fd fd 15 fd 5b 9a 56 57 fd fd 2a 65 45 49 13 55 fd 7b fd f8 fd 25 75 fd 13 fd 14 fd 0f 08 fd fd fd 46 fd 7d fd fd fd 67 39 48 fd 31 fd 56 20 fd fd 05 6b fd 22 fd fd 45 72 fd 1b fd fd 05 fd fd fd 2e 76 fd fd fd 6b 13 fd 53 73 6d 18 fd fd fd 65 33 fd fd 87 fd fd fd	`2sY55U]rB3t@n]pU$pC\]WcQtqb\|%L&W7ko$(cAjp3WEZ22lJ[VW*elU{%uF}g9H1Vk"Er.vkSsme3	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FENIVHOIKN.png	1026	256	5b fd fd fd 18 fd 72 fd fd fd fd 4c fd fd 05 fd fd fd 0b 7a fd fd 96 02 72 fd fd fd 43 0e fd 6b 69 fd fd fd 38 fd fd fd 6e fd fd 33 2a fd fd fd 7f fd 1f fd 18 fd 76 4d fd fd fd 20 26 26 fd 0b 39 fd 1b fd fd fd 43 fd fd fd 68 fd 17 fd 4c 3f fd 66 fd 78 fd 11 59 fd 2d fd 35 3d 6c 6c 13 0a fd fd 2a 36 fd 69 fd 66 fd 1f fd 1d fd 02 fd 32 fd 2c 4f fd fd fd fd 4b 3c fd 41 fd fd 44 03 fd 6b fd 62 2a 56 33 32 1e 62 fd 19 fd 51 fd 61 fd 77 11 fd fd 2e fd 04 fd 20 2c 61 55 48 fd fd 65 25 13 4f fd 5d fd fd 44 fd 77 fd 77 fd fd fd 02 62 fd 16 76 fd fd 05 09 fd 18 fd 1e 36 22 05 54 fd fd fd 44 fd 2c 19 fd fd fd fd fd 25 0a fd 3c fd fd fd fd 33 fd fd fd 21 fd fd 57 88 78 26 fd fd 26 6f 73 fd 06 02 fd fd 6e 24 09 06 fd fd 6a fd fd	[rLzrCki8n3*vM &&9ChL?fxY-5=ll *6if2,OK<ADkb*V32bQa.,aUHe%O]Dwbv6"TD,%<3!Wx&osn$j	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\FENIVHOIKN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\FENIVHOIKN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\JSDNGYCOWY.mp3	5	1021	fd 56 fd 5a fd 0b fd fd fd 51 fd 06 fd 33 57 fd 71 fd fd 84 2f 70 7f 3c fd 45 64 1c fd 0c fd fd 62 69 4f fd 31 73 1d fd 41 0b fd fd fd 23 fd 71 fd 34 fd fd 47 6c 57 00 9b 2b 47 48 fd d3 3b fd 01 fd 2f 08 29 76 1b 4a fd 11 fd fd fd 1a 10 fd 26 fd fd 21 33 fd fd 9c 27 fd fd 5a fd 28 fd fd 7a fd 62 24 fd fd 50 02 fd fd 04 fd 2a fd 2a fd 27 fd 42 fd 66 fd 09 fd fd 26 fd 57 49 fd 01 fd 2d 4b fd 66 20 fd 6d fd 76 62 fd fd fd fd 0d fd 1b 58 67 fd 3b fd 0a 1d fd fd 09 fd 21 fd 2f 04 51 fd fd 7f fd 0f fd fd fd fd 07 fd 64 37 fd fd fd fd 75 69 fd 5e 68 fd 13 fd 15 fd 70 6a fd 29 fd fd fd fd 44 fd 1b fd 57 fd 4c fd fd 05 fd 72 43 65 2f 5f 44 13 fd 1f 4c 78 19 18 fd 36 fd 4d 1d fd fd 16 2f fd fd fd 5b 4c 3a fd 19 fd 7a 2e 3a 29 fd 68 50 5f	VZQ3Wq/p<EdbiO1sA#q4GlW+GH;/)v J&!3'Z(zb$P**'Bf&WI-Kf mvbXg;! /Qd7ui^hpj)DWLrCe/_DLx6M/L:z.:)hP_	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\JSDNGYCOWY.mp3	1026	256	52 fd ba fd 5d fd fd 49 fd fd 54 2b 6f fd 24 fd 41 00 08 43 09 68 fd 73 33 fd 32 fd fd 3b 44 fd 7a fd 75 fd fd fd 1f 38 1c fd fd fd 79 fd fd fd 3d 1d fd 02 31 67 43 04 fd 07 fd fd fd fd 5f fd 31 15 7a fd 41 fd 23 1a 77 70 31 09 fd fd fd fd fd 00 fd 3d 75 fd 56 fd 7b fd dd fd fd 6e fd 40 6d fd 27 fd 5c fd 77 37 01 fd fd 3d fd 17 71 fd fd 5c 07 fd fd 11 72 fd 25 fd ab fd 00 fd fd fd 44 fd fd 18 fd fd fd 57 3c fd fd 49 5c 76 fd 24 1d fd 28 fd 53 73 1a 42 63 5b 4f 38 04 fd fd 75 fd fd 64 48 fd 1a fd ef 00 42 52 27 3e fd 4f fd 41 78 06 fd 3a 17 74 46 fd 69 29 32 73 68 89 60 fd fd fd fd 54 3c 41 fd fd fd fd fd 6d 7b 22 4a fd fd 37 fd fd 73 4b fd 02 fd 7b 08 15 fd 2f fd 43 07 fd fd 5b 1e fd fd fd fd 09 fd 2b fd 71 5d 4a 23 fd 1f	R]T+o$AChs32;Dzu8y=1gC_1z#wp1= uV{n@m'\w7=q\r%DW<l\ v$(SsBc[8u dHBR'>OAx:tFi)2sh`T<Am{"J7sK{/C[+q]J#	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\JSDNGYCOWY.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\JSDNGYCOWY.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	5	1021	05 fd 7f 12 fd 3c fd 57 56 fd 05 fd fd 72 fd 5d 4e 7d 22 fd 7c 11 fd fd fd fd 00 7a 3e fd fd fd 1f 45 3d 35 1a 38 fd 78 fd 4e 04 fd 54 75 fd fd 61 fd 3b 4c fd fd 6e fd 1c 41 5a fd fd 1b fd 17 54 33 fd 4b 6e 50 43 fd fd 6c fd 4d 47 fd fd 3d 69 fd 2e 20 33 fd 10 fd fd fd fd fd 21 fd 3f fd 38 fd 3c 67 fd fd 55 fd 0b fd fd 91 fd 3b 44 fd 42 fd fd 3a fd 11 6f 5c fd fd fd fd fd 73 fd c9 7e fd 70 fd fd fd 61 fd 50 fd 17 fd fd 4d fd fd fd fd fd 79 65 45 fd fd 02 fd 73 fd 77 54 0a fd 15 fd 4d fd fd fd 5b fd 32 fd fd fd fd fd 3b 7a 7d fd 46 79 fd 67 fd fd 4e 01 fd fd 1d 02 57 06 fd 69 44 50 fd fd 18 57 61 5a fd fd 59 fd fd 7b 73 76 34 01 fd fd fd fd 1a fd 18 5e fd 1e fd 43 fd 2d fd 62 74 47 fd 50 fd 1c 61 fd fd 18 1c 19 6c 4c 3b 41 fd	<WVr]N}"|z>E=58xNTua; LnZT3KnPClMG=i. 3!? 8<gU;Do\s~paPMyeEsw T M[2;z}FygNWiDPWaZY{sv4^C-btGPalL;A	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI.docx	1026	256	fd 73 76 70 31 11 fd 67 fd 1e fd fd 4b 3a 28 fd 72 fd 74 fd fd 2d fd 27 28 24 fd 1f 27 fd 35 7e 6b 24 14 fd fd fd 59 fd 5e 59 29 4f 0e 12 fd fd 54 fd 3e 10 fd fd 50 3d 6a fd 50 fd fd 2f fd fd fd 66 79 63 fd 03 78 fd fd 31 fd 1b fd fd fd fd fd 2c fd 2d fd 5e fd fd fd 35 1f fd fd fd 2e fd 06 34 0e 64 fd 3e 0d 59 fd fd fd 74 fd fd fd fd fd 47 20 3e fd fd fd fd 11 fd fd fd 04 71 3a 43 3f 21 fd 02 70 65 fd fd fd fd fd 6e fd 3b fd 33 5d fd fd 76 fd 4e fd fd 0b 58 fd 5f fd fd 4b 36 9f fd 54 fd fd 33 fd 01 fd 74 fd 51 04 fd fd fd 48 62 55 fd 36 bd fd 34 7a fd 48 1b 42 fd 65 fd 48 05 42 4a 13 fd 14 fd 42 41 fd fd 20 fd 42 07 fd 4b 77 52 5a 5c fd 0a fd 3b 35 1e fd fd 34 5e fd 37 fd fd 64 fd 2e fd fd fd e2 fd fd 08 4d fd fd fd 1b	svp1gK:(rt- '($5~k$Y^Y)OTP=jP/f ycx1,-^5.4d>YtG >q:C?!pen;3]vN X_K6T3tQHbU64zHBHB JBA BKwZ\;54^7d.M	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.png	5	1021	fd fd 47 fd 79 0e fd 45 fd fd fd 0e 2c fd ad 65 fd 47 56 6b 4f 6b 18 fd fd 7e 11 0b 72 fd 3d fd fd 33 52 fd 1b 73 fd 34 4d fd 3b 35 fd fd fd fd fd 51 49 53 fd 0c fd 03 78 1d fd fd 5e 2d 48 58 fd fd fd fd fd 19 fd fd 01 fd 2b fd fd 01 65 1a 39 fd 46 35 40 47 46 fd 14 fd fd fd 29 6f 36 fd fd 27 5c 31 fd 46 1d fd 52 1c fd 2c 6e 0c 88 24 41 fd 28 1a fd fd 65 fd 4e 33 45 01 0f fd fd 61 6f 43 20 fd 0f fd 17 5b 88 fd 4e 7c 57 fd 61 fd 63 fd 5a 17 fd fd 62 fd fd 30 3a 08 fd 31 38 38 41 67 fd 69 13 10 78 fd 28 74 3a 1a 74 fd 43 fd 45 16 fd 47 fd 3d fd 3a fd 94 fd 34 07 72 2a fd fd 4c 71 fd fd fd fd 03 fd 69 04 fd 7b ab 0e 51 fd fd 75 5c fd 21 1e fd 60 fd fd fd 70 14 24 fd fd fd fd 3f 17 5d fd 46 fd fd fd 4b fd 76 75 37 06 fd 32 fd fd	GyE,eGVkOk~r=3Rs4M; 5QISx^-HX+e 9F5@GF)o6'\1FR,n$A(eN 3EaoC [N\| WacZb0:188Agix(t:tCEG =:4r*Lqi{Qu\\!`p$?]FKu72	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI.png	1026	256	4f fd fd 02 fd 33 3a 45 fd fd 46 51 fd fd fd 6f fd fd fd 37 fd 03 fd fd fd 1d 71 6e 26 4a fd 7b fd 45 fd fd fd fd fd 67 04 fd fd fd 02 fd 42 2e 00 1f 22 fd 76 fd 50 fd fd fd fd 28 57 fd fd 79 7b fd 6a fd 04 fd 43 64 fd fd 29 fd fd 1a 31 7a 0a 1c 2e fd 6a 25 46 58 fd fd 2c fd 45 fd fd fd fd fd fd fd 73 fd fd 41 fd 6f 18 fd 1c fd fd 27 fd fd fd fd 19 fd 47 fd 6b fd fd 24 fd fd 66 fd fd fd 40 19 fd fd 0f fd 1d 4b fd fd fd 4b fd fd 40 fd 4b 1f 53 fd 2a ac fd 51 4b fd 58 53 fd fd e0 fd 29 6e 13 40 1c fd 6c fd 65 5b 61 fd 71 72 68 41 fd fd 78 61 ba 47 13 29 21 fd 52 15 fd fd fd fd 21 57 fd fd fd 46 03 fd 66 08 63 29 fd fd fd fd 7e fd fd 36 2a 7a fd 20 26 fd fd 59 fd 4a 70 16 fd 22 23 4b 7a fd 35 fd 12 fd 4d 6d fd 5a 54 42 18 fd	O3:EFQo7qn&J{EgB."vP(WyjCd)1.j %FX,EsAo'Gk$f@KK@KS*QKXS)n@le[aqrhAxaG)!R!WFfc)~6*z &Yp"#Kz5MmZTB	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	5	1021	fd 60 fd 0e 7c fd 40 fd 64 2e 22 fd fd 38 18 fd 6e 2d fd 55 51 62 55 fd fd b2 1b 5d fd 78 fd fd fd 7e fd 7e fd 68 fd 46 1c fd fd 74 1f 64 fd fd fd fd fd 43 fd fd 71 2d 7f 2b 52 35 fd fd 06 fd 35 fd 59 08 fd fd fd 71 58 fd 63 fd fd 39 fd 71 17 fd 08 5a 78 8a 78 fd fd 13 62 fd fd fd 71 fd 37 77 fd 5d 6d fd fd 39 11 03 fd 37 06 01 fd 18 fd fd 58 fd 22 fd fd 26 7a fd 05 fd 47 fd 1e 2c 4a 71 fd 69 32 fd fd fd 3a 10 fd fd 5c 78 fd fd 2a fd 1f fd fd 26 fd 6b fd fd 52 fd fd 6d 42 27 fd e4 4e fd fd 29 fd 2e 2e 27 59 fd 40 66 17 44 52 51 fd 53 50 40 83 0c 2e 88 12 60 65 58 1b 1b fd d5 fd 42 fd 13 53 fd fd 34 07 49 33 fd 01 5a 1c 06 fd 6c fd 18 fd 09 fd fd fd fd 16 fd 3b 27 74 0e 61 5d fd 2a 17 76 fd fd fd 6b fd 26 e2 26 fd 57 51	`|@d."8nUQbU]x~~hFtdCq-+R55YqX cqZxxbq7w]m97X"&zG,Jqi2:\x*&kR mB'N)..'Y@fDRQSP@.`eXBS4I3Zl;'ta]*vk&&WQ	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	1026	256	fd 6b 2c fd fd 74 71 fd fd 21 79 fd fd fd fd 51 71 fd 96 2d 28 38 4d fd 51 fd 42 fd fd 48 11 fd 22 fd 56 fd 60 6c fd 67 fd fd 7a fd 7c fd 27 fd 43 41 fd 5c fd fd 14 67 77 fd fd 3d fd 07 73 77 1e 4d fd 3f 74 fd 74 fd 4f 3d fd fd 4e 2c 49 fd 7d fd fd fd 2c 75 0d 44 55 27 16 fd fd fd 91 1f fd 5d 77 2b 46 fd fd 3c 37 fd 37 fd fd 35 fd fd 34 fd 5d fd 49 fd 5a 48 fd 03 10 35 15 34 5c fd 27 fd 44 5e 3a fd 27 fd fd fd 00 fd 2d 47 fd 0a 61 00 29 fd 31 fd 5f fd fd 3f fd 3b fd 5b fd 0f fd 49 21 58 33 16 fd 6e 38 16 7d 62 6f 22 32 74 fd 04 fd fd fd 6a 02 10 fd fd 79 4d fd fd 7e 7d fd fd 24 fd 53 78 79 fd fd 35 0f 4e fd 01 fd 6f 33 42 6d fd fd fd 34 23 50 49 fd 6c fd fd 24 fd fd 20 9e 7a 7c 0f 77 fd 21 fd 3a fd 3b 58 fd	k,tq!yQ-(8MQBH"V`lgz|'CA\gw=wM?ttO=N,I},uDU']w+F<7754]IZH54\'D^:'-Ga)1_?;[I!X3n8}bo"2tjyM~}$Sxy5NoBm4#PII$zw!:;X	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ.docx	5	1021	40 3c 32 20 fd fd fd 3e 50 fd fd fd 38 fd 51 72 fd 48 fd 6a 56 fd 75 fd 34 21 fd 61 fd fd 7c fd fd 08 fd fd 47 fd 21 00 fd fd 6e fd 5d fd 04 02 fd fd 04 fd fd fd 58 44 6f fd fd 6f fd 2d 4d fd fd 25 fd 1f 54 fd 5b fd 50 12 fd 45 7b 32 fd fd 55 7e fd 1a 56 7f 5d 68 7d 2a 0d 76 41 16 47 52 11 05 fd 53 fd 2c 48 fd fd 0e 61 fd fd fd 3a 1c fd 14 fd fd 3d fd 17 35 1c fd fd 32 5d 02 2f fd 1b fd 32 43 11 fd fd fd 49 07 39 02 2f fd 00 66 03 fd fd fd fd 9b 76 fd 38 02 68 5f 19 3a 23 fd fd 64 fd 68 4b fd fd fd fd 16 73 fd fd f4 fd 2f 10 6b fd 75 fd fd 41 62 fd 0e 6c fd 76 7e fd fd fd 2a 2f 76 fd fd 22 31 fd fd 1b fd fd fd 3d fd fd fd 25 0c fd 2b fd 36 47 11 fd 07 05 fd 70 2f 78 0b fd 22 5f fd fd fd fd 35 27 fd 56 fd 65 fd fd	@<2 >P8QrHjVu4!a|G!n]XDoo-M%T[PE{2U~V]h}*vAGRS,Ha:=52]/2CI9/fvh_:dhK/kuAblv~*/v"1=%+6Gp/x"_5'Ve	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ.docx	1026	256	fd 28 67 fd fd 47 79 34 54 4d 65 3c fd 39 53 fd 69 0d fd 63 fd 71 fd 3c fd 0f fd fd fd fd 3a 43 fd fd 7f fd 0f 63 fd 4b 7a 17 5d 2d 4a fd 1c 42 6d fd 38 6e 0f fd fd 6a 4f 0b 59 fd 22 79 24 51 76 58 fd fd 6f 46 2b 2a 34 fd fd 64 67 fd fd 01 56 66 68 73 1c fd 06 fd fd 22 00 5d 30 3d fd fd 58 3b 37 3c 18 fd 58 61 3c 5a fd 27 fd fd 3f 17 49 19 12 3b fd 1c fd fd fd 50 7c fd 1f fd 57 51 60 fd fd 1a fd 6b fd fd fd 4c 6d fd 2f 56 fd 0c 53 11 6b fd fd fd 3e 35 fd fd ad 7d fd fd 21 2e fd fd fd 0a 7b fd 1b 1f 40 62 02 fd 4c 24 fd 5e 31 45 da fd 48 fd 71 54 63 fd fd 43 fd 6c fd df fd fd 54 4b 2e 5a 74 5e 79 72 44 53 6d fd 55 fd 35 1b fd 32 31 fd fd 55 1b 1c 47 19 6a fd 1d 70 fd fd fd 53 64 fd 5f 65 0e fd fd e8 ed ae fd	(gGy4TMe<9Sicq<:Ccz]-JBm8njOY" y$QvXoF+dgVfhs"]0=X;7 <Xa<Z'?I; P\|WQ`kLm/VSk>5}!. {@bL$^1HqTcCl TK.Zt^yrDSmU521UGjpS d_e	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS.png	5	1021	67 fd fd 1f fd 3c 39 fd 74 47 38 14 22 09 fd 21 12 22 03 3c fd 45 fd fd fd fd 06 fd 60 43 25 10 fd fd fd 27 fd 1d fd fd fd 69 fd fd fd 7c 07 11 fd fd fd 2b 38 fd 4f 70 0c fd 89 7c fd fd 32 7a 66 fd 3f fd fd 19 1b fd 2c fd fd fd 2e 7c 53 fd 77 fd fd 0c fd fd 1a 40 47 fd 44 fd fd 45 fd fd 7c fd fd fd fd fd 71 fd 7d 27 02 fd fd 42 27 fd 00 10 4f 22 24 fd 4c 59 fd fd fd 4f fd 36 1d 35 0e fd 02 16 fd 76 5b 5f 43 fd fd fd 2d fd fd fd 67 58 1a 02 38 75 25 65 14 58 50 fd fd fd 76 70 61 2e fd fd fd 16 54 fd fd fd 07 fd 58 fd 18 fd 17 7e 6c 1c 7d fd fd 36 28 fd 04 fd 0a 13 fd fd 68 76 fd 3d fd 58 fd fd 2a fd 99 49 fd fd 33 1e fd fd fd 70 75 58 3d 5e fd fd fd 3b fd 77 fd fd 0f 63 2e 07 19 fd 6e 7a 25 2a fd 4b fd 2f 17 09 fd 51 fd	g<9tG8"!" <E`C%'i|+8Op|2zf?,.|S w@GDE|q}'B'O"$LYO65v [_C-gX8u%eXPvpa.TX~l} (hv=X*l3puX=^wc.nz% *K/Q	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NEBFQQYWPS.png	1026	256	3e fd fd 44 65 48 0b 3a 36 fd 2b fd fd fd 76 30 56 73 72 fd 1f fd bb 65 fd fd 40 d7 1c d1 46 17 fd 24 2b 2b 32 0d 73 5f fd 65 44 3c 36 fd 51 fd 0e fd fd 08 fd fd fd 06 fd 05 fd fd 79 fd 14 fd fd fd 38 5c 47 57 20 3f 12 fd 01 fd fd fd 6b fd fd 25 18 73 16 3c fd 0b 73 29 b5 fd fd 32 fd 06 01 2d fd 26 fd fd fd fd 0e fd fd 3e fd 1f 18 fd fd fd 23 36 fd fd 10 14 fd fd 15 4f fd f2 00 fd 01 fd a9 40 2d 17 1e fd fd 68 fd 08 fd 09 fd fd 7e 03 fd fd fd 28 03 4d fd 11 fd 2f 50 fd 79 60 fd fd 2f 05 14 fd 63 1a fd 74 51 34 fd 2e fd 12 fd fd fd 3d 0c 64 10 fd fd 49 fd 22 73 0e 3f fd 61 4a 75 fd 2e fd fd fd fd fd 58 fd 38 fd fd fd 75 fd 5a fd fd 4e 17 fd fd 03 51 fd fd fd fd 6e fd fd 2a fd 41 fd 12 5e fd 1e 5e 4a fd fd fd 73 1d 4d	>DeH:+v0Vsre@F$++2s_eD<6Qy8\GW ?k%s<s)2-&>#6O@-h~(M/Py`/ctQ4.=l"s?aJu.X8uZNQn*A^^JsM	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	5	1021	de fd 52 36 fd fd 9e fd 3c 0b fd 3f fd fd 57 fd fd 58 fd 07 fd 55 14 0c fd 4b fd 19 6f 01 6e fd fd 48 5c fd fd fd fd fd fd d0 28 fd fd 2c 5b 48 4b fd fd 05 6e fd 02 3d fd 30 fd fd fd 7c 59 fd fd 17 16 41 fd 5a fd fd 3a 07 fd 36 25 fd 1c fd 41 7a 01 fd 0b fd 7b fd 70 fd fd 11 0c b4 39 1b fd 0f 79 fd 4f fd 0a 58 5b 03 fd fd 56 fd 75 50 fd 30 fd 01 11 51 fd c0 77 6d fd 2d fd fd 55 fd fd fd 2a 69 6f 46 fd fd fd 38 fd 12 1e fd 30 fd 0a fd fd fd fd 7c 51 67 4c 62 fd 0b 75 fd fd fd fd 6d fd fd 67 fd fd 15 fd fd 65 1c fd fd 76 fd fd fd 7a fd 5b fd fd 62 fd 51 1d 56 fd fd 4d fd fd 22 4f fd 67 fd 67 fd 1e fd 08 76 fd 2e 18 fd fd fd 70 fd 55 fd 70 00 1e 6b fd 7f 5d 3f 78 fd 42 fd 0c 2f fd fd fd fd fd fd fd fd 92 ca 19 6e 6b 76 7d	R6<?WXUKonH\(,[HKn=0|YAZ:6%Az{p9yOX[VuP0Qwm-U*ioF0|QgLbumgevz[bQVM"Oggv.pUpk]xBnkv}	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	1026	256	fd 40 fd fd 44 fd fd fd fd 3a 6e 61 fd 67 61 fd 1a 20 54 fd 70 7a fd fd fd 10 fd fd 51 0b fd 20 fd 7c fd 6e fd 12 fd 3e fd 59 fd 9d 20 1e 69 fd fd 0a 16 fd fd 58 69 43 fd fd 1c fd 04 fd fd fd 0e fd fd 04 fd fd 7a 29 fd 16 31 fd fd fd 29 37 57 fd 1f 22 fd 5f fd fd fd 38 1e 39 fd fd 23 fd fd fd d4 fd fd fd 1d fd 3a fd fd fd 5b fd 74 22 49 78 33 2e fd fd fd 51 03 66 74 fd fd fd 3d 49 76 fd fd 3b fd fd fd fd 64 7d fd fd 4f fd 19 fd 73 4a 41 53 55 62 75 fd 14 41 fd fd 24 54 fd 1a 58 40 2e fd 28 02 fd 65 37 fd fd 38 0a 69 fd fd 02 6e fd 38 fd fd fd 21 fd 57 fd 6b 56 76 10 fd fd fd 1d fd fd 4f fd 43 15 fd 4c fd fd fd 76 c0 59 7a fd 22 fd fd fd 4b fd fd 07 fd 36 37 66 fd 42 d7 fd fd 4e 11 6c 69 fd fd 54 54 53 7e 69 3c 41 1b 08 39 fd 4f	@D:nag TpzQ |n>Y iXiCz)1)7W"_89#: [t"lx3.Qft=lv;d}OsJASUbu A$TX@. (e78in8!WkVvCLvYz"K67 fBNliTTS~i<A9O	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	5	1021	fd 6f 03 77 46 fd 31 fd 79 6b 58 fd 3b 1a fd 00 fd fd 70 fd 35 08 fd 38 fd 0d 21 5b 11 fd 12 fd 4f 74 fd 34 fd 26 59 22 58 f2 fd 52 fd 72 2e 56 fd fd 36 35 fd fd 64 12 fd 1e 20 0e fd 4b fd fd fd fd 73 fd fd 49 32 fd 90 6d 50 fd c7 fd 7c 15 5b fd fd 46 79 fd 04 e1 fd fd 26 fd fd 40 3a fd 64 0b fd 69 fd 33 fd 29 1a 28 fd 0b fd fd 04 0f fd 65 6d fd fd 74 4f 60 fd 16 70 fd fd 45 fd fd 78 2b 6f 74 fd fd 70 67 fd fd fd fd 52 fd 23 2d fd fd 40 fd fd 6c 2e fd 58 28 04 06 fd 24 78 fd 6f fd fd 03 fd fd fd 68 5b fd 3b fd fd 13 5d fd fd 5f fd 7e 0e 1c fd 39 1b fd 17 fd 22 4c 54 29 fd fd 05 4b 18 fd fd fd 66 fd 4b 1a fd 3a 08 60 fd 4b 38 34 33 fd 5e 0f 04 fd 2f 4a fd fd 70 04 53 fd 37 fd 0e fd fd d9 51 fd 71 fd fd 12 79	owF1ykX;p58! [Ot4&Y"XRr.V65d Ks l2mP|[Fy&@:di3) (emtO`pEx+otpgR#- @I.X$oh[;_~9LT)KK:`K84 3^/JpS7Qqy	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	1026	256	78 5b 26 fd 54 fd fd 60 fd 57 fd fd fd 4b 36 76 89 73 5b 5f 04 fd 1b 57 fd fd 62 79 fd 03 fd 01 fd 6d fd fd fd fd fd 02 52 3d 56 fd 0c 01 23 fd 6c 02 26 fd 52 13 4b fd 5b 09 25 14 5c 14 fd 0b fd 30 00 36 73 2f fd fd fd fd fd 5c fd fd 5d fd fd 5b 20 0e 58 29 fd fd 10 fd 71 53 fd 72 6d 7e 26 fd fd 65 fd fd 5b 56 fd 11 fd 79 14 fd 77 fd 3b 0b 5e 78 fd fd 63 fd 49 fd 45 7e 57 fd 05 3b fd 1a 5f fd fc 17 fd fd fd 20 5c 53 1c 02 48 77 61 07 fd fd fd 47 30 fd 47 fd fd 1c 27 fd fd 7e fd fd 1f fd 65 34 fd fd 3e 71 29 fd fd 02 34 7f 42 06 0b 28 42 fd 0f fd fd 41 fd 4a 1b 5c 01 0e fd fd 7d 68 fd 1b 25 fd d3 12 46 fd 6e 5a fd 34 fd 4d fd 32 27 12 fd 33 10 40 42 fd 27 6f 24 53 77 7b c2 fd 67 fd 00 76 fd 08 fd 02 fd	x[&T`WK6vs[_WbymR=V#l&RK[%\06s\][X)qSrm~&[Vyw;^cIE~W;_\SHwaG0G'~e>q)4B(BAJ\}h%FnZ4M'3@B'o$Sw{gv	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\RAYHIWGKDI.pdf	5	1021	57 fd fd 6d fd fd fd fd 44 fd 1d 75 16 42 fd 79 fd 65 fd fd fd c2 4d 72 fd 7b 0b fd 59 44 14 fd fd fd fd 07 5c 6e 19 22 6b 40 74 48 fd fd fd fd fd 59 20 11 fd 33 55 6e 7a 49 51 2f fd 40 fd 26 fd fd 2b 5f 24 fd 12 fd 40 fd fd fd 0b 00 fd fd 5f fd fd fd 0a fd 22 fd fd fd 44 27 fd fd 55 19 fd fd fd 51 20 23 fd fd 0f 65 02 fd fd fd 18 fd 74 fd fd 64 2b fd fd fd 3e 36 fd 24 40 1c fd fd 6a 14 fd 00 64 fd 53 fd 2e fd 71 fd fd 64 1c fd fd 27 5e fd 06 1d 0b fd 40 fd 41 fd 33 c9 23 7f fd fd 12 37 2f 13 fd fd fd 1b fd 3a fd 57 fd 76 4a fd fd 55 1a fd 0d 7c 06 fd 7a 38 74 57 fd fd fd fd 7a 0a 72 1d fd fd 68 fd 74 49 fd fd 3f 19 fd 0c 05 37 1a 74 21 fd fd fd fd fd 03 fd 0a 20 45 07 fd fd 58 fd fd 36 44 9f fd 25 68 fd 7d 31 fd fd 10 fd	WmDuByeMr{YD\n"k@tHY 3UnzIQ/@&+_$@_"D'UQ#etd+>$@jdS.qd'^@A3#7/:WvJU|z8tWzrhtI?7t!X6D%h}1	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\RAYHIWGKDI.pdf	1026	256	fd 41 fd fd 5a 08 fd fd fd fd 5c 69 fd 62 78 fd 12 fd 7c fd 27 0e fd 72 fd fd 2b 4b fd 59 fd 5f 4e fd fd 5a fd fd fd fd 37 16 fd fd fd 49 e4 67 fd 3f fd fd 4c 10 fd 49 30 fd 45 22 fd 11 3e fd 3d 4e fd 0c 64 1c 5a 94 33 fd fd 20 21 54 fd 5a 4c fd fd fd 34 fd fd fd fd fd 1d 13 04 3e 18 fd 3a fd 1c 2b fd 43 21 2b 40 fd 3f fd 39 23 fd fd 0e 48 37 fd fd 19 08 4a 0c fd fd fd fd 26 5b 69 75 fd 4f fd fd 3d 3c 17 fd 7b 02 02 fd 0d fd 09 fd fd fd fd fd fd fd 56 fd 0f fd fd 0c 76 fd 3d fd 18 6b 7a 15 fd fd fd 02 1a 6a 1d fd 16 fd 11 0c 70 fd 26 53 53 76 40 fd 4b 30 fd fd fd ad 6b 03 35 71 1c fd fd 75 5d 46 fd fd fd 40 fd 50 61 1b fd 08 fd fd 15 03 fd 0e 47 fb fd 01 5b fd 5b fd 2e 43 79 fd 0c fd 24 76 5d 11 fd 60 24 fd 77 fd 6b 1b fd	AZ\ibx|'r+KY_NZ7Ig?LI0E">=NdZ3 !TZL4>:+C!+@?9#H7J& [iuO=<{Vv= kzjp&SSv@0k5qu]F@Pa[[.Cy$v]`$wk	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\RAYHIWGKDI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\RAYHIWGKDI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\SFPUSAFIOL.mp3	5	1021	fd 64 32 76 fd fd fd 37 fd fd fd 6f 74 2a 23 fd 75 36 18 10 fd fd fd fd 09 15 6d fd 54 8e 3d 0e fd 60 60 fd 17 fd fd 27 39 5f fd 64 76 fd fd 73 7f fd 01 fd 6d 32 fd fd 53 2f 0a fd 48 1c 1d fd 64 fd fd 67 53 15 65 fd 2c 15 60 1d fd fd fd 09 fd 14 12 fd 5e 49 fd 2f fd fd eb 34 fd 31 fd 32 17 fd fd 28 fd f7 fd 4d fd 13 fd 73 fd 36 09 7f 28 fd 78 fd fd 19 fd fd 59 25 55 28 fd fd 23 16 32 fd 0e 75 45 fd fd 32 fd 18 fd fd fd 16 fd fd 26 fd 24 fd 4c fd 64 30 60 02 fd fd 3c fd fd fd 26 37 fd fd 7a fd 18 32 fd 10 41 60 fd fd fd 67 0c fd 28 fd 9a fd 18 fd fd 2f 5b fd 3a fd 19 fd 17 42 fd 3c fd 36 23 fd fd fd fd 26 36 7a 63 fd 09 59 fd fd 7b fd fd 2a 0d e5 fd fd fd fd fd 57 7d fd fd fd 52 fd fd fd 19 3a fd 3f fd 8a 04 fd 02 43 6a 7c	d2v7ot*#u6mT=``'9_dvsm2S/dgSe, `^I412(Ms6(xY%U(#2uE2 &$Ld0`<&7 z2A`g(/[:B<6#&6zcY{*W}: ?Cj|	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SFPUSAFIOL.mp3	1026	256	fd fd fd fd fd 70 78 60 03 33 06 fd 38 0e fd fd fd 13 fd fd fd 0b fd fd 27 38 fd 5b 29 fd 4a 54 28 33 64 07 64 14 fd 68 fd 66 44 fd 3d 7a 40 2e fd 05 35 39 48 fd fd fd 59 fd 00 7c fd 1c 6d fd fd fd 68 7b fd 04 fd 4b fd fd fd 55 78 76 06 11 fd 06 24 fd 3e 48 48 2a 61 fd fd 4f 36 fd 59 10 fd fd b5 fd fd 12 ca fd 4c fd 55 57 3e fd 36 08 6c 12 fd fd 04 56 70 fd 16 11 fd 10 fd fd fd 58 fd 6d 4a fd fd fd 23 3d fd 59 fd fd 0d fd 2c fd 05 fd fd fd 71 fd 5b fd 68 08 c7 50 07 5f fd fd fd fd fd 3c fd fd 47 fd 38 73 fd 14 0a e2 fd fd 0d 3d fd fd 29 38 01 16 61 24 1c fd 3a fd 77 15 14 fd 42 55 fd 75 46 fd 1b a5 fd 12 fd 25 70 fd 7e fd f6 fd fd 45 fd fd 5c 30 fd 51 1e fd fd fd 08 3c 00 65 6c 1d 30 fd 03 2d fd 4f 3e fd	px`388[)JT(3ddhfD=z@.59HY|mh{K Uxv$>HH*aO6YLUW>6l VpXmJ#=Y,q[h P_<G8s=)a$:wBUuF%p~ E\0Q<el->	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SFPUSAFIOL.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SFPUSAFIOL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\SQRKHNBNYN.png	5	1021	53 95 fd 0c fd 10 6f 55 51 10 4c fd fd fd fd 19 00 fd 41 00 1e fd fd fd 59 33 fd fd 22 fd 70 e0 51 fd 3e fd 77 28 34 7b 0a fd fd 2c 4b fd 7d fd fd fd 63 05 09 4f 34 fd fd 30 fd 5a fd 57 6b fd 01 fd 1c fd 6c 23 fd 2b fd fd 1f 6f 09 fd 1f fd fd 21 fd fd 3a 35 63 fd 05 2f fd fd 52 2d 5c 75 19 fd 0b 27 1c fd 04 6e fd 50 fd fd fd 7f 66 fd 68 fd 64 fd 76 3d fd 7e fd fd 75 77 4b 43 30 fd 22 fd 57 77 51 30 64 fd fd fd fd fd 54 16 00 1d fd 41 fd fd fd 62 1b 0d 4c fd 5e 0d fd fd 37 fd 3b fd 5f 23 1c fd fd 38 fd 3b fd fd cc fd 3e fd 38 14 fd 46 02 55 fd 05 33 72 34 67 fd fd fd 13 fd fd 3b fd 79 44 7a fd fd fd fd fd fd 50 fd 4d 13 fd 11 fd fd 43 78 fd 76 56 fd 18 41 fd 06 61 46 fd 36 31 f1 fd 4f 76 6e fd fd 50 40 20 fd	SoUQLAY3"pQ>w(4{,K}cO40Wkl#+o!:5c/R-\u'nPfhdv=~uwKC0"WwQ 0TAb L^7;_#;>8FU3r4g;yDzPM CxvVAaF61OvnP@	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SQRKHNBNYN.png	1026	256	51 7e 69 21 fd fd 75 31 69 fd 0e 2f 4d 6e 3c 6a 5c 25 53 32 fd fd fd 5d fd fd 38 0d fd 0a 36 fd 6a 20 7c 2f 0b fd fd 2f 1f fd 1b 4f 23 6e fd 06 fd 26 61 6d fd fd fd 0e fd 7a 01 43 fd fd 7e 15 47 fd 09 5f 7c fd fd 06 fd 58 75 71 fd fc fd 7e 1e 55 6b 21 42 28 5f 06 fd 36 5c 47 58 fd fd 05 7f 24 fd fd 50 7f fd fd 03 29 fd 68 06 fd 25 18 a7 3b 38 fd 77 33 62 28 fd fd 1e 6f fd fd fd 71 25 3f fd 2a 43 fd 0d fd 4f fd fd 76 fd fd 29 44 0f fd 4c 03 fd fd 2f d7 fd fd 6a fd 1d fd 3b 15 1c 61 45 fd 4f 67 79 fd 5e 26 fd 2e 38 fd fd 2a fd 5b 2c fd 66 fd fd 4a fd 5a fd c6 fd 7c 54 fd 5a fd 70 7a fd 22 fd 3d fd 92 fd 3f 42 77 49 4a 64 fd fd 3a 1d fd 56 fd 17 2b fd cd fd fd fd fd fd 28 41 24 30 25 0e fd 3a 1d fd fd fd fd 53 53 7f fd fd	Q~i!u1i/Mn<j\%S2]86j |//O#n&am zC~G_|Xuq~Uk!B(_6\GX $P)h%;8w3b(oq%? *COv)DL/j;aOgy^&.8* [,fJZTZpz"=?BwlJd:V+ (A$0%:SS	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\SQRKHNBNYN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\SQRKHNBNYN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\UOOJJOZIRH.jpg	5	1021	fd 61 12 fd fd fd 79 2a fd db 51 56 09 fd 56 fd 19 fd fd fd fd 12 fd 4f 74 77 00 06 fd fd 41 fd 75 33 65 63 fd fd 44 fd ae 5b fd 2c d8 fd fd 70 1f 32 40 fd 29 fd 2e 69 39 3b 26 fd fc d5 7c 6d 33 5d fd 05 18 fd fd 01 1e 15 fd fd fd fd fd 09 49 76 6c fd 33 fd 29 fd 45 33 fd fd 62 42 fd fd fd fd 09 fd 00 fd fd fd 6c 96 13 fd fd 2a fd 11 fd 4b 1a 62 7b fd 21 2c 2a fd 2f 47 3b fd 16 6f fd 50 fd fd 7d fd 02 74 fd fd 2c 6c 55 77 16 fd 2a 18 29 fd 19 77 2a fd 0c fd 7d fd a7 1e 75 0b 16 fd 4c 1b 5a fd 2e fd fd fd 67 fd 4f 6a 2d 4f 61 fb fd fd 35 32 fd fd 6c fd fd 04 0d 31 0b fd 14 3d 3e 78 21 1d fd 00 fd 26 fd fd 43 fd 5a 27 fd 19 7e fd fd fd fd 41 fd 2e fd 18 13 fd fd 39 fd 67 72 5d fd 4a 5a da fd 3e 4e 57 fd 38 fd	ay*QVVOtwAu3cD[,p2@) .i9;&|m3]I vl3)E3bBI*Kb{!,*/G;oP}tlU w*)w}uLZ.gOj-Oa52l1=>x!&CZ'~A.9gr]J Z>NW8	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\UOOJJOZIRH.jpg	1026	256	fd 3c 15 fd fd fd fd fd 0f fd 17 fd fd 6f 56 5b 4d f3 01 34 fd 0c 6d fd 39 55 0f fd fd fd 5a 3c 2a 51 fd 07 00 68 fd 16 fd 40 fd fd 31 46 1f 09 6c fd 65 58 fd fd 5b fd 00 ed 0d fd fd fd 51 3d 47 21 fd fd 70 60 26 64 78 fd 28 fd 3d fd fd b1 6e fd fd 5b 22 ef 59 fd fd fd 50 fd fd 60 41 fd 5e 1c fd fd fd fd 48 3b fd 0d fd 4c fd 50 fd fd 70 72 0e 0c fd 0f fd 30 7a 72 fd fd 2b fd fd fd fd fd 21 fd fd 00 01 4d fd fd 2b fd 72 45 fd 6b fd 4c 36 fd 74 45 37 fd 5e fd 77 fd 0f 7b 54 6c b1 fd 77 fd 65 7a 09 fd fd 42 60 fd 35 07 fd fd 22 4e 35 45 fd fd 1e 17 44 fd 71 fd fd 0e 67 fd fd 44 4e fd 4f 49 fd 3b fd 77 0c 1d 6a 1d 56 59 fd 18 05 fd fd 07 fd 11 6b fd fd 6e fd 03 fd 3e 40 6a fd 7e 14 42 5a fd fd fd fd 04 1f 7d 7d fd 0c fd fd	<oV[M4m9UZ<*Qh@1FleX[Q=G!p`&dx (=n["YP`AH;LPpr0zr+!M+rEkL6tE7 w{TlwezB`5"N5EDqgDNOI;wjVYkn>@j~BZ}}	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\UOOJJOZIRH.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\UOOJJOZIRH.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.jpg	5	1021	fd 63 36 fd 30 7e 53 32 fd 1c fd 08 01 fd 69 fd fd 5f 74 fd 06 fd fd 41 fd fd 43 18 fd 66 4b 03 fd fd 56 02 fd fd 57 70 6b fd 66 4a fd 47 23 4a fd 07 fd 43 fd 63 fd fd 41 fd 41 64 70 fd fd fd f1 39 78 36 1b 15 7c fd 20 04 1a fd fd 0a 7a fd 72 75 b9 2c 00 fd 3b 33 46 d8 58 0a fd 71 66 36 fd fd 2c fd 2e 73 fd 6e fd 72 fd 6d 4a fd fd 19 fd 14 fd 55 fd 5f 60 fd 02 19 fd fd 1d fd ee 57 fd 56 fd 74 fd 10 fd 5b 54 1b fd 66 6a fd 7b fd 61 6c 01 46 fd 1b 4c fd fd 28 fd 02 18 3d fd 1f 75 fd 32 75 77 26 fd fd 6a fd 3d fd fd 36 fd fd fd 44 6c 44 1d 1a fd 1d fd fd f2 56 fd fd 66 2b fd 32 02 fd fd fd 38 44 3e 0d fd 19 40 fd 74 fd fd fd 0b 65 fd fd 5a 48 fd 11 51 0a 14 50 fd 23 45 fd fd 5e 06 51 72 fd fd fd 09 fd 23 fd 08 fd fd	c6~S2i_tACfKVWpkG#JCcAAdp9x6| zru,;3Xqf6,.snrmJU_`WVt [Tfj{al FL(=u2uw&j=6DlDVf+28 D>@teZHQP#E^Qr#	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WKXEWIOTXI.jpg	1026	256	63 16 fd 39 fd df fd fd 09 fd 7b fd fd 1c 24 0a 70 26 0b 71 fd 79 fd fd 78 03 4b 02 fd 07 fd 77 15 2c fd 25 10 27 fd 05 fd 7c fd 76 fd fd fd fd 32 50 fd fd fd fd 43 fd 20 26 fd 2d 1b 55 11 fd 31 fd fd fd fd 08 fd 42 6b 74 20 fd 18 fd 22 1d 4d 32 fd 79 6a fd 76 3b 3e 3f fd fd 28 74 fd 09 38 1c 40 42 37 3f 28 fd 7e fd fd fd 23 fd 74 fd 5a fd fd 37 fd 6c fd 06 fd fd 08 fd 09 fd 50 fd fd 7c 33 0c 2f fd 72 3d 7c fd fd 1f 22 7c 63 0e 34 77 7e 55 fd 4d fd 76 fd 2f fd ad fd 66 fd fd 13 fd 4b 3e 77 fd 61 29 0d fd 34 fd fd 75 47 fd 66 6c 59 23 23 fd 1b fd 42 63 4d 5f 5e 48 87 fd 6c 28 4b 4d fd fd 6c 28 27 fd 6a 2e 03 fd 0f fd fd 25 51 fd fd 58 02 fd fd 3c bb fd fd 1a fd fd 54 fd 5d 6a fd fd 16 fd fd 37 69	c9{$p&qyxKw,%|v2PC &-UBkt "M2yjv>?(8@B7?(~#tZ7l|3/r|"|c4w~UMv/fK>wa)4uGflY##BcM_^l(KMl('j.%QX<T]j7i	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.mp3	5	1021	fd 3f 7c fd fd fd 0c fd 37 fd 70 fd 55 fd 2e fd 79 fd 51 18 01 fd 22 fd 33 4e 56 28 41 35 fd fd fd 43 73 2e fd fd fd 3a fd fd 7d 70 fd fd 76 fd 69 fd fd fd 43 16 fd fd 0f 6f fd 64 75 1c fd 7d 07 fd fd 03 fd fd 34 58 55 0a 7d fd fd fd fd 0a fd fd 5a fd 05 fd fd 0e fd 99 23 fd fd 5e 17 fd 6f 57 4c fd fd fd 2d fd 64 fd fd 6b 3a 47 fd fd fd fd fd 6b fd 2e 77 7e 70 fd 54 49 13 fd 6f 14 fd fd 65 64 fd fd 7e 7d fd 36 7b 6a fd fd 2d 65 74 79 fd 49 fd 08 40 fd 75 fd fd 5c fd 0a 14 fd fd 37 5f 09 fd 5c 59 fd fd fd 71 fd 10 fd 39 fd 26 fd 39 fd fd 29 fd 05 a8 17 fd 20 59 74 d9 41 46 2b fd 23 fd fd fd 16 26 fd 57 fd fd fd fd 26 0f fd 2e 67 fd 63 fd 27 49 2d fd fd 46 5e fd fd 10 2b 1d 2c 36 fd 76 fd fd 41 35 46 28 70 3d fd fd fd 0f	?|7pU.yQ"3NV(A5Cs.:}pviCodu}4XU}Z^oWL-dk:Gk.w~pTloed~}6{j-etyI@u\7_\Yq9&9)YtAF#&W&.gc'I-F^+,6vA5F(p=	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WKXEWIOTXI.mp3	1026	256	fd fd fd fd fd fd 00 fd 38 fd 32 fd fd 50 fd fd 21 5b 1e fd 0e fd fd 41 fd 44 43 28 fd fd 3c 41 fd fd fd 3b 76 fd fd fd fd 3f fd fd 35 4c fd fd 38 fd 0f fd 4d fd 67 fd 2f 0a 7d 1d 6c 37 fd 18 37 c0 2c fd 4e 54 fd 74 53 fd fd 18 7e fd 14 fd 1f fd 55 49 4c 58 fd 34 6c fd fd 4b fd fd fd fd fd 20 c1 fd 1e fd fd 2a 36 fd 0d 5f 35 fd fd 67 fd 35 57 78 43 c9 79 7e 71 2e fd 07 3b fd fd fd fd 0a 54 76 74 3f fd fd 71 fd fd fd 0e 0d 36 fd 2d 4c fd 14 63 fd 00 17 fd fd 25 fd fd 22 48 fd fd fd 64 14 fd fd 2a fd fd 0b d4 5d fd fd fd 5b fd fd 01 fd fd fd 1c fd 6a 72 fd 08 fd fd 35 fd 1f fd 2d 12 fd 3c 4f 4d fd fd fd fd 33 5d fd fd 04 2d 00 7d 3d fd 14 fd fd 53 4f fd fd fd 1f fd fd 64 fd ef 09 fd fd 3b 21 4b 57 16 45 fd 31 44 32 47 fd	82P![ADC(<A;v? 5L8Mg/}77,NTtS~U ILX4lK *6_5g5WxCy~q.;Tvt?q6-Lc%"Hd*][jr5-<OM3]-}=SOd;!KWE1D2G	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.pdf	5	1021	0e 0b fd fd fd 52 fd fd 2b fd fd 78 fd 02 7e 22 fd fd fd 25 fd 13 fd fd 60 4c fd 1b fd 64 46 fd fd fd fd 53 13 fd fd 5e fd fd 32 7d 19 fd 3d fd fd fd 23 29 03 39 fd 17 fd 25 65 fd 6b 30 fd fd fd fd 41 59 0c 79 0a fd fd fd 6d fd 20 fd 2a fd 2f 3b 14 fd 55 48 02 29 56 21 fd 5d fd 64 7b fd 02 0a 0e 37 30 fd 63 1b fd 15 fd fd fd fd fd 1d fd 06 fd fd 20 38 fd 47 fd 46 66 56 fd 0f 29 09 24 fd fd fd fd fd fd fd 64 fd 04 07 fd 7d fd 02 41 fd 1c 55 fd 3a 3d 35 fd 22 14 fd fd fd fd 3f 6e 12 fd 15 24 fd 6e 3a fd fd 65 72 6e 4c fd fd 68 fd fd fd fd 3a fd 09 fd fd 1a 5d 0b 78 fd fd d3 fd fd 18 fd 32 fd fd 56 fd 54 5c fd fd fd 5b fd fd 55 fd fd fd 09 fd fd fd fd 13 1d 25 fd 71 fd 44 3e fd 42 fd fd 79 fd fd 42 fd 76 fd 3b 4a 38 50 14 a8 01 70 5f fd fd 7f fd	R+x~"%`LdFS^2}=#)9%ek0AYym */;UH)V!]d{70c8GFfV)$d}AU:=5"?n$ n:ernLh:]x2VT\ [U%qD>ByBv;J8Pp_	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WKXEWIOTXI.pdf	1026	256	fd 73 20 fd fd fd 1d fd fd fd 09 fd 20 1c fd 4b fd fd 70 04 fd fd fd 0c fd fd fd 65 fd 28 fd fd fd 2a fd fd 02 ed 0e fd fd 6d fd fd 53 fd fd fd fd 62 fd 36 fd 7b 0b fd fd 6d fd 68 fd 6b 12 7e fd 2e fd 36 fd 62 fd 25 03 43 3b 13 5a 47 0a 68 46 fd fd fd 43 fd fd fd fd fd fd 58 4a fd 45 59 fd 6f 57 fd 5c 63 fd fd fd fd 74 fd 15 fd 44 0e fd fd fd 30 7c 05 1a 14 fd fd fd 32 fd 5b fd 0c fd 1c 6d fd fd 7c fd 6b 06 72 3e 3a 69 53 fd 42 fd 5d 38 75 fd 2a fd fd fd 1c fd 7a fd fd 0b fd 5f 69 fd fd 3d fd fd fd fd 58 fd 7c 65 55 53 2f fd fd 32 fd 26 43 38 fd fd 3b 0f 57 52 23 2b 28 fd fd 6c 5a fd 3e 61 18 66 fd 63 fd fd 44 78 fd fd 5c 7d 6e 52 fd 0b 38 fd 61 f6 0b 77 fd fd 6f fd 5f fd fd fd fd 4a fd fd 29 fd fd 3c fd fd	s Kpe(mSb6{mh~.6b%C;Z GhFXJEYo W\ctD0|2[m|kr>:iSB]8u*z _i=|eUS/2&8;WR#+ (lZ>afcDx\}nR8awo_J)<	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WKXEWIOTXI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	5	1021	49 fd 75 fd fd 5a 16 fd 59 74 4a 41 fd 4d 3c 55 34 fd 02 41 fd 14 fd 09 75 fd fd fd fd fd 62 fd fd 2c 21 47 62 33 fd 5d fd 74 fd fd 2a 04 41 28 fd 0d 77 11 01 fd 38 fd 02 fd fd 36 07 22 53 08 fd 32 4b 44 fd fd fd 78 61 fd 4d 5c fd fd 5f bf 78 fd fd 4f fd 72 fd 39 fd fd 2b ec 1f 2e 4d 27 fd 3b fd 37 2c 6a 75 7c fd fd 77 4f fd af 5d 38 fd 3a 04 39 2b fd fd 54 59 fd fd 2c fd 53 75 fd fd fd fd fd fd 40 fd 7f fd fd 77 47 20 fd 6c db 40 fd 1d 45 fd 1f fd fd 79 43 25 01 44 fd 3b 10 fd 40 fd fd fd fd fd 08 fd fd fd fd 32 d3 0a 6f fd 4d fd fd 77 fd 56 59 fd 6d 5f 03 fd fd 1e 02 0e 46 fd 5c fd 0b fd e0 fd 2f fd 60 1b fd 62 fd fd 18 62 64 03 58 65 19 fd 6f fd fd 66 57 7f 3b fd 6d 00 fd 30 fd 2c fd fd fd fd fd fd 7b 4d	IuZYtJAM<U4Aub,!Gb3]t* A(w86"S2 KDxaM_xOr9+.M';7,ju|w O]8:9+T,SuwG l@EyC%D;@2oMwVYm_ F\`bbXeofW;m0,{M	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX.docx	1026	256	65 59 1e fd 50 0d 3b 04 fd fd 4a 57 2c 35 fd 75 5f 52 fd fd 4f fd 12 9d 35 7d fd 5b 03 fd 33 fd 71 fd fd fd 12 fd 61 75 fd 13 56 11 fd 53 fd fd fd 63 fd 06 fd 35 7d fd fd 3c 7e 23 fd 42 7e fd 71 51 fd fd fd fd 53 fd 45 fd 6f 25 4f 57 fd fd fd 42 54 67 6d 0b fd 1e fd fd 1e 1f fd fd fd 2a fd fd fd fd 5d 25 33 11 fd 06 fd 1a 34 64 fd 4c 3d 4d 56 63 fd 58 38 fd fd 48 fd fd 22 1f 73 23 fd fd fd 0a 3f fd 13 75 45 fd 24 fd fd 28 fd 13 5e 1f fd 0f 22 fd 3d 35 11 00 fd 5a 55 fd fd fd fd 0a fd fd 3b fd 07 56 1e fd 58 fd fd fd 0b 77 fd 23 0a 65 fd fd fd 37 7a 14 48 26 fd 06 fd 1a 68 fd 3f 61 fd 55 61 3e 77 fd 77 4e fd 64 fd 3d 79 3c fd 62 fd 71 4a fd fd fd fd fd 45 5d 07 fd fd fd fd fd 6f fd fd fd fd 21 5f 3d 59 fd 01 34 44 67 20 7f 27 fd 78 54	eP;JW,5u_RO5}[3qauVSc5}<~#B~qQSEo%OWBTgm*]%34dL=MVcX8H"s#?uE$(^"=5ZU;VXw#e7zH&h?aUa>wNd=y<bqJE]o!_=Y4Dg 'xT	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.pdf	5	1021	fd 44 fd 78 fd 40 fd 41 72 fd fd fd fd fd fd 65 5f 70 fd fd 79 fd 60 fd fd 0b fd fd 65 fd fd 6d 2a 0d fd 23 fd fd fd fd 31 fd fd 67 70 fd 64 24 fd 0c 65 5c fd 74 0c 33 0c 70 fd 57 1d fd 7e fd 43 fd fd fd fd 69 5d fd 40 fd fd fd 6c fd 4a 16 29 fd fd 57 fd fd 12 fd 4f 45 fd fd 47 fd 13 fd 07 fd fd fd fd 26 fd fd 1c 17 fd fd 79 57 54 fd 10 01 fd 11 2c fd fd fd 4c 2c fd 1b 69 1b fd fd 1f fd 70 5e 36 5b 7e 06 20 51 6b fd 2c 2a fd 0b 19 61 0e 38 fd 67 fd fd fd 29 fd fd fd 03 63 fd 34 fd fd 14 73 fd f3 fd 7e fd 34 fd 36 28 24 1d fd 0f 2c fd fd 32 32 3f b4 25 fd fd fd 58 0c fd fd fd fd 65 54 fd fd 09 2e 47 fd fd 0f fd e3 7e 5c fd 4f fd fd 13 fd 30 fd 06 fd fd 78 fd 2a 7e 34 20 68 18 1a 43 fd fd fd 48 f3 61 fd 33 fd fd fd ea	DxArepy`em*#1gpd$e\t3pW~Ci]@lJ)WOEG&yWT,L,ip^6[~Qk,*a8g)c4s~46($,22?%XeT.G~\O0x*~4 hCHa3	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX.pdf	1026	256	0b fd 60 fd fd fd 45 fd 0f 62 40 09 fd 56 fd fd 33 45 49 0e 1d 41 fd 65 fd fd fd fd 29 fd 33 7e fd fd fd 4c 4d fd 2d fd 10 04 fd fd 31 14 fd fd 48 fd 72 06 35 fd fd 21 fd fd fd 04 fd fd dc 85 fd 2c 62 0d 26 a4 0d 16 7f fd 59 fd fd 3c fd 2e 3b 60 6e fd 48 fd 44 fd 26 fd 00 6e fd 2c 6e 6f 0b fd 57 fd 75 b4 1c 66 fd 2e 6e fd 37 0b fd 56 37 0c 63 02 03 fd 38 5e fd 4d 04 3b 2e fd 06 3a 1a fd fd 90 6d 2d 21 15 fd df fd 3f fd fd 52 fd fd 6c fd 51 fd 54 fd fd 4f fd 58 fd 09 fd 77 2d fd fd fd fd fd 01 fd 75 fd 04 02 4a fd 55 71 1a fd 47 fd 72 12 67 fd 74 fd 1b fd 1f 2f 79 62 fd 3e 19 1a 45 a5 54 fd e6 1d 70 6d fd fd 3d 30 69 c3 4e 1a fd 70 fd ab 21 fd fd fd 55 19 fd fd fd fd fd fd 31 62 0d 2e 1e fd fd 4e fd 2a	`Eb@V3EIAe)3~LM-1Hr5!,b&Y<.;`n HD&n,noWuf.n7V7c8^M;.:m-!?RlQTOXw-uJUqGrgt/yb>ETpm=0iNp!U1b.*	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.docx	5	1021	fd 11 51 17 fd 01 20 3c 4e 1c 3f fd 0f fd 34 fd fd fd 32 c7 4a 26 fd 34 40 fd 18 fd 5a 6f fd fd ff 1a 46 71 23 3b 1a 64 fd fd 42 fd 7b fd fd fd 09 4b fd 05 fd 04 34 4c fd 68 fd 3b 2c 16 fd 15 75 44 53 fd fd 66 b3 fd 35 5b fd 1a fd 4b fd fd 22 1b fd 71 fd fd 04 fd fd 2f a5 50 3d 37 64 fd fd 3a fd fd fd 11 2b 4a fd 7a 7f 51 fd fd fd fd 11 11 fd fd fd 22 fd 0c fd fd 52 25 60 4b fd 01 76 69 76 7e fd fd 27 fd fd 26 3a 5b fd 79 7b 12 23 79 34 fd 02 3d fd 35 fb fd 21 fd 4d 1b 57 7b 59 66 fd 35 fd 68 fd fd fd 59 59 6c 0f 41 fd 5d 53 fd 47 fd 4a 05 fd 32 3d fd 2a fd 27 55 7b fd fd fd 7f 29 61 7f fd fd fd 13 6d 58 fd 61 fd fd 37 67 4e 1a 7a 40 fd 73 fd fd fd 47 02 fd 7b 1c 3e 01 fd 97 fd 0b 0c fd fd 63 fd 32 18 36 2e	Q <N? 42J&4@ZFq#;dB{K4Lh;,uDSf5 [K"q/P=7d:+JzQ"R%`Kviv~'&:[y{y 4=5!MW{Yf5hYYlA]SGJ2=*'U{}amXa 7gNz@sG{>c26.	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW.docx	1026	256	fd 70 fd fd fd 3d 2a fd 31 fd 28 fd 38 21 3f 2d 0b 2c 6b 1d 60 41 13 05 9e fd 2e fd 01 fd 23 29 7c fd 5e fd fd 64 fd 66 fd 68 fd fd 69 fd 4b 5d fd 3d fd 77 16 3c fd fd 1e fd fd 01 fd 0d 48 6c 75 69 2a fd 1f fd 37 fd c9 8e 48 60 08 2e fd 69 1d 07 62 fd fd 1b 4f fd 67 fd 3b fd 12 31 21 6e 4b 54 fd 03 fd fd 0a 38 9d fd fd fd fd fd 1b 60 49 0f 06 fd fd 54 fd 13 fd 19 3e fd 5b fd 25 00 53 fd 42 34 fd fd fd 55 fd 14 fd 18 68 fd 2e 2d 02 fd 17 aa 5c fd fd fd 54 fd fd fd fd 11 56 fd 6d 00 fd 47 fd fd 7a 26 fd 62 52 fd 12 57 fd fd 50 fd fd fd 3d fd 22 fd fd 58 48 fd fd 75 1a fd fd 54 fd fd fd 3d 4e fd 33 fd 64 fd 78 fd 1a fd 4a fd 6b 7b 1c fd 59 7e fd 52 5b fd 8c fd 5a 55 fd 03 1b 58 fd fd 0c 69 fd fd fd 75 2b 63 fd	p=*1(8!?- ,k`A.#)|^dfhiK]=w<Hlu i*7H.ibOg;1!nKT8`I> [%SB4Uh.-\T VmGz&RWP="XHuT=N3 dxJk{Y~R[ZUiu+c	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.jpg	5	1021	fd 4e fd fd 03 fd fd fd fd 21 64 fd a2 60 fd 37 20 fd fd 17 fd 20 31 14 78 fd 50 63 fd fd fd 1f fd fd 6a fd fd 5b fd 51 23 fd 7b fd fd 10 fd 51 fd fd 5a 28 fd 12 57 fd fd 3a fd 49 4d fd fd 09 4d fd 04 05 fd 7f fd 34 01 fd 55 fd 4b 43 fd 76 fd fd fd 48 fd fd 34 41 fd 17 3e 79 fd 7f 49 53 2c fd fd 24 fd fd 36 fd 2f fd 21 a8 fd 1b fd 7a 47 4c 66 fd fd f4 7d fd 86 3e fd fd 11 fd 64 fd 2b 27 7d 51 4f 31 08 fd fd fd 44 59 21 fd 05 fd 04 5e 44 fd fd 31 67 4e fd 0d 47 fd 78 10 23 fd fd 53 11 80 75 fd 51 50 14 fd fd fd fd 74 fd fd 04 fd 68 14 69 fd 64 0d fd fd 29 03 6c 20 fd 00 5c 2f 61 fd fd fd fd fd 4e 5f fd fd fd 3f 2c 51 fd fd fd fd 3e 4b 3e 10 47 61 68 fd 4c 00 63 1d fd 23 76 25 fd 5e fd 1c fd 4b fd fd 14	N!d`7 1xPcj[Q# {QZ(W:IMM4UKCH4 A>yIS,$6/!zGLf}>d+'}QO 1DY!^D1g NGx#SuQPthd)I \/aN_?,Q>K>GahLc #v%^K	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW.jpg	1026	256	fd fd fd fd fd 5c 7f 0b 09 ff 40 fd fd fd fd 57 03 0f 1f fd 6d 7b fd 0b 3b 76 21 64 fd 68 30 11 fd fd 76 2e 17 44 02 44 4a 16 0e fd fd fd 59 fd 5d 49 6b 6c 30 62 1f fd fd 6d 0b fd 4b fd fd fd 13 fd 2b 43 fd fd 76 0e fd 45 fd fd 33 fd 35 03 05 4f fd 09 fd fd fd 42 fd 22 02 60 fd fd b2 fd fd fd 18 fd fd fd fd 6a 29 b2 fd fd fd fd fd 10 fd fd fd 4b fd fd 6c fd fd 5d 2c fd fd fd fd fd 08 fd 41 fd fd 2e fd fd fd fd fd fd fd 52 fd fd 57 fd fd b2 30 fd 23 fd fd fd 40 fd 12 00 fd fd 4c 3f fd 77 fd 3a 2c fd 40 1b 11 fd 76 5c 28 0d fd fd fd fd 41 10 37 11 26 5a 73 fd 41 fd fd 1a fd 43 40 fd 79 fd fd 08 09 65 3c fd 47 fd 7a 60 fd fd fd 07 fd 13 3e fd 28 0f 4e 2d fd 06 2f 51 25 fd 62 03 5f 07 4a fd fd fd 1e fd 0f 5a fd fd 36 48 78	\@Wm{;v!dh0v.DJY]lkl0bm+CvE35O B"`j)Kl],A.RW0#@L?w:,@v\(7&ZsA C@ye<Gz`>(N-/Q%b_JZ6Hx	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	5	1021	2d 63 60 fd 73 3c 10 4b 25 fd 7c fd 10 fd 12 fd fd 3a 04 5a e1 fd fd 66 fd fd 56 3e 14 61 fd fd 61 72 65 fd fd fd 31 52 fd 01 fd 4b 7a fd 57 fd fd fd 2c fd 66 fd 14 fd fd 31 fd fd 03 fd 43 fd fd 78 fd fd fd 03 30 1d 4a fd 3c 2e 19 5f fd fd 1b 23 3a fd 8e 7a fd fd 14 0e fd fd 76 26 fd 06 02 fd fd fd 59 fd 5d fd 6f fd 1f 42 49 21 fd fd 0d 3d fd 50 fd 5d 5a fd 5c 18 fd fd 7e fd 4d fd fd 70 44 26 5d fd 7c fd 19 3a fd 6e 45 fd 6d 4d fd 49 fd 6c 2a 6b 0b 19 63 16 fd 79 63 fd 7e 60 fd fd 7e fd fd fd 23 fd fd 64 5e 26 fd 28 66 02 fd 73 fd 0d 42 fd fd 62 f9 72 57 4e fd 2f fd 09 46 fd 0b 38 71 67 6d 9c fd 3c 44 fd fd 3a fd 54 fd fd fd fd 7d fd fd 1b 7a fd fd 47 24 4a 29 2d 26 79 33 00 fd 2c fd fd 6e 03 fd 0a 09 fd 29 62 15	-c`s<K%|:ZfV>are1RKzW,f1Cx0J<._#:zv&Y]oBI!P]Z~MpD&]|:nEmMIl*kcyc~`~#d^&(fsBbrWN/F8qgm<D:T}zG$J)-&3,n)b	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	1026	256	60 fd 0b 4c 05 fd 28 27 3a fd 6e fd fd fd fd fd 52 6f fd 2b fd 0d fd fd fd 65 42 fd 59 59 fd fd 21 fd fd fd 0d 50 fd 50 46 7e 1b fd fd f0 51 fd fd 69 fd fd a2 42 fd 28 77 fd 19 fd fd fd 51 59 c9 25 53 fd 26 4d fd 51 fd fd 0c 66 7f fd 32 03 fd 13 fd fd 6e 27 16 fd fd fd 2a fd fd fd 59 fd 3b 53 61 3d 67 45 61 fd fd 74 64 0c 01 fd 6b 73 04 fd 1a fd fd fd 0d 20 06 fd 9f 76 fd fd fd 7c fd 77 fd fd 76 31 fd fd fd fd fd fd 7b fd fd 1d 18 01 fd 23 fd fd fd 1d fd 2a 2d fd fd 1d fd fd 6b 4d fd fd 68 fd 0d fd fd fd 1a 4a 12 fd fd ae 32 12 fd 4a 8a fd 1a 2c 2e 48 fd 52 fd 2a fd 2b 71 fd fd 55 5f fd fd fd 27 6d fd fd fd 48 03 fd fd 03 78 0e fd 78 fd fd 5a c6 fd 02 fd 72 20 4a 77 fd fd fd 42 fd fd 73 4b 0f 2e 1b 1a	`L(':nRo+eBYY!PPF~QiB (wQ%S&MQf 2n'*Y;Sa=gEadks v|wv1{#*-kMhJ2 J,.HR*+qU_'mHxxZr JwBsK	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	5	1021	fd fd 13 4f fd 75 fd 75 fd 28 4a fd 23 fd 63 4d fd 2e 59 30 fd 7b 35 16 fd 55 51 42 69 48 53 fd fd 77 69 fd 50 52 fd 42 fd fd 1d 6a 3a 41 fd 23 fd 5f 55 53 fd 38 fd 06 22 fd fd fd fd fd 28 28 fd fd 6f fd 61 52 fd 0e 3a 1c fd fd fd 23 fd fd fd 04 fd 4f 5f 47 fd fd fd fd 1d 4b fd fd 21 5f fd 85 fd fd fd bd fd 66 fd fd 2e 6e 3c fd 34 44 fd fd fd fd 06 37 fd 54 fd 60 54 fd 0b fd 74 fd 01 72 54 f7 3f fd fd 43 6e 0e 26 12 fd fd 5c 39 fd fd 14 4e fd fd 39 58 fd fd 37 1f 47 71 68 42 fd 7b 4d 50 fd fd 3c fd 04 65 2a fd 1c fd 00 09 fd 4c 25 58 69 c5 fd 28 7c 02 fd 7f 43 fd fd 54 fd fd 12 4a 74 6f 42 fd fd fd 49 14 fd 58 fd 7b fd 43 68 fd 61 fd 1a fd fd fd 1d 74 09 fd fd 51 01 52 79 fd 2a 7a 60 36 44 11 3c 61 fd 16 00 fd fd fd fd	Ouu(J#cM.Y0{5QBiHSwi PRBj:A#_US8" ((oaR:O_GK!_f.n<4D7T`T trT?Cn &\9N9X7GqhB{M<e*L%X i(|CTJtoBIX {ChatQR*z`6D<a	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	1026	256	31 6e 23 17 2f fd fd 51 fd fd 1f 70 18 fd fd 1c 7d 68 64 fd 7f 2c fd 0a 1e fd 24 fd fd 91 6a fd 6c fd fd 0d 59 fd 76 fd fd 59 fd fd fd 41 fd 24 fd 64 58 fd 2d fd fd 4c fd 13 fd fd 43 15 fd 18 40 fd 09 fd 0f fd fd 7c fd 48 fd fd 39 36 7a 02 f3 fd 00 fd 6f 0f fd fd 30 fd fd fd 58 fd 2d 51 24 fd fd 66 48 38 67 fd fd 1a 07 fd 3b 0d 37 fd fd fd fd 01 fd 05 78 fd 29 fd fd fd 52 76 fd 3b 0f fd fd 1a fd 57 fd 1e fd fd 39 fd fd fd 6b 4f fd 76 48 fd fd fd 38 fd 68 6a fd 51 6e 82 fd fd 20 57 58 fd 32 6d 0f fd fd fd fd 14 fd fd fd 14 fd fd 36 fd fd fd 1f fd 0e 4b 77 fd 43 73 fd 50 12 fd 40 fd 00 fd fd 20 75 fd fd fd fd 79 48 fd 7b 39 fd fd 7e 69 fd 6e fd fd 6b fd 6f fd 7e 0f fd fd 17 28 2e 6e 64 fd 3d 7e fd fd fd 5b 21 fd 25 fd 0e fd	1n#/Qphd,$jlYvYA$dX-LC@|H96zo0X-Q$fH8g;7x)Rv;W9kOvH8 hjQn WX2m6KwCsP@ uyH{9~inko~(.nd=~[!%	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.jpg	5	1021	60 fd 7e 46 31 50 fd 5b fd fd fd 57 fd 58 7e a1 09 52 7c fd 6a 2c 5a 1c 72 26 fd fd 75 18 fd 5c fd 1b 40 39 fd 80 fd fd 6c 0a fd fd 7e 71 fd 7b 7b 0d 6c 40 fd fd fd fd 0f fd 03 10 6c fd fd 7f 06 3e fd 7a fd fd 71 22 fd 51 fd fd fd 7a 2e 1a fd 3d 4a fd 2f 22 fd 6c fd 04 fd 3f fd 35 20 fd 73 18 7d 65 68 05 fd 02 fd fd fd 70 fd 14 37 5d fd 3d 1e fd fd 45 0e fd fd 1b 27 05 fd 02 fd 25 36 7b 26 65 08 25 70 3f 27 6a 4c fd fd 1c 32 7f 23 74 fd 0c 41 0b fd fd 72 fd 2c 06 fd 31 5c fd fd 58 69 fd fd 09 fd 30 fd 27 62 72 7c 17 58 00 fd fd 1e 31 fd 79 67 fd 37 fd 2a 5b 6e 3d fd fd 72 fd 17 fd 5e 03 fd fd fd 3c fd fd fd fd 4c 25 fd fd fd fd fd fd 4d 3e fd fd fd 53 02 fd 18 fd fd 73 fd 45 fd 4e fd fd 39 fd fd fd fd fd 29 12 73	`~F1P[WX~R|j,Z&u@9l~ q{{l@l>zq"Qz.=J/"l?5 s}ehp7]='%{&e%p?'jL 2#tAr,1\Xi0'br|X1yg7*^<L %M>SsEN9)s	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BPMLNOBVSB.jpg	1026	256	44 fd fd 32 54 fd 0f fd fd fd 55 fd fd 51 0a fd fd 32 fd 3e fd 5b 6b fd 52 5a fd 15 fd fd fd 24 fd fd fd fd 6d 45 fd 22 54 f9 fd 3b 1d fd 0f 37 4d fd 36 6a fd 66 71 54 fd fd 52 fd 19 0a fd fd 1e fd fd fd fd 6e fd fd fd 00 fd 01 13 fd fd fd 83 fd fd 2e 5c 46 fd fd 6d 72 69 41 27 0e 6b 05 fd 79 fd 21 fd fd 48 2a fd c3 75 73 20 23 fd 31 61 75 11 fd 43 fd 44 2e fd 5d fd fd 77 fd fd e5 74 fd 20 5a 6b 4d fd fd fd fd fd 4e fd fd 28 fd fd fd 41 fd fd fd 55 79 69 fd 6a fd 68 fd 12 7b fd fd fd 15 fd fd fd fd 0d fd fd 7d fd 34 fd 0f fd 7a 52 55 fd fd fd 74 3e 17 34 fd 59 e3 55 99 fd fd fd fd 4e fd e3 fd 72 fd 00 fd 52 51 fd fd 47 fd 3a fd fd fd fd fd 1b 71 fd fd 05 fd fd fd fd fd fd fd fd 45 fd 4f 1c 13 fd 63 62 fd 5a 39 3b	D2TUQ2> [RZ$mE"T;7M6jfqTRn.\FmriA'ky!H*us #1auD.]wt ZkMN(AUyi jh{}4zRUt>4YUNrRG:qE OcbZ9;	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.xlsx	5	1021	fd fd 78 0b 52 4a fd 70 44 68 2c 79 67 04 1d 01 fd fd fd f8 5c 32 6c fd 4b fd fd fd 16 fd fd fd 28 76 4f fd 2c fd 53 fd 41 fd 0f 30 fd 7f 50 5b fd fd 6d 15 fd 4d 05 fd 74 fd fd fd fd fd 2a 2d 1b fd fd 27 10 63 fd 6e a5 1a 3b fd 06 fd fd fd fd fd fd 2d fd fd fd 00 fd fd 7b fd 1a fd 27 2c 6a 3d fd fd 20 fd 0e 04 fd fd 21 12 fd 6b fd 3c fd fd fd 4c fd fd 09 fd 31 67 fd fd 50 00 72 fd 48 75 fd fd 16 fd 27 7e 18 fd 34 fd 36 68 fd 23 fd fd 57 fd 37 0e 4f 31 fd fd fd 79 fd 56 16 fd 1b fd fd 2a fd fd fd fd fd 01 58 fd fd 03 fd 17 fd 16 1a 39 fd 01 fd 31 fd 1f fd 1f 17 2d fd fd fd 28 fd 2b 6d 0a 15 fd fd fd 41 fd fd 2c 1d fd 60 b5 19 fd fd fd fd 48 fd fd fd 65 fd 73 4f fd fd fd 2d 62 6e 25 fd 45 33 25 fd 39 4b	xRJp,yg\2lK(vO,SA0P[m Mt*-'cn;-{,j= !k<1gPrHu'~6h#WO1yV* X91-(+mA,`HesO- bn%E3%9K	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BPMLNOBVSB.xlsx	1026	256	6c 77 65 31 6f fd fd fd b6 42 fd fd fd fd 5e 11 04 40 2a 47 49 5e 70 fd 70 65 fd 0d 7a fd 73 fd fd fd 6d fd 38 cc fd fd 63 43 fd 31 27 7c 38 fd 01 fd 27 fd fd fd fd fd fd 1e fd 5b fd fd 34 0e 6d fd fd fd fd 00 fd fd 0d fd 69 fd 5f 14 fd 53 3a fd 4f fd fd fd fd 57 fd fd 0c fd fd fd fd fd 44 7d fd 63 fd 5f fd fd 37 69 fd 71 58 fd 65 fd fd fd f0 27 26 fd 3d fd fd fd 4d fd fd fd fd 84 fd fd 2f 6f fd 0f 03 fd fd fd 10 0e fd 4c 35 fd 11 fd fd 65 fd 76 fd 67 fd 5c fd 09 31 37 fd 42 18 01 45 3f fd 05 0f fd fd fd 56 40 fd 41 03 fd fd 14 3b 34 fd fd fd fd 60 73 d1 25 0d fd 37 fd 68 fd fd 36 27 42 fd 6d fd fd fd 38 fd 09 fd 9e fd fd fd fd 38 fd 1f 51 10 fd 1d 16 fd fd 36 58 76 74 59 fd 23 fd fd fd fd 5e 49 25 fd 52	lwe1oB^@*GI^ppezsm8cC'|8'[4mi_ S:OWD}c7iqXe'&=M/oL5evg\17BE?V @A;4`s%7h6'Bm88Q6XvtY#^l%R	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\BPMLNOBVSB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\FENIVHOIKN.png	5	1021	4c 05 fd fd fd 73 fd 34 6a fd fd 1e fd 46 33 02 fd fd fd fd fd fd 5b fd 7e 7a fd 34 65 fd 2d 76 77 fd 07 fd 2a 3b fd 33 1e 39 11 0a 2f 67 fd 5a fd fd fd 6f 21 fd 7f fd fd 36 4c 5a 5a fd 64 fd a9 fd fd fd fd 38 7a fd fd 45 fd 30 4b 68 47 fd fd 01 fd 37 fd 45 fd 14 ce fd 16 53 5b 2d 56 3f bf 18 fd fd fd 29 79 fd 7a fd 2e 20 2d 22 fd 6f fd fd 0e 0d fd fd fd 1e fd 2f 40 69 22 fd 57 fd 68 40 54 62 2e 5d 59 0c fd 29 fd fd 61 1e 3f 0a fd fd 53 fd 5c fd 4a fd 07 fd fd 60 29 44 03 e8 fd 34 0e 76 69 4d fd fd fd fd fd fd 4f 62 6f 64 1e fd 09 43 fd fd 25 0b 09 31 24 fd fd fd 28 24 fd 13 fd 6b fd 20 03 fd 64 65 fd 2e 03 fd fd 26 61 11 71 67 fd fd 12 0d fd fd 26 7d 2d fd fd fd fd fd fd 71 fd 10 03 40 39 fd fd fd fd fd fd fd fd 68 fd 1b fd	s4jF3[~z4e-vw*;39/gZo!6LZZd8zE 0KhGES[-V?)yz. -"o/@i"Wh@Tb.]Y)a? S\J`)D4viMObodC%1$($k de.&aqg&}-q@9h	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\FENIVHOIKN.png	1026	256	fd 2e 2a 64 27 fd fd fd 7a fd 69 fd 78 6d fd 36 73 fd 57 fd 3c 50 fd 3a fd 54 12 40 48 7b fd fd 35 1a 50 50 5d 72 2a 56 fd fd 76 21 03 8b 78 fd 3e 3a 24 fd 74 fd fd fd 3e 33 4f 53 2d 27 fd 31 70 fd fd 0e 2d 63 fd 5c fd fd fd fd 7f fd 66 fd 49 6a fd 5d 90 37 3f eb 16 fd fd fd fd 29 fd fd fd fd 68 0c fd 48 63 7e 1b fd 66 1e 3e 37 fd 71 6e 6e 06 1f fd 6e 1f 13 3d 73 03 36 4b 37 6f fd 60 fd 4d fd 15 fd fd fd 01 1f 1e fd fd 6d 69 fd 1c 66 13 0e fd fd 6f 2b fd 20 fd 08 fd 11 fd fd 06 fd 4d 0c 10 d4 fd b1 fd 7e 4a 60 76 fd fd fd 77 fd fd 3d fd 53 fd fd fd 76 20 fd 06 19 fd fd 4a 0c 39 37 26 fd 73 fd 2d fd 76 fd fd 23 fd fd 25 fd 4c fd fd 0c 66 fd 56 fd fd fd 10 46 fd 36 fd 4d 26 fd 79 13 fd fd fd 4f 5d fd	.*d'zixm6sW<P:T@H{5PP]rVv!x>:$t>3OS-'1p-c\flj7?)hH~f>7qnnn=s6K7o`Mmifo+M~Jvw=Sv J97&s-v%LfVF6M&yO]	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\FENIVHOIKN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\FENIVHOIKN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\JSDNGYCOWY.mp3	5	1021	50 26 26 68 fd 68 fd 12 fd 29 fd fd fd fd 09 fd fd 10 6f fd 29 fd fd fd 30 fd fd 76 fd 5d 18 fd fd 00 39 71 11 53 44 fd 0f 48 fd fd fd fd 04 fd 1c fd fd fd 23 fd fd 50 55 14 fd 63 fd 40 fd fd 4e fd 29 fd 52 fd fd 32 1b 2f fd fd fd fd 0c fd 1a fd fd 5d 19 fd 71 fd fd 2b 67 fd 05 18 70 34 72 43 04 07 fd fd 48 00 fd 2e fd fd 5a 44 fd fd f0 2b 12 fd fd 59 fd 22 fd fd 56 43 53 2c fd fd 74 fd fd 4b fd 35 6a 34 fd fd fd fd fd 0a 10 fd fd fd 67 00 65 17 fd 9a fd fd 10 00 08 1d 05 1b 66 fd fd 6b fd 52 fd fd 10 38 37 66 fd 4a 66 6f 01 3d 34 fd fd 59 fd fd 0a fd fd fd fd 13 1d fd 35 1c fd fd fd fd fd fd fd 23 fd 3e 0e 71 fd fd 6e fd fd fd 6c fd 39 fd 32 fd 27 28 fd 57 20 13 10 fd 6f fd 7f fd 3b fd fd 14 41 06 fd fd fd fd 36 49 07 fd 75	P&&hh)o)0v]9qSDH#PUc@N)R2/]q+gp4rCH.ZD+Y"VCS,tK5j4gefkR87fJfo=4Y5#>qnl92'(W o;A6lu	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\JSDNGYCOWY.mp3	1026	256	fd 3e 49 69 fd 33 fd 14 56 fd 66 fd fd 43 fd fd fd 23 20 fd 04 6f fd 09 fd fd 69 fd fd 6b 52 fd fd 18 fd fd 60 fd 63 fd 0f 79 11 1b 5b fd 6c 7a fd fd 96 0c fd 21 fd fd fd 75 06 fd 20 fd fd fd 4e 04 fd fd 1d fd 10 fd fd 4c fd 7d fd 20 61 fd 15 55 fd 58 fd fd 11 fd 21 0b fd fd 3b 30 2e fd 2e fd 51 fd 7b fd 4a fd 71 34 5a fd fd fd fd fd 25 fd 30 fd 24 13 fd 27 02 fd d2 5b fd 02 16 0e 03 fd fd fd fd fd 4a 45 fd 06 7c fd fd 5e fd fd 4b fd 21 3c fd fd fd fd 53 fd 55 52 fd 40 fd 1f fd fd fd 21 fd fd 6f fd fd b2 52 58 65 fd fd fd fd 0e fd 51 33 fd 51 fd fd 47 5e 7a fd 1d fd fd 2e fd 39 5e 03 48 d3 f5 fd fd 1a 03 7c 66 1f fd fd 5e fd 13 6f 52 6c 7c 0c 65 fd 35 02 2b 50 78 fd 21 61 fd fd fd fd fd 23 fd fd fd 33 62 35 48 fd fd fd 4c	Ii3VfC# oikR`cy[Iz!u NL}aUX!; 0..Q{q4Z%0$'[JE|^K! <SUR@!oRXeQ 3QG^z.9^H|f^oRI|e5+Px!a#35HL	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\JSDNGYCOWY.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\JSDNGYCOWY.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.docx	5	1021	42 fd fd 6d fd 2f fd 61 fd 4e fd 0d fd 77 fd 10 78 10 3c fd 91 27 6c fd 26 fd 69 fd fd fd 03 0e fd 51 fd 59 78 fd 2c 1f fd fd fd 56 6c 06 45 21 57 04 7f fd fd fd 0a 60 fd 12 58 fd 68 fd fd 45 69 53 fd fd fd 44 36 fd 51 73 24 fd fd fd 37 45 74 fd fd fd 4d 33 fd fd fd fd 0e 34 ab 52 fd 70 fd fd 4c fd 2e 32 7a fd fd 02 00 21 fd 31 fd 66 6e 09 17 1b fd 45 35 7c 02 fd 68 fd fd fd 3d 0a fd fd fd 69 fd 71 67 37 fd 25 2f 0c 11 fd fd fd 52 fd 45 fd fd 53 0b fd cc 68 fd fd fd 44 fd fd fd 77 69 69 fd 52 15 fd fd fd 5a 07 fd fd 06 fd fd 90 56 fd fd 36 08 2e fd fd fd a3 2a 02 35 fd 26 0b 2b fd fd 23 7d fd 7e fd 3d fd 75 50 fd 33 54 3d fd 5c 72 25 71 fd fd fd fd 30 57 fd 65 6d 94 fd 54 4f 37 fd 31 4d 20 32 08	Bm/aNwx<'l&iQYx,VlE!W `XhEiSD6Q s$7EtM34RpL.2z!1fnE5|h =iqg7%/R ESDwiiRZ6.*5&+#}~=uP T=\r%q0WemTO71M 2	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI.docx	1026	256	fd fd 2f 3e 72 38 40 62 70 60 fd fd 7c 40 62 61 08 2b fd 60 fd fd 6e 3b da 5b 2b fd 55 1a fd 4d 7d fd fd 2f 17 fd fd 62 e5 31 1a fd fd fd 20 72 75 04 fd 5c 42 fd 3f 6a fd fd 57 40 fd 67 1b fd fd fd 4a 23 21 fd fd 3b 78 fd 58 04 fd fd 0a 18 73 41 fd 6d fd 45 5b fd 3d 41 fd fd fd 57 78 58 47 68 01 fd fd 34 5b 20 35 68 2f fd fd fd 62 5e 7e fd 40 1c 2f 31 fd fd 4d fd 52 33 30 fd 0d fd 31 52 fd fd fd 5b 72 69 5f fd fd fd 4d 66 71 1e 27 fd fd 1b 56 fd 40 fd fd fd 21 24 02 fd 41 4e 37 5d 49 fd 65 68 1a fd 53 fd fd a0 28 fd 7f 39 fd 54 fd fd fd 43 fd ad fd fd fd 5b 3f fd fd a3 63 55 6a 78 10 10 1c 4e 2d fe fd 00 4e fd fd 6c 04 48 fd fd 55 68 0a 32 2f 86 1b 39 fd fd 3d 2d 50 5f 2a 59 fd fd 71 2d 6b	/>r8@bp`|@ba+`n; [+UM}/b1 ru\B? jW@g#!;xXsmE[=WxXGh 4[5h/b@/1M R301R[ri_Mfq'V@!$AN7]IehS(9TC[?cUjxN- NlHUh2/9=-P_*Yq-k	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.png	5	1021	26 19 fd fd 52 fd 5d 07 fd 0f 5f 42 02 fd 70 fd fd fd fd fd 7c fd 02 fd b8 fd 47 fd fd fd 3a 73 2d fd 06 6f 6d 52 15 5e 03 73 22 fd 45 02 fd fd 4b 5c a7 4f fd 2c 04 0d 17 fd fd fd fd fd 61 02 fd 19 fd 4f fd fd 63 fd fd 05 fd 75 18 fd 0c fd 4c fd 77 14 59 fd fd 70 74 61 05 63 07 fd d7 fd 5a 3f 46 67 fd fd 51 55 18 fd 7e 62 2e 3a fd 12 27 fd 14 01 25 fd 59 fd fd 03 fd 09 31 fd fd 0d 14 17 6b fd fd fd fd 44 25 fd 6d fd 56 fd fd fd 36 33 40 3d fd fd 41 fd 25 1b fd 66 fd fd 01 fd fd f1 fd fd fd 00 3e fd 65 fd 7a fd 76 45 fd 13 fd 23 63 fd 7c 10 fd 3a 33 16 47 fd fd fd fd fd 55 72 39 6c fd fd fd fd fd fd fd 05 fd fd fd fd 70 51 57 78 fd 0f fd 15 fd 7e 48 fd fd fd 57 fd 2b 28 3f 6e 0e 25 fd 3a 2f fd 21 fd fd fd fd 12 fd 01 fd fd 56 69 fd	&R]_Bp|G:s- omR^s"EK\O,aOcLwYpt acZ? FgQU~b.:'%Y1kD%mV63 @=A%f>e zvE#c|:3GUr9lpQWx~H W+?n%:/!Vi	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI.png	1026	256	33 6d 31 33 7f 28 28 29 fd fd 50 61 fd ab fd 73 fd 03 66 fd 01 fd 11 4c fd 72 fd fd fd 40 fd fd 3b 24 1e 1f fd fd 57 fd 57 fd fd fd fd fd 5d 53 fd 2f fd 21 64 56 17 10 23 38 11 51 4c 71 fd 6c fd 54 3e 59 fd fd 4b 75 fd 74 02 22 fd 76 67 fd 40 fd 00 fd fd df 1b 6b 45 31 75 fd fd fd 52 3f 18 fd fd 33 11 fd fd 11 40 31 02 41 fd 4d 51 7d fd 6e fd fd fd fd fd 29 60 19 fd fd 15 37 71 6c 22 fd 7d fd 4b fd fd fd fd 00 fd 36 fd 08 fd fd 7e 49 fd fd fd fd fd 34 4e 77 fd 33 24 fd 4a fd fd fd 40 fd 6b 1b 2a fd 17 71 fd fd fd fd 5b 4e fd fd fd 53 52 63 16 05 5f fd 13 49 fd 32 fd 08 44 fd fd fd 02 fd 76 bf 38 2e 6b 76 40 fd 7c 7d fd fd fd 49 fd fd b5 ea 72 fd 0b fd fd 09 33 fd 1f fd 16 6a fd fd fd 9d 1d 60 3f fd 7f fd fd fd fd	3m13(()PasfLr@;$WW]/!dV#QLqlT>YKut"vg@kE1uR?3@1AMQ}n)`7ql"}K6~l4Nw3$J@k*q[NSRc_l2Dv8.kv@|}r3j`?	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.xlsx	5	1021	fd 65 fd fd 33 fd fd fd 4d 7f 44 16 26 fd 42 3f fd 5d 2d 44 fd 70 34 fd 0e 77 fd 33 35 fd 11 79 78 78 5d 51 fd 75 fd 98 1b fd 39 fd 0c 15 75 fd fd 71 1c fd 75 11 fd fd 62 fd fd fd fd fd 22 16 fd 50 46 fd 2a 78 fd fd fd fd 5c 67 fd 60 12 fd fd 39 2a fd fd 3d fd fd 3e fd 24 6d 3f fd 7e 4e fd 6e 07 fd fd 7c fd 63 fd 4b fd 3f d6 f5 2e fd 79 22 6d 68 fd 44 fd fd fd 71 fd 75 fd fd fd 7f fd fd 3d 4c 6f 20 3c 28 37 77 59 fd 00 2a 69 70 3c fd fd 43 fd fd 09 fd fd fd 16 fa 3f fd 55 fd 2d 49 fd fd 78 fd fd 32 1f 65 fd fd 75 fd 11 53 49 57 36 fd fd fd 21 2f fd fd fd 14 fd 5f 19 fd fd 65 3d fd 34 63 77 3b f3 73 fd 1e 07 0f fd fd fd 4c 10 71 54 fd fd fd fd fd fd fd 06 fd c1 63 39 68 fd 33 fd 76 32 59 56 58 0b fd 46 37 fd 5f 2a fd fd	e3MD&B?]-Dp4w35yxx]Qu9uqub"PF*x\g`9*=>$m?~Nn|cK?.y"mhDqu=Lo<(7wY*ip<C?U-Ix2euSIW6!/_e=4cw;sLqT9h3v2YVXF7_*	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI.xlsx	1026	256	fd ad 61 fd fd fd b9 fd 40 04 6e 19 38 38 fd fd 53 53 4f fd fd fd d1 62 fd fd 4d 76 7c fd 61 2b fd fd 49 75 04 08 6c 08 44 53 fd a4 fd 3b fd fd fd fd fd 1f fd fd fd 56 76 fd 40 73 7d 1d 26 17 fd fd fd 62 fd 4f 01 fd fd 59 8d fd 4d fd fd 3b 4f 72 38 57 66 0f 79 fd 45 78 fd fd 77 49 fd 20 46 fd fd fd fd 1b 07 fd 13 fd 57 16 fd fd fd 19 fd fd 31 50 fd 25 2a fd 42 53 fd 4c 73 fd 73 59 24 33 fd 0f 08 77 fd fd 08 fd 07 fd fd 66 31 fd 63 05 5e fd 66 fd 5f fd 51 7f 6b fd 6b fd 21 fd 47 fd fd fd 10 17 28 73 fd fd fd 23 38 fd fd 30 02 6e fd 58 20 fd 4f 55 65 2e fd 5a fd 07 fd 50 fd fd 69 61 fd fd fd 54 49 fd 25 79 fd 00 fd fd 61 55 fd 69 fd 42 54 37 fd fd 0c fd fd 04 75 6a fd fd 3f fd 46 fd 13 d1 69 33 74 fd fd fd	a@n8SSObMv|a+luIDS;Vv@s}&bOYM;Or8WfyExwlFW1%*BSLssY$3wf1c^f_QkkG(s#80nXOUe.ZPiaTI%yaUiBT7uj?Fi3t	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ.docx	5	1021	5d fd 52 fd 4a 54 48 22 fd fd 24 fd 63 67 fd f1 05 fd fd fd fd fd 73 fd e3 0d 71 6a fd 53 1a fd 49 1e 66 55 fd fd 13 fd fd fd fd 66 fd 28 65 fd fd 5b 17 fd 1d fd 4e fd fd fd fd 1d fd 23 16 fd 02 fd 4c fd fd 3f 1e 0f 0e 62 16 4f fd fd 16 fd 27 79 fd 1e 1e fd 16 31 14 fd fd 48 fd 0c fd fd 70 fd 2d 1d fd 17 35 fd 50 27 6b fd fd 0f fd 2d 2a 44 36 1f 6f fd 1a 7f 04 06 fd fd fd 0b fd fd 30 20 fd fd 38 6c 4e fd fd 72 fd 5a fd 9f fd 0a 59 fd 05 06 fd 0f fd fd 21 2b fd fd 39 55 fd fd 5f fd 4a 72 77 0d fd fd 37 fd 41 6b fd fd fd fd 54 fd fd e0 0f 6d fd 63 fd fd 67 1d 9b fd fd 19 33 fd 62 fd 63 fd 04 0c 4a fd 0e fd 3e 50 fd fd 18 6c 2e 65 fd fd 7c fd 29 68 fd 1e fd 43 4c fd 4f fd 09 fd 0e fd fd 0c 0f fd 12 70 0b 2c 22 55 14	]RJTH"$cgsqjSIfUf(e[N#L?bO'y1Hp-5P'k-*D6o08lNrZY!+9U_Jrw7AkTmcg3cJ>Pl.e|)hCLOp,"U	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ.docx	1026	256	07 fd 7d fd 45 fd fd fd 0b fd 14 fd 3e 1f fd 6c fd fd e8 fd 3f fd 3f fd 3d 3b 0b 46 fd fd fd fd fd 3a 6e 30 fd 0b 53 07 fd 52 fd 30 fd 39 fd 47 fd 45 bf 03 1d 39 fd 0a 36 fd 1c 26 3f 1f 53 fd 32 fd 08 7a 66 21 3a 7d fd fd fd 12 22 06 1c fd fd 20 fd fd 62 67 33 43 24 05 7e 08 4d fd 1a fd 35 fd 6c fd fd 38 fd 66 2a fd 46 5e 78 fd 05 fd fd 00 fd 1f 74 fd 38 fd fd 36 fd 4b d6 fd fd fd fd 5b 6b fd 2a 04 fd fd fd fd fd 50 64 fd 71 79 78 fd fd fd fd fd 91 7c 9d 4c fd fd 41 fd 0f fd 1d fd 5b fd 5f fd 1a fd fd fd fd fd 5a 0e fd fd fd fd 19 fd fd 48 2b fd 63 0f 0e fd 32 15 73 63 fd fd 75 fd 17 fd fd fd 2e 06 fd 71 fd 5a 7b 3d fd 6c fd 71 0a 3c 6c 01 55 fd fd fd fd fd fd 7b fd 53 01 fd 29 34 0b 79 fd 06 fd 50 45 02 42 c1 fd fd	}E>l?? =;F:n0SR09GE96&? S2zf!:}" bg3C$~M5l8f*Fxt86K[k*P dqyx|LA [_ZH+c2scu.qZ{=lq<lU{S) yPEB	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\NEBFQQYWPS.png	5	1021	3c 44 fd fd 51 fd fd fd fd fd 37 fd 4b 59 48 0c fd 7e fd 40 00 fd fd fd fd fd 67 68 6e 13 4d fd 07 09 72 fd 2d fd 2d fd 0c 68 2d 7f 5e fd 33 fd 4b 79 00 fd 56 03 12 73 fd 11 59 3f 09 18 2e fd 19 67 74 72 4e fd 2d 71 3e fd fd fd 53 fd 16 fd fd fd fd 52 5c 50 fd fd 33 26 fd 79 21 09 fd 4a 65 08 fd 64 fd 27 26 0a 5e 09 fd fd 73 fd 4c 48 fd 10 fd fd 67 7b 42 3e 3c 29 fd 01 fd fd 55 fd fd 5a 47 55 34 fd 54 fd 4e 39 fd 70 fd fd fd fd 1d fd 62 27 fd d9 2a fd 66 7d 51 fd 7e 25 fd 2f fd fd 01 08 75 fd fd 06 77 22 fd 03 fd 7b fd 18 fd fd 74 fd 0b 71 fd fd fd fd 66 ab 64 fd fd fd fd d6 fd fd fd 22 fd fd fd fd fd fd 07 73 3e fd 6c 32 fd fd 33 11 56 fd 00 fd fd fd fd 5f fd fd 7b fd fd 4e 68 fd 05 35 fd 56	<DQ7KYH~@ghnMr--h- ^3KyVsY?.gtrN- q>SR\P3&y!Jed'&^sLHg{ B>)UZGU 4T9pb'f}Q~%/uw" {tqf"s>l23V_Nh5V	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQYWPS.png	1026	256	26 fd fd fd fd 2a 5e 0f 79 fd fd 4c 7d fd fd fd 06 7e 45 2f 1a 7c 28 74 48 40 19 62 fd 7a 0e 67 fd 49 fd fd 68 79 55 27 38 fd fd 03 55 0c fd 40 fd 03 fd fd e6 f8 fd 1c fd fd 24 6b 2f fd 0c fd 64 fd 6f 45 4a fd 05 23 fd 64 1a fd 14 4d 0a 50 66 11 51 fd 50 08 fd fd 17 fd 60 76 2a 53 58 1f fd 6d 67 66 2e 6d 5b fd 7e fd 00 fd fd 51 fd 6b 58 48 fd fd fd fd fd fd fd 70 fd 1d fd 52 fd 57 fd fd 16 5c fd fd 34 45 fd fd 1b fd 74 fd fd 04 7b fd fd fd 07 2b 75 fd fd fd 2c fd 24 fd 7a 7f 39 fd 06 fd 4e 14 41 23 fd 09 fd 07 fd 40 fd 6a fd fd 63 c1 0e 53 20 fd fd 35 fd 68 57 fd fd 56 fd fd fd 7a 61 5c 57 fd 05 69 7d 23 71 fd 1b 74 fd 5b fd fd 0e 38 12 fd 6e 15 fd 22 5c 2e fd fd fd 3c 4e fd 2f fd 1b 27 0e fd fd fd 4f fd fd fd 3a fd 7b fd	*^yL}~E/|(tH@bzgIhyU'8U@$kdoEJ #dMPfQP`v*SXmgf.m[~kXHpRW\4Et{ +u,$z9NA#@jcS 5hWVza\Wi}#qt[8n"\. <N/'O:{	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\NEBFQQYWPS.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\NEBFQQYWPS.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\NWTVCDUMOB.xlsx	5	1021	7e 2a fd 24 48 fd 7a 08 fd 5c 47 fd fd 05 fd fd 30 1f fd fd fd 7d 74 fd e5 fd fd 73 fd fd fd fd 2d 6c fd 76 fd 1b 02 fd 53 67 73 48 63 fd 30 fd fd 55 1c fd fd 1a fd fd 7d 3a fd fd fd fd fd 04 56 fd 33 52 fd 47 44 5f 53 fd fd 6d 07 60 fd 7e 2b 5b fd fd 39 fd 52 fd 1d 22 20 fd 69 0c 11 0f fd 0b 7d fd fd 02 fd 64 fd 68 1e 03 7c 00 fd fd fd 09 fd fd 62 9a fd 7d fd 44 fd 02 fd 33 fd fd 18 fd fd fd fd 5d 33 fd fd fd 10 50 fd 75 fd fd fd fd 35 14 0b 01 20 22 0f fd 21 fd 79 fd 2f fd fd 55 fd 24 6a 2f fd 46 fd 10 2c 51 3d 73 23 58 fd fd fd fd fd fd 37 1d 4a 57 4b 53 fd fd 40 71 13 fd 18 37 fd 2f ee 09 fd d8 fd 28 fd 3c fd 30 fd fd fd fd 69 04 fd fd fd 19 fd fd 07 46 fd 67 fd fd 3a 1c fd fd fd 1d fd fd 31 65 63 30 06 28 4d 25 26 fd	~*$Hz\G0}ts-lvSgsHc0U}:V3RGD_Sm`~+[9R" i}dh\|bD3]3Pu5 "!y/U$j /F,Q=s#X7JWKSq7/(<0iF:1ec0(M%&	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NWTVCDUMOB.xlsx	1026	256	6a fd fd 7f 5c 5c 06 7a 06 fd fd 26 6e 60 fd 60 fd e1 29 4a 46 fd fd 61 07 fd 2c 03 fd 66 fd 6a fd fd 61 fd fd 7e fd 3f fd 11 2b fd 5b fd fd 54 27 fd 57 0c fd fd 26 7f fd fd 51 34 46 3a 22 30 fd 19 fd 20 0d 1c fd 5e 53 fd 71 39 44 4d 62 fd fd 7c 46 5a 23 fd 7c 2a fd fd fd 61 1e fd 50 fd 0c 4f fd 0f 54 fd 7e fd fd 07 fd 27 fd fd fd 09 60 74 45 fd 2d fd 79 34 57 fd 67 fd 27 30 fd 7e 18 7b ee 15 fd 25 7a 01 0a fd fd 23 fd 46 fd 52 3a fd 4d 44 72 fd fd fd fd 21 48 1f fd 2c 16 31 70 fd 3f 77 30 fd fd fd fd fd 3d 1f fd fd 35 61 13 2a 7d 23 62 fd 7f 64 fd fd 78 7a 3b fd fd 60 10 fd 4a fd fd fd fd 5a fd 1a 0e fd 5a 6f 49 4f 18 fd fd fd 0a 1c fd 48 fd fd 4a 48 7a fd 63 43 fd fd 37 3f 77 07 19 fd 3f 31 75 74 7a fd 1a 19 fd 73 fd fd fd fd 63 fd 63 fd	j\\z&n``)JFa,fja~?+ [T'W&Q4F:"0 ^Sq9DMb|FZ#|*aPOT~'`t E-y4Wg'0~ {%z#FR:MDr!H,1p? w0=5a*}#bdxz; `JZZoIOHJHzcC7?w? 1utzscc	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\NWTVCDUMOB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\NWTVCDUMOB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\QNCYCDFIJJ.mp3	5	1021	5f fd 18 fd fd 7a fd 7d 0f fd 28 fd 00 e4 fd fd 7b 74 10 fd fd fd 12 4e fd 17 fd 7b 10 fd fd 29 fd 17 01 fd fd 78 53 75 fd fd 79 fd 42 fd 0c 64 39 23 0b 4c 49 fd fd fd fd fd 1a 7e 6b 71 16 fd 78 fd fd 19 fd fd 49 fd fd 60 25 2d fd 6d 4e fd fd 40 11 fd fd 3f fd 4d 21 3e fd 35 fd 05 2b fd fd fd 3b 22 fd fd 11 6c fd fd 7a 49 70 fd 2c 39 fd 22 17 28 fd fd 68 fd 6c 35 fd 4f fd fd 41 fd fd 48 14 fd fd 5a b8 fd 1d fd 7b 0e 7c 7b 75 37 fd 40 fd 7a fd fd 03 06 49 48 3c 22 fd ff fd 77 6c fd 9e fd 58 fd fd 6a fd fd fd fd 00 fd 78 57 fd 05 fd fd 24 61 3b 2c 27 28 fd 34 fd 11 60 fd 7c 35 50 59 7a 32 fd 54 fd fd 4a fd 17 30 fd 26 fd fd 63 5d 1d 55 63 fd 6f 4d fd 43 fd fd 29 35 7e 6f 74 fd 18 fd 75 03 77 06 01 fd fd fd 6c fd fd 1b fd 4c fd fd 54	_z} ({tN{)xSuyBd9#LI~kqxl`% -mN@?M!>5+;"IzIp,9" (hl5OAHZ{|{u7@z IH<"wlXjxW$a;,'(4`|5PYz 2TJ0&c] UcoMC)5~otuwlLT	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\QNCYCDFIJJ.mp3	1026	256	4c fd 67 79 55 fd 0b 72 fd fd 4c fd fd 53 fd 76 fd fd 7e fd 69 fd fd 30 fd fd fd 4b 5e 3f fd fd 41 fd 3a 14 fd 72 52 fd fd 23 34 6e fd 4d 1c 61 fd 5f fd fd fd 3c 2a fd fd 18 45 6e fd 32 fd 43 43 fd 19 fd fd 6b 2e fd fd fd 3d 70 fd fd 37 04 2c 23 30 79 05 fd 33 fd 1f fd 4a 0f 2a 23 fd 2f fd fd 1d 7b fd 77 fd 0e fd 03 2e fd fd fd 35 fd fd fd 6e fd 56 06 0e fd 12 fd fd 3e 1a 2e 75 65 79 76 fd fd a8 52 5c fd 3f 4d 1a fd 36 3c 7a 20 42 9c fd 31 fd 4a 18 fd fd fd fd 1b fd 13 fd fd 33 6f fd fd 02 64 b9 fd fd fd fd 1a 02 fd 15 fd fd dd fd bf fd 4d 6f fd 30 fd fd fd fd 37 24 10 25 fd 04 18 fd 4d 36 4c 30 fd fd 77 fd fd 4b fd fd 57 fd fd 44 fd 1d 45 7e 2b fd fd 6f 30 fd 09 76 fd 05 21 fd 2d fd 57 fd 48 4f 61 5a 7f fd 16 fd fd fd 06	LgyUrLSv~i0K^? A:rR#4nMa_<*En2C Ck.=p7,#0y3J*#/{w.5nV>. ueyvR\?M6<z B1J3odMo07$M6L0wKW DE~+o0v!-WHOaZ	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\QNCYCDFIJJ.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\QNCYCDFIJJ.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\RAYHIWGKDI.pdf	5	1021	fd fd fd fd 3d 3d 02 48 76 fd fd 3f fa fd 4a fd 79 24 fd 5f fd 30 70 fd fd 45 1b 47 fd dc 47 18 2e 44 6a fd fd 4b 29 fd 5f 07 50 48 fd 4e 7f fd fd fd fd 20 7d 9f fd 35 fd 2b 32 fd 13 fd 66 fd 63 fd 2a fd 75 42 43 fd 4c 43 fd 1f 02 fd 59 54 2d 0b 58 08 59 fd 7c a4 fd 40 31 fd 43 fd 65 fd 60 fd 29 0b 3d 6c 4f fd 51 4b fd 55 6b 40 71 0b fd 7b fd fd 5c 00 fd 34 64 01 fd 45 fd 2b 0e 38 fd 11 fd 29 50 3e fd fd fd 5a 20 28 00 16 fd fd fd 39 fd 05 55 fd 2b 64 fd 24 66 fd 05 fd 68 2e fd 19 6b fd 5f fd 0f fd 1b 6a fd fd 31 fd 16 34 fd 35 18 61 72 fd fd fd fd 62 6b fd fd fd 45 26 fd 59 4d 72 fd fd fd fd 26 7a fd fd 11 3e fd 68 fd fd fd fd 70 fd fd fd fd fd 0f fd 5c 4f fd 4c 41 fd 3e 5b 79 1a 24 50 fd 03 52 3c 5f 69 56 fd 26 7c 12	==HvJy$_0pEGG.DjK)_P HN }5+2fc*uBCLCYT- XY\|@1Ce`)=lOQUk@q{\4 dE+8)P>Z (9U+d$fh_j14arbkE&YMr &z>hp\OLA>[y$PR<_iV&|	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\RAYHIWGKDI.pdf	1026	256	23 fd fd fd fd fd fd 43 4b 2b fd fd fd 65 fd 5f 75 12 71 63 5a 38 21 6e 94 fd fd fd 1b 5e 69 94 fd fd 35 fd 2b fd 00 0a fd 0c 6f 03 22 fd fd fd fd fd 5b fd fd fd 42 fd fd 07 30 fd 10 fd fd fd 06 fd 4b 78 28 25 4c fd fd fd fd 09 fd 28 fd fd 50 fd 20 25 fd fd fd 6a fd fd fd fd 44 6b 4f fd 0f fd fd 13 71 fd fd 3b 0a fd 2e 01 17 fd fd 65 2d 19 fd 0d fd 3c 4c 4e fd fd 1a fd fd fd fd fd fd 77 fd fd 60 fd 02 42 fd fd 1e 31 7c 2b 25 fd 0f fd 41 78 66 fd 19 fd 36 fd fd fd 57 17 09 4e fd 78 08 fd 76 37 35 fd fd fd 2c 2d fd fd fd fd d1 5e 3c 2b 18 65 12 1e 36 fd 69 66 34 fd fd 47 6f fd fd 40 05 62 fd 1e 0d fd 35 55 fd fd fd 8d fd 3d fd dc fd 22 fd 68 fd fd 58 fd 37 13 fd 43 fd 78 fd 50 fd 3c 3a 7c 23 62 55 fd 20 fd	#CK+e_uqcZ!n^i5+o"[B0Kx(%L(P%jDkOq;e-<LNwB1|+%Axf6WNxv75,-^<+e6if4Go@b5U="hX7CxP<:|#bU	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\RAYHIWGKDI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\RAYHIWGKDI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\SFPUSAFIOL.mp3	5	1021	fd 78 fd 0c fd fd 7d fd fd 4b 71 fd fd fd 18 fd 53 21 23 45 fd 44 fd fd 45 62 17 fd 50 36 fd 3a 53 fd 1b 44 fd f2 fd 51 fd 04 27 fd 3f fd 53 64 fd 79 fd 3f 50 1d 5c fd fd 75 fd 3e fd 6c 4e fd fd 39 65 fd fd 08 fd 09 62 7f fd 4a fd 2e fd fd 52 fd 38 7d 7e 52 fd fd fd fd 05 66 fd fd 53 fd 64 24 1c 56 fd fd fd 05 fd 19 58 7b 27 fa fd fd fd 24 39 25 fd 60 4d 27 fd 0b 37 fd 0a fd 06 2e 13 fd fd fd 0d fd fd 5f fd fd 76 59 fd 48 0d fd fd 77 fd fd fd 74 fd 17 3e 43 02 fd 7a fd 3e 7e 2b 7d fd fd fd 63 fd 56 fd 2d 1b 56 fd 07 2a 56 0e fd 42 fd fd fd fd e3 fd 5d fd 36 04 14 fd fd fd 3d fd 6b 5e 15 68 fd fd 74 fd fd fd fd 29 6a 3e 26 6c 16 1b fd 4f fd 55 d7 2b 14 fd fd fd 38 0f fd fd 3d fd 3b 04 67 50 fd fd 25 66 fd fd 6a 25 21 5a 6a 76 fd 25	x}KqS!#DEbP6:SDQ'?Sdy?\u>lN9ebJ.R8}~RfSd$VX{'$9%`M'7._vYHwt>Cz>~+}cV-V*VB]6=k^ht)j>&lOU+8=;gP%fj%!Zjv%	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SFPUSAFIOL.mp3	1026	256	07 fd fd 24 4d c3 50 6c 04 7a 2e 0a 46 1a 40 fd 2c 02 fd 37 5e 5b fd fd fd 69 fd a9 fd fd 3b fd fd fd fd fd fd 34 6e 0c fd fd fd fd fd 26 fd fd 43 fd 7d fd 35 fd 49 fd 51 0c fd 01 72 fd 1b 43 fd 6a fd fd fd 16 fd fd 43 fd fd 58 0b 65 fd 27 fd fd fd fd 39 fd fd 07 fd fd 22 51 fd fd 7c 03 69 fd fd 73 71 fd 24 fd fd fd fd fd fd 8d 21 25 fd fd 1a 44 21 05 33 fd 2f 4e 36 5d fd fd 51 1b fd 86 39 fd 23 fd 75 fd fd fd fd 11 fd 60 fd 79 28 34 43 19 fd fd 2a 65 fd fd 69 25 fd 7a 5d 5e ea fd fd fd fd 2f fd 63 fd 04 3e fd fd fd 1d 3b 76 fd fd 49 22 4c fd fd fd fd 34 1b fd 42 6d 70 fd fd 2f 28 fd 1d 26 fd a1 fd 11 37 2a fd 63 5f 27 fd fd 53 fd fd fd 09 fd 67 fd fd 46 1f 3f fd fd 1a 74 fd fd fd 47 35 fd 17 57 fd fd fd	$MPlz.F@,7^[i;4n&C}5IQ rCjCXe'9 "Q\|isq$!%D!3/N6]Q9#u`y(4C*ei%z]^/>;vI"L4Bmp/(&7*c_'Sg F?tG5W	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SFPUSAFIOL.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SFPUSAFIOL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\SQRKHNBNYN.png	5	1021	fd 07 58 3e 38 7c 6b fd fd fd fd fd 4c 18 09 6c 0e 1f fd 1e fd fd fd 0a fd 52 fd 52 11 41 3e 4c fd 31 2c 29 fd fd 5a 04 38 14 55 29 fd fd 5b fd 7a fd fd 05 4c 71 2e 4f 33 58 2a fd 3e fd fd fd 24 fd fd 5a fd 52 17 fd 55 49 fd 7c fd fd fd fd fd fd 63 4a fd fd 6e fd 75 fd 25 0b 08 49 fd c6 7e fd fd fd fd fd fd fd 57 fd 5c 53 fd fd fd 08 41 06 fd ae fd fd fd 40 10 fd fd fd b5 fd 03 fd fd 6c 22 1b fd 47 6c fd fd 52 66 27 66 fd 6c 5c 44 fd 2d fd 14 48 fd 03 6a fd fd fd fd fd fd fd 60 7d 15 03 4e 0e fd fd 66 65 59 13 fd fd fd fd fd fd 54 0f fd 6c 43 2e 4e 62 67 fd 0e fd 32 fd 6e 30 1c 6a fd 10 3f fd fd 19 fd fd fd fd 5d 7a fd 29 fd 3a a6 36 fd fd 38 63 43 fd 4a fd fd fd fd fd fd 2c 55 fd 6b fd	X>8|LIRRA>L1,)Z8U) [zq.O3X*>$ZR I|cJnuI~W\SA@I"GlRf'fl\D -Hj`}N feYTIC.Ng2n0j?]z):68cCJ ,Uk	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQRKHNBNYN.png	1026	256	39 45 fd 2b 79 53 fd 17 fd fd 5c 0e fd fd fd fd 72 fd 37 3e fd 21 fd 7e 55 22 05 22 5b fd 47 fd fd fd fd 45 fd fd 39 fd fd 88 77 6d fd fd 60 2e fd fd fd fd 0d fd 71 35 79 2c 49 fd fd 55 fd 61 fd 6e fd fd 29 28 fd 0f 59 08 fd 29 7e 43 6b 03 62 fd 70 51 fd fd 28 38 fd fd 21 10 fd 39 67 2a 17 fd fd 54 3a 10 5b 45 04 fd 5e 32 fd 59 fd 5c 64 36 fd 4a fd fd fd 06 fd 28 2b 3d 06 65 fd 0a 11 fd fd fd 77 87 fd fd 4f fd fd 2e fd 04 92 57 67 50 fd fd fd 2c 09 fd fd 3a 52 fd fd fd 0d 17 fd fd 80 2c 93 62 61 fd 2e 58 61 fd 74 46 fd fd e5 0f fd fd 55 2d 62 fd 25 fd 7c 57 fd fd b6 53 03 fd 2a fd 48 fd fd 25 0f fd 48 7a fd 1c fd 55 64 fd fd 7a 66 60 47 fd fd fd fd fd 65 fd f5 b2 75 06 28 fd 5d 28 fd 6d fd fd fd	9E+yS\r7>!~U""[GE9wm`.q5y,IUan)(Y)~Ckbp(8!9g*T:[E^2Y\d6J+=ewO.Wg,:R,ba.XatFU-b%|WS*H%HzUdzf`Geu()(m	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\SQRKHNBNYN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\SQRKHNBNYN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\UOOJJOZIRH.jpg	5	1021	0a 32 5a fd 1e 19 68 1e 6f 3b fd 04 39 3e 1b fd 66 08 fd fd fd fd fd 66 04 25 fd fd 3e fd fd 38 fd 2e 2e 5b 15 fd 3c 3c fd 31 fd 03 67 75 33 fd fd fd fd fd 6f 5c 50 fd fd fd 21 fd 61 fd 04 fd 14 33 29 0f 77 fd 44 fd fd fd fd fd 3b 35 fd 02 76 fd 77 fd 17 4d fd 4e 7a 40 15 fd da fd 0a 57 fd 72 fd fd fd 48 fd 57 1d fd fd fd 7a fd fd 3c 23 70 6e fd fd 25 17 fd 00 2e fd fd 4c fd 43 73 24 7c 4e fd 50 fd fd 13 13 00 48 0a fd fd 3b 7f 70 70 fd 09 6a 25 64 12 1b fd fd 68 63 68 63 fd fd 2d fd fd 35 3c fd fd 5a 2f 1b fd 44 35 45 38 fd fd 59 78 fd fd 00 fd 7c 43 42 fd 0d 7c 66 fd 1f fd fd fd 2c 09 00 fd 19 fd fd 60 fd fd 2a 6b 31 78 18 fd 75 fd 45 58 6e fd 68 12 43 fd 64 45 4d fd fd 74 fd 27 fd fd fd 3e fd 09 00 16	2Zh;>ff%>8..<<1gu3o\P!a3)wD;5vwMNz@WrHW<#pn%.LCs$|NPH;ppj%dhchc-5<Z/D5EYx|CB|f,`k1xuEXnhCdEMt'>	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\UOOJJOZIRH.jpg	1026	256	64 30 fd 54 fd 77 fd fd fd 40 fd fd fd fd 5f 56 18 01 50 58 fd 2f fd 0b 34 fd 55 06 57 fd fd 52 fd 44 fd fd fd 52 26 69 cf 30 fd 41 6d 09 a4 fd 13 15 fd 58 fd 3e 48 03 fd 01 fd fd 43 60 fd 39 fd fd 4e 76 5b 68 0f fd 37 fd 1b 29 71 3c fd 48 fd 7d fd fd fd 46 73 fd 76 3d fd fd fd 3c fd fd fd fd 06 2d 27 69 fd fd 15 fd fd 30 6f fd 32 fd fd 20 fd fd 7e 61 fd fd 03 fd fd 1d fd 75 fd fd 42 37 fd 15 63 28 63 fd fd 14 fd fd 73 c4 46 fd fd 11 24 fd 54 06 fd 15 1d 41 fd 5d fd fd fd 6d 20 fd 24 fd 05 fd 64 5d fd 79 fd 5a fd 5b fd 3f 5c 59 fd 48 fd 62 fd 0f 48 48 0b 7a fd fd fd fd 0d 50 fd 13 fd 78 04 fd 74 fd fd fd 1c 3b 1b fd 46 fd fd 58 4f fd 39 fd 55 15 fd 4b fd fd 15 14 45 54 45 fd 50 fd 78 16 5c fd 08 fd fd 4e 7e fd 58 70 fd 6d 57	d0Tw@_VPX/4UWRDR&i0AmX>C`9Nv[h7)<H}Fsv=<-'i0o2~auB7c(csF$TA]m$d]yZ[?\YHbHHzPxt;FXO9UKETEPx\N~XpmW	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\UOOJJOZIRH.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\UOOJJOZIRH.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.jpg	5	1021	fd 61 fd fd fd 45 06 fd fd 5b fd fd c3 50 3a 0b 67 44 52 fd fd fd 66 04 55 0d 27 fd 68 3d 40 fd 5c fd 66 fd fd fd fd 61 fd 18 70 fd 35 fd 75 7a 7b fd fd 15 fd 11 57 fd fd 68 fd fd 2b fd 21 62 03 5a 12 1b fd fd c4 fd 33 17 20 fd fd fd 49 fd 24 fd fd 47 fd fd 15 63 fc fd 2d fd 79 fd fd da fd 07 0a 78 2a fd 79 fd 67 56 1f 5a 78 fd 31 fd 44 48 fd 58 0f 56 fd 30 29 fd fd fd fd fd 19 6d 39 fd fd fd fd 04 fd 42 fd fd 0a fd 75 fd 1a fd fd fd 6d fd 2f 3c 0e fd 57 fd 1d fd 75 fd 68 c5 69 1d 4a fd 34 55 3c 5c fd 1e fd fd 5d fd 4a 01 fd 12 17 65 fd fd fd fd fd 64 7e fd 0a 37 75 5f 19 fd fd 4c 93 39 fd 23 05 42 1a fd fd fd 41 fd 6e fd 62 fd fd 10 1e fd 72 fd 76 fd fd 3c 7c fd 03 fd 12 28 74 62 00 fd 22 73 60 17 fd fd	aE[P:gRfU'h=@\fap5uz{Wh+!bZ3 I$Gc-y*ygVZx1DHXV0)9Bum/<WuhiJ4U<\]Jed~7u_L9#BAnbrv<|(b"s`	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WKXEWIOTXI.jpg	1026	256	fd fd 22 fd 6d 77 fd 3b fd 21 fd fd 6f 7a fd 6b fd 68 38 fd 5f fd 4b 37 3e fd 17 71 fd 2f 6b fd 5d fd 39 1c 52 fd fd 50 fd fd fd 6d 1c fd 4c 36 1f 3f 77 21 12 32 d0 fd 60 46 fd fd 5f fd fd fd fd fd 30 fd f3 fd 11 7f fd 36 23 fd fd fd 5d fd 0f fd 7c 02 2c 42 fd 5e fd fd fd 62 fd fd fd 7b 56 fd fd 7c 24 2c fd fd 5d fd 4e fd 52 07 24 fd 45 6d 62 56 75 12 fd 31 fd 28 33 fd 39 15 3f 2c 3e 02 fd 5e fd fd 37 fd 2e 01 5f fd 36 2b fd 2d 2a fd fd 79 03 fd 00 50 fd fd 57 0f 0b 00 fd fd fd fd 7e fd 78 48 fd 11 68 35 49 fd 4a fd 44 23 fd fd fd fd fd fd 04 50 4d 3f 26 03 5e 35 fd fd 3c 1e 00 fd 44 fd 2a 42 1f fd 31 6a 6c 6c 7f fd 63 fd 73 30 fd 06 60 2c 27 2d 54 fd 1f 50 54 fd fd fd 05 1c fd fd 06 fd 1b fd 32 53 fd fd fd 54 fd 38 53 fd 47 fd 3a	"mw;!ozkh8_K7>q/k]9RPmL6?w!2`F _06#]|,B^b{V|$,]NR$EmbVu1(39?,>^7._6+-*yPW~xHh5lJD#PM&^5<D*B1jllcs0`,'-TPT2ST8SG:	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.mp3	5	1021	fd 4a 17 fd 20 fd fd ff fd 76 fd 23 26 fd fd 7c 24 7e 30 fd 02 66 fd 5e 03 fd fd 53 fd fd fd 03 65 fd 7f fd 65 fd fd 41 fd 0f fd 63 fd 17 fd 53 22 13 55 64 fd 60 04 fd 64 fd 64 fd 47 fd 5f fd 4b 50 fd 49 fd fd 72 fd 15 fd 2c 02 21 35 fd fd fd fd 4f fd 58 73 59 11 09 fd 67 fd d7 2d fd fd 45 fd fd 7a fd 04 fd 0a fd fd fd fd 27 fd 35 14 7f fd 70 fd 31 0c fd 18 fd 36 fd 7c 48 34 fd 41 02 05 fd 4a fd 54 54 fd fd 66 03 27 04 fd 05 fd 1a 27 fd 29 fd 1c 49 fd 2b 07 6f fd fd 1f 70 fd 1c 36 fd fd 09 fd fd fd 1a fd fd 08 fd fd 03 6a 10 fd fd 32 19 fd 05 fd 56 fd 3a 61 6d fd 3d fd fd fd fd fd 59 02 fd fd 34 6a 49 fd 79 fd fd fd fd fd fd 1e 49 fd 64 08 1a fd fd fd fd fd 0a 5c 46 16 fd fd 3c 7a 65 1d 14 fd 42 fd 78 2b 39 16 64 03 41	J #&|~0f^SeeAc"Ud`dG_KPlr,5XsYg-Ez'5p16|H4AJTTf")I+op6j2V:a m=Y4jIyId\F<eBx+9dA	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WKXEWIOTXI.mp3	1026	256	6a 2c 5a fd 5b 70 4e fd fd 64 fd 69 4e 9e 00 36 45 25 fd 33 fd 6e fd 1a 11 fd fd 47 75 47 3b 39 fd 4c 26 fd fd 66 fd fd fd 1f fd 00 fd 64 38 fd fd fd 0a 65 fd fd 16 05 04 2c fd 5d fd 4c 7f 0d fd 01 0e fd 44 3b fd 3e fd fd 13 fd fd 44 fd 6d 6d fd e9 fd fd 78 41 55 5f fd fd 73 13 4b 02 11 fd 58 3d 49 fd 67 1a a0 02 fd fd 5a fd fd 4d fd fd 47 fd fd 3d 67 fd 9e 45 fd fd fd fd fd 71 fd 1e fd fd fd 30 72 79 fd 69 fd fd fd fd fd 5f fd 44 fd fd 6e 3a fd 1b 6d fd fd 66 03 79 fd fd fd 69 fd fd 1d 4d fd 53 fd 2c 49 06 7c 51 fd 35 11 46 fd 57 fd 8a 05 79 62 7b 61 fd fd 1c 24 34 09 fd 2b 0e fd 5f 2b fd 56 fd fd fd 3b fd fd 20 38 59 79 83 fd 48 68 fd fd fd 7a fd fd fd fd 03 fd fd fd 2f 31 fd 6d fd 4a fd 6f 72 fd fd fd 70 fd fd 37	j,Z[pNdiN6E%3nGuG;9L&fd8e,]LD; >DmmxAU_sKX=IgZMG =gEq0ryi_Dn:m fyiMS,|Q5FWyb{a$4+_+V ; 8YyHhz/1mJorp7	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.pdf	5	1021	fd 6f 40 fd fd 0c 2f 11 fd fd 42 78 fd fd fd 43 fd 19 fd 26 59 56 fd fd 13 31 fd 62 18 7b fd fd fd 46 fd 35 41 78 fd 2c 33 41 30 fd 3f fd 17 07 24 11 30 fd fd fd 52 40 fd fd fd fd 46 fd 70 6e 43 4c 2e fd 2a 2e 14 4f 53 fd fd 0b 49 fd fd fd fd 42 39 fd 7b fd 5d fd 4d fd fd fd 01 fd fd fd 30 6a fd 3d fd 21 fd 6b fd 42 fd fd 66 fd 13 46 fd fd 3c fd 7f fd fd 02 fd 0d fd fd 37 14 fd fd 0b fd 23 fd 49 10 7d fd 65 6a 78 fd fd 59 5b 7e fd 32 11 5e fd fd 0d 71 3d fd fd 3b 67 fd 1b 44 58 72 fd 08 fd 7e 43 2a fd 78 fd fd 5f fd 3c fd fd fd fd 77 54 fd 45 fd fd fd 1e 04 fd 00 fd fd 3d 7d fd 3f 65 3f 42 fd 23 fd 57 00 0f 23 56 09 fd 6d fd fd 2b fd 75 fd 2b fd 5d 0a af 5a fd 45 97 3b 5a fd 30 fd fd 0d 66 1c fd fd	o@/BxC&YV1{F5Ax,3A0 ?$0R@FpnCL. *.OSIB9{]M0j=!kBfF<7#I} ejxY[~2 ^q=;gXr~C*x_<wTE=?e? B#W#Vm+u+]ZE;Z0f	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WKXEWIOTXI.pdf	1026	256	fd fd 04 0b 6c 2e fd 01 32 00 6c fd fd fd 7b 0a fd 6c fd 2f fd 67 04 71 fd fd 93 0b fd fd 60 56 fd fd fd fd 2c 6a fd fd 17 09 04 fd fd 00 24 fd 23 fd fd fd 15 67 fd 3f 7a 5c 3e fd 47 fd 73 2f 3c fd 6d fd b4 fd 12 fd c3 31 33 19 fd 3e 0e fd fd 12 14 fd 6a 1a 4c fd 04 fd 1e fd 11 5d fd fd fd fd 5e 13 02 fd fd 2c fd fd 76 19 fd fd fd fd 19 fd fd fd 21 fd 1f 17 55 0c fd fd 2b 91 5b fd 44 fd 32 fd fd 53 1f fd 3a 20 fd fd 52 2e fd fd 19 50 fd 4c fd 32 fd 02 2e 2a 57 5c fd 56 4f fd 16 fd fd 6e 50 fd fd fd fd 5d fd 65 2e fd fd fd 7d fd 0a 64 74 fd 54 73 17 5a fd fd fd fd 10 fd fd fd fd 09 fd fd fd fd 30 fd fd 51 fd 1c fd fd fd 1d fd 67 fd 61 36 53 28 6a 30 5b fd 3e fd 2f fd 6f 4e fd fd 41 42 2c 71 53 3d fd 27 fd fd 3c 3b fd fd 3a	l.2l{l/gq`V,j$#g? z\>Gs/<m13>jL]^,v!U+ [D2S: R.PL2.*W\VOnP]e.} dtTsZ0Qga6S(j0[>/oNAB, qS='<;:	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\WKXEWIOTXI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.docx	5	1021	33 58 35 fd fd 2d fd 62 56 fd 72 fd 2b 6f 1b 3a fd 38 4c fd fd 67 fd 00 55 fd 62 01 10 69 25 7d 3f fd 3b fd fd fd 03 fd 1a fd 52 77 1c fd 0d fd fd 2f fd fd 75 fd 4b fd 69 95 fd 41 fd 58 46 41 fd fd 79 20 28 10 43 fd 48 1d 00 2b 50 06 fd 69 fd 14 78 fd 3e fd fd fd fd fd 5e fd 12 fd fd 46 fd 28 10 fd fd fd 08 fd fd fd fd 0a 4d fd fd fd 15 fd 00 fd fd 19 fd 18 fd 66 3c fd 60 32 fd fd 1c 3c 1a 03 fd 1a 3a 50 3c 05 fd 00 fd 48 73 fd fd fd 4e 3e 48 2b 4a fd 62 fd 51 0f fd 2d fd fd 6f fd 22 fd 35 42 fd 1c 25 3d 77 fd 67 fd 39 84 fd 26 1d 67 fd fd 5d fd 11 fd fd fd fd fd 76 43 4c fd 2c 54 1d 72 2c fd 15 fd 21 fd fd 47 fd fd 20 15 42 fd fd fd 7c fd 72 fd fd fd fd fd 5d 20 49 4a 58 fd 0c 1d 2d 79 fd 57 45 fd fd fd 4f 12	3X5- bVr+o:8LgUbi%}?;Rw/uKi AXAy (C+Pix>^F(Mf<`2<:P<Hs N>H+JbQ- o"5B%=wg9&g]vCLTr,!G B|r] IJX-yWEO	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WUTJSCBCFX.docx	1026	256	fd 7e fd fd fd 2a 27 1a 2d fd 35 fd fd fd 22 fd 3b fd fd 23 fd 70 fd fd 48 71 25 70 56 fd 5e fd 7a f8 f4 12 fd 4e fd 76 70 fd fd fd fd fd 35 fd fd fd fd fd fd fd 56 fd 03 72 17 fd 5b 01 86 7d fd 58 fd fd fd fd fd fd 09 fd 29 5a fd 24 fd fd fd fd fd fd 3c fd 7e fd 01 42 58 42 fd 61 39 fd 4d fd 0d 48 0c 66 fd 38 fd 28 4b fd 77 13 fd 3a fd 54 57 50 fd 4a fd fd fd fd 3e 6d 5a fd fd fd 31 5f 40 47 fd 22 fd f0 59 fd 7e 55 57 43 5d 04 4e 6f 43 68 fd 74 39 fd 5b 0c 02 fd fd fd fd 37 fd 5c 18 fd 19 fd 25 fd 5a fd 10 33 fd fd 5a fd 5f 5c fd 3d fd 73 fd fd fd fd 40 4d 0e fd fd fd 4b 69 1a 3b fd 0b 04 6d 49 e9 5c 30 fd fd fd fd 02 fd 01 34 fd fd fd 1a 27 fd fd fd fd fe fd 2d fd 2b 75 fd fd 4b fd 4c fd 6d 59 fd fd 19 5a fd fd	~*'-5";#pHq%pV^zNp5Vr{}X)Z<~BXBa9MHf8(Kw:TWPJ>mZ1_@G"Y~UWC]Not9[7\%Z3Z_\=s@MKi;ml\04'-+uKLmYZ	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.pdf	5	1021	fd fd fd 2f 06 05 fd 6b fd 39 fd 4c 28 35 fd fd 7a fd 08 fd 23 74 fd fd 7a fd fd fd fd fd 3d fd 61 fd fd 47 fd 72 fd 23 17 fd 3d 6c fd 2b 0b 68 fd 3f fd fd 47 fd 52 19 73 41 42 fd fd 01 fd fd fd 6a fd fd 1f 47 fd 7e fd fd 58 fd 54 fd 74 7d 16 fd c0 12 0b 7c f5 fd 79 06 c6 62 4e fd 28 fd 3c 31 fd 1d 04 fd 43 5e 03 fd 32 36 fd 01 fd fd 6f 1d 67 4e 19 25 fd 4f fd 56 00 fd fd fd fd 29 08 3a fd fd fd fd 66 5e fd fd 6f fd 16 66 48 fd fd 5e 4c 30 38 0d 34 35 11 fd 64 fd 44 1d fd 2c 58 06 46 fd fd fd fd 65 62 fd fd 3c 49 59 14 31 6c 6b fd fd 40 fd 71 32 50 fd 28 fd fd 50 12 9b 42 3b 05 33 59 fd fd fd fd fd 10 31 5c fd 5f 6e 21 fd 3c 53 fd 14 fd 15 26 fd db 01 fd 19 fd fd 26 33 fd 36 fd 27 fd 50 fd 5f fd 2c fd 3a fd fd 13 21 fd 36 fd fd	/k9L(5z#tz=aGr#=lh?GRsABjG~XTt}|yb(<1C^26ogN%OV):f^ofH^L0845dD,XFeb<lY1lk@q2P(PB;3Y1_n!<S&&36'P_,:!6	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WUTJSCBCFX.pdf	1026	256	fd fd 12 79 13 fd fd 2d fd 58 fd fd 11 17 fd 53 fd 08 fd 57 6a fd fd fd 85 3f 60 fd fd fd fd fd 73 fd fd 7a 0d 75 fd fd fd 7a fd 61 fd 5f fd 0c fd fd 94 50 fd 11 18 fd 02 fd 18 1f 09 3f fd fd fd fd fd bc 10 7d 1b 6d fd 2e fd 42 3d fd 45 fd fd fd 01 fd 3f fd fd 71 7e fd 10 2a fd fd 39 63 44 fd fd 10 5f fd 33 fd fd fd 28 6a fd 67 54 0a fd 7d fd fd 3e 1a 54 fd fd fd fd 4b 4d fd fd 7f 2c fd 15 fd 07 6d 0e 52 56 26 54 15 38 fd 55 fd fd 57 fd 78 66 1d fd 65 fd 71 fd 1f 40 66 58 fd 44 fd fd fd 38 11 fd 5c fd 4a fd fd fd 34 26 47 fd 4e 4c fd 7b fd 67 78 07 fd 6a 2d 52 fd fd fd 4a fd fd 0b fd fd fd 0a fd fd 44 fd 43 3a 31 fd fd 02 fd 01 72 fd fd fd 65 fd 09 72 ba fd 2f 43 fd fd fd fd fd 69 56 fd fd 3c 12 4e fd 7b fd fd fd 42 fd 3a	y-XSWj? `szuza_P?}m.B=E? q~*9cD_ 3(jgT}>TKM,mRV&T8UW xfeq@fXD8\J4&GNL{gxj- RJDC:1rer/CiV<N{B:	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\WUTJSCBCFX.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\YPSIACHYXW.docx	5	1021	26 fd 42 fd fd 07 fd 49 fd 3d 69 55 fd 1a 41 5a fd fd fd fd fd 14 fd 5f 24 5c fd 54 73 44 fd fd 35 fd fd 66 1a fd 50 fd 15 20 49 34 3b 3a 15 fd fd 70 23 fd 3b 68 05 13 fd 38 4f fd 1d fd 31 2c 10 fd 1f 74 26 02 16 6e fd 50 fd 2a fd 70 fd 7a fd fd 31 7d 22 1c fd 27 3d fd db 36 60 1f fd b4 fd 76 fd 24 0a 04 31 3f 22 3f 45 fd 2b 17 fd 17 fd fd fd fd 79 fd 5b fd 04 fd 4f fd fd 07 fd 60 27 fd fd 6c fd 70 fd 46 fd 12 1e fd fd 50 fd 2a 36 64 fd fd fd 02 fd 57 3b 2a 1f fd 6a 25 fd fd 64 40 fd fd 60 fd 34 fd fd 65 3f fd 7a fd 38 22 2c 59 23 fd 98 fd fd fd 32 fd 7a 7b fd fd 66 21 fd 1e fd fd 5b fd 0a 44 6a fd 3c 7f 35 1b fd 4a fd fd 36 fd fd 74 fd fd fd fd 58 fd fd 0a fd fd 27 fd fd 63 fd fd 52 fd 48 fd fd 49 69 25 4f fd 72 15	&BI=iUAZ_$\TsD5fP l4;:p#;h8O1, t&nP*pz1}""=6`v$1?"? E+y[O`lpF P*6dW*j%d`4e? z8",Y#2z{f![Dj5J6 tX'cRHIi%Or	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\YPSIACHYXW.docx	1026	256	6b 68 15 43 2f fd 27 fd 07 fd 18 4f fd 6e fd 31 fd fd 31 fd 11 fd 15 3e 72 fd 72 0a 7e 78 fd fd fd 6e fd 18 fd fd fd 2a fd fd 24 fd 5b 2d 7f 33 20 37 fd fd fd 62 54 fd fd 76 fd 7e fd 69 74 fd 74 4b fd 26 fd 6d fd 43 fd 6c fd fd fd 00 fd fd 03 1f 2b 61 fd fd 32 fd fd 28 fd 4a 76 fd 49 fd 4d fd fd fd fd 3f fd fd 74 67 53 1c fd fd fd 2e 4f fd 76 30 35 fd 5f fd 6a 71 59 fd fd fd fd 7d fd 3a 74 03 42 fd 2a fd fd 16 f1 22 27 fd cc fd 7a 6c fd 2f 29 3a 2a fd 7d 51 fd 03 fd fd fd fd fd fd fd 72 2f 0e fd 00 fd fd 74 66 fd d8 fd 31 1b 0e 2e 67 fd 70 fd 01 04 34 22 39 fd 1c fd 74 13 2d 06 4f 4c fd 6e fd fd fd 73 15 35 49 32 79 fd 49 6e 24 fd 2f fd 75 fd 6d 25 42 fd 2e fd 13 11 0d 46 60 fd fd fd fd fd fd 58 0c 1d 7e 47 fd fd 28 fd b7	khC/'On11>rr~xn*$[-3 7bTv~ittK&mCl+a2(JvIM? tgS.Ov05_jqY}:tB* "'z):"}Qr/tf1.gp4"9t-OLns5l2yI n$/um%B.`X~G(	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\YPSIACHYXW.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\YPSIACHYXW.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Documents\YPSIACHYXW.jpg	5	1021	fd fd fd 68 fd 7a 36 37 fd 07 fd 95 46 0b fd fd 26 69 08 fd 6e fd 79 08 0d 44 fd 76 3e 5b 42 55 20 54 fd fd 0c 68 2e fd fd fd 7e fd 17 fd fd 56 fd fd 17 fd 40 fd 77 fd fd 0a fd 69 fd fd 6d fd fd 58 fd fd 39 15 3e 43 42 fd fd fd fd fd fd 35 fd 0d 13 fd fd 39 66 fd fd 7e fd fd 9b fd 67 fd 7c 5f fd fd 19 fd fd fd 51 5e 6f 4c 06 7a fd fd fd 03 fd fd fd fd 63 fd fd fd fd fd fd 10 54 fd 76 29 40 00 0e fd fd fd fd 3c 33 fd 49 fd fd 7b 19 fd 74 fd 33 21 60 fd fd 21 fd 2a 0b fd 38 fd 5d fd fd 23 fd 91 77 4d fd fd 45 10 fd fd fd 68 08 e9 fd fd fd fd 2c 1e 6d 4c fd 6a 72 64 fd fd 4d fd fd 26 fd fd 39 fd fd fd fd 3f 3c 1a fd 16 fd fd 04 fd fd fd 6f fd 83 08 78 f4 08 21 fd 7b 73 fd 0a fd fd 34 fd fd fd fd 14 39 46 43	hz67F&inyDv>[BU Th.~V@imX9>CB5 f~g|_Q^oLzcTv)@<3l{t3!` !*8]#wMEh,mLrdM&9? <ox!{s9FC	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\YPSIACHYXW.jpg	1026	256	fd 5b fd fd 00 fd fd 27 fd fd 61 fd 56 fd fd 57 fd 9a 07 fd 2d 3d 3a fd 88 54 26 fd fd 77 4c 34 fd 7e 58 44 14 5d fd 25 fd fd 4d 19 4d 2a fd fd 49 16 09 2b 11 3a fd 08 fd 6e 66 1f 0c 2a 24 12 29 fd 08 fd 66 64 fd fd 7d fd 53 fd 1b fd fd fd 38 48 fd 04 fd e4 63 0d 34 28 fd fd 94 44 fd 21 fd 67 fd 78 2f 0a fd fd fd 56 fd 23 fd fd 45 4e 50 fd 61 fd fd 24 fd 7a 35 03 fd fd 00 4c fd 3a 17 19 fd fd 34 03 42 4d 6c 08 2d fd fd fd fd fd 21 fd fd 39 fd fd fd 52 fd fd 38 09 0a 69 28 fd 55 4f fd fd fd 79 fd 51 fd 2e 09 1c fd 69 fd 0b 31 6b fd fd 32 fd fd 4c 1a fd fd fd 45 5b fd fd 53 fd fd 1a 25 6d 13 68 fd a8 65 33 75 fd fd fd 37 fd 44 0e 2a fd fd fd fd 17 1d fd 0a 2d 3f fd fd fd 00 fd 46 0d fd 15 fd fd 7c 4b fd 27 4d 06	['aVW-=:T&wL4~XD]%MM*I+:nf*$)fd}S8Hc4(D!gx/V#EPa$z5L:4BMl-!9R8i(UOyQ.i1k2LE[S%mheu7D*?F|K'M	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\YPSIACHYXW.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\YPSIACHYXW.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe	0	9728	4d 5a fd 00 03 4f 41 fd fd fd fd 1f fd fd fd 2d fd fd fd 67 fd 4f fd 71 fd fd 39 24 c3 40 34 66 fd fd 13 45 22 fd fd 30 0d 7f 41 48 fd fd 7c fd 76 16 10 73 fd 10 06 fd 16 fd fd 50 60 77 31 fd 78 27 fd 51 fd b0 00 fd 70 2a fd 7d 75 28 3d 4e fd 79 0b 29 34 fd fd 74 6a 3d fd fd 5c fd fd 33 6b 68 61 41 fd 27 53 fd 2b fd fd 63 13 fd 2e fd 64 fd fd fd 11 fd fd fd 32 3f 31 fd 0d fd 40 5f 38 1d 31 fd fd fd fd fd db 27 ac 15 fd fd fd 44 69 2e 13 fd 04 fd 38 fd fd fd 4f fd 11 fd fd 01 25 23 20 2f bc fd fd 37 33 fd 71 10 04 fd 3a 06 fd 70 3a fd 52 33 fd 1e fd 5c fd 27 fd 50 fd 2c 27 cd 78 96 71 2a 79 fd 38 55 fd 6c fd 16 59 63 fd 04 26 1c fd fd fd 7c 2e 01 fd fd 22 70 1c 4d fd fd fd fd 36 3f 42 fd 23 39 fd 45 53 31 fd fd	MZOA-gOq9$@4fE"0AHvsP`w1x'Qp*}u(=Ny)4tj=\3khaAS+c.d2?1@_81'Di.8O%#/73q:p:R3\'P,'xq*y8UlYc&|"pM6?B#9ES1	success or wait	1	41E301	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\ZBEDCJPBEY.pdf	5	1021	16 fd fd 64 fd fd 79 45 6f 2b 4a fd fd 31 fd fd 20 68 7b fd fd 09 fd 12 fd 10 6c 2d 7b 68 12 fd 3e 03 7c 6c fd fd fd fd 77 00 61 fd 56 fd 0e 56 fd fd 0e 16 06 fd 0c 6d fd fd 19 15 fd fd fd 1d 43 fd fd 0d b2 44 3c 24 fd 62 fd 20 fd 27 76 64 2f 2e fd fd fd fd 08 fd fd fd 64 fd 4a 46 1e fd 20 fd 19 73 68 1c fd fd 11 34 54 17 fd fd fd 55 1b 10 fd 1c 72 fd 74 fd fd fd fd f5 fd fd 71 fd 0b 41 77 66 14 3b 78 fd 3a 78 21 fe 1c 1a fd 3c 54 fd 0e fd 6c 58 fd 6f 15 33 fd 66 74 fd 48 6d fd 13 0f fd fd fd 4a fd fd 09 fd fd 13 0c fd 49 33 31 fd 4e fd fd 14 fd 2c 7c fd 11 33 fd 2e 98 fd 55 fd 54 fd 19 60 4c fd fd 0a fd 54 24 fd 56 72 07 01 20 fd 2f fd fd fd fd 17 fd 45 fd 2c fd 38 fd fd 74 18 fd fd fd 27 4f fd 49 fd 63 fd fd 68	dyEo+J1 h{l-{h>|lwaVVmCD<$b 'v d/.dJF sh4TrtqAwf;x:x!<TlXo3ft HmJl31N,\|3.UT`LT$Vr /E,8t'Olch	success or wait	1	411859	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.pdf	1026	256	fd 55 fd fd 5f fd 13 7a 49 fd 6d fd fd fd 4a 05 fd 77 50 5c 08 fd 56 fd fd fd 6b fd fd 23 fd 1d fd 7e fd fd 08 76 fd 72 54 fd 06 66 fd fd 3d 2f 48 15 78 fd fd 3a fd 4f 19 0a 1b fd 34 fd fd fd fd 41 fd 0b 21 fd fd fd 5e fd c0 fd fd 63 4b fd 45 fd 7f fd fd 26 fd 29 fd fd fd 75 04 4a fd 7b 37 fd 37 34 fd fd fd fd fd 4f fd fd fd 4b fd 6a a8 0a 58 63 fd fd 40 fd 04 67 fd 7b fd 41 fd fd 01 fd 68 0d 52 af 23 fd fd fd 0b fd fd fd 5c fd fd 5c 29 7d fd 23 4f 28 65 5d 25 fd 7a fd fd 2b fd fd 07 31 14 fd fd fd 13 17 4f fd fd 4a 3b 66 fd 14 fd fd fd fd 43 fd 72 3a 43 fd fd 0b fd fd fd 2b fd fd fd fd 53 fd fd fd 49 fd fd fd fd 2d 30 38 fd fd fd fd 1c fd fd fd 4d fd 08 37 5d fd fd 1c fd 7c 62 79 fd fd 26 37 fd fd fd 45 66 67 05	U_zImJwPVk#~vrTf=/Hx:O4A!^cKE&)uJ{774OjXc@g{AhR#\\)} #O(e]%z+1OJ;fCr:C+SI-087]|by&7Efg	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	5	1021	fd fd fd 66 2f 25 1d 4b 3c fd 68 00 27 fd 62 1e 47 fd fd 32 fd fd 79 6b 6d 21 79 fd fd fd 28 fd fd fd 7b 00 3a fd 59 06 fd 61 20 09 fd fd fd 04 fd fd 04 35 fd 17 fd 05 fd fd fd 2d fd 79 5e 1e 61 fd fd 37 10 fd 7f 33 fd fd 1e 2d 03 fd fd 2a fd 51 34 1c 0d 01 fd 41 fd 1e fd 0c 79 fd 0b fd b2 51 fd 72 fd bb fd 6c 9d 57 fd fd fd fd 28 76 28 f7 fd 7a 58 0b 38 fd 73 fd 31 4c 7c 56 19 1f 0f fd 20 75 fd 73 fd 4e 5a 57 70 2a fd fd fd 75 76 fd 11 29 57 2f fd fd fd fd fd 35 fd fd fd 34 fd 6d 43 95 fd 3e 45 76 fd fd 76 65 fd 51 6e 6c fd 34 49 fd fd fd 7a 01 5c fd 07 fd fd fd 73 fd 58 15 fd fd fd fd fd 13 fd fd fd 39 fd 7b 72 fd 50 fd 09 fd 2a 2a fd a1 fd fd 7e fd 4e 36 22 3a 71 58 fd 67 44 43 00 8c 63 fd fd 3f fd fd 76	f/K<h'bG2ykm!y({:Ya 5-y^a73-*Q 4AyQrlW(v(zX8s1L|V usZWp*uv)W/ 54mC>EvveQnl4Iz\sX9{rP**~N6":qXgDCc?v	success or wait	1	411859	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	1026	256	fd fd 1f fd fd 72 fd fd 62 48 fd 0d 12 32 fd fd 3a fd 3d fd 3b fd fd 5f fd fd 00 29 2d fd fd 32 fd 58 3e fd fd fd fd 60 3e 7f fd 28 fd fd fd 6a 45 fd fd 5b fd 1a 3c fd 2a fd 76 70 fd 06 17 fd fd fd fd 61 fd 2f 01 56 6a fd 3f 5c 48 fd ba fd 52 62 56 6e 36 56 5e 5c a2 1f fd fd 20 33 fd 19 73 fd fd 25 27 fd 08 fd fd fd fd 28 49 fd 7a 7e 39 2e fd 43 3a fd fd fd fd fd 74 fd fd fd 6a fd 0e fd 64 0c 60 fd fd 2b fd 7f fd 58 fd fd 6d 11 26 01 fd 2a 27 fd 10 33 62 fd fd 7c fd fd fd 60 1c 68 24 fd fd 7b 69 66 6c fd fd 6b 52 fd fd 2e fd 1e 55 77 fd fd fd fd 51 11 fd 0e fd 6f 11 fd 1f 04 fd fd 5f fd 11 fd e0 fd 5b fd fd 15 fd fd 22 fd 67 4d fd fd 6d f5 0c fd fd fd 7c 58 fd fd 2c 1e fd 57 74 fd 2b fd fd 12 fd d4 fd 2a fd fd 31	rbH2:=;_)-2X>`> (jE[<*vpa/Vj?\HRVn6V^\ 3s%'(Iz~9.C:tjd`+Xm&*' 3b|`h${iflkR.Uwo_["gMm| X,Wt+*1	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BPMLNOBVSB.jpg	5	1021	fd 59 08 68 50 2a a3 fd 5e fd 1a 13 fd 7b fd 47 fd fd fd fd fd 77 09 3b fd 4f 10 fd fd fd fd 72 fd 60 58 5a 7c 69 1d 34 fd fd 26 0b 64 3f 41 fd 52 7f fd 19 4d fd fd 6d 15 fd 4a fd 33 0d fd 6e 67 fd 3c fd fd fd 0b 74 fd fd 03 fd 75 fd fd 53 73 fd fd fd fd 34 4e fd 3f fd 5b 2f fd 1b fd fd 13 fd 3a fd 26 42 06 fd 68 fd fd 66 fd 38 7b fd 18 6b 38 0b fd 4e fd fd 43 fd 40 fd fd 51 fd fd 54 0f 54 fd 4d fd 55 15 fd fd 0c fd fd fd 3a fd 73 76 fd 1a fd fd 10 fd fd 07 2e 7f fd 22 d1 4f fd 4c a3 53 7f 3f fd 27 fd 08 66 75 fd 57 26 5d fd 0b fd fd 02 fd 50 1b 28 fd 3f fd 0c 2f 13 47 2c 54 02 28 42 fd 36 17 fd 0b 0b 08 4b fd fc 1b 26 fd 3c fd fd 79 30 fd 37 fd fd 36 66 fd 5d 31 fd 4c 6b 6a 02 fd fd fd 29 0d fd 14 5c 22 fd fd 18 08 2e	YhP*^{Gw;Or`XZ|i4&d?ARMmJ3ng<tuSs4N?[/:Bhf8{k8NC@QTTMU:sv."OLS?'fuW&]P(?/G,T(B6K&<y076]1Lkj)\".	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.jpg	1026	256	fd 55 fd 2c 78 fd 49 fd 09 28 24 05 22 fd 7c fd 33 6e 06 fd 0b 36 2f fd fd fd 10 52 3f 2b 2c 46 fd fd 1b fd fd 64 fd 08 29 18 61 3e d4 fd 67 6a 27 1a fd fd 4c 20 fd fd fd fd 14 fd 1e 07 0b 33 2c 48 6f 3a 2f 54 13 fd fd fd fd 2a 56 fd fd fd 7e fd 39 4e 5e 10 fd fd 48 fd 7c 48 68 3f fd 0b fd 57 fd fd 75 70 54 fd fd 54 fd 3f 5b 4a 0c fd fd fd 3e 19 fd 38 65 fd 00 55 fd 71 fd 3f 4a 20 0a 26 fd fd fd 0d 09 fd 33 fd 44 0d fd 68 21 64 fd 19 7a fd fd fd fd fd 6a 1c 00 fd fd 21 fd 75 5f 11 3f 40 4c fd fd 34 fd 07 fd fd fd 2f fd 16 2e 2d fd 71 fd 3e fd 49 76 52 3b fd fd fd fd 9f 76 60 34 27 53 fd 0e 6f 04 fd fd fd 70 fd 0f 3b 2e fd 0a fd 6d 1c fd fd fd 20 fd fd fd 6b fd 60 fd 1a 0d fd fd fd 4e fd 67 fd 4f 2e 39 00	U,xI($"|3n6/R?+Fd)a>gj'L3,Ho:/T*V~9N^H|Hh?WupT?[>8eUq?J &3hdzj!u_?@/.-q>IvR;v4'Sop;.mk`NgO.9	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	5	1021	fd fd 46 fd fd 67 fd 5a fd fd 58 40 fd 7b fd 07 25 fd 6f 42 3f 1d fd 3d 0f 6c 1e fd 0c fd fd 6d 14 52 fd 36 fd 76 00 c7 16 fd 01 73 fd 7d 22 fd 67 fd fd 5a fd fd 71 fd c8 39 6f 30 57 fd fd fd fd fd 43 fd 72 fd 5c 34 1a c6 7d 3f 21 d3 79 fd 47 5d fd 40 fd 03 23 3b fd 39 fd 28 fd fd fd 1a fd fd 76 39 fd fd 17 fd 5c 5e fd 1a 6d 35 3b fd fd fd 52 24 79 fd fd 7c 59 14 23 fd 17 2e 05 fd 5f 02 2f 73 fd 1d 7e fd 4e 1e fd 6a fd fd 15 fd fd 76 fd fd fd fd e1 11 fd 55 fd 2b 5d fd 07 fd fd 67 ee fd fd fd 12 27 65 fd fd 2b 17 04 58 12 fd 22 30 fd fd 62 4e fd 19 6f fd fd fd 16 66 fd 3e fd fd 45 7d 1d 2f fd 09 2a 1e 13 fd 16 fd 52 fd fd 24 60 1e 1a 2e 41 fd 01 24 03 0a 1d fd fd 5f 4e 6a 4a 4f fd fd 0a fd fd 7b 02 5f fd 61	FgZX@{%oB? =lmRvs}"gZq9o0WCr\4} ?!yG]@#;9(v9\^m5;R$y\|Y #._/s~Nj vU+]g'eX"0bNof>E}/*R$`. A$_NjJO{_a	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	1026	256	77 31 56 f5 fd fd 76 20 fd 10 0a 68 6a fd 32 2a fd fd fd fd 63 fd fd 7c 39 fd fd 62 fd 37 fd 63 fd 0c fd 38 fd fd fd 5b 38 fd 6f fd 99 18 42 4a 17 3c 27 6e fd 50 6a 26 02 fd fd 17 fd 31 fd fd 00 04 3e fd 13 34 fd fd 52 04 37 fd 29 fd fd 5e fd fd 7e 68 a3 fd fd 3c a6 fd fd 30 6b 45 0e 4a fd fd 40 32 fd 73 44 04 fd fd 70 fd 07 fd 6b 7f 38 70 fd fd fd fd 05 11 32 5b 2c 11 7e fd fd fd 50 77 fd 09 fd 0f fd 75 77 fd 0f 1a fd 40 fd fd fd fd 6b fd fd 4e 26 24 06 7d fd 50 53 fd 14 12 fd 22 fd 7c fd 03 63 06 fd fd fd fd 0a 6b fd 6e 6f fd 7f 75 6f 05 07 fd 62 fd fd 4d 21 0f fd 60 38 fd fd 2f 7b fd fd 76 61 fd 34 37 69 fd fd 10 24 fd 40 fd fd 27 fd 79 27 5d fd fd 7a fd 35 5f 41 00 64 4a 03 10 48 69 fd 77 fd 67 fd 78 79 55 36	w1Vv hj2*c|9b7c8[8oBJ<'nPj&1 >4 R7)^~h<0kEJ@2sDpk8p 2[,~Pwuw@kN &$}PS"\|cknouobM!`8/{va 47i$@'y']z5_AdJHiwgxyU6	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\FENIVHOIKN.png	5	1021	60 4d 6b 08 fd 55 11 33 fd fd 0e 63 fd 4e fd fd 12 04 fd fd 29 34 7f fd fd fd 15 fd 1c 1e 4c fd fd 3e fd 33 0a fd 65 3a 30 fd 11 43 6a fd 1b 69 fd fd fd fd 4c 21 fd fd 10 fd fd fd fd 39 3b 4f fd 7f 6a 5c fd 4b 57 17 13 fd 08 05 1c 34 fd 56 14 fd fd 25 fd 1c 2f 1c fd fd fd 09 35 fd fd 2a 83 fd 03 76 49 3e fd 20 fd 76 fd 2a fd fd 2d 18 fd 53 78 35 3d fd 45 17 73 fd 26 fd 27 fd 67 59 6f 7b fd fd fd fd 17 06 fd 5e 16 fd 5b 35 fd 32 fd fd fb 66 fd 7f 0c fd 16 52 fd 66 74 06 2b fd 6e fd 17 fd 7d fd fd fd fd 78 fd fd fd 44 fd 7b 74 2c fd 5b 2f fd fd 10 19 fd fd 18 fd 00 42 17 67 fd fd fd 0b fd 30 0e fd 09 28 fd fd 3a 53 fd fd 23 7a 71 39 fd 3a fd 4c fd fd fd fd 4a 42 fd fd fd 20 fd 19 fd 4e 6f fd 7a fd 7a 40 fd fd fd fd 78 fd fd fd 16 fd 08	`MU3cN)4L>3e:0CjiL!9;Oj\KW4V%/5*vI> v*-Sx5=Es&'gYo{^[52fRft+n}xD{t,[/Bg0(:S#zq9:LJBNozz@x	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\FENIVHOIKN.png	1026	256	6c 57 fd fd 49 7e 42 60 fd fd fd 32 56 20 56 24 64 fd fd 22 61 fd 54 10 07 fd 45 fd 73 fd 25 fd fd 26 c0 65 55 01 07 74 fd fd fd 5b fd 74 09 65 fd 0e 3c 3c 29 fd 44 1b fd 58 fd fd fd fd 38 28 11 18 fd 19 2e fd fd 13 fd 4d fd 55 60 73 fd fd 60 fd fd 01 fd fd 3e 2a fd 2b 50 fd fd fd 0f fd fd fd 02 45 23 fd 3e fd fd fd fd fd e7 fd 0f 03 fd 4e 1a fd fd fd fd 1c 71 09 fd 4c fd 21 64 fd 1b fd 4f 0d 1d 49 3f fd fd 25 fd 06 fd 45 0c 1b fd fd fd 05 fd fd fd 69 7e 08 28 70 fd 62 7d fd 34 15 66 7f fd fd 10 0b 24 fd 4c 19 fd fd fd 47 28 fd fd 1a fd fd fd 76 fd 28 2f fd 0d fd fd 46 fd fd 1c fd fd 09 fd fd fd 24 7f 3a 66 2e fd 5d fd fd 17 fd fd fd fd fd fd 35 60 fd 4f 3f 2a fd 14 fd 11 fd 08 23 fd fd 72 fd fd 1b 0b fd 1c fd	IW~B`2V$d"aTE%&eU[te<<)DX8.MU`s`>*+PE#>NqL!dOI?%i~(pb}4f$LG(v(F$:f.]5`O?*#r	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\FENIVHOIKN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\FENIVHOIKN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\JSDNGYCOWY.mp3	5	1021	5a fd fd 5c fd c3 fd fd 33 fd 7d 64 62 22 4b 45 13 fd 30 5f fd 12 56 fd fd 49 6b fd 0a 13 fd 54 fd 2a fd 74 fd fd fd 3d 29 3d 5a fd fd fd 23 2f 28 fd fd 7f 07 fd e8 fd fd 1c fd fd 4c 25 56 fd 75 fd 11 fd 66 70 01 46 15 fd fd 3a 10 02 fd fd 16 77 76 78 fd fd 19 fd fd fd fd 7d 6d 7c fd 49 a2 fd fd fd 5d 24 7a fd fd 15 5f 7a fd f0 fd 50 fd 4e fd 42 00 fd 42 fd 80 fd fd fd fd fd fd fd 5d fd 6d fd fd 6e fd 4e fd 19 1f fd 62 fd fd fd fd fd 13 fd 65 75 fd fd 1c fd 41 31 fd fd 36 5e fd fd fd fd 75 fd fd fd 51 64 76 3a fd 3d fd 76 1e 66 fd 53 33 fd 20 fd 34 fd fd 7f 12 fd 50 58 fd fd fd fd 4e 41 fd fd 46 15 1d fd 62 65 fd 33 21 16 49 c4 41 fd 6c 6d 0b fd 4e 2d 05 12 fd 73 fd 79 5b fd 1f fd fd fd 06 55 fd fd fd	Z\3}db"KE0_VIkT*t=)=Z/(L%VufpF :wvx}m|I]z_zPNBB]mnNbeuA1^uQdv:=vfS3 4PXNAFbe3!IAlmN-sy[U	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\JSDNGYCOWY.mp3	1026	256	fd 54 35 2e 33 fd 40 fd 07 fd fd 1e 7a 75 18 fd 63 fd 52 1d 42 fd fd 1a fd 5a fd fd fd fd 10 fd 01 fd fd 13 62 59 fd 23 fd fd 70 3e 17 66 fd 79 27 61 6f 45 fd 29 fd 2f fd fd 21 59 f1 4d fd fd fd fd 67 23 0a fd fd 5a fd fd 23 fd fd 7c fd 6c fd 2b fd 76 fd 39 0c 3d fd fd 39 fd fd 3e fd 53 58 26 fd fd fd 53 5c fd 4c 09 fd 70 09 60 43 19 38 fd 4c 1f fd 07 33 21 03 fd c1 09 4a fd cc 27 fd 08 4a fd fd 0f 30 17 13 fd 2f fd 5c fd fd fd 26 57 fd 70 17 fd 28 fd fd 7c 1a fd b8 fd 4e 75 5e 3f fd 16 32 1c 62 fd fd 71 6b 78 43 6a fd fd fd fd 19 6d fd fd 12 2e fd fd fd fd fd 75 58 fd 76 fd fd 7c 58 75 69 3d 74 40 fd 2a 50 fd 44 fd 79 5e 7f fd fd 3f 1d fd 5b 24 00 66 71 5f 71 09 34 76 a0 35 fd 16 6f fd 67 03 fd 66 fd fd 2b	T5.3@zucRBZbY#p>fy'aoE)/!YMg#Z #|+v9=9>SX&SLp`C8L3! J'J0/\&Wp|Nu^? 2bqkCjm.uXv|Xui=t@*PDy^?[$fq_q4v5ogf+	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\JSDNGYCOWY.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\JSDNGYCOWY.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\KZWFNRXYKI.docx	5	1021	fd 41 fd f7 63 09 72 af 62 51 27 fd 45 fd fd 78 12 fd fd fd 10 fd fd 9e 42 65 18 61 62 4f fd 78 14 79 38 80 28 fd fd 46 fd 2d fd fd fd fd 1f 3a fd 4c 54 09 73 71 61 fd fd 60 73 fd 1a fd 2b fd 2f 4e 10 06 54 fd fd 6d 55 6a 63 5c 0b fd fd fd 0c 73 fd 6b 12 fd 22 63 fd fd 06 39 fd fd 17 25 fd 24 77 51 fd 5a fd 73 78 76 0a fd 55 42 10 fd 12 22 6f fd 3f fd fd fd 29 fd 77 04 4d fd 30 cb fd 19 fd 68 fd fd 39 fd 4a fd 49 fd 0d 7d fd 70 5c 72 6e 4d fd 1d fd 30 6f 21 fd fd fd fd 74 0f 24 26 fd fd fd 13 5b fd fd 21 62 06 fd 30 78 fd 7b fd 26 06 30 fd 33 fd fd 74 2e 6a fd fd fd fd 7b 5a 41 fd 3f 5b fd 63 3f 56 18 49 fd 56 43 55 4c 4a fd 16 1c 34 1e 6d fd 45 7a 0d 71 fd 19 02 fd f0 fd fd 71 1c 35 49 2d fd 4c 12 fd fd fd	AcrbQ'ExBeabOxy8(F-:LTsqa`s+/N TmUjc\sk"c9%$wQZsxvUB"o?)wM0h9 Jl}p\rnM0o!t$[!b0x{&03t.j{ ZA?[c?VIVCULJ4mEz5l-L	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.docx	1026	256	fd fd 39 fd 33 fd 11 fd 14 20 58 74 fd 11 6d fd 33 4b 25 55 fd fd 35 fd 54 05 38 1d 0d fd 72 fd 3e fd fd fd 01 fd 2b 1e fd 51 fd 23 fd 04 fd fd 13 fd fd fd 73 1e fd 68 45 73 fd fd fd fd 7d 3f fd fd 38 3c 15 05 3f 79 7e 64 7d fd 32 36 fd 47 fd 67 fd 55 fd 0a fd 47 07 17 23 2f fd 15 fd fd fd fd 69 fd 6a 45 61 1a fd fd 3a 22 11 04 fd 34 fd 42 fd 02 fd fd 5a fd 23 fd 1c 76 fd 5f fd 57 fd 60 fd 37 1f fd 13 fd 21 6a 40 fd 57 5b fd fd 74 6e fd fd 67 fd 05 fd 57 fd 6e 68 05 fd 75 fd fd 13 32 50 fd fd 27 fd 0e fd fd 10 fd 44 fd 70 fd 76 fd fd 17 1a 39 fd 2f fd 2b fd 32 3b fd 1e fd 4a fd 2a 0d 97 72 fd fd fd fd fd 2d fd fd 22 52 37 fd 5e 73 7c 60 fd 6e fd 40 61 fd 03 66 fd fd 1b fd fd fd 2e fd 7c fd 5d 18 fd fd 62 54 fd	9 Xtm3K%U5T8r>Q#shEs} ?8<?y~d}2 6GgUG#/E:"4BZ#v_W`7!j @W[tngWnh u2P'Dpv9/+2;J*r- "R7^s|`n@af.|]bT	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\KZWFNRXYKI.png	5	1021	fd fd 4b fd fd fd 12 12 fd 1a fd fd 00 bd fd 07 07 fd fd fd 31 63 5d 4e b4 5c bc 72 fd 45 fd 42 fd fd 65 fd fd 52 71 67 fd 07 fd 27 74 5b fd fd 7a fd 26 53 fd fd 47 fd fd 5a 2b fd fd 71 fd 41 fd 38 fd fd fd fd 61 4b fd fd 3b 44 54 fd 79 fd 1b fd fd fd fd fd 58 fd fd fd 72 fd fd fd 24 fd fd fd 6a 7d 7c 1e 74 79 98 73 56 fd fd fd 4c fd fd fd fd fd 28 fd 29 53 5f 71 fd fd 66 3f fd 1c 4e 46 43 5c 2c 18 2e 30 fd 22 60 51 25 4f 26 fd 61 66 3c 55 fd 6b fd 41 70 2f fd 7f 33 fd 34 16 fd fd fd 51 00 25 39 fe fd fd fd 42 fd fd 27 29 33 fd 5f 12 5b 7c 1f fd fd 40 0e fd fd fd 20 4d 50 fd 00 fd 2c 5b fd fd fd 7c fd fd 68 4b fd 39 42 46 2e fd 24 5d fd 2d fd fd 43 fd 7d 27 fd fd fd 3a 36 fd 36 3b 42 fd fd 5d 3f fd 77 fd fd fd 36	K1c]N\rEBeRqg't[z&SGZ +qA8aK;Ty Xr$j}\|tysVL()S_qf? NFC\,.0"`Q%O &a<UkAp/34Q%9B')3_[\| @ MP.[\|hK9BF.$]- C}':66;B]?w6	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.png	1026	256	5f 58 fd fd fd 42 66 c2 fd 7e 66 fd 59 2e fd 66 fd 24 fd 4a 4d 61 1d fd b8 7a 26 58 16 fd fd fd 56 0b 2b fd 66 fd 21 7a 1b fd 46 55 fd fd fd 62 46 2b fd 25 2a 56 fd 56 01 08 7b fd 7c fd fd 2b 00 25 fd 16 fd 5e fd 62 73 fd fd 42 5c 42 fd fd fd fd fd 5d 03 fd 26 78 0f fd 5a fd 43 79 fd fd 6f 3f 7b 6b fd 39 94 77 01 2d 4c fd fd fd 70 66 fd 12 fd 45 46 17 16 fd 27 6e 7d 4a fd 49 fd fd 2d fd 6f 32 fd 78 03 43 51 fd fd 74 fd 6f fd 52 fd 65 fd 6a fd fd fd 19 37 fd 68 fd 79 0c 0f fd 50 fd 18 fd 1a 67 fd fd 28 fd 02 6f 67 fd 18 54 fd fd fd 2c fd fd 5c fd fd 3a 11 06 5c 2b 67 3a 34 23 1b 4c fd fd 77 5b 63 64 23 5a 6f 6a 24 fd 56 fd 4b fd 4d fd 24 0f 31 4a fd 76 fd 31 70 59 1f fd 77 fd fd fd 16 4d 75 fd fd fd 51 60 1a 6a 6d 37 63 fd	_XBf~fY.f$JMaz&XV+f!z FUbF+%*VV {\|+%^bs\B]&xZCyo?{k9w- LpfEF'n}JI- o2xCQtoRej7hyPg(ogT,\: \+g:4 Lw[cd#ZojVKM1J1pYw uQ`jm7c	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	5	1021	2b fd 5e fd 59 68 00 22 fd 75 fd fd fd 65 fd 33 fd fd fd fd 65 29 fd 01 fd 23 32 79 fd 3b 72 2e 77 1e fd 00 fd fd 38 fd 3a 04 fd 46 2b fd fd fd 72 1a fd 3f fd 24 5d 45 fd 6a fd 0b 47 fd fd fd 1c fd 7e 4f 7c 59 fd fd 10 0f 16 19 40 fd 07 fd fd fd 54 fd 02 4f 7d fd 2e fd fd 60 fd fd 12 71 fd 6d fd fd 52 fd fd fd fd fd 3f fd fd 6f fd 2f 51 24 2e 0b fd 1b 63 6d 25 fd fd 61 58 fd 36 fd fd fd fd fd 07 fd 25 1a 6b fd 04 45 fd 7f 24 fd fd 6a 8c fd 32 fd 15 fd 0c fd 8c 17 64 fd fd 59 00 fd 7b fd f3 fd fd 74 fd fd fd 08 0e fd 0f fd 2f fd 7f fd 3c fd 2e e7 5a 5a fd fd fd fd fd 37 fd a1 18 61 13 52 41 79 a4 fd 02 fd fd 23 fd 55 66 41 75 fd 18 fd 77 fd fd fd 12 fd 65 0d fd 36 47 fd 00 3e fd 29 21 fd 0e 42 51	+^Yh"ue3e)#2yr.w8:F+r?$]EjG~O\|Y@TO}.`qmR?o/Q$cm%aX6%kE$j2dY{t/<.ZZ7aRAy#UfAuwe6G>)!BQ	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	1026	256	6e 4a ff fd fd 26 0c 7f 1b fd 43 fd 2d 1d 19 57 3a fd b0 fd 4b fd fd fd 09 3d fd fd 06 fd 71 32 fd 3f fd fd fd 48 fd 35 fd 12 1a fd 3d fd 55 fd fd 78 fd 49 49 66 57 d0 52 2c 34 4d 01 fd fd 4f 0b fd 78 fd 12 2d 86 2b fd 26 fd 77 fd 20 fd fd fd fd fd 3a 23 fd 3f 0e fd 47 6a fd fd 59 39 09 26 4a 59 fd fd 00 4b fd 7a 01 5f 57 4e fd 72 51 78 30 fd 15 fd 1a 62 fd fd fd 17 7f 3e 3b 41 10 67 55 42 7d fd fd 09 fd fd fd 77 fd fd fd 76 fd fd fd b8 fd fd 2d 16 fd 47 22 fd 40 fd 55 6e fd 61 1d 70 fd 31 fd 48 fd 4a fd 17 2f 1a 79 fd fd fd fd fd fd 6b fd fd fd 13 fd 52 fd 23 fd 00 fd fd 6f 70 5f fd fd fd fd fd 0b 1a 7b 75 50 fd 70 2b eb fd 60 58 fd 6f 7a 1d fd fd fd 0d fd fd 7a 35 fd fd fd 19 45 59 63 18 1a fd 1a fd fd 7c fd 33 0b 14 fd	nJC-W:K=q2?H5=UxIIfWR,4MOx-+&w:#?GjY9&JYKz_WNrQx0b>;AgB}wv-G"@Unap1HJ/ykR#op_{uPp+`Xozz5EYc|3	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\LTKMYBSEYZ.docx	5	1021	fd 19 7d 3e fd fd 65 fd fd 03 fd fd 07 31 44 2a fd fd 17 43 fd 14 6d 27 1c fd 6b fd 60 3a fd fd 2f fd fd 02 fd 63 1e 73 fd fd fd 32 67 fd 35 58 70 1f fd 62 fd 76 61 fd 2f 0b 74 fd 58 fd 5a 2d fd 33 fd fd fd 7b 58 56 fd 65 fd 36 fd 53 fd fd fd 5a 3f 66 47 25 fd 39 fd 36 49 04 fd fd fd fd 5c 69 fd fd 52 fd 2a 52 59 65 fd fd 6e 5c 2e 22 3f 09 7c 58 5c fd 6b fd 6c 01 10 3f 37 fd fd fd 09 fd fd fd 3c 43 93 fd fd fd 64 fd 14 fd fd fd 47 26 4b fd 26 01 fd 4b 21 1f fd 79 fd fd 48 fd 6e 67 19 17 fd 21 fd 77 7b 57 69 59 fd 28 57 04 09 16 fd fd 7e fd fd fd 6f fd fd fd 50 00 fd fd fd fd fd fd 02 fd fd fd 1f fd 30 fd 18 44 6b fd 20 1b fd 6a 76 7c 30 6d fd fd fd 6c 69 fd 21 fd fd 70 fd 4a 44 fd 55 fd fd 68 fd fd 49 09 fd 1a 32 5e	}>e1D*Cm'k`:/cs2g5Xpbva/tXZ-3XVe6SZ?fG%96l\iR*RYen\."?|X\l?7<Cd&K&K!yHng!w{WiY(W~oP0Dk jv|0mli!pJDUhI2^	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\LTKMYBSEYZ.docx	1026	256	fd fd fd 55 6d fd 57 0d 28 6d fd 1d 15 fd 02 fd 39 d3 14 37 34 62 fd fd 58 2e fd 51 21 4d 24 fd ce fd 2f fd 69 25 fd 36 fd 4d fd 2f fd 65 4a 10 14 fd fd fd 09 57 0e fd fd fd 4a 52 fd 6b fd 1b 7e fd fd fd a2 fd 76 6e 0e 37 7f fd 4b fd 72 13 fd fd 4f 4b fd fd 57 14 fd 5f 2b fd 4e fd 69 3f fd fd fd fd 5f 36 23 16 7f fd 11 38 7b fd 38 66 fd 24 fd 37 fd 6d d6 fd fd fd fd 6a 70 3b 63 61 0c 74 65 fd 4f 2e 18 fd fd fd fd 06 fd 02 72 fd fd fd 36 1f fd 28 49 1f 0b 5d fd 54 fd 19 fd 38 49 fd 5c 13 50 0d 42 fd 56 4e fd 37 fd 5d 07 fd 7c fd fd fd 5f fd fd 78 6e 63 a3 12 1d 03 fd fd 66 fd 65 7f 5b 7b 76 53 fd fd 7e 59 60 fd fd fd fd 08 56 6d 27 6b fd 51 fd 1d fd fd 18 4a fd 50 3e 36 4b fd fd 0e fd 7b 8d fd 37 58 fd 6b	UmW(m974bX.Q!M$/i%M/eJWJRk~vn7KrOKW_+Ni?_6#8{8f$7mjp;cateOr6(I]T8I\PBV7]|_xncfe[{vS~Y`Vm'kQJP>6K{7Xk	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\LTKMYBSEYZ.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\LTKMYBSEYZ.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NEBFQQYWPS.png	5	1021	59 b7 fd fd 65 fd 28 fd 62 fd 15 fd df 74 fd fd 18 6d fd fd fd 4a fd 3f fd 71 26 fd fd 59 49 2e fd 59 fd fd fd 79 fd fd 19 4f 37 fd 57 43 fd fd 7c 7f 23 03 4c 57 69 7a 20 fd 2a fd fd fd 3b 34 fd fd 26 63 4e fd fd 2e 52 49 32 fd 4c 84 fd 51 20 70 fd fd 77 2b fd 0d fd 3a 51 c6 fd 07 fd 5f fd 58 17 24 2d fd fd 54 fd fd 73 fd fd 52 fd 17 4f 78 fd fd 5f 4f 04 08 3b 4b fd 63 6b fd fd fd 10 fd fd fd 38 39 fd fd 2b aa fd 09 fd fd fd 7a 11 3f fd 53 19 74 2c 5c fd 42 fd fd 57 fd fd 2d fd fd 78 68 48 fd 13 fd 01 4c fd 1e fd 60 7e fd 48 72 fd 41 6b fd fd fd fd 31 27 fd fd fd fd fd 10 06 54 55 35 6e fd 18 04 fd 70 32 32 fd 7d fd fd 13 fd 64 fd 77 4c ce 10 05 35 70 fd 02 fd 7d fd 71 3b 38 2d 24 22 1c fd 16 13 fd fd fd fd fd fd	Ye(btmJ? q&YI.YyO7WC|#LWiz 4&cN.RI2LQ pw+:Q_X$- TsROx_O;Kck89+z? St,BW- xhHL`~HrAk1'TUnp22}dw L5p}q;8-$"	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\NEBFQQYWPS.png	1026	256	42 fd 00 62 0a fd fd fd 1b fd fd 5d 1c 70 20 fd 12 fd fd fd 5a fd fd 0c 6b fd 3d fd 69 fd 79 fd 10 3e 69 35 32 fd 47 fd fd 3b 02 fd 3a 17 27 fd 6e 35 0c 7a fd 62 0d fd fd fd fd 69 3d 30 fd 68 70 79 58 32 fd fd 08 fd 0f 45 27 03 14 fd 52 5c 37 66 73 1a fd 34 62 50 09 2d 09 fd fd fd fd 6b fd 32 fd 04 65 fd 41 4c 13 fd fd fd fd 68 2c 6c fd fd 2d 19 59 46 fd 7c fd fd 38 73 6e 7f 27 27 fd 63 69 3d 5a 16 38 fd 3a 5c fd 22 42 14 27 4a fd 72 fd fd fd 4c 3c 1e fd 65 fd 35 fd bd fd fd 32 5a 7d 5f fd fd fd fd 3e 6f 62 fd 00 66 30 fd 3a 40 5e 59 77 16 fd 33 fd 54 6d 1f 31 29 fd 7e 23 1b fd 27 fd fd fd 29 24 40 fd 08 fd fd 1f fd fd 20 7d fd 51 75 68 55 64 fd fd 2a 15 5c 1e 3e 73 fd fd fd fd fd fd 2b fd 60 fd 23 50 fd 0a d5 fd fd 46	Bb]p Zk=iy>i52G;'n5zbi=0hpyX 2E'R\7f4bPk2eALh,l- YF|8sn"i=Z8: \"B'JrL<e52Z}_>obf0:@^ Yw3Tm1)~#')@ }uhUd*\>s+`#PF	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\NEBFQQYWPS.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\NEBFQQYWPS.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	5	1021	62 fd fd 10 fd fd fd 2d 16 fd 31 fd 37 fd 42 07 fd 3a 17 fd fd fd fd fd fd 46 fd fd fd 3f 17 2b 2b 0b 57 fd 54 fd 1e 42 fd 48 04 fd fd fd 0f fd fd 54 23 fd 10 fd 13 fd 6a 13 fd 2d 3b fd 0f fd fd 07 02 31 fd fd 73 72 ee fd fd fd 19 7b 30 49 fd 27 3b 03 63 fd 5d 16 fd 7d fd fd 02 0f fd e0 73 33 fd 78 fd fd 02 27 fd 1e 75 7c 58 fd 68 64 43 57 7d 3e 2b fd fd fd 2c 6a 28 fd 49 56 26 fd 71 14 66 5a fd 39 2e 0b fd fd 15 2d 23 0e 51 fd fd fd 30 fd fd 0f fd fd fd 3e 07 08 6e 57 3f 10 00 75 fd 74 fd c7 fd 46 fd 5a fd 4d 55 52 37 35 24 fd 5a 53 22 55 26 19 fd fd fd b2 48 09 73 12 5e 64 0c 49 fd 73 1f 6b 13 fd 7d fd 66 02 fd 1d 12 1c fd fd fd fd 04 fd fd fd fd 74 fd fd 2a 56 fd 65 5e fd fd fd fd 13 7a 4b fd 78 16 76 fa 7c	b-17B:F?++WTBHT#j-;1sr{0l';c]}s3x'uXhdCW}>+,j(IV&qfZ9.-#Q0>nW?utFZMUR7$ZS"U&Hs^dIsk}ft*Ve^zxv|	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	1026	256	44 0b 5f 52 fd 7e 3b 61 12 52 fd 5b 4d f1 03 41 fd fd 4d fd fd 60 fd 7d fd 09 fd 6b 7b fd fd 6f 23 23 fd fd 3b 26 fd fd 74 5c fd fd fd fd fd 25 26 fd fd fd 56 54 00 7a fd 48 74 fd fd 5e fd fd fd 57 fd 1e 3b 54 19 45 fd fd fd fd fd 36 5c 28 1d 28 42 fd 0a fd 33 fd 7a fd 4e fd fd 6d 46 fd 39 fd 0f fd 00 04 fd 1f 19 01 fd fd 29 fd 40 10 fd 43 fd 0d 32 96 fd 5c fd 44 2b 26 9e fd 40 fd fd 57 3a 44 fd fd fd fd 15 fd 11 45 fd 56 1f 43 fd 47 fd 11 2b fd 77 2a 6a 3b 6e 3b fd 51 50 2e fd 09 75 40 5f 2f fd 1a fd 25 fd 4f 1f fd fd 6a 4e 39 3e 09 fd fd fd 63 fd fd 6f fd fd 06 fd fd 6d 08 13 62 02 fd 0d fd 44 1e 32 2e 79 68 fd 7d 29 7b 54 fd fd 4f fd 61 fd 64 fd fd 4c fd fd 40 fd 22 7f fd 0a 14 fd fd fd fd 04 fd 1c fd 47 fd fd 15 7a 70 7b 76 4f	D_R~;aR[MAM`}k{o##;&t\%&VTzt^W;TE6\((B3zNmF9)@C\D+&@W:DEVCG+w*j;n;QP.u@_/%OjN9>combD2.yh})\{TOadL@"Gzp{vO	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	5	1021	35 1e 64 fd fd 7f fd fd 58 75 fd 07 3b 70 1a fd 0b 47 fd 69 fd fd 78 fd 39 fd fd fd fd 09 fd 19 60 05 e2 fd 3e 25 2c fd fd 01 03 45 61 fd 2f 3f fd 13 7e 30 76 1a 08 08 35 fd 3f fd fd 5b da fd 40 fd 2d fd 2c fd fd fd fd 28 fd 1b 34 fd 07 50 6b 25 fd 47 3e 36 67 42 1b fd 4d fd 72 fd fd 57 fd fd 2d 04 25 fd 2c 18 fd fd 59 fd fd fd fd 28 6d 0f fd 76 62 fd 5a fd f3 61 fd fd 1e 53 60 fd 01 fd fd fd 0c 71 fd 1a 67 fd 18 61 fd 34 fd 67 33 fd 32 fd 02 fd fd 0a fd fd fd 00 fd 06 fd 57 7f fd 04 fd 2c 4c 5d 06 fd 5d fd 46 79 fd fd fd 1f 7b 7e de fd fd 1e 63 2b fd fd 79 50 36 fd 5c 59 54 24 fd 7a fd fd 7e fd 25 69 fd 1c 4c fd 2f fd 19 7d 41 fd fd fd 09 fd fd 5e 61 1e 10 55 fd fd 02 92 fd 22 fd 5e fd fd 17 29 64 fd	5dXu;pGix9`>%,Ea/~0v5?[@-,(4Pk%G>6gBMrW-%,Y(mvbZaS`qga4g32WL]]Fy{~c+yP6\YT$z~%L/}A^aU"^)d	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	1026	256	0d fd fd 13 09 2d fd 51 52 47 4c 3b 31 fd 1c 2c fd 59 fd fd 00 54 fd fd fd 60 fd 69 1c 29 02 49 28 0e fd fd fd 2b fd fd 59 fd 7e fd fd 3f fd fd fd fd 45 fd 3e 3f fd 66 5e 71 1a 54 74 7a 35 2f 63 fd fd 26 41 fd fd cc 6c 5b fd fd fd 67 61 3e 3e 67 63 fd 25 fd 57 2f fd 6a 9f fd fd fd fd 54 9e fd fd 0d 3b fd 4a fd 39 fd 25 17 51 fd 0a fd 52 02 fd 69 09 fd fd 4c 0a 46 48 fd fd ed fd 2a 56 4c 03 fd fd 3c fd 55 fd 51 21 66 fd fd 02 fd fd fd fd 6f 16 46 13 46 fd 75 fd 78 53 12 32 6f fd 74 fd fd fd 3c 37 fd fd 0b fd fd 06 fd fd fd fd fd fd fd e3 fd fd 7f fd fd 29 fd 0f fd fd fd fd fd fd 3d 3d fd 1f fd 06 77 fd 05 fd 6a 10 1d fd 1f 6b fd 34 11 fd fd 58 fd 08 1b 32 3e 29 06 77 50 79 79 72 5a 62 fd 7a 52 fd fd 1d fd fd 2c	-QRGL;1,YT`i)I(+Y~?E>?f^qTtz5/ c&Al[ga>>gc%W/jT;J9% QRiLFH*VL< UQ!foFFuxS2ot<7)==wj4X2>)wPyyrZbR,	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\RAYHIWGKDI.pdf	5	1021	fd fd 75 4b fd 41 34 1a fd 5e 6f fd fd 2d fd fd 74 fd 11 fd fd fd 3b fd 76 fd fd 46 fd fd 3e fd fd 3b fd fd fd 74 2f 46 fd 52 1b 50 fd 35 fd 37 fd 1c 02 37 3e 37 fd fd fd 79 72 fd 50 7c f8 0d fd 43 0b 58 3d 7d fd fd fd 0d fd 3e fd fd 1a 57 6c 46 32 51 fd fd 34 48 fd fd 60 fd 3c fd 12 fd 3e fd fd fd 67 fd 42 28 10 46 6a 60 04 fd 69 46 36 fd 74 18 fd 2b fd fd fd 6f fd 72 fd 63 fd fd fd fd fd fd fd fd 51 fd fd 60 fd 3c 28 fd fd fd fd 6e 56 59 17 fd 34 fd 3a 1e 26 fd 5e 73 fd fd 6b fd 18 71 01 96 29 24 41 32 fd fd 4f 4e 02 79 6b fd fd 37 45 3e fd 40 69 fd 1f fd 76 fd 28 fd 7f 61 fd fd 53 fd 75 6b 2b fd 6c 08 fd fd b2 60 71 40 41 fd fd 11 7a 15 07 16 38 51 59 fd 02 fd 2e 47 fd 6d fd 7e fd 7b fd 5f 2b fd 4c fd fd fd fd 39 fd	uKA4^o- ;vF>t/FRP577>7yr|CX=}> W IF2Q4H`<>gB(Fj`iF6t+orc Q`<(nVY 4:&^skq)$A2ONyk7E>@i v(aSk+lq@Az8QY.Gm~ {_+L9	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\RAYHIWGKDI.pdf	1026	256	6a 75 fd 32 2c fd fd fd 72 73 fd fd dd fd 75 36 5c fd 14 fd 25 fd fd 0f fd fd 0d 79 0a fd 57 24 fd 7e 68 fd 42 58 fd 5a fd fd 54 fd fd fd 42 fd 15 26 fd 29 fd 9d 2c 7e 23 fd fd fd 10 70 63 fd fd fd 1a 38 fd 96 05 37 fd fd fd 72 fd 53 45 2a fd 37 5e 89 13 fd 3b fd 72 13 fd fd 7d 51 26 22 7b 19 09 68 37 fd 64 fd 78 fd fd fd 4f 0e 16 29 4b fd fd fd 05 7d fd fd 10 fd 0b fd fd 03 3a fd fd fd fd fd 2c fd 6e 21 31 46 75 fd 0b 02 5e fd 64 7b 3d fd fd 0d 7b fd fd 58 fd 45 34 1b 47 fd 31 fd 4d fd 76 72 78 fd fd 63 77 fd 73 76 28 fd 24 fd 2d fd 4f 4c fd fd fd fd 0d 0f fd 0c 11 21 48 61 fd 47 69 fd fd 02 72 fd 4b 69 fd 44 fd 3c 51 59 1d 72 fd fd 3a fd 7c 6f 75 fd 25 fd 62 fd 6f fd 42 fd 6e fd fd 6e fd	ju,rsu6\%yW$~hBXZTB&),~#c87rSE*7^;r}&" {h7dxO)K}:,n!1Fu^d{={X E4G1Mvrxcwsv(- OL!HairKiD<QYr:| ou%boBnn	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\RAYHIWGKDI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\RAYHIWGKDI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SFPUSAFIOL.mp3	5	1021	7f fd fd fd fd 7b fd 5d fd fd 01 fd 2e 0a fd fd 4c fd fd 5e 24 fd fd 6d 38 fd fd 3c 26 0a fd 0b e7 fd 63 26 fd 0b 4e fd 3d fd 08 4d fd 20 fd 2c 3b 1d fd fd fd fd 12 fd 6f fd 39 50 75 39 fd fd fd 0c fd fd 2a 8e fd fd fd 18 2c fd 65 fd 26 33 78 64 94 fd fd fd fd fd 27 26 2a 6c 50 7a fd 1b fd fd fd 69 06 fd 53 6c 52 3e fd e3 24 fd fd fd 33 fd fd 77 fd fd fd 52 fd fd fd fd fd 2b 4e fd f6 fd 3c fd fd 18 fd 55 19 2d 17 fd 07 fd 4f 61 17 3a 69 fd fd 1a 13 55 fd 6e fd 3f fd 6b fd 3e 25 fd 70 04 fd 60 fd 4a 0a fd fd 42 6c 33 fd 56 fd fd fd fd fd 1c fd 4f 2d 7f fd fd 37 fd fd 03 fd fd fd fd 09 2e 6e fd 51 60 78 7a fd fd fd 60 fd 04 0e 6c fd 2c fd fd 08 4b fd 60 3d 49 24 fd 19 15 fd 32 fd 39 fd 63 2c 37 61 bf fd 30 14 fd fd fd 3d fd	{].L^$m8<&c&N=M ,;o9Pu9,e&3xd' &*IPziSlR>$3wR+N<U-Oa:iUn?k>%p`JBl3VO-7.nQ`xz`l,K`=$29c,7a0=	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\SFPUSAFIOL.mp3	1026	256	6f 6c fd fd 14 07 fd 34 fd fd 45 04 fd 0a 59 fd 5c fd 4a fd 13 42 4d 75 1f 70 7d 76 4e fd fd 73 fd fd 69 fd 1d fd 69 1d fd fd db fd fd 04 74 3a 2a fd 32 0a 7e fd fd 20 03 13 fd 60 66 fd fd 3f 32 3b 4b 71 fd 50 1c 62 fd 09 74 fd 23 fd fd fd 36 fd 71 65 2e 7c f5 fd fd fd 51 1c 47 fd fd fd fd 66 32 fd fd 3d fd 0e 0b 2c fd fd fd fd fd 7b 67 2d fd fd fd fd fd fd 4d fd 61 1b 6d fd fd fd fd 00 2e 5b fd 66 62 fd fd 06 4f fd fd 22 fd fd fd 3b fd 0e 30 27 fd fd fd 77 fd 73 69 7c 14 fd 35 fd 73 79 6a 0a 2a 77 63 fd 4d fd 10 fd 6b 6e fd 57 27 ea 5c 6e fd fd 7a fd 5e fd 09 fd fd 7e fd 02 fd fd 25 fd 06 fd fd fd 47 3f 20 59 fd fd fd fd 3c fd 75 fd 23 d5 fd 71 70 fd 1a 43 fd 1c fd 66 fd fd fd 36 57 77 fd fd fd fd 6e fd 52 fd 09 33 fd 0e	ol4EY\JBMup}vNsiit:*2~`f?2;KPbt#6qe.|QGf=,{g-Mam.[fbO";0'ws i|5yj*wcMknW'\nz^~%G?Yu#qpCf6WwnR3	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\SFPUSAFIOL.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\SFPUSAFIOL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SQRKHNBNYN.png	5	1021	fd fd fd 58 fd fd 51 19 38 05 13 68 fd fd fd 43 fd 46 04 39 fd 29 40 fd 3d fd fd 28 fd 3a fd fd 47 0c fd 5e fd fd 7a 66 fd fd fd fd fd fd 36 fd 4f fd 1b 59 fd 5f fd 4a fd 01 fd 09 01 52 fd fd fd 4d 67 56 fd fd 6e fd fd 76 fd fd fd fd 28 fd 33 fd fd 30 fd fd fd fd 45 7f 2c fd fd fd 18 08 fd 70 fd fd fd fd 08 fd fd 0c 0c 7d 01 24 57 fd 0b fd fd 4f 11 12 0f fd fd fd fd 45 fd fd 43 5b fd fd fd fd 19 fd fd 11 fd fd fd fd 79 3b 6d 5d d2 fd 5e 6a fd 3a 0e 3a 77 03 fd 6a 3a 67 fd fd fd 13 76 fd 79 5f fd 39 39 7b fd 0a fd fd 5a 65 7e fd fd 7d 3e fd 24 fd 7e fd 35 1f 13 fd fd fd 29 fd fd fd fd 2d fd 12 fd 41 fd 75 65 72 1b fd fd 0e fd 6b fd 44 fd fd 02 fd 49 fd fd 01 41 26 fd 55 fd fd 3a 45 fd 29 57 fd fd fd 01 fd 52 63 3d 00 fd fd 3f fd fd 44 fd fd 26	XQ8hCF9)@=(:G^zf6OY_JRMgVnv(30E,p}$WOEC[y;m]^j::wj:gvy_99{Ze~}>$~5)-AuerkDIA&U:E)WRc?D&	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\SQRKHNBNYN.png	1026	256	49 fd fd fd fd 14 12 79 01 fd fd 55 7e 75 fd 36 fd fd fd 33 22 fd 71 28 41 4c fd 74 18 94 fd 3c 53 58 47 64 fd 75 fd 54 52 0e fd 57 fd 60 fd fd 05 7e 6f fd fd 45 fd 0e fd 40 fd 73 fd fd 3f 76 16 17 fd 01 fd fd fd fd fd fd 2f fd fd fd 18 fd fd 5a 3a 53 fd 01 fd 3c fd 14 45 fd fd 48 fd fd 67 75 fd 18 fd 2e fd 50 7c 08 75 04 fd 63 38 fd 25 31 fd 23 77 fd fd fd 4d fd 72 fd fd 1f fd fd 0e 60 19 34 fd fd fd 74 38 fd 2c fd fd fd fd 1d fd fd 0c 03 26 fd fd fd 38 fd fd fd fd 1b fd fd fd fd fd 67 0d fd fd 5c fd fd fd fd 53 fd fd fd fd 11 fd fd fd 32 13 fd fd 13 26 39 2a 05 fd fd 76 fd 49 22 57 60 4a fd 48 1e fd fd fd 22 43 fd 66 48 51 fd 11 fd 5b fd fd fd 7e fd fd 48 41 fd fd 67 fd 76 2a 7a fd fd 35 71 fd 64 5a fd fd fd fd 62 08 4a fd	lyU~u63"q(ALt<SXGduTRW`~oEs?v/Z:S<EHgu.P|uc8%1#wMr`4t8,&8g\S2&9*vl"W`JH"CfHQ[~HAgv*z5qdZbJ	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\SQRKHNBNYN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\SQRKHNBNYN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\UOOJJOZIRH.jpg	5	1021	7e 79 fd 56 20 fd 26 fd 07 5a 12 fd fd 35 60 65 1e fd 01 fd 2d a2 fd fd 3e 6f 2e 1e 52 fd 5f fd 4d fd 10 60 2e fd 01 fd fd 5d fd 23 fd 7e fd 62 fd 5c fd 78 fd 68 fd fd fd 1f fd 51 fd 2c fd fd fd fd 11 5d 7f 27 fd 40 fd 6c 55 fd fd 79 fd 68 fd 57 62 75 68 fd fd 7d 19 fd 2f 12 fd 5c fd 06 3d fd 40 52 fd fd 71 96 fd fd f4 fd fd fd 2e 7d fd fd 0f 3c fd fd ee fd f3 fd 39 fd 40 fd 34 46 fd fd fd 25 4a fd fd fd fd fd 5e fd 43 fd 2d 24 12 3f 68 fd fd fd 36 3a 12 fd 1c 6f 2f fd fd 7b fd fd fd 47 76 fd 6f fd fd 0b 7a fd 25 49 fd fd 0a fd fd 4a 79 6c 5f 46 fd fd 70 fd 5e 7b fd fd 45 53 fd 1a 37 41 70 fd 5f 02 13 fd 6c fd 62 1a fd 7c 27 fd fd 27 fd 43 fd 6a fd fd fd 25 fd 4c fd fd fd fd fd fd 19 07 16 73 24 7a fd 40 fd 13 20 61 4c 69 fd	~yV &Z5`e->o.R_M`.]#~b\xhQ,]'@ lUyhWbuh}/\=@R.} <9@4F%J^C-$?h6 :o/{Gvoz%lJyl_Fp^{ES7Ap_lb\|"Cj%Ls$z@ aLi	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\UOOJJOZIRH.jpg	1026	256	fd fd 62 10 60 73 1b fd fd 46 7d fd fd 48 fd fd 7c fd fd 07 2d fd 1b fd fd fd fd 0b fd 5f 7b 16 fd 4f fd fd 3c fd 79 6b 5c 3d fd 0b fd ac f9 28 15 fd 30 fd 21 69 fd 04 fd fd fd 02 24 fd 56 5b fd fd fd 6c 5c 01 6b fd 73 6b fd 26 4c fd 01 13 fd fd 7a 40 fd 5d 72 04 32 0d fd 24 6a fd 22 fd fd fd 14 54 fd 72 fd fd fd 45 fd fd fd fd 24 fd fd fd 4a 0b fd fd 6d 58 20 44 52 fd 68 fd 2f fd 11 66 55 fd 13 2f 1c fd 49 fd fd 67 08 5d fd 61 23 fd 20 fd fd 0d fd 64 fd 48 48 57 fd 52 fd fd fd 4a fd fd 1c 5a 67 fd 64 fd 5c fd fd fd fd 26 fd 8c 44 7a 1e fd 2a 19 fd 59 fd fd 07 fd 23 fd 7f 1b fd 5f fd 13 fd fd 05 10 fd fd 79 fd 7a fd 77 fd 32 fd 51 fd 21 41 fd 3a fd fd 3f 07 1f 10 fd 1c 09 fd fd ed 79 fd fd fd fd 38 fd 75 fd 3b	b`sF}H|-_{O<y=(0!i$V[I\ksk&Lz@]r2$j"TrE$JmX DRh/fU/Ig]a# dHH WRJZgd&Dz*Y#_yzw2Q!A:?y8u;	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\UOOJJOZIRH.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\UOOJJOZIRH.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WKXEWIOTXI.jpg	5	1021	e5 fd 75 fd 0a 03 64 fd 3d fd fd 32 27 fd 7d fd fd 45 14 fd fd fd 2a fd fd 17 25 fd 3d fd 5b 57 57 fd fd fd 2b 56 70 32 26 02 fd 10 38 fd 39 3e fd 1d fd 0d fd 66 10 fd 53 fd 06 2a 0f fd 3c fd fd fd fd fd 18 fd 1d fd 1f 59 17 67 4f 36 fd 05 0a 75 7f 49 fd 72 66 fd fd fd fd 6d fd fd c0 31 fd 44 4c 2c 4c fd 2d fd fd 34 fd fd 0f fd 56 52 6a fd fd 00 62 36 75 64 35 fd 37 70 fd 22 fd fd fd 6b fd 00 fd fd 2f fd 65 06 fd 5d 2e 6f fd 48 fd 13 fd fd 5b 15 fd 3f fd 25 32 35 fd fd 4c fd 27 fd fd 28 fd fd fd fd 63 fd 3e 04 fd 7c 63 fd 28 fd fd 2b 48 fd 79 fd fd 24 fd fd 3f 18 fd fd 1f 3c 62 fd 25 02 17 47 fd 1f fd fd fd 24 10 fd 78 47 67 33 6a fd 2a fd fd 36 fd 62 fd fd fd fd 2b 14 fd 09 02 37 5d fd fd 3f fd fd 54 fd 1e	ud=2'}E*%= [WW+Vp2&89>fS* <YgO6uIrfm1DL,L- 4VRjb6d5p"k/e]oH[?%2 5L'(c>|c(Hy$? <b%G$xg3j*6b+7]?T	success or wait	1	411859	WriteFile

C:\Users\user\Downloads\WKXEWIOTXI.jpg	1026	256	fd fd 33 1f 77 fd fd fd fd 58 23 fd 0e fd fd fd 3e fd 3b 8a fd fd fd 65 fd 7b fd 26 fd 31 fd 36 fd fd 59 44 29 1b fd 58 fd fd fd 01 01 34 fd 4e fd fd 38 fd 51 fd fd 71 4e 45 fd 5e fd fd fd fd 58 5d 2a fd fd 0e fd fd fd 33 0e 5f 09 fd 60 fd 47 fd 7b 64 79 fd 0a 21 2f fd 66 1f fd d8 15 fd 2e 43 0f fd fd 67 34 fd fd fd 64 fd 78 1e fd fd fd fd 75 5b 11 64 fd 45 0e 33 2b fd 57 57 fd 2f fd fd 0a fd 59 06 75 fa 5a 61 00 fd 3f 12 fd fd 37 44 fd fd 75 28 fd 78 76 fd fd fd fd 68 fd fd 78 69 74 22 7f 5f 79 67 4a 29 fd 5d fd fd fd 12 55 fd 11 fd 3d fd 4f fd 72 72 48 fd 14 fd b7 07 09 fd aa 32 fd 6d 40 fd fd 05 fd fd 77 0b fd 71 fd 49 61 3a fd 71 fd fd 5b 7e fd fd 22 50 6c 00 63 fd 3c fd 0f 72 6f fd fd fd 61 62 5e 0f fd 55 7b	3wX#>;e&16YD)X4N8QqNE^X]*3_`G{
				dy!/f.Cg4dxu[dE3+WW/YuZa?7Du(x
				vhxit"_ygJ)]U=Orr2m@wqIa:q[~"Plc<roab^U{
					success or wait	1	4115FA	WriteFile

C:\Users\user\Downloads\WKXEWIOTXI.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WKXEWIOTXI.mp3	5	1021	fd fd fd 24 04 77 fd 6a 09 fd 6d 30 e0 fd fd fd 77 77 7a fd fd 58 25 15 5f fd fd fd fd 68 fd c2 fd fd 60 fd fd fd 13 19 4f 71 35 0c 34 29 64 fd 1b fd 59 fd 20 fd 3b 7d fd fd fd fd fd fd 4c fd 5d fd fd 1c 40 fd 18 fd 7d fd 78 50 fd fd fd 7d fd fd fd fd fd 3f 6a 0e fd 24 fd fd 2f 1f fd 22 fd 59 fd 4f fd 51 fd fd 58 fd db 5d 4d fd fd 1e 8d fd fd 1b 14 fd 65 47 4f fd 02 32 fd fd fd 27 fd ff 28 fd 5c 3c fd 7d fd fd fd 5f 73 fd fd 71 fd fd 27 fd 73 fd 05 fd 10 75 fd fd 7c fd 79 5d fd 24 03 fd 47 33 fd 04 fd fd 70 fd 4a 40 1d 42 69 fd 09 3d 3e fd fd 33 fd fd fd 0a 13 36 75 fd fd fd 79 0f fd 2f 23 70 64 fd 5b fd 69 fd 05 31 fd ad 55 fd 65 75 18 fd 0a 7a fd 9e fd 09 ef bc fd fd fd 0f 6c fd 7b fd 67 5a fd fd 33 fd	$wjm0wwzX%_h`Oq54)dY ;}L]}xP}? j$/"YOQX]MeG2'(\ <}_sq'su|y]$G3 pJ@Bi=>36uy/#pd[i1Ueuzl{gZ3	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.mp3	1026	256	72 fd 1c fd 7f 65 fd fd 71 fd 4f fd fd fd fd 0d 75 fd fd 07 4e fd 15 61 5e fd fd 60 27 fd 6d fd fd fd 37 02 2d fd 2d 6a fd 7e fd fd fd 62 fd fd 23 63 44 32 fd 1f 33 fd fd fd fd 76 fd 42 fd 0c 21 71 fd fd 2b fd 07 fd 6f fd 38 fd 32 3b 69 fd 41 fd fd 24 75 4f 5b 6e 6e 2c fd 1e fd fd fd fd 77 7b fd fd 43 1f fd fd 30 43 fd 73 7a fd db fd 55 10 fd fd 71 46 78 fd 50 fd 55 40 fd fd 0a 1a fd 16 fd 79 6f 06 fd 33 fd 1c fd 4b fd fd fd fd fd fd 20 17 fd fd fd 70 3e fd 0f fd fd 23 5e fd 24 7d fd 23 fd fd 53 2f 76 57 fd 7c fd 22 45 01 fd 17 21 1f 28 73 fd 47 fd 63 fd fd fd fd 52 93 2e 09 fd fd 40 76 fd 2c 05 3d 8d 03 fd 2d fd 62 28 7d fd fd fd fd 68 fd fd fd fd 36 2d 33 fd fd 76 fd 5b 72 5a fd 36 64 fd 75 45 fd 3d fd 0d 5a fd	reqOuNa^`'m7-- j~b#D23vB!q+o82; iA$uO[nn,w{C0CszUqxP @yo3K p>#^$}#S/vW"E! (sGcR@v,=-b(}h6-3[rZ 6duE=Z	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WKXEWIOTXI.pdf	5	1021	04 25 fd fd fd 5b 42 fd fd 5f 5a fd 59 2b fd 58 fd 60 6f fd fd 0f 1b fd fd 22 6a fd 00 27 10 07 44 fd 11 fd 55 4a 3b fd 18 13 2f 3e 58 7b 5b 41 26 fd 59 29 fd 57 fd 52 49 19 49 fd fd fd 17 67 fd 19 75 fd fd 91 fd fd 00 2f fd 56 7b 63 fd 03 61 fd fd 4c 14 fd 20 1f fd 4b 7a 56 39 fd fd 3a fd 75 fd fd 0d 6c 66 43 10 fd fd 5a d0 3a 65 57 fd fd 7c fd 0a 59 66 53 fd fd 46 3c 72 fd fd 28 b7 1d 58 fd d5 49 6e fd 38 74 fd 04 42 fd 6b 05 4a 08 fd 6b 7f fd 47 52 58 fd fd 78 0b a3 1c fd fd fd 78 fd fd 60 fd 6a fd 11 0a 27 2d 08 fd 1a 6d fd fd fd 70 fd 1a 5a 2d 68 fd fd fd 3e 7b 10 3f 43 31 54 47 fd fd fd fd 6c fd 5d 78 fd fd 71 fd 7a 57 47 fd fd 64 fd 76 77 fd 46 fd fd 05 6e fd 4e 1c fd 62 fd 1f 1b fd 9f 3a 68 11 fd fd 55 fd fd	% [B_ZY+X`o"j'DUJ;/>X{[A& Y)WRIIgu/V{caL KzV9:ulfCZ:eW|YfSF<r( Xln8tBkJGRXx`j'-mpZ-h> {?C1TGl] xqzWdvwFnNb:hU	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.pdf	1026	256	3a fd fd 37 fd 43 fd 2f fd fd fd fd 64 fd 2a 33 6d fd 57 3b fd 6d fd 0c 32 fd 0e fd fd 76 fd fd 1a 03 fd fd 20 fd fd 3c 38 fd fd fd 53 06 39 39 fd fd 59 fd 55 29 fd 48 6f fd 5d fd fd fd 22 fd 49 fd 52 fd fd 34 03 fd 60 fd 77 fd 1c 5a fd fd fd fd 36 fd fd fd fd fd 25 35 5d fd 1a fd 03 24 fd fd fd fd fd fd 6f fd 51 2a fd fd fd fd 44 40 fd 50 5f fd 7f 30 70 54 41 4c 2a 17 21 fd 5e 33 fd fd fd fd 37 18 fd fd 45 fd 73 62 76 e1 25 fd 02 1e 7d 13 fd fd 1c 07 35 fd 01 fd 6e fd fd 0e 5d 38 14 5d fd 30 fd 64 46 fd fd ab fd fd fd 1f af fd 10 4f fd fd 31 fd fd 5e 51 69 33 3e fd 2d fd 2a 3d 1c 51 fd 08 fd 09 fd fd 69 21 48 fd b4 3a fd fd 3f ec 56 17 73 7b 3e fd 43 67 7c fd 63 fd 6d fd fd 11 30 fd fd 44 fd fd fd fd 39 76	:7C/d*3mW;m2v 8S99YU)o]"IR4`wZ 6%5]$oQ*D@P_0pTAL*! ^37Esbv%5n] 8]0dFO1^Qi3>-*=Qi!H:? Vs>C|cm0D9v	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\WKXEWIOTXI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WUTJSCBCFX.docx	5	1021	04 66 fd 4f 00 7c fd fd fd 20 fd 7a 0e 37 fd 20 fd 51 2f fd 92 00 fd fd 0e 37 76 fd 01 4b fd 35 fd 2f 76 fd 4b fd 5d 1b 6c fd fd 13 fd 64 0b 43 fd fd fd 16 6d fd 54 61 fd 06 58 02 69 fd 34 fd 7b fd fd 1b 36 fd 39 7a 6e fd fd fd 6b 18 2a 4e fd 4b 5b 77 24 1e fd 7f 6e fd 1c 1f fd 14 51 02 1b fd 4b 0d fd 7e 44 56 fd 3c fd 71 14 31 75 fd fd 72 35 39 fd 08 57 61 8c 26 fd 45 fd 44 66 fd fd fd 18 3b 76 fd fd fd 4f fd fd fd fd 24 fd fd 32 fd 8c fd fd 7f 6b 0a 5e 49 fb 03 08 fd 4d 38 fd fd fd 5b 67 23 46 fd 7a 5f fd fd 33 fd fd 11 23 fd 73 7f 57 fd 7f 2b fd 26 05 fd fd 0a fd 25 70 fd fd 3a 24 58 7f 54 fd fd fd 5c fd fd 5e fd fd 46 43 fd fd fd fd fd 67 fd 05 fd 30 fd fd 55 15 fd 7d 6b fd 20 fd 04 fd 0c 34 68 fd 08 fd 52 fd fd fd	fO| z7 Q/7vK5/vK]ldCmTaXi4{69z nk*NK[w$nQK~DV<q1ur 59Wa&EDf;vO $2k^IM8[g#Fz_3#sW+& %p:$XT\^FCg0U} 4hR	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.docx	1026	256	10 fd fd fd 3a 0a 15 fd 16 fd 00 23 fd fd fd fd fd 1a fd 7e fd 3f 04 43 fd 0f fd 10 fd 2a 76 7c 7e 68 fd fd fd fd 16 fd 01 fd 2c fd 0e fd fd 7e 64 fd 1e 66 fd 6d 07 7b fd fd fd fd 1b 07 fd 57 6a 66 fd 13 9b 3c fd 5a fd 12 fd 68 17 a3 fd fd fd 0e 5e 00 0a 2a fd fd 14 72 05 fd 3d 21 fd fd 6a 5c 37 38 fd 12 07 2c fd 03 fd fd fd 29 fd 41 fd 53 0b 7e 47 ec 20 fd 0f 46 fd c2 63 41 fd 0e fd fd fd fd 4f 77 40 3c 72 fd fd 4d fd 7c 70 2c fd fd 24 fd fd 7b fd 3f 64 fd 3d fd fd 1f 01 fd fd 23 fd fd fd 66 fd fd fd 24 68 fd 2a fd fd fd fd fd 44 fd 1c fd 7f 1e 5d 15 14 69 13 75 fd 19 51 fd 79 58 6d 36 fd fd fd 0e fd 04 61 68 fd 1c fd 95 fd 47 44 fd fd 0d 23 fd 4c fd fd fd 32 4d 0a fd fd 3f fd 20 fd 57 fd fd fd 56 02 fd	:#~? *v|~h,~dfm{WjfZh^*r!j\78,)AS~G FcAOw@<rM|p,${? d#fh*D]iuQ yXm6ahGD#L2M? V	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WUTJSCBCFX.pdf	5	1021	0c fd 1e 7b fd 0d 4f fd 59 0b fd fd 41 19 0e fd fd 0c fd fd 1a 3a 4e 03 fd fd 7f 4d 6d 56 fd fd fd 09 31 fd 9c fd fd 5f 7e fd fd fd 68 fd 86 00 fd fd fd 7d fd fd 3a 22 4e 50 fd 4a 73 5b fd 54 49 fd fd fd 25 0d fd 05 4f 09 20 66 19 fd fd 02 fd 54 fd 52 0d 5c 69 fd fd fd fd 63 3e fd 16 3c 02 78 fd fd 2c 64 09 7a 77 fd fd 64 5b 7b 6e fd ea fd fd fd 31 fd 02 fd fd 49 7b 1e 54 fd 1e 19 52 36 5e fd fd 4b fd 07 28 5a 26 7d 3b 5f fd 0f fd 4e 09 7c 74 fd 0d 3d 66 22 fd 84 fd fd fd fd 69 33 29 fd 79 75 3b 55 54 fd fd 57 fd 56 75 42 fd c4 fd fd fd fd 7c 23 fd 07 3b 59 6e fd 1e fd 17 4a fd e9 fd 3d 28 21 fd 40 fd 29 47 2f 37 29 56 7b 51 fd fd d8 fd 14 fd 25 fd fd 01 fd 78 44 fd 34 fd 1b 6e 4e 2b fd 40 72 7e 2c 5c fd fd fd 32	OYA:NMmV1_~h}:"NPJs[TI%O fTR\ic> <x,dzwd[{n1I{TR6^K(Z&}; _N|t= f"i3)yu;UTWVuB|#;YnJ= (!@)G/7)V {Q%xD4nN+@r~,\2	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.pdf	1026	256	44 49 fd fd fd 5b 5a 52 fd 57 fd fd 15 fd fd fd 02 41 fd 46 33 fd 74 fd fd fd 68 17 30 27 fd 41 0e fd fd fd 53 50 61 71 fd 20 fd fd fd fd 57 65 0b 26 21 fd fd 11 55 4e fd 11 fd 31 65 fd 77 1b 72 5d fd fd 5f 16 fd 68 fd 0f 6c 25 3d 43 75 19 61 d9 fd 76 29 fd 5d 36 fd fd fd 4e fd 46 fd fd fd 6c fd 0e fd 59 02 fd 55 66 71 78 1d fd 16 fd 79 77 fd fd 20 fd 15 70 fd a8 05 fd 72 e3 fd fd fd 6c fd fd 7d 53 fd fd 5c 3b fd fd 6c 71 4a 67 59 d6 20 fd 21 fd fd 76 73 2b fd 4f 25 fd 36 0a fd fd 74 2b 2f fd fd 79 fd fd 05 fd 45 fd 2f 69 fd 14 1d 65 98 fd fd 26 fd 60 20 78 0a fd fd 11 07 fd 69 1c fd 34 fd 60 74 fd 72 33 00 74 fd 4f 76 fd fd 26 51 fd 4e fd 0e fd fd 1b 5a 77 26 30 58 14 fd 7b fd fd fd 7e fd fd 4f fd 31 fd fd	DI[ZRWAF3th0'ASPaq We&!UN1ewr] _hl%=Cuav]6NFlYUfqxy w pr}S\;lqJgY !vs+O%6t+/yE/ie&` xi4`tr3t Ov&QNZw&0X{~O1	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\WUTJSCBCFX.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\YPSIACHYXW.docx	5	1021	fd fd fd fd fd 51 59 ca 43 2a fd 8c 69 35 fd 78 fd fd 0f fd 39 48 fd 11 6b 37 48 fd fd fd fd fd 65 28 fd 6d 57 7b 44 fd 74 fd 3d fd 69 17 fd fd fd 6a 46 33 fd 30 fd fd fd fd 7a 3c 7f 26 47 06 fd fd 0c fd 5a 64 6d 20 fd 02 49 ea 69 07 79 3b 71 fd fd 26 6d 03 7c fd fd fd 5e fd fd 5a fd 75 fd 15 03 37 21 38 fd fd 06 61 02 7a fd fd 1f fd 25 fd 49 fd 2d fd 12 3e 21 6a 64 7d fd 6f fd fd fd 41 39 0f 1a 43 3b fd fd fd fd 7f 17 fd fd fd 16 fd 28 1b aa 0f 6b 2f 0d fd 3f 4d fd fd fd 1b fd 49 07 fd 69 75 fd 72 25 fd 52 0b fd 58 3a 1f 71 fd fd 46 fd 60 fd 55 fd 4b fd fd fd 7f fd fd 20 fd 74 00 01 58 fd 7a 33 08 67 fd 02 3e fd fd fd 13 7b fd 06 6f 31 4e fd fd fd 05 fd 68 12 38 fd 6b 63 fd 1c 79 7e fd 44 fd 0e fd 25 46 21 70 71 fd fd	QYC*i5x9Hk7He(mW{Dt=ijF3<&GZdm iy;q&m|^Zu7!8az%I->!jd}oA9Ck/? MIiur%RX:qF`UK tXz3g> {o1Nh8kcy~D%F!pq	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.docx	1026	256	fd fd fd 66 1a 5d 3c fd fd 32 fd 25 1b 62 fd 24 fd fd fd 17 fd fd a1 24 25 fd 40 45 fd fd 44 08 35 fd fd 13 fd 55 5f 1b 26 18 fd fd fd fd 5d 67 55 fd fd 21 fd 13 fd 62 fd fd 01 38 fd fd 6e fd 34 70 fd fd fd fd fd 25 fd fd 5f fd 60 fd fd fd fd 49 1b fd 21 fd fd 72 01 11 34 1f fd fd 34 6f 6a 23 fd fd 63 54 fd fd 29 fd 16 60 fd fd 1c fd fd 0e fd 3f fd 6d 20 fd 23 04 36 fd 16 fd 5b 56 6d fd fd 2a 56 fd 49 fd fd 0e b3 fd fd 6b 78 fd fc 20 fd fd fd 09 43 fd fd 3d 66 7c fd 70 fd 3c fd 77 fd fd 66 5b 0b 28 fd fd 40 02 fd 75 fd fd 1e fd 4f 28 2b fd fd 0c fd 05 fd 78 fd 7b 34 06 fd 7e fd fd 98 fd fd fd d3 fd 11 fd fd fd 01 fd fd 18 31 4e fd fd 00 76 fd fd fd fd 73 fd fd fd 68 d0 29 31 a3 fd 68 7e 51 fd fd 57 22 fd	f] <2%b$$%@ED5U_&]gU! 8p%_`I!r44oj#cT)`?m #6[Vm*VIkx C=f|p<f[(@u(+x{4~1Nvsh)1h~QW"	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\YPSIACHYXW.jpg	5	1021	fd 09 1a 7a 54 39 7f 61 0c 50 fd 21 40 fd 02 fd 66 7f fd 4c fd fd 3a 20 62 fd fd fd 48 24 39 fd 4c 70 4a fd 1c fd fd fd fd fd 0b 2d fd 20 22 fd 33 76 5f fd fd 1b 35 18 fd fd 08 fd fd 0d 29 46 60 fd 4a fd af 6c 2f 56 2c fd fd fd 28 4c fd 53 60 38 fd 67 fd 3b 47 fd fd 51 7f 5f fd fd 44 5b 34 fd c0 28 fd fd fd 49 54 fd 47 6a 1e fd 74 fd 2c 37 fd fd fd 78 07 fd fd 40 15 88 fd 10 fd fd 4c 2b 54 fd fd fd 58 fd 90 0c fd 00 01 20 18 fd fd 0d fd 19 4b fd fd 74 fd 62 fd fd fd 20 fd 6a 70 38 26 7a fd fd fd fd fd fd 43 fd fd fd 59 53 0d 6f fd 3b 6a fd 40 fd 0a 27 fd fd 4a 7c fd fd 3d 8c 3d 79 15 77 3a 7f fd 3d fd fd 53 fd fd 7a 6f f7 25 fd 4d fd 46 70 1d 32 fd 9b fd 45 00 27 51 62 17 2c fd 3f 72 6a fd fd 28 31 fd 69 fd fd	zT9aP!@fL: bH$9LpJ-"3v_5)F`Jl/V,(LS`8g;GQ_D[4(ITGjt,7x @L+TX Ktb jp8zCYSo;j@'J|==yw:=Szo%MFp2E'Qb,rj(1i	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.jpg	1026	256	fd 30 fd 24 fd 7b fd 00 fd 5c 4d 47 fd 60 fd 1e 72 7c fd 46 52 fd 48 42 2f fd fd 3f 36 fd 08 22 59 45 7e 40 fd 02 fd fd 16 fd fd 59 55 25 fd 2d fd 63 fd fd fd fd 7e fd 20 3c 1f 32 7c 4a fd 46 fd fd 35 51 fd 4d fd 88 fd fd 28 72 fd fd fd fd 04 fd 0d fd fd fd fd 16 fd fd fd fd fd 38 27 46 0e fd 10 fd 0c fd fd 28 05 fd 50 fd 75 04 fd fd 23 27 20 fd 02 7b 1d 73 fd 4d fd 48 fd fd 03 fd 06 39 5d fd fd fd 59 fd 82 5c fd 0a 09 22 69 fd 66 7b 63 fd 19 fd fd 36 fd fd fd fd 37 66 fd fd 6a fd fd fd 22 2f 32 26 fd 7f 3a fd fd fd 21 09 7f fd fd 39 6e fd fd 0e 75 61 fd fd fd 62 51 fd 04 27 fd fd fd 3f fd 49 fd fd fd fd fd fd fd fd 22 fd 52 b8 63 19 3c 25 fd fd 65 fd fd 65 21 fd 1c 21 5c 3a fd 26 71 2b 71 fd fd 56 fd 63 1a fd 52	0${\MG`r|FRHB/?6"YE~@YU%-c~ <2 |JF5QM(r8'F(Pu#' {sMH9]Y\"if{c 67fj"/2&:!9nuabQ'? I"Rc<%ee!!\:&q+qVR	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\YPSIACHYXW.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	5	1021	41 70 72 5d fd fd fd 3a fd fd 08 3f fd fd fd 23 59 7d fd fd fd 77 fd fd 15 25 fd 0e fd 03 1f fd 79 32 fd 4f 78 2e 06 3d fd fd 33 14 55 fd 24 fd fd fd 2f 65 53 41 47 fd 50 fd 3a fd fd e9 fd 3d 52 1d fd fd 05 63 fd fd 7c 39 fd 13 fd 35 4b 50 fd fd 30 43 2e 65 05 fd fd 3a 76 fd fd 1a 5a 7d 34 6a 29 fd 06 77 fd fd fd fd fd 4c fd fd fd fd 18 93 5a 5c fd fd fd fd 01 fd 78 54 25 fd 15 49 71 22 51 07 4c fd 4e fd fd 2f 01 1d fd 15 fd 79 16 35 fd fd 36 fd fd 14 68 fd 48 fd fd 20 72 4d fd 0d 32 19 18 3e 49 3a 62 fd 2d fd 0f 62 7e 14 0d 79 6b 5d 1b fd 36 41 56 fd 2f fd fd 31 fd fd 44 fd fd 37 46 56 41 fd 39 52 36 fd fd fd 66 6b 5d e7 fd fd fd fd 4d fd 44 fd fd 51 27 fd fd 1e 11 59 fd 6d 18 59 fd 01 4b fd 3e fd fd 3f 93 3d 25 08 4a 6a	Apr]:? #}w%y2Ox.=3U$/eSAGP: =Rc| 95KP0C.e:vZ}4jwLZ\xT% Iq"QLN/y56hH rM2>I:b- b~yk]6AV/D7FVA9R6f k]MDQ'YmYK>?=%Jj	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	1026	256	4d fd 6c fd 43 fd 2c 9b 10 2d 2c 32 46 fd 12 5b fd fd fd 78 7b fd fd 7f f7 39 33 f8 1a 10 fd 6a 65 fd 92 73 fd 6f 28 23 4f fd 4f 25 23 fd 52 3d fd fd 39 fd 53 2f 0e 50 fd 5a 49 fd 5e fd fd 3f fd fd fd 7c 19 fd 43 fd fd 71 15 04 76 48 05 fd 12 4c 0a 62 fd fd fd fd 50 42 fd 70 22 39 44 68 fd 0c fd 4d fd f3 2f 56 fd fd a4 fd fd fd 32 1e 14 fd 31 fd 2f 01 2b 0c fd 53 2b fd 6e 74 30 32 10 fd 2e 34 26 fd 39 39 36 38 fd 20 fd fb 04 fd fd fd fd 4d fd fd fd fd 76 2a fd 34 13 fd fd 0e fd 21 fd 10 fd fd 43 42 fd fd 30 2d 49 fd 50 2c 46 fd 7b 34 fd 7a fd fd 6d fd fd 01 53 6d fd fd fd fd 27 47 fd 7d fd 75 2b 03 fd 67 4c fd 0d fd 14 fd 0b 13 6a fd 02 fd fd fd 5b fd fd fd 2b 2d 1f 6f 02 fd fd 77 fd fd fd 2e 17	MIC,- ,2F[x{93jes(#OO%#R=9S /PZI^? |CqvHLbPBp"9DhM/V21/ +S+t02.4&996 Mv*4!CB0- IP,F{4zmSm'G}u+gLj[+- ow.	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	5	1021	fd fd fd 5d fd 0e fd 2e fd 21 fd 55 fd 0b 52 fd fd fd fd fd 4c 66 5a 34 fd fd 1d fd fd 76 fd fd 79 fd 5c fd fd 11 67 fd 75 fd fd fd 18 1f 2c 78 70 7c fd fd fd 04 fd fd fd fd fd 11 fd 03 70 46 fd fd 25 1f fd 4b fd d5 7c 4f 27 fd fd 4d d6 fd fd 4f fd fd 5b fd fd fd fd 52 fd fd 00 fd 54 46 fd fd 21 71 fd 4e fd 42 7b 61 23 07 fd 7a fd fd a3 bc fd fd 63 fd fd fd 44 7c 23 fd fd fd fd 72 39 16 fd 0f 21 48 fd fd 4e fd 75 48 62 4a 02 7f 6a 75 63 fd 87 fd fd 49 fd fd 2a fd 12 12 23 fd fd 57 71 2a 7d fd 03 fd 31 30 fd fd fd fd 46 fd 1d fd 72 2c 5c 2d 74 fd 60 60 fd 64 fd fd 0a fd 34 57 fd 9f 65 34 5b 0b fd 30 74 37 3a 46 fd 1f 3a 4f fd 7c 5b 75 fd 17 fd 68 fd fd 33 56 fd fd 03 42 fd 0d fd 20 fd 76 fd 32 fd 7e fd	].!URLfZ4vy\gu,xp|pFK|O'MO[RTF !qNB{a#zc|#r9!HNuHbJucI*#Wq*}10F,\-t``d4We4[0t7:FO[uh3VBv2~	success or wait	1	411859	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	1026	256	3e 13 69 fd 77 46 35 62 28 2a 1c 59 fd 53 fd fd fd 1b fd fd 5b b0 6f 29 fd 2f 74 04 fd 83 0c fd 20 fd 51 1e 46 fd 82 fd 72 fd 15 15 fd 06 fd 59 fd 52 fd fd 1a 79 70 4a fd fd fd 72 fd 11 23 36 5e 20 33 fd fd fd fd 75 15 58 75 fd fd 00 fd 4d fd 4b 3b fd fd 52 fd fd 5b fd 1f fd fd 3e fd fd fd fd fd fd fd 49 6d fd fd 31 fd 3b fd fd fd fd 29 0e 5e fd fd ab 09 42 fd fd 31 fd fd 6e 02 6f fd 5a 53 2b fd 23 fd 09 fd 50 46 fd 7d 45 fd 0d 6c 00 07 54 fd 72 2e 1f 6a 5d fd fd 2a fd 33 fd db fd 62 78 0c 17 3b fd fd 7f fd fd 3e 6c fd 43 fd 30 68 17 fd fd 00 fd 0f 47 69 08 fd 37 10 66 fd fd 17 4c 6f 61 fd 4c fd 1f fd 3c 10 00 08 5b cc fd 62 fd fd 7a fd 60 fd fd 6d fd 10 fd 53 36 fd 63 56 53 57 fd 77 05 5b 61 73 28 fd fd 2d 13 52	>iwF5b(*YS[o)/t QFrYRypJr#6^ 3 uXuMK;R[>lm1;)^B1noZS+#PF}ElTr .j]*3bx;>lC0hGi7fLoaL<[bz`mS6cVSWw[as(-R	success or wait	1	4115FA	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Amazon.url	5	106	fd fd 7b 19 79 7a 73 28 89 fd 37 fd fd 20 4f fd fd 2e 0f fd 1f 1a 5d 5f fd 51 69 24 75 22 fd fd 4b fd 31 68 61 fd 16 fd fd fd 6c fd fd 05 fd fd fd 01 fd 45 66 7c fd 34 53 fd 32 fd 47 fd 7a 34 7f 06 fd 28 fd fd fd 48 6c 76 34 6c 6c 2a 61 0a 5e 60 72 fd 69 fd fd 1b 0f 48 fd fd 34 fd fd 51 fd 1f fd 4a fd	{yz(7 O.]_Qi$u"K1halEf|4S2Gz4(Hlv4ll*a^`riH4QJ	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Amazon.url	111	256	58 50 5c fd 59 fd fd fd 44 1f fd fd fd 9e 48 fd 67 fd fd 3e 65 fd 16 fd 43 3b ea fd 40 0c 29 fd 35 fd fd fd 7c fd 42 fd 7e fd 5a fd 39 fd 45 fd 57 fd f7 2e 73 fd 58 fd 35 fd fd 69 27 fd 01 fd fd fd 64 09 fd fd 55 0b fd fd d2 72 0f fd 02 fd fd fd fd fd 7f fd fd fd 25 fd 13 65 3f fd fd 02 7a fd 4a fd 7d fd fd 07 42 fd 1b 20 08 fd 1e fd 52 fd 70 fd 13 fd fd 74 fd fd 50 fd 65 51 68 4a fd fd fd 22 29 fd 57 2f fd fd fd 0f 13 fd fd fd fd 50 de 02 fd 59 2d 62 fd 57 3a fd 1a fd 0d 38 2c fd fd 48 7a fd fd 42 2b 72 fd 6c fd fd fd 75 02 fd 2a fd 62 fd fd 4d 3a fd fd 74 65 6f 28 fd 36 fd 6f 02 1c 0f fd 40 05 fd fd fd 43 fd 28 fd fd fd 7a 7d fd 2a 16 63 fd fd 3d fd 16 0f 30 79 fd 5c fd fd fd fd 23 fd fd fd 11 37 56	P\YDHg>eC@)5|B~Z9E W.sX5i'dUr%e?zJ}B RptPeQhJ")W/PY-bW:8,HzB+ rlu*bMteo(oC(z}*c=0y\#7 V	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Amazon.url	367	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Amazon.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Bing.url	5	203	3f 01 fd fd fd 3f fd fd 69 2e 48 19 64 fd 01 21 22 fd 3e fd 17 fd 46 fd fd 05 fd fd 49 fd 46 2b 5c 5b 26 fd fd fd 00 3f fd 39 35 33 65 21 12 51 fd fd fd 61 fd 66 16 27 fd fd 09 5e 00 5a fd 30 fd fd fd fd 3b 78 08 45 fd fd 7a 75 54 fd 7f fd fd 7a 03 fd fd 12 6f 32 fd fd 79 fd 7a fd fd fd 0f 2c 71 3b fd fd 42 fd 0d fd 1e 2a fd 77 fd 35 fd 35 fd 6d fd 13 4f 1f fd 62 32 5c 95 4c 3f 60 46 fd 6d fd 14 59 7c 12 fd fd 32 fd fd 41 a5 fd fd ae fd 31 fd 1e 4b fd fd 46 fd fd 18 46 75 fd 29 3f fd fd 40 6d 26 fd 36 fd 66 2c fd 35 fd 09 36 fd fd 1c fd 53 fd fd fd fd 2c 45 fd fd 26 05 fd fd	??i.Hd!">FI+\[&? 953e!Qaf^Z0;x EzuTzo2yz,q;B*w55mOb 2\L?`FmY|2A1KFFu)? @m&6f,56S,E&	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Bing.url	208	256	07 58 5b 35 fd fd 0c 5a fd fd fd fd 6f fd 48 fd d6 35 2b 6a 35 58 3d 56 52 24 52 fd 43 fd fd 7a fd fd 74 04 6b 6c 42 75 54 71 fd fd 4c 17 fd 1e 79 fd 19 fd 0a fd fd 1f fd fd fd 69 fd fd 2b fd fd 33 07 fd 71 44 fd 26 48 04 71 fd 48 59 fd 2d 26 3d 05 54 64 fd fd 3c 7c 48 fd 24 3f 66 14 fd fd 4a fd fd 59 fd 70 fd 36 12 fd fd 06 fd fd fd 6e fd 4d fd fd fd 06 23 38 11 24 55 1b fd fd fd fd 29 fd 6c fd 33 fd 33 1e 3a 2f 21 fd fd fd fd fd 38 1a 4b 19 fd 61 66 5b fd 10 fd fd fd 16 52 fd 7b 2a fd fd 33 fd 25 fd fd fd 18 fd fd fd fd fd fd 6d 6d 09 2d 20 25 cb fd 1b 32 55 fd fd fd 3e fd fd 61 fd 76 4e 25 01 56 4c 6a fd 3a 42 fd fd 2b 71 fd 7c fd fd fd 6b fd fd 62 fd fd 16 3a 06 29 2a 03 70 fd 69 7e 0c fd 3b 2f fd	X[5ZoH5+j5X=R$RCztkI BuTqLi+3qD&HqHY-&=Td<\|H$? fJYpnM#8$U)l33: /!8Kaf[R{*3%mm-%2U>vN%VLj:B+q |kb:)*p~;/	success or wait	1	4115FA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Bing.url	464	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Bing.url	504	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Facebook.url	5	108	fd fd 1e 7a 66 fd 05 34 61 64 fd 75 fd fd fd 65 fd 3d fd fd fd fd fd fd fd fd 04 5a fd fd 5a fd 07 41 71 fd fd 4e 6f 02 52 66 fd 64 53 fd 40 5d 43 fd 46 fd 00 fd 48 fd 5f 1d 11 fd 48 fd 51 60 2e fd 74 fd 44 24 21 19 db fd 52 09 75 1a 49 5c fd fd 4c fd fd 16 fd 7c fd 5d fd fd fd 51 fd 3a fd fd fd 19 fd 0d fd 3e fd	zf4adue=ZZAqNoRfdS]CFH_HQ`.tD$!Rul\L]Q:>	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Facebook.url	113	256	09 3f 18 24 fd fd 0f fd 55 70 3e fd fd 58 fd fd fd fd 1b 16 fd fd fd 41 fd 69 fd 24 fd 56 fd 70 06 36 c1 67 08 42 fd 78 65 36 64 2c 51 2a 26 6a 05 fd 6c fd fd 24 05 48 79 6e 54 4c fd fd 1d 7b fd 59 45 16 fd 6d fd fd fd 1d 44 2b 5b 72 2a 30 fd fd 6d fd 4f fd fd fd 77 fd 35 fd 6a 3f 68 35 48 39 0f fd 25 25 06 fd 36 fd 33 fd fd fd 44 fd fd 04 fd fd fd fd 49 66 fd 5c fd fd 0c fd fd 68 fd 42 38 fd fd 2e 48 fd fd 40 3c 48 5d 41 fd 4a fd 71 1c fd 44 53 fd 12 fd fd fd d0 fd fd fd fd fd 41 74 fd fd fd fd fd fd 4d 76 03 29 40 66 fd fd fd fd 53 5f fd fd fd 56 0d 7f 43 32 62 fd fd 75 cb fd fd 26 38 3a fd 21 0a 04 59 28 fd 7c 56 fd fd 32 27 2c fd 5e 4f 63 18 08 55 fd fd 94 1e 65 fd 1e fd fd 0d fd 24	? $Up>XA$Vp6gBxe6d,Q* &jl$HynTL{YEmD+ [r*0mOw5j? h5H9%%6DIf\hB8. H@<H]AJqDSAtMv)@fS _VC2bu&:!Y(\|V2',^OcUe$	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Facebook.url	369	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Facebook.url	409	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Google.url	5	106	02 20 fd fd 60 fd fd 01 fd fd 4b fd 6e 5e 36 5f fd fd fd fd 78 fd 45 19 fd fd 58 fd 7b fd 4a d4 fd fd fd 5a fd fd fd 4b 2e 35 fd fd 79 fd 41 34 4c 00 20 fd 7d fd fd fd 49 fd 4f fd 57 fd fd fd 6c 6a fd fd 78 fd 6d 03 fd fd 41 fd fd 60 fd 65 fd fd fd 49 32 21 42 fd 23 fd 75 75 fd 42 fd 70 fd 51 7d fd	`Kn^6_xEX{JZK.5yA4L }IOWljmA`eI!B#uuBpQ}	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Google.url	111	256	fd fd 4e 4d fd 46 fd fd fd 40 1c fd 5a 26 43 6c 3b fd 78 1b fd 5f fd fd 59 fd 42 53 4f 5b 3a 71 fd 5e fd 76 fd fd fd 4f 5b 79 62 46 fd 58 fd fd 2a 07 43 3f 57 fd fd fd 1f fd 29 fd fd 27 fd 4b fd 4a 0c 73 fd 7d 64 fd 2e fd 79 fd fd 36 09 fd fd 46 fd 0d 79 32 fd 62 4b 2b 70 07 47 fd fd 5c fd 54 72 5f fd fd 39 fd 26 30 fd 07 6e fd 08 1f 1a fd fd 4e 53 fd fd 95 fd fd 27 07 fd fd 00 6b fd 7d fd c8 fd fd 25 22 6c fd 2b 20 fd 54 fd 45 fd 0e fd 78 fd 20 fd 36 25 78 52 12 1e fd 45 fd fd 39 06 41 44 21 fd fd 3a fd fd 04 1a 37 fd fd 5a 17 fd 0a 25 fd fd 69 09 6e 3d fd fd 5b 29 fd 4d 2a fd fd 6f fd 3c fd fd fd fd 2f fd fd fd 7f fd 5d 1a fd 7b 65 fd fd fd 11 fd fd fd fd fd fd 77 20 fd 04 fd fd 48 65 fd 15 72 69 58 fd 4d fd 7e 39 fd 44 fd 11 fd fd	NMF@Z&Cl;x_YBSO[:q^ vO[ybFX*C?W)'KJs}d.y6Fy2bK+pG\Tr_ 9&0nNS'k}%"l+ TEx 6%xRE9AD!:7Z%in={)M* o</]{ew HerXM~9D	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Google.url	367	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Google.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Live.url	5	104	fd 64 fd 77 fd 22 d8 fd 7b 39 fd fd fd fd fd 77 2a 6f fd fd fd fd fd 4e 6b fd 76 6b 4d 39 fd 0a fd fd 1a 7d fd fd 5e fd 03 fd 3a fd fd 3f 3b 49 fd fd 62 fd 38 0b fd 52 09 3e 1f 70 1d fd fd 1f 49 59 2f 3d 7c fd 48 7c 12 03 fd 58 fd 55 fd fd 24 fd fd 6f fd 1d 06 fd fd 3b 7f 7a fd fd 3e fd	dw" {9w*oNkvkM9}^:?;Ib8RpI Y/=|H|XU$o;z>	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Live.url	109	256	fd 26 07 fd fd 17 68 3d 64 fd 41 fd 31 6f 2b fd fd 00 57 fd 4f fd 08 4a 49 4c fd fd fd 7f fd 46 fd 48 fd 79 45 10 0b fd 08 20 45 fd 2a fd 26 33 fd 0c 30 fd 0b 26 fd 78 f2 a7 53 ed 0a 7a 4b 0c fd 02 fd 56 fd fd fd 04 fd 28 fd 53 fd fd 46 fd 37 6b 72 75 fd a3 0f 10 1f fd fd fd 56 5c fd 4e fd fd b7 e8 5c fd 68 fd 6b 75 fd fd fd 65 0c fd 15 48 fd 06 fd 2c fd fd 16 62 7f 47 1d 39 17 fd 26 fd fd 64 96 77 fd 4d 3b 77 49 31 1f fd 41 fd fd 79 fd 68 29 47 5a 93 36 fc 26 fd 7a fd 7a 17 1e 19 fd fd 43 0b 29 fd fd fd 64 fd fd fd fd 1c fd fd fd 50 23 fd fd fd fd 25 e3 fd fd 41 5f 7d fd fd 64 fd fd 40 7f 78 08 5d 63 fd 67 2b fd 07 fd 00 fd fd fd fd 54 fd fd 1e fd 50 73 fd 72 54 03 25 52 7b 4f fd 1c 4b 65 36	&h=dA1o+WOJILFHyE E*&30&xSzKV(F7kruV\N\hkueH,bG9&d wM;wIAyh)G Z&zzC)dP#%A_}d@x]cg +TPsrT%R{Ke6	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Live.url	365	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Live.url	405	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\NYTimes.url	5	107	fd fd fd fd 39 41 fd 5b fd 45 fd 75 fd 77 2a 27 fd fd 79 fd fd fd 6b fd 3d fd fd fd 69 1f fd fd fd 4b 45 fd fd 4f fd fd fd 2b 7e 2d fd fd 19 2b fd 54 fd fd 28 72 fd 27 fd fd fd 33 4f 32 fd 09 4a 41 4a 42 7d fd 2a 55 fd 31 2b fd 5c fd fd fd 60 25 40 fd 51 fd 7c 52 2a 2d 7c 59 40 fd 43 6d 19 23 fd	9A[Euw*'yk=iKO~-+T(r'3O2JAJB}*U1+\%@Q|R*-|Y@Cm#	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\NYTimes.url	112	256	0f fd 7e fd 03 fd 1f 5a 3a 66 fd 79 01 74 37 66 fd 73 74 fd 15 fd 33 65 0d 32 fd 06 57 71 fd fd 49 fd 7d fd 63 fd fd fd 01 fd 0d fd fd 58 fd 43 77 fd fd 5c 06 fd 2b 7b 46 fd fd fd 30 fd 66 fd fd fd fd 05 fd fd fd fd fd fd fd 5a 08 70 4f 1b 21 fd fd 45 06 49 1a 68 fd 72 fd 7d fd fd 14 fd fd fd 68 6d fd 41 33 fd fd 26 59 fd 05 0f fd 7e fd fd 15 fd fd fd fd 38 fd fd 32 fd 73 fd 12 29 29 10 2c fd fd 62 fd 47 1f fd 30 36 fd fd fd 79 fd fd 56 75 35 04 32 fd 0d 46 fd 76 fd 6c fd fd 0a fd 5e fd fd 35 06 fd 18 1a fd 02 6f fd 39 fd 63 fd 0d fd 70 2a fd 0e 7e 75 5e fd fd 6e fd fd fd 78 41 7c 3d 7b fd 4e fd 65 5b 1e 28 38 fd fd 50 fd fd fd 74 6a 58 26 32 fd fd fd 77 5c 48 35 fd 4d fd 77 66 fd 74 fd 7b 2f fd fd 26 fd 0e fd fd 71 fd 62 6a 19 05	~Z:fyt7fst3e2WqI}cXC\+{F0fZp!E Ihr}hmA3&Y~82s)),bG06 yVu52Fvl^5ocp*~u^xA|={Ne[(8PtjX&2w\H5Mw ft{/&qbj	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\NYTimes.url	368	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\NYTimes.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Reddit.url	5	106	fd fd 59 fd 35 fd 0a fd 30 47 fd 19 fd 2f 5c fd fd 1d 15 30 1a 39 79 fd 72 fd 72 77 fd 17 6c 39 fd 45 33 fd 15 fd 58 16 50 7e fd fd 7d 21 fd fd fd 35 5e 55 2c 72 31 6c fd fd 19 23 fd fd 05 70 17 fd 41 fd 07 fd 7c fd 2f 1f 7c fd 47 fd 16 fd fd fd 57 77 fd fd fd fd fd 61 fd 36 3d 71 68 fd fd fd 6f fd 37 fd fd	Y0G/\09yrrwl9E3XP~}!5^U,r1#pA|/|GWwa6=qho7	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Reddit.url	111	256	56 fd 2f fd 10 7f 55 01 fd fd 64 32 1f 42 fd 77 fd 21 fd fd fd 70 61 fd 12 46 4c 22 fd fd fd fd 06 fd 12 5e fd 2d fd fd af 29 fd 41 51 67 fd fd fd 13 2d fd 28 61 fd 6c 1c fd 41 fd fd 0a fd 50 fd 65 fd fd fd 54 7d 24 fb fd 54 1e fd 52 39 fd 38 6a 53 46 20 27 5f 5a 53 fd 5d 3e fd 76 6e 72 28 fd fd 29 fd fd 76 09 4f fd fd fd fd fd fd 05 fd fd fd 35 1b f0 66 fd fd 05 0e 0a fd 5d fd fd 2b 65 0e fd fd 20 73 5d 7f 76 fd fd 1c 6b 49 fd fd 36 3c fd 43 6a fd 5c 5b 66 4a 25 22 26 fd fd fd fd fd 68 1c fd fd fd 6d 59 fd fd fd 12 fd 0b fd 3d fd fd 68 fd 5f fd 29 0d 00 09 fd fd fd fd 3a fd 01 6c 2b 59 0e 4f fd 73 0b 7b 1f fd fd fd 07 fd 14 6f fd 59 6d fd 37 64 27 fd 0d 74 09 26 4a fd fd 37 fd 07 7e 6f 6a fd 11 48 0e fd fd 1c 09 fd	V/Ud2Bw!paFL"^-)AQ-(lAPeT}$TR98jSF '_ZS>vnr()vO5f]+e s]vkl6Cj\ [fJ%"&hmY=h_):l+YOs{o Ym7d't&J7~ojH	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Reddit.url	367	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Reddit.url	407	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Twitter.url	5	107	fd 17 0c fd 57 fd fd 6e 77 fd 47 7f 51 fd fd 15 fd 1f fd 62 66 1d 45 71 0a 0a 5c 1f 7f 7e 02 17 5c 72 fd 52 fd 2e 51 fd 78 40 17 0e fd fd 11 fd 25 fd 39 45 fd 3c 2a 04 45 fd 9b 07 05 59 fd 23 fd fd fd fd 16 fd 4f fd 59 fd 10 fd fd fd 3b fd fd 13 fd 59 4e 01 fd 3f fd fd fd fd fd 43 fd 0e fd fd 71 08 fd fd 4b 36	WnwGQbfEq\~\rR.x@%9 E<*EY#OY;YN?CqK6	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Twitter.url	112	256	fd fd fd 0b fd 53 6d 04 fd 41 fd ec 0f fd fd 46 fd 63 fd 33 fd 1b fd 29 68 fd fd fd fd 37 fd fd 1f fd 40 fd 55 02 38 fd fd fd 39 fd 3e fd fd 22 78 47 fd fd 79 fd fd fd 47 41 fd fd 76 fd 07 fd fd fd 7b fd 3e fd fd fd 33 55 40 27 6a 12 fd fd 17 7d fd 30 fd fd 12 0c 2b fd 60 41 61 76 47 42 fd 05 fd fd fd fd 5f fd 3b 11 7b fd 64 fd 36 fd fd 56 fd fd 0b fd fd 77 fd 02 fd 2a 27 fd fd 7e fd 3c 49 fd fd 63 4a 2e 2d 9b fd 7b 58 33 27 1f fd fd 23 fd 3a fd fd 4b 32 30 fd 27 fd fd 6b 7c 02 fd fd fd fd 69 53 18 5a 09 fd 27 14 5d 42 fd 4b fd 11 fd fd fd 51 fd fd 64 fd fd fd 3f fd fd 0c 7f fd 78 fd fd fd 3c fd fd fd 11 fd 36 44 5d 4f fd 76 1f fd fd fd fd 21 69 74 fd 33 fd fd 46 43 08 22 2e 7a 00 6a 2b fd fd fd 64 79 45 fd 78 fd 6e fd fd fd	SmAFc3)h7@U89>"xGy GAv{>3U@'j}0+`AavGB_; {d6Vw*'~<IcJ.-{X3'#:K 20'k|iSZ']BKQdx<6D]Ov!it 3FC".zj+dyExn	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Twitter.url	368	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Twitter.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Wikipedia.url	5	109	fd fe 15 ff 12 58 27 fd 32 7a fd fd fd fd 57 21 fd 1c fd fd fd 0f fd 3f fd 7d fd 37 4e 38 23 fd 48 fd fd fd 2e 25 fd fd 5d 33 3c 01 fd fd fd 01 51 3f fd 1e fd 7d fd 27 07 49 26 55 fd 39 7b 53 68 7a fd fd fd 19 fd 26 2c 0e 00 7a fd fd fd fd fd 0b fd 53 fd fd 15 3f fd fd 31 17 fd 68 fd fd fd fd fd 0b 3a 39 4a 3b fd	X'2zW!?}7N8#H.%]3<Q?}'I&U9{Shz&zS?1h:9J;	success or wait	1	411859	WriteFile
C:\Users\user\Favorites\Wikipedia.url	114	256	fd fd fd 66 fd 15 00 3d 12 fd fd fd 29 fd 75 fd fd 4d 76 56 fd fd fd 7e fd fd 69 fd fd 61 4e 43 55 fd fd 0f 0f fd 67 66 29 fd 65 45 52 fd 64 54 fd 24 fd 0e fd fd 2e 7c 5f fd 28 01 57 72 fd 6f 6a 6c fd 75 fd fd fd 4e 3a fd 0e 25 07 24 26 67 fd 39 fd 50 d2 48 0c fd fd 01 05 5a fd 69 fd 44 33 fd 57 4c 20 4a fd 28 37 67 1e fd fd 70 fd 09 3e 4b 57 3d 14 fd 25 35 43 fd 33 0e fd 19 fd fd fd fd 48 fd 79 72 fd 63 fd fd 55 44 fd fd fd 0f fd 65 6c fd fd 29 fd 45 16 fd 25 fd 43 3e 7a 17 c3 38 2d fd fd fd e2 17 fd fd fd 65 01 00 25 6e fd 3c fd 14 00 4e fd 6a fd 38 02 63 19 fd fd 60 4c 7a 02 59 fd 62 6b fd 1b 69 41 0a 6b 55 fd fd fd 7a 06 fd 78 12 09 fd 5e 19 60 55 fd ba fd 30 fd fd fd fd 57 fd 49 5b fd 02 fd 13 fd fd 6b 4c fd fd fd	f=)uMvViaNCUgf)eERdT$.\|_(WrojI uN:%$&g9PHZiD3WL J(7gp>W=%5C3H yrcUDeI)E%C>z8-en<Nj8c`LzYbkiA kUz^`U0WI[kL	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Wikipedia.url	370	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Wikipedia.url	410	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\Favorites\Youtube.url	5	107	fd 3a fd 37 53 fd fd 22 4f fd 31 1b fd 5d fd 05 73 fd 58 44 47 0e fd fd fd fd 4d fd fd 44 fd 01 0e 3c 6a fd 23 fd 2f fd fd 2f 2a fd 35 66 fd 55 63 fd fd fd 02 4b 7a fd fd 2e 5b 6d fd 3e 79 46 fd ca 7f 3a fd 5a 46 00 66 2a fd 5b fd fd 2c fd 16 fd 1d fd fd fd fd 27 59 fd 3c 4c 3e fd 7b 5c fd 32 fd fd 2d	:7S"O1]sXDGMD<j#//*5f Uc.[m>yF:ZFf*[,'YL>{\2-	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Favorites\Youtube.url	112	256	fd fd fd 7f 22 03 fd 37 68 45 fd fd fd 5b 10 fd fd fd fd 73 fd fd 73 f2 fd 05 73 12 fd 13 02 77 1a 25 79 6e 51 fd 3b fd 1d fd a6 34 fd fd 72 fd fd 6d a4 fd fd 21 29 0a 32 fd 6b 04 24 fd 0d fd 28 fd fd 79 fd 3e 7e 57 fd fd 79 fd fd 25 3b 71 21 4c fd fd 09 fd fd be 26 18 fd 13 fd fd 7d fd c0 2b 64 fd 62 1c 14 1a 05 2a fd 11 fd fd 03 7f fd 0e fd 64 e7 48 fd fd fd 4d fd 6c 23 fd fd 1e fd fd fd fd 6d fd 2d 37 3a fd 74 fd 15 fd 25 fd 1d 1e 18 fd 73 48 04 18 6a 6b fd fd fd 11 36 fd fd 50 bb fd fd fd 58 11 81 fd 7e 0b fd 64 fd 6b 6b fd 11 fd 66 14 fd fd fd f1 fd 0c fd fd 19 5e fd fd 25 03 fd fd 4d 09 fd fd 60 fd 53 fd 51 fd fd fd fd 47 06 fd 2e 7a 47 70 4c 65 fd fd fd fd 73 fd 22 a2 01 00 fa 53 fd 16	"7hE[sssw%ynQ4rm!)2k$ (y>~Wy%;q !L&}db*dHMl#m- 7:t%sHjk6PX~dkkf ^%`SQG.zGpLes"S	success or wait	1	4115FA	WriteFile
C:\Users\user\Favorites\Youtube.url	368	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Favorites\Youtube.url	408	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	5	557	fd 0d fd 03 5a fd 4d 0b fd 58 fd 5d 72 26 69 59 18 44 fd fd 15 29 7b 38 74 27 fd fd 44 fd fd 0d 5b 23 fd fd 6d fd 3c 57 fd 33 fd fd fd 63 fd 09 37 30 fd fd 4a 00 41 28 71 74 fd fd fd 7f 72 52 68 fd fd 7f 0f 37 09 69 03 7f fd 0a fd 1f 6a 36 fd fd 07 0e fd fd fd 0c fd 3d fd 5f fd 07 fd 15 fd fd 1e fd fd 20 fd fd 20 6c db 34 fd fd 1f fd fd fd 04 44 09 39 5a fd 5e fd 6c fd fd fd fd 57 54 fd 6e 0c 32 79 7c 5a 1d fd fd 74 fd 5d 77 5e fd 4c 5f fd 4f 5c fd fd fd fd fd 59 4e 55 fd 0a 50 c6 7b 49 07 5e fd fd fd fd 0b fd fd 66 fd af 1c fd fd fd 15 23 68 fd 49 60 0f fd 58 75 62 fd 27 0d 42 3b fd fd 63 68 11 44 03 fd 2e 6a 22 3c fd fd 1d fd 28 7a 7f 71 32 5b 2c fd 57 52 fd 7e 58 0e 28 20 c5 7c 3e fd fd 40 35 fd fd 1d fd fd	ZMX]&iYD) {8t'D[#m<W3c70JA(qtrR h7ij6=_ l4D9Z^lWTn2y|Zt]w^L_O \YNUP{l^f#hl`Xub'B;chD.j (zq2[,WR~X(|>@5	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\bowsakkdestx.txt	562	256	0b 73 fd 18 fd fd fd fd fd 42 69 7e fd fd 31 fd fd 16 2e fd fd 4d fd 4b 7e 0a 0c fd fd fd 5c fd 46 52 0d fd fd fd d1 fd fd 27 39 fd 57 59 30 fd 66 1a 51 2e fd fd fd fd 6e fd 38 5a 05 77 fd 16 55 77 fd 5f fd fd fd 33 fd fd fd fd fd fd fd 20 df fd 67 4f fd fd fd 24 fd fd 56 fd 6b fd 0c fd fd 3d fd 36 fd 68 2d fd fd fd fd fd fd fd fd 66 03 27 01 fd 48 fd fd 1a fd fd fd fd fd 56 01 fd 3d fd 22 fd fd fd 72 17 fd fd 30 4e 79 fd 98 fd 14 46 41 fd fd 8a 7d 2e 1a fd 30 fd 37 39 9c fd 7b 53 39 fd 20 fd fd fd fd fd fd 50 fd 3c fd 32 fd fd fd 58 6d fd 13 fd 4e 77 68 22 1d fd 27 fd 1e 35 63 72 fd 21 50 12 26 fd 31 35 fd fd 76 28 fd 3c 44 fd 07 fd fd fd fd 3e 11 fd fd fd 44 02 fd 23 fd 79 fd fd fd 55 4c 45 6b 26 fd 2b 15 4b fd fd fd fd 57	sBi~1.MK~\FR'9WY0fQ.n8ZUw_3 gO$Vk=6h-f'HV="r0NyFA}.079{S9P< 2XmNwh'"5cr!P&15v(<D >D#yULEk&+KW	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	818	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	858	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Local\IconCache.db	5	17957	1c 2c fd 04 fd 55 fd 20 3f 1a 19 47 5b 64 29 fd 09 3e 31 14 fd fd fd 43 43 fd 2f ce fd 49 fd fd 48 fd 2c 5f 0c 3d 05 1d 4f fd 14 fd fd fd 15 26 70 fd 78 fd fd 1b 1a fd fd 14 fd 27 31 fd 03 fd fd 1f 0f fd ff 6d 57 fd 00 2a 1c 6a fd fd 02 31 7f fd 23 3f fd fd fd 57 fd e5 58 37 fd 5e fd fd fd fd 10 42 7c 43 1f 23 7b fd 2b 28 fd 5c 62 fd fd 1d fd 75 fd 60 fd fd 7e 57 fd 7f 21 70 fd 53 5d 71 fd fd fd 48 fd 18 79 fd fd 6b fd fd fd 39 fd fd 49 fd fd 77 24 fd fd 6c 46 fd fd 0e 30 fd 55 fd fd 51 fd fd 11 31 18 01 2c fd 42 6e 01 fd 68 53 fd fd fd 30 fd 66 fd fd 21 1c fd 71 fd 69 79 fd fd 0a 67 22 fd 72 48 27 1e 44 19 fd c0 1d 72 47 40 35 fd fd 4e fd fd 2b fd 2d 2e 33 fd fd fd 75 5d fd fd fd 47 22 17 fd 18 fd 43 fd 65 57 fd 25 1b	,U? G[d)>1CC/lH._=O&px'1mW*j1#?WX7^B|C#{+ (bu`~W!pS]qHyk9Iw$lF 0UQ1,BnhS0f!qiyg"rH'DrG@5N+-.3u]G"CeW%	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IconCache.db	17962	256	05 fd 25 02 fd 43 6d fd 77 fd fd fd fd fd 5a fd fd fd 3b 25 40 5e fd 02 48 67 fd 0b fd 07 6c 41 4c fd 69 fd fd fd 66 fd 2d fd fd 18 2a fd fd fd fd 4c fd fd fd fd 44 fd fd fd 30 4c 6b fd 74 12 1a fd fd 15 60 15 fd fd 47 7f 5a fd 1b fd 40 33 fd 06 fd 5d 64 72 fd fd fd 3b 0b 1f 74 08 10 fd 08 7c 2f fd cc fd fd 28 22 fd 35 57 fd 2f 7e fd fd 68 4f fd 5b 14 6c 55 fd 26 74 fd fd 21 70 fd fd 34 1f 2d fd fd fd 3b fd fd fd 55 fd 2a fd fd 03 fd 2f fd 06 fd 5b fd fd fd 0b 47 fd fd fd 2d 5a fd fd 59 44 fd fd 0e 5d 0d fd 36 fd 0b fd 20 2e 6c fd 14 32 fd fd 45 3a 52 4b fd 26 fd 56 36 fd 0f 08 45 fd 35 25 1d 14 42 fd 45 79 fd e2 74 fd fd fd fd 2f fd fd 25 72 fd 39 39 02 fd fd 03 13 fd 52 fd 5f 0b fd 3f 52 50 fd 75 0b 65 10 fd 0c 32 fd	%CmwZ;%@^HglALif-*LD0Lkt`GZ@3]dr;t|/("5W~hO[IU&t!p4-;U*/[G-ZYD]6.l2E:RK&V6E5%BEt/%r99R_?RPue2	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Local\IconCache.db	18218	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Local\IconCache.db	18258	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	5	1044	34 12 1f fd 2a 16 65 fd 2c fd 33 fd 66 66 fd 6b fd fd fd fd 07 06 7d fd 6c fd fd 18 0b fd fd 15 52 fd 2e fd 7c 18 4a 0c fd 19 fd 42 fd fd 63 61 74 fd fd 09 fd f0 fd 10 6e fd 4e 68 49 4d fd 4c 6b fd fd fd 1e 36 1b 36 fd 63 fd 23 fd fd 3e fd 26 fd fd 39 7e fd 05 fd fd fd fd 46 fd fd fd 5d 1d fd 64 fd 60 fd fd fd 3d 27 16 29 fd fd 0e 29 fd 70 fd 67 70 fd 1e fd 52 57 fd 1d fd fd fd fd 2e 59 54 18 84 6a fd fd 50 05 fd 06 fd fd fd b4 fd 5b fd fd fd 23 fd fd 07 7c 46 44 75 2f 33 6d 56 52 55 5b e4 83 fd 2f 6e fd 68 fd 02 fd 3b 57 2c fd 47 fd fd 64 fd 73 37 7e 53 57 06 2f 0a fd b0 2a fd fd 52 5d 16 fd fd 73 fd fd 6c 00 fd 09 7f 81 fd fd 29 fd 41 fd 7b 2a 5d 06 05 73 fd 35 47 fd fd fd 0b 2e fd fd fd 38 6a fd fd fd 3b fd fd	4*e,3ffk}IR.JBcatnNhIMLk66c#>&9F]d`='))pgpRW.YTjP[#|FDu/3mVRU[/nh;W,Gd7~SW/*R]sl)A{*]s5G.8j;	success or wait	1	411859	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1049	256	7c 78 28 67 fd 06 fd 76 74 fd 67 fd 39 41 47 fd 24 fd fd fd 4a fd fd fd 74 03 fd 13 fd fd fd 75 57 fd fd 17 54 fd 3f 5f 20 fd fd ed 47 fd 6c fd 7a fd fd 1e 6c fd 73 1a 22 37 fd 7b 2d 00 4f fd 56 fd fd 2e fd fd 72 5a 7a fd fd 3d 41 68 fd 48 79 8a fd 2b fd 15 7e fd fd 72 fd fd 11 4b fd 6c 36 fd 63 7c 2b aa b4 fd 7e 40 fd 04 74 7e 44 fd fd fd 38 2d 75 fd 7f fd fd 09 16 2d 40 fd 0f fd 36 1a fd fd 17 fd 03 fd 55 fd 37 fd fd 25 fa 35 65 5b 64 fd 0b fd 61 71 fd fd fd 33 65 3a 0c 1a 7f 25 fd 4a 18 0e 43 fd 7b fd 21 fd fd 12 fd fd 12 51 66 fd fd 3b fd fd 4f fd fd 56 0e fd fd 52 22 3b 3a fd fd 3e fd 1e 5a 49 fd 64 57 fd 47 fd 23 fd 04 fd 24 73 32 fd 0b 5d fd 40 fd 2d fd 51 fd 6c 6e 48 fd 35 fd fd fd 61 57 fd 2f 44 fd 3a fd	|x(gvtg9AG$JtuWT?_ lzls"7{-OV. rZzAhHy+~rKl6c\|+~@t~D 8--@6U7%5 e[daq3e:%JC{!Qf;OVR";: >ZIdWG#$s2]@- QlnH5aW/D:	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1305	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	1345	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	5	2	fd fd		success or wait	1	411859	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	7	256	77 fd fd 04 87 fd 6f fd 79 23 fd fd 06 37 6e fd fd fd 18 04 fd 4b 2b 74 77 07 3b fd 52 20 d0 51 fd fd 43 74 6d fd fd 7a 63 fd fd 0d fd fd 42 21 fd 59 74 fd fd fd fd fd 54 fd 13 fd 6e 4f 08 71 fd 74 1d fd fd 5a 3e fd 29 fd 12 4a 3e 0b fd 18 41 7e 1b fd 27 8b 7f 65 41 fd 6b 78 fd 06 58 fd fd fd fd 41 fd 0d 15 fd fd 13 67 fd 36 3e 26 fd 65 67 3e fd 2b fd 2d fd fd fd 46 78 fd 48 fd fd 11 16 fd fd 6b 5b 3d 44 18 fd 3c 63 2c 07 08 29 fd 4b fd fd fd 60 fd 7e fd 62 71 fd 3c fd fd fd fd fd fd 77 fd 61 45 5f 04 55 1a 1f 62 fd fd fd fd fd 22 03 fd fd 41 3c fd fd fd fd 51 fd fd 2b fd fd 76 fd fd 75 fd 3a fd 7c 16 64 7c 2f 48 53 27 fd 21 fd 3e 60 fd 20 6c fd fd fd fd fd 1f 5a fd fd 7f 34 68 57 42 fd fd fd fd fd 2f 25 5c 3c 36 fd 31	woy#7nK+w;R QCtmzcB!YtTnOqt>)J >A~'eAkxXAg6>&eg>+- FxHk[=D<c,) K`~bq<waE_UbA<Q+vu:| d|/HS'!>` Z4hWB/%\<61	success or wait	1	4115FA	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	263	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	303	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	5	1021	fd 40 26 68 fd 40 fd 6b fd fd fd 06 75 42 fd 6e fd fd fd 19 fd 13 60 fd 62 03 41 fd 67 fd 60 1e 19 fd fd 09 fd fd 6d fd 2c 2a fd 12 2f fd 41 fd 00 38 4c 53 fd 2f fd 42 0c fd fd 57 16 fd 3f 54 fd 6c fd 20 fd fd 34 1f fd 77 40 52 4e fd 2d 3f 6f 3a 3a 09 fd 79 50 fd 03 fd 9a fd 54 1b 58 fd fd 60 fd 00 30 fd fd 47 fd 01 49 2f 0a 47 2e 17 fd 71 42 22 fd 3c 7d fd 72 fd 01 fd 38 fd fd fd 22 65 4d fd 3f fd 10 fd fd 57 38 fd fd fd 13 fd fd 04 11 fd fd 03 47 fd 34 3e 0b fd 41 7a 45 03 fd 5f 5e 2b fd 48 7a 74 fd fd 19 fd 4a 19 fd 4b 3b 33 05 36 fd 0e 3e 19 2c fd fd fd 16 16 7c 04 11 35 fd 35 07 fd 72 10 78 50 5a fd 63 63 0f 70 fd fd fd 09 fd 4c 5e fd fd 41 fd 13 2e fd fd 10 57 fd fd 7f 59 fd fd 61 fd 65 fd 4a fd fd fd fd 52 a8 76	@&h@kuBn`bAg`m,*/A8 LS/BW?Tl 4w@RN-? o::PTX`0Gl/G.qB" <}r8"eM?8 4>AzE_^+HztJK;36>,|55r xPZccpL^A.WYaeJRv	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	1026	256	fd fd fd 6d fd 55 46 fd 6c 60 7f 27 22 fd 4e 51 fd 67 fd 45 fd 7a 3f 2c 01 fd 17 fd 1d fd fd 04 fd 75 54 50 2f 7f fd 0d 0d 01 62 fd 7d fd fd fd 48 50 fd 12 37 73 fd 27 fd 0e fd 3d 5e 3a fd 4c b4 fd 1f fd 19 5e fd fd 17 fd 4f 46 5e fd fd 02 fd 20 57 6a 7d fd fd fd fd 5f fd fd 13 fd 2e 25 6d fd 27 22 52 5c fd 0e 36 fd 49 fd 37 43 19 51 78 fd fd fd 31 fd fd fd 63 2e 14 2a 16 fd 72 fd 50 fd 6a fd c5 02 74 fd 1c 08 25 fd 4e 0f fd fd 2f 5e 5f 33 4a 38 71 fd 22 5a 7b fd 0b 0e fd fd fd fd fd fd 4c 74 26 25 fd fd fd 65 7f fd fd 0f 46 fd fd fd 7d 24 5e 1d 25 50 33 fd 3e 5c fd fd 0c 55 58 fd 1c fd 2b 5e fd 5b 57 36 fd fd fd 00 21 fd 19 68 fd 66 20 fd fd 70 fd 56 fd 69 6d fd fd 5e 68 fd 1d fd 56 6e 17 35 6f fd 37 fd fd fd 50 cc fd fd 11	mUFl`'"NQgEz?,uTP/b}H Ps'=:L^OF^ Wj}_.%m'"R\6I7CQx1c.*r Pjt%N/ ^_3J8q"Z{Lt&%eF}$^%P 3>\UX+^[W6!hf pVim^hVn5o7P	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	5	1021	fd 49 0c 39 46 26 57 fd 40 fd 15 fd fd 42 07 21 5d 31 fd fd fd 30 7e 67 fd fd fd fd 70 fd cb 52 fd 02 fd fd 42 fd fd 3c 08 fd 1e fd 4e 0f fd f5 06 fd 7d fd fd fd 3e fd fd 39 fd 4b 59 2b fd 5f fd 5e 6c fd fd 71 7e 6e fd 55 fd 61 7d fd 6c fd fd fd 5f fd 38 47 fd fd 33 08 fd 4d fd 30 fd fd 5d 24 fd 2b 04 fd 4b e1 fd 65 fd 1f fd 64 0b 57 fd 5d 38 79 fd fd fd 34 fd fd 20 57 0f fd fd 47 fd fd fd 3c 43 6b 0b fd 50 3b fd fd 10 fd fd 2d fd fd 17 0d 4a 18 07 fd 67 3a fd 6e 75 66 0d 08 fd fd 45 14 fd 4d fd 32 fd 1c fd fd fd 4e 33 fd 5e 33 c5 ce fd 34 fd fd fd fd 6a fd 0a fd fd fd 02 fd fd 84 18 fd 6d 0b 60 1b 31 fd 1e fd 55 fd 01 fd 22 3f 09 fd fd 56 fd 29 5d fd fd 44 fd 7c 5d fd 02 fd 4e fd fd 5a fd 59 38 05 34 2b fd 51 fd 33 fd fd	I9F&W@B!]1~gpRB<N}>9KY+_^Iq~nU a}I_8G3M0]$+KedW]8y4WG<CkP;-J g:nufEM2N3^34jm`1U"?V)]D|]NZY84+Q3	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	1026	256	09 6f 2a fd fd 6b fd fd 48 75 31 73 17 40 02 54 fd 07 67 fd 65 fd fd 31 fd 3a fd 5f fd fd fd fd fd 69 25 fd fd 0a fd 3a 08 f2 38 fd 2e 13 2c fd fd 24 fd 11 fd fd 4f fd 0d 46 fd fd 46 fd 4b fd 50 fd fd fd 1e fd fd 3b 3c 01 fd fd 21 0f fd fd fd cd 5b fd fd a3 fd 39 14 61 fd fd 48 70 20 0a 5d fd 6a fd fd 2b fd fd 6d fd fd 3c db 2b fd 61 fd 03 fd fd 35 3c 20 fd fd 40 35 1a fd 11 1a 5e 20 fd 3b fd 20 17 fd fd fd 1d 78 fd 0a 2a fd 4e 3d fd 09 fd 01 fd e7 4e 46 fd fd 64 57 fd fd 03 fd 4a fd 72 fd 55 36 fd 22 3d 09 54 fd fd 3d 7f 08 fd 78 fd fd 23 fd 30 fd fd fd 6a 03 fd fd fd fd 2e 2f fd 61 fd 72 fd 27 58 fd fd 6b fd fd 45 fd 05 fd 71 fd 49 4a fd 5e fd 73 fd 30 61 2a fd 7c fd 1d 75 fd 30 fd 04 66 6b 0b fd 28 13	o*ku1s@Tge1:_i%:8.,$OFFP;<![9aHp]j+m<+a5<@5^ ; x*N=NFdWJrU6 "=T=x#0j./ar'XkEqlJ^s0a|u0fk(	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	5	1021	fd 3a fd fd fd 14 fd 23 fd 7d fd fd fd 26 48 fd 4a 3f fd 7e fd 6c 08 fd 7d fd 39 37 70 fd fd 55 60 fd 3d fd 24 fd fd 5d 04 6c 6d fd 78 0e fd fd 39 37 8f 75 76 49 fd 19 fd 30 fd 5d 58 fd 72 2d 70 58 08 fd 11 fd 6c 5a fd 31 50 56 28 fd 4e 76 7c 67 1f fd 4b fd fd fd 5d fd fd 33 04 fd 73 00 5d 28 22 45 1c 28 fd fd 1d 2a 0f fd 0a 39 14 4f fd 7e fd 46 76 26 1b 51 39 fd fd 31 fd 05 2f 1a fd 0e 69 39 45 fd fd fd 35 1c fd fd 3e fd 5d fd 14 fd 11 55 62 fd fd 24 fd fd fd fd 3d fd 04 fd fd 27 68 1f fd 48 53 12 2d fd fd 01 fd 2e 5c fd fd 78 22 fd fd 67 00 55 09 fd fd 40 fd fd 56 fd fd fd 52 21 32 fd fd 00 22 1f fd fd 0c fd fd 73 33 fd fd 1b 03 fd 19 fd 53 41 fd 5c fd 7e fd fd 05 16 4a 2f 0d 0f fd 52 fd fd 72 36 fd 37 42 6d 60 54 fd 5e 7d fd	:#}&HJ? ~l}97pU`=$]lmx97uvl0]Xr- pXlZ1PV(Nv\|gK]3s] ("E(*9O~Fv&Q 91/i9E5>]Ub$='hHS- .\x"gU@VR!2" s3SA\~J/Rr67Bm`T}	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	1026	256	00 1c fd 7f 2c fd fd fd 0e fd fd 0d fd 04 fd 2c fd 1a 37 24 5e fd fd fd fd 7c fd fd 0c fd 22 fd fd 35 fd fd 47 fd fd fd 0c fd 69 fd 49 17 fd 1a fd fd fd fd 1b 59 fd 2f 1e fd fd 16 76 fd 31 fd 20 6a fd fd 6b fd 3a 20 fd fd 00 fd 61 43 fd fd fd 64 fd 3f fd 5f fd fd 3a fd fd 47 39 fd fd 19 fd 24 fd 6f fd fd 3c fd 1b fd fd fd fd 56 13 47 09 64 58 04 fd 4e 92 52 78 fd 71 7b 50 45 fd 11 fd 03 fd 13 fd fd 07 5e fd fd fd fd fd 03 61 fd 4d 6d 17 fd fd fd fd 53 2d fd 20 fd 31 7b fd fd fd fd 01 31 3c fd 5b fd 6c 5d fd 71 70 fd 3d fd fd fd fd fd fd fd 73 76 fd 0a 4f fd 18 1e fd 3d 4c fd fd 63 fd 1f fd fd 7c 53 fd 60 fd fd fd 67 05 fd 1e 38 38 fd 70 50 fd fd 73 74 fd 38 fd 05 fd 71 1b 5f fd fd 60 fd 68 34 43 fd 7d 82 fd fd 0b fd 36 fd	,,7$|"5GilY/v1 jk:aCd? _:G9o<VG dXNRxq{PE^amS- 1{1<[l]qp=svO=L c|S`g88pPst8q_`h4C}6	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3	5	1021	fd fd 57 fd fd 51 73 07 fd 24 fd fd fd 09 f9 3b 3f fd 2c fd 72 fd 0c 14 57 4a 55 fd 13 fd 56 fd 64 73 fd f1 fd 31 75 fd 10 fd fd fd fd fd 69 64 fd 48 1f 69 44 fd fd fd 50 4a 5c 40 fd 61 79 fd fd fd fd 55 fd 0b 53 fd 04 5d 47 dc 33 fd fd 29 fd 53 52 24 fd fd fd 51 51 21 fd 48 72 fd fd fd 75 fd 23 12 fd 46 fd 74 fd a5 fd fd 50 fd 53 71 fd fd 5c 37 35 5f 05 3c fd 0f 49 fd fd 5b fd fd fd 3a 22 fd 59 4f fd 23 fd 5e fd 5a fd 3a 1d 65 2e 1c fd fd 74 fd 08 fd fd 25 2b 14 fd fd fd 24 fd fd fd fd fd 3c 09 fd fd fd fd 42 3d fd fd d4 fd 39 22 fd 3e 07 10 fd 40 fd 46 fd 0a 5a 0c 05 5c 31 fd 7b fd 2e 29 fd fd fd fd 47 fd fd fd fd fd 34 4c 47 fd fd fd fd 52 1e fd fd 03 fd 46 5c 33 76 1a fd 0c fd 53 fd 16 5e fd fd fd 25 59 fd fd fd 30	WQs$;?,rWJUVds1uidHiDPJ\@ayUS]G3)SR$QQ!Hru#FtPSq\75_<l[:"YO#^Z:et%+$<B=9">@FZ\1{.)G4LGRF\3vS^%Y0	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3	1026	256	fd 24 2b 66 fd fd fd 54 fd fd fd f4 9b 54 2f 62 fd fd 6b fd 1f 46 52 6d fd fd fd fd 3c fd 7a fd 4c fd 08 6e 27 3e 3c 36 08 1d fd 4c 29 27 fd 29 1d 77 fd fd 3f fd fd fd fd 38 31 42 fd fd fd 76 fd 51 29 fd 5c 38 fd 02 fd 64 fd 3d 2a fd 56 5b fd fd fd fd 02 20 7b fd fd fd fd 26 40 5e fd 6f fd 32 fd 0a 32 00 10 fd fd 5b 45 7e 66 68 fd 6a 34 74 00 42 52 00 62 46 fd 49 47 6b fd 57 73 fd 1b fd 06 fd 69 54 14 49 fd 2f 71 33 2a 2e 77 21 fd fd 04 3e 70 fd 51 fd fd 52 03 fd fd 4f fd fd fd 68 6d 51 fd 05 61 fd 00 33 26 fd 50 fd fd 45 65 fd fd 19 fd 2a 1a fd fd 62 15 1a fd fd 79 fd fd 50 3e 5e fd fd fd fd fd fd 0c 3f fd fd fd 7c fd 3c 06 6e 78 2a fd 46 60 fd 73 27 22 70 35 fd fd fd 6f fd fd 23 fd fd fd 10 fd 62 fd fd 6d fd fd	$+TT/bkFRm<zLn'><6')w?81BvQ)8d=*V[{&@^o22[E~fhj4tBRbFIGkWsiTI/q3*.w!>pQRhmQa&PEe*byP>^?|<nx*F`s'"p5o#bm	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFIJJ.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	5	1021	fd 53 fd fd fd fd 25 fd 52 35 7b 19 fd 58 fd 38 b1 4c 77 31 fd 30 fd fd 65 fd fd 48 58 42 3c 16 fd 64 fd 17 51 1a fd 2d 6c fd 6e 6f fd 03 fd fd 52 44 fd fd fd fd fd 20 fd 4d 31 fd 28 fd 35 5c 1c fd 2f 78 fd 6d fd 33 36 36 fd fd 07 35 65 60 5b fd 77 23 48 4c 6a 5e 62 42 fd 2d 40 03 32 fd 33 09 fd fd 61 fd 29 fd 6c 14 09 3a fd fd 4d 17 54 6e 56 6c 14 23 fd fd 17 fd fd 58 0e 5c fd fd 74 1d 36 37 fd 00 00 fd fd fd 61 62 fd 0d fd 17 fd fd fd 11 22 43 fd fd 0c 55 1c fd 59 fd 14 30 fd 17 52 06 fd 06 fd 2c fd fd 32 1e 49 fd fd fd fd 0b fd fd 9a fd fd 1a 68 fd fd fd fd fd 2c 14 11 27 fd fd 26 fd 26 0e fd 22 fd 49 fd fd fd fd fd fd 57 35 fd 23 6b 01 fd 4c 6b fd 72 0b fd fd 21 fd 06 fd 56 fd fd b0 fd 53 fd 73 2d 61 fd 4e fd fd fd	S%R5{X8Lw10eHXB<dQ-lnoRD M1(5\ /m3665e`[w#HLj^bB-@2a)I:MTnVl# X\t67ab"CUY0R,2Ih,'&&"lW5#kLr!VSs-aN	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	1026	256	fd fd 38 2a 3b 27 fd 41 56 fd 08 42 40 67 54 3d fd 11 fd 6e fd fd 69 fd 17 0c 70 fd 3b 7e fd fd 2c fd fd 3c 0b fd fd fd 7d fd 36 fd fd fd 3f fd 76 35 75 09 06 16 12 4d 1b fd 74 7c da fd fd fd 34 fd 3b 3a 76 7b be 2d fd 5c fd fd 24 74 5f 04 3f fd 29 fd 1e ad fd 46 19 16 50 fd 46 36 31 fd 52 79 fd fd 74 fd fd 07 54 50 fd fd fd fd 32 fd 79 1d fd 28 53 fd 0e fd 01 33 fd fd 2a 2b fd 75 30 fd fd 26 07 6e fd 09 46 fd fd 7b 48 46 fd 43 fd 15 bb fd 62 6d fd 6b fd fd 44 fd fd 31 64 fd fd fd fd fd 64 6b 19 fd 59 fd fd 20 20 fd fd fd 77 4f 77 2b fd 2d fd fd fd fd 65 fd fd 09 60 7f 1a 78 23 21 5f fd 64 fd fd fd 54 fd 47 71 17 fd 58 fd 57 fd fd fd 12 39 fd fd 41 fd fd 2f 1b fd 61 33 fd 25 fd 4d 08 0b fd 33 fd fd 50 56 25 3b fd fd 2d 0e	8*;'AVB@gT=ip;~,<}6? v5uMt|4;;v{-\$t_?)FPF61RytTP2y(S3* +u0&nF{HFCbmkD1ddkY wOw+-e`x#!_dTqX W9A/a3%M3PV%;-	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	5	1021	fd 20 09 fd fd 40 44 fd fd 28 fd 7b 4e fd fd 0c fd 14 fd 55 fd 14 fd fd fd fd fd 13 fd fd 2b 1b fd 00 fd 2f 64 fd fd 33 fd 25 fd 2b 3f 58 0c 04 3a 67 fd 00 2a fd fd fd fd fd 0c 16 fd fd 27 4b fd 2a fd 78 32 fd fd fd fd fd 1e fd fd fd fd fd 0e fd fd fd 04 32 fd 13 fd fd 6e 6d 9c 35 fd 30 fd 50 fd fd fd fd 1b fd fd fd 25 0b fd db 90 fd fd fd 44 29 56 31 4d fd 65 55 fd 1b fd 04 16 2f 3d fd 16 fd 7b fd fd 1a 23 53 fd 29 fd fd fd fd 75 6b fd fd 1a fd fd 01 4f fd fd 08 4a fd 24 fd 13 fd 21 fd fd f1 31 49 5a 19 fd 3f fd 20 77 57 fd 72 fd fd fd 6a fd fd 3e 68 fd fd 08 3b fd fd 49 5c fd fd 30 fd fd fd fd 11 75 1e fd fd fd 0e 0f fd 0f 3f 47 fd 6c 10 fd 1f 74 5a 65 41 fd 25 7c 74 0d 45 2b 62 fd 4e fd 2d 0d 51 fd 54 fd fd 1a fd	@D({NU+/d3+?X:g*K*x22nm50P%D)V1MeU/={#S)ukOJ$!1IZ?wWrj>h;I\0u?GltZeA%|tE+bN-QT	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	1026	256	fd fd 5e 49 11 fd 42 fd 0e 53 fd 05 fd 48 fd 54 fd fd fd fd 19 33 fd fd 30 18 33 fd 04 5a 5d fd 32 fd 47 fd fd fd fd 39 fd 2c fd fd fd fd 4b 01 54 fd fd 4a 36 fd 13 fd 6e fd 7f fd 60 fd fd fd fd 34 4d 21 36 09 75 fd fd 6f 20 fd 22 fd 16 7e fd 6a fd 5d fd fd fd 28 42 37 fd fd 56 48 fd fd 44 68 fd fd 55 fd 52 fd 07 69 42 fd 11 fd 32 60 fd fd fd fd 25 fd 05 39 0e fd fd fd 6e 67 6a fd fd fd 52 0b 55 fd 60 1f fd 49 28 fd fd 01 17 05 fd fd 54 fd fd fd fd 38 49 fd 78 fd 7a fd 16 3a fd fd fd fd fd 3e 2f fd 25 67 fd fd fd 04 fd 7a fd fd fd fd 27 24 63 fd 0c 75 0d fd fd fd fd 31 fd 43 fd fd fd fd 3f fd fd fd 0a fd fd fd 4e 7c 36 fd fd 6d 32 19 4d 16 4f 1c fd 6e 6c ec fd fd fd 73 3a fd 23 fd fd 27 fd fd 91 fd 0f fd 79 fd 24 5f fd	^IBSHT303Z]2G9,KTJ6n`4M!6uo "~j](B7VHDhURiB2`%9ngjR`I(T8Ixz:>/%gz'$cu1C?N\|6m2MOnls:#'y$_	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	5	1021	fd 62 4a 32 fd fd fd fd 7b 6a fd 7b 27 7d 31 0e 0e fd fd 25 60 4d fd fd fd 28 fd 60 fd fd 00 34 fd a6 fd 56 60 12 fd fd 6d fd 0e fd 69 fd fd 33 39 fd 72 24 13 00 fd 2c 52 39 a4 fd fd 3c fd 33 fd 6c fd 2e 5e 43 74 fd fd 37 fd 2e fd 6b fd 60 fd fd 6e fd fd fd 76 2c 2c 05 e6 30 43 2a 5b 14 33 79 fd fd 04 d6 fd fd 6f 33 fd 52 fd 11 fd 30 fd 29 fd 7f fd fd 68 fd 15 fd fd 2a fd 00 fd 2b fd fd 05 6f 08 61 21 fd fd 6b 58 02 fd 30 fd 1d fd 55 4a 38 fd 11 67 13 76 fd fd fd fd 0c 3a fd 52 fd fd 1b 4f 41 51 fd fd fd fd fd 32 5b fd fd fd fd fd fd fd fd 15 47 0a fd fd 53 57 32 fd fd fd fd fd 01 fd 00 1e 62 3d 27 fd fd fd fd fd fd 0c 34 49 28 6a 30 49 fd fd 4e fd fd 21 2a 65 06 fd 1c 7f fd 68 fd 47 5f 3e fd 17 21 05 fd fd fd 36 fd	bJ2{j{'}1%`M(`4V`mi39r$,R<3l.^Ct7.k`nv,,0C*[3yo3R0)h*+oa!kX0UJ8gv:ROAQ2[GSW2b='4l(j0lN!*ehG_>!6	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	1026	256	40 fd 11 fd fd 13 fd fd fd 39 41 2c 37 68 3f 40 27 16 fd fd fd fd 32 e1 77 fd 64 63 10 4d fd 79 58 fd fd fd fd 66 0b fd 1a 35 35 2f fd fd fd fd fd fd 2e fd fd 52 fd fd 45 7e fd 16 fd fd fd fd 14 42 fd 19 64 fd 0f fd 4f 3b 45 33 77 fd 6f 16 fd 1c 6a 48 fd 7d 57 fd 1b fd 14 3e fd fd 7a 60 45 0a 60 15 59 fd 68 7b fd 3d 32 5c fd 05 fd 59 4e fd 70 40 51 19 52 fd 42 66 fd fd 7a 1d 3e 02 4e fd fd 21 01 fd 7a 3f fd 7b 31 fd fd 5b 4f fd 17 17 30 18 fd fd 6a fd fd 32 42 fd fd fd 47 36 fd 59 6e 56 fd fd 28 fd fd 3f fd fd fd 21 43 35 11 36 fd 64 48 fd fd fd fd 14 27 17 fd 21 7c 15 fd 6e fd 67 fd fd fd fd 71 35 f3 fd 07 fd 52 25 5b fd fd fd 5c 55 27 7c 0f 69 47 3f 45 23 70 fd 72 4d fd 33 fd 7f fd 0d 7a 39 07 fd 55 5b 1d 71 fd 19	@9A,7h?@'2wdcMyXf55/.RE~BdO;E3wojH}W>z`E`Yh{=2\YNp@QRBfz>N!z?{[O0j2BG6YnV(?!C56dH'!|ngq5R%[\U'|iG?#prM3z9U[q	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	5	1021	cc fd 46 64 fd 70 6f 33 7f fd fd 5d fd 77 fd fd fd 34 fd 46 70 7d 2a 7a fd 41 fd 2c fd 73 17 fd fd 57 3f fd fd fd fd 68 7d fd fd 79 fd fd 7d 5a fd fd 3e fd 07 1c 3d fd fd fd 5e 95 44 fd fd 33 16 fd fd 5f fd 45 35 fd 28 fd fd fd 74 fd 55 fd 5a 72 fd fd 7c 57 16 fd fd fd fd 08 45 fd 11 fd fd fd 05 00 fd fd fd fd 15 34 fd fd 7d 7e 68 fd 36 60 73 57 3a 0f fd fd 6d fd 43 20 fd 72 5d 2a fd 51 fd fd 21 fd 27 59 0b fd 7a fd 1a fd fd fd fd 04 34 fd 5f 7e e8 fd 32 6a fd 5a 13 3d 22 fd 0e 13 fd fd 84 fd 6d fd 3e 07 9a 61 8e fd fd 23 6e fd fd 70 29 2e fd 21 60 0e 31 3f fd 55 fd 79 0f fd 37 6e fd 29 fd fd fd fd fd 15 fd fd fd fd 26 fd fd 5c fd 11 fd fd 5c 41 26 50 64 4f fd 60 11 1b 43 fd fd 40 01 4c fd 6d fd 02 33 2c fd	Fdpo3]w4Fp}*zA,sW?h}y}Z>^D3_E5(tUr|WE4~h6`sW:mCr]*Q!'Yz4_~2jZ="m>a#np).!`1?Uy7n)&\\A&PdO`@Lm3,	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	1026	256	12 fd 40 10 40 fd 7c fd 3f fd fd fd fd 0c fd fd 59 5a fd 66 1d fd 4a fd fd fd 5c 89 fd fd fd 8a 47 fd 32 fd 62 fd 47 fd fd fd 7f fd 6a fd 7c 2d 2f 9f 27 fd 0d 3e 0d 3f fd 22 79 09 b7 fd 0c fd 5e 2b 9f 06 fd fd fd fd fd 08 7f fd fd 0e 69 51 fd 76 3a 06 fd fd fd 02 fd 43 6a fd 4e fd fd 52 fd 6a fd fd 4b 0c fd 76 fd 31 fd 00 fd fd 20 0c fd fd 47 fd fd 19 fd 6b fd 15 0e fd 68 35 00 4b fd fd fd 78 4d fd 2a fd 76 53 11 59 74 1f fd 69 0b fd 08 fd fd 33 fd fd e0 fd 67 fd 63 fd 2b fd 63 fd fd 6e fd fd 10 3b fd 5f fd fd 2f 39 75 24 fd fd 43 fd 74 2a 42 fd fd 79 55 7c fd fd fd 4a fd fd 00 fd 1f fd 48 fd 29 fd 0a 17 fd fd fd fd 02 7b fd fd 59 fd 76 fd 35 2b 51 fd 77 fd 07 fd fd 1d 1a 0d 64 5b 09 fd fd fd fd 7c fd 09 55 24	@@|?YZfJG2bGj|-/'>?"y^+iQv:CjNRjKv1Gkh5KxM*vSYti3gc+cn;_9u$Ct*ByU\|JH){Yv5+Qwd[\|$	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	5	1021	73 58 fd fd fd 56 16 59 36 1d 16 fd 3c fd fd fd 2a 67 07 fd fd 5c fd 0a fd 6f fd 56 fd fd 0e fd 49 61 4d 55 4d 21 fd fd e5 fd 27 fd fd 02 50 79 55 67 4b 51 3d fd fd fd fd 14 30 60 fd 7f 50 fd 4b 6f 63 59 59 fd 15 fd fd 40 fd fd 3b 6a fd fd 4e 47 fd 30 56 fd 59 fd 4d 4e 3d fd 4c fd 12 79 fd 16 1b fd 2f fd 72 fd 35 fd cf 06 fd fd 32 09 76 fd 31 fd 37 fd fd 76 33 0b 22 fd fd 08 41 21 fd fd 1c fd fd 74 1e 74 06 52 04 74 fd 25 46 2a 7a fd 03 fd fd fd 16 fd 50 63 fd 7b 57 fd 39 fd fd 5d 33 5d 61 1e 6b 5d 4d fd 57 fd fd 48 31 53 2a 7e 76 fd 59 01 47 63 fd 7d 4a 4b 58 20 35 53 fd 5a fd 42 fd fd 03 fd fd fd 71 fd fd fd fd 47 38 78 fd fd 18 22 09 35 fd fd de 5a fd 68 fd fd fd 2a fd 6c 44 66 fd fd fd fd 50 fd fd fd 4f 05	sXVY6<*g\oVIaMUM!'PyUgKQ=0`PKocYY@;jNG0VYMN=Ly/r52v17v3"A!ttRt%F*zPcW9]3ak]MWH1S*~vYGc}JKX5SZBqG8x"5Zh*IDfP	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	1026	256	06 fd 26 3f 02 55 fd 49 fd fd 1d fd fd 2d 77 37 fd fd 5d 3f fd 17 fd 4e 74 fd 5d 5d 70 fd 62 fd fd 3e 58 fd fd 0a fd 33 fd fd 50 0e 29 23 fd fd fd 59 fd 6a 43 fd 7e fd fd 59 43 6b 3d 4b fd 2c 26 fd fd 21 fd 6b 20 fd 42 fd fd 76 fd fd 33 22 21 3f fd 6b 1a 0b fd fd fd 48 11 6b fd 12 2b 38 1a 49 18 fd fd fd da 4e 42 76 fd 5c 32 fd 47 fd fd 65 fd 1b 1c 06 73 0b 27 fd 77 fd 6e 05 fd 1f 3c fd 5b 78 77 64 23 48 fd fd e4 fd fd 3d 29 fd 5c fd 3e 4f fd 56 6a 63 50 44 fd 14 fd fd 60 77 73 10 32 72 fd 72 fd 5a fd 31 fd fd 03 fd fd fd fd 01 fd 2e fd 4e 10 11 2f 72 0f fd fd fd fd fd 6b 14 23 fd fd fd fd 56 53 fd fd fd fd 45 fd fd 4a fd 23 fd fd 74 62 fd fd fd fd fd fd 36 fd fd 34 06 fd f4 2a fd fd 1a fd 66 49 fd fd fd fd 70 3f fd fd 03	&?UI-w7]?Nt]]pb>X3P)#jC~YCk=K&!k Bv3"!?kHk+8INBv\2Ges'wn<[xwd#H=)\>OVjcPD`wsrrZ1.N/rkVSEJ#tb64*flp?	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	5	1021	fd 79 51 fd fd 18 fd fd 0f 38 fd fd fd 41 8a 03 fd 69 52 11 fd fd 41 3f 47 fd fd 53 fd fd 6f 35 fd 3c 1d 65 49 fd fd 10 33 7c fd fd fd 16 fd fd fd 7a 3e 65 fd fd 1e fd 1c 23 2d fd 2c 26 1b 61 fd 74 c3 36 fd fd 6d fd fd 54 fd fd fd 1e fd 0b 78 39 50 3c fd 76 fd 75 50 fd fd fd 7a fd 12 fd 4d 16 fd 3d 6d 30 fd 75 02 fd 4e fd 69 3a 03 fd fd fd fd fd fd fd fd 6f fd 0c fd 3f fd 43 fd 82 70 fd 13 5b fd 53 fd 23 fd 26 fd 01 fd 2e fd fd 21 3c 36 fd 09 fd d5 fd 28 52 fd fd fd fd fd 4f fd 6c fd fd 1f 3f 4e 32 5c 0c fd fd fd fd 12 1e 11 47 fd fd fd 20 1d fd 37 fd 7c 10 0c fd 4c fd fd fd 6f fd a8 fd fd fd 73 fd fd 4a fd 02 3a 55 fd fd 06 45 fd 6e fd 5c fd 69 78 fd fd fd fd fd 60 fd 7b fd 17 03 fd 40 fd 09 fd 52 fd 51 fd 4b fd	yQ8AiRA? GSo5<el3|z>e#- ,&at6mTx 9P<vuzM=m0uNi:o? Cp[S#&.!<6(ROl?N2\G 7|LosJ:UEn\ix`{@RQK	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1026	256	fd 02 54 18 23 59 1d fd 58 21 40 fd 02 4a fd 22 89 6c fd 26 45 fd fd 15 fd fd 31 fd 4a fd fd 14 fd 21 fd 45 fd 1b fd 12 51 02 fd fd 17 fd 1d 10 fd 5e 31 fd 43 45 4a 5f 37 fd fd 5d fd fd 20 20 4f fd fd fd 7a 45 18 62 47 fd 7f fd 51 2e 7e fd fd 19 fd 20 73 fd 71 fd fd 3f 2b 3e fd 78 1d 55 26 fd 30 43 7d fd fd 42 fd fd fd 2e 01 6c fd 62 fd fd 1d f4 d9 44 2c fd fd fd 3b fd fd 49 fd 6f fd 6f 64 75 67 62 fd 45 fd 15 36 24 11 fd 10 fd fd 46 7b 3d cc 61 51 77 fd fd 15 fd fd 4d 5b 23 fd 10 3d fd fd fd fd 50 63 fd fd 5e fd fd 2c 04 fa 40 72 fd 39 fd 41 fd fd 53 01 41 08 48 fd 43 fd 5a fd 4d 12 fd 4e fd 24 5c fd 07 fd 64 4c 28 fd fd fd fd bc 6a fd fd 51 6c fd 48 fd fd fd 4e fd 02 58 fd fd fd 5c 6f 3f fd 5f fd	T#YX!@J"l&E1!Q^1CEJ_7] OzEbGQ. sq? +>xU&0C}B.lb,;loodugbE6$F {=aQwM[#=Pc^,@r9ASA HCZMN$\dL(jQlHNX\o?_	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	5	1021	fd fd c5 3f 70 4b fd 5f fd 7e fd 05 7f 4c 6f fd fd 48 fd 2d fd fd 07 fd fd fd 70 55 6d 4c 0c 02 7f 55 7d 31 34 02 1b 20 fd fd 28 2c fd fd 3c fd 4a fd 2d fd 12 fd fd 4f 4c fd fd fd a6 51 2f 4e f3 7a fd fd fd 50 fd 21 fd fd fd fd 01 fa fd 03 fd fd 45 fd 75 53 fd 5b fd fd 11 70 fd 2b 08 08 fd 08 fd 60 21 fd 1b 68 48 91 0c 58 fd fd 1d 29 1b fd fd 72 fd 50 63 fd 46 fd 25 fd fd 08 fd fd 09 fd fd fd 3d 45 11 6d 5d 05 fd d2 2d 5a fd fd fd 18 2c fd fd fd 67 02 fd fd fd fd fd fd fd 30 2f 70 fd 1f 60 fd fd fd 25 fd fd 71 34 30 fd fd ab fd 2d fd 25 76 58 3f fd 57 fd fd a3 fd b8 fd fd fd fd 79 fd fd fd 4f 41 5f fd 5c fd 4b fd 17 fd 3f 1f fd fd 2a fd 7b fd 5c fd 37 f6 fd 1d fd fd fd fd 3c 18 5e 02 25 fd fd 7a 09	?pK_~LoH-pUmLU}14 ,<-OLQ/NzP!E uS[p+`!hHX)rPcF%=Em]-Z,g0/p`%q40-%vX? WyOA_\K?*{\7<^%z	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	1026	256	fd fd 24 75 22 fd 31 fd fd 74 fd 60 fd 7d fd 4d 19 fd 77 fd 2c fd fd 41 4a 4d fd fd 0e fd 62 0b fd 68 0a fd 74 fd 71 fd 0c 29 42 7c fd 0b 37 0f fd 25 fd 08 1f fd 3c 24 fd fd 7c fd 80 3c 09 00 22 fd 3e fd 42 10 fd 3e 3f 27 22 fd 69 fd 5b 4d 0e fd fd 68 fd 10 fd 56 35 21 fd 05 18 3d fd fd 13 fd 31 20 55 fd 68 fd fd 5c fd fd 38 78 19 53 fd 2b fd 03 69 fd fd fd 6a 66 fd 66 50 4c 6b fd fd 55 62 fd 08 fd 1c fd fd fd fd 2f fd 07 46 64 2b fd 4a 20 7d 73 0d fd fd 5a fd fd 20 0b 34 4d 7a fd fd 03 4d fd 58 07 fd 75 fd fd 79 fd 24 a1 13 fd 24 48 fd fd fd fd fd 28 70 fd 12 fd 3c 31 14 fd fd 2f 47 31 64 fd 7f fd 09 50 fd fd 0f 4e 5f 31 fd 6e fd 0d fd fd fd fd 36 6b fd 64 fd 33 66 fd fd 26 bc 64 3f fd fd 4e fd 3a 7c fd 07 6d 00 54 df 08 6a	$u"1t`}Mw,AJMbhtq)B\|% <$|<">B>?'"i[MhV5!=1 Uh\8xS+ijffPLkUb/Fd+J }sZ 4MzMXuy$$H(p<1/G1dP N_1n6kd3f&d?N:|mTj	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	5	1021	fd 25 fd fd 4e 1b 3a 59 fd 51 44 39 fd 07 21 fd 7c fd 8f fd 12 2e fd fd 6e 42 fd 5e 15 fd 7e 27 76 28 90 18 fd fd 5e 09 33 fd fd 55 fd fd 73 fd fd 79 fd 4a fd fd fd 2c fd fd 29 fd 05 74 fd 3e 47 5e 34 1a 1d fd 46 fd fd 7e fd 35 43 7c fd 63 6d 16 fd fd fd fd fd 75 fd 5b 2e 23 fd fd fd 3f fd 10 fd 0e fd fd fd fd 28 fd fd fd 77 fd fd fd 63 5b 2d fd 4c fd 45 cd fd fd 73 fd fd 7b 1e fd 09 fd fd fd fd 5b 56 fd 25 fd 67 2c 06 02 fd 37 fd 5d fd 5f fd 02 fd 0e fd 3f 67 3d 7b 4b 1c fd 0b fd fd fd 64 30 fd fd fd 7f fd 72 77 72 fd 0b 4f fd fd 7c 78 fd 49 fd 2a 34 39 10 08 fd fd 37 5b fd fd 56 fd 48 16 fd 59 fd 17 fd 55 fd fd 07 80 fd fd fd 5a 77 59 6d 7d 32 1a fd 24 39 3e 54 38 14 fd 49 7d 33 53 4f fd 22 fd fd 00 6e 22 fd 2f fd fd 4f fd	%N:YQD9!|.nB^~'v(^3UsyJ,)t>G^4F~5C|cmu[.#?(wc[-LEs{[V%g,7]_?g={Kd0rwrO|xl*497[VHYUZwYm}2$9>T8I}3SO"n"/O	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	1026	256	59 59 fd 67 fd 1c 3a 30 fd 3d fd fd fd fd fd 61 fd 18 31 7e fd 5e fd 71 fd fd fd fd 4a 39 fd 7c 18 45 fd 64 1d fd fd 6d fd fd fd 6c fd 18 52 47 fd 05 fd fd 43 32 fd 81 fd fd fd 5d 7f 3e fd fd 4b 3e fd fd fd 05 6b 7f 29 fd 64 4c 6b fd 6f fd fd fd 4f fd 5e fd fd 63 63 fd fd 3c fd fd fd fd 54 fd 66 fd 28 fd 5c fd 41 71 05 fd 03 44 3e fd fd 42 fd 1b 5a 42 03 3b fd 13 27 06 7a 31 27 fd fd fd 2e fd 46 fd fd 42 3c 4f fd 47 1f 2e 7e 0b fd fd 25 fd 45 12 2f fd 5b 01 fd fd 0b fd fd 43 08 4b 13 fd 0c fd 51 fd 6f fd fd fd 08 13 7a fd fd fd 64 0e 75 37 73 0a fd 74 26 43 01 fd fd fd fd 57 fd 1b 33 39 37 fd 17 fd 6b 5f fd 3c fd fd 57 fd fd fd 3a fd 06 5f fd fd 39 fd a8 60 fd 53 6f 60 5d 24 68 fd 3d 69 98 78 17 11 fd 5f fd fd fd 09 03 fd 68 fd	YYg:0=a1~^qJ9|EdmlRGC2]>K>k)dLko^cc<Tf(\AqD>BZB;'z1'.FB<OG.~%E/[CKQozdu7st&CW397k_<W:_9`So`]$h=ix_	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	5	1021	68 93 03 fd 1f fd fd fd fd fd 6e 63 fd fd fd 3c fd 3d fd fd fd fd 14 17 60 fd 47 55 55 49 fd fd 0a fd 49 68 55 ff 74 25 3d 53 fd fd 16 fd fd fd 68 fd fd fd fd 7d 0a 78 fd 1b 42 fd 4d fd fd fd 13 fd 26 fd fd fd fd 4c 4c 7b 54 fd fd fd fd 68 5e 0e fd fd 55 0b fd fd fd fd 5d fd 30 55 fd 68 2c 6e fd fd 6f 20 fd 60 67 fd 1e fd fd fd fd fd fd fd fd 10 fd fd 1a 77 fd 58 fd fd 11 fd 37 4a 68 4a 73 1c 20 6b 5d 0e 59 fd 0e fd 4e 3a 74 71 34 fd 23 27 fd fd fd 41 fd 6f fd fd 15 fd 50 fd 70 1c fd fd 21 49 26 0a 39 fd fd 77 fd 07 0f 08 6d fd fd fd fd fd 5a 7c fd 04 46 fd fd 14 38 23 fd fd fd 94 fd 38 1a fd fd 68 fd 1e fd fd fd 52 3e 52 fd fd 26 fd 32 18 fd fd 43 fd 43 52 59 fd fd 17 fd 1d 0c 01 31 fd fd 5b 5f fd 1b fd fd 45 fd 25 7b	hnc<=`GUUIIhUt%=Sh}xBM&LL{Th^U]0Uh,no `gwX7JhJs k]Y:q4#'AoPp !l&9wmZ|F8#8hR>R&2CCRY1[_E%{	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	1026	256	65 76 11 fd 5f fd fd 12 26 11 79 fd 20 1a 30 5d 16 fd 1f 7d fd 11 fd fd fd 6a fd fd 1c 14 fd 14 60 6b 7b fd fd 1f fd fd 51 fd 50 54 fd 24 fd 3b fd 43 1b fd fd 65 fd fd 5d fd 0a 47 1f 0c 61 46 74 18 fd 61 fd 3e fd fd fd 2a 5a fd 58 4e fd 18 fd fd fd 35 fd fd 69 fd fd 3e fd fd fd 2e 00 fd 24 fd 5d 00 1b fd 5e fd 10 fd fd 12 fd 75 16 fd fd 16 fd 21 02 fd fd 46 fd fd fd 77 fd fd 1a fd fd 62 fd fd 3c fd fd 5a 2d fd fd 4e fd fd fd 46 77 fd 48 2d 33 fd fd 34 54 25 fd 59 4c 26 77 26 33 fd 45 fd 1b fd 78 7a 7a 57 61 fd 7b 75 fd 63 32 fd fd 6f 75 fd fd 03 79 4b fd fd 67 fd 73 97 fd 67 3f 3c 71 fd fd 00 19 fd fd fd 17 fd fd 39 fd fd 61 fd fd 70 fd 0e fd 45 fd 5b fd fd fd fd fd fd 54 53 73 fd 51 4a 62 fd 31 fd fd fd fd fd 7e 6f 66	ev_&y 0]}j`k{QPT$;Ce]GFta>*ZXN5i>.$]^u!Fwb<Z-NFwH-34T%YL&w3E xzzWa{uc2ouyKgsg? <q9ap[TSsQJb1~f	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	5	1021	01 2f fd 45 7f fd fd 4b fd fd 65 28 fd fd fd ad 22 39 fd fd 45 20 7b fd 0b fd fd 60 23 0e fd 23 32 fd 61 62 fd 62 2a 24 fd 51 2b 4f fd fd fd 54 fd fd 37 6e fd fd fd 02 fd 51 37 63 fd 15 03 2f 0a 55 fd fd 78 6e fd fd 6f 73 3c 32 fd 06 37 fd fd 55 7f fd 2f 24 74 fd 56 fd fd 13 71 18 fd fd 2f 17 76 fd 65 5e 2f 69 fd fd fd 78 37 fd 4e fd fd 3d fd 63 5f 43 59 48 4e fd 2b 53 fd 41 7d 79 7d fd 25 fd 7c fd fd 65 0f fd 76 4d 39 fd fd 2f 0e fd 01 fd fd fd 78 57 fd fd 7c fd fd a7 36 fd fd 2a 7c fd fd fd 0c fd 7e 21 fd 20 fd 45 7a fd fd 0a fd fd 6b 76 25 7d 35 61 a7 fd fd fd 6c 0e 25 fd 1c 5f 39 64 fd 28 fd fd 05 2d 44 01 11 6e 24 fd 0c fd fd fd 32 fd fd fd 3b fd 66 fd 52 55 fd 78 fd fd 00 70 4c 54 fd fd fd fd fd 49 77 68 fd 43 14	/EKe("9E {`##2abb*$Q+OT7nQ7c/U xnos<27U/$tVq/ve^/ix7N =c_CYHN+ SA}y}%ev9/xW|6*|~! Ezkv%}5al%_9d(-Dn$2;fRUxpLTlwhC	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	1026	256	fd 63 fd fd 7f fd fd fd fd 6b fd fd 4f 20 3b 53 fd fd 6a 0b fd fd 42 fd fd fd 2f fd fd 61 47 fd 21 7d fd fd 07 fd fd fd 7c fd 5c 48 2c 36 fd fd 15 6d fd 73 fd 37 fd fd 73 2c fd fd fd fd 77 fd 64 fd 0f 38 5f fd fd 4f fd 33 50 fd fd 3f fd fd 2e fd fd 64 4d fd fd fd fd fd fd fd 46 fd 18 fd 2e 3e 29 bf 5d fd 65 7c 2b fd 61 0d 6c 68 10 f8 37 2f fd 57 64 fd 6d fd 3f 4a fd 03 3a fd 5e fd 6d fd fd fd fd 4b 4d 7e 6a 3d 73 7b fd 06 fd 7d 17 fd fd 50 2e 68 21 fd 76 1d fd fd 21 2e fd 10 fd fd fd fd fd 3d 7d fd fd fd 19 fd 24 fd fd fd 59 fd 36 6b 53 fd 1b 04 fd 38 fd fd 72 4c 78 fd 29 1f fd 04 fd 1e 1b fd 0b fd fd 4f fd fd fd 14 14 1f fd 4d fd fd 56 fd fd 52 fd fd 69 37 fd 53 40 fd 64 fd 6f 6d fd fd 2d 05 fd fd 79 16 fd 2a 2e 46 7d fd 0c fd fd	ckO ;SjB/aG!}|\H6ms7s,d8_3P ?.dMF.>)]e|+alh7/Wdm? J:^mKM~j=s{} P.h!v!.}$Y6kS8rLx)OMVR i7S@dom-y*.F}	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	5	1021	fd 21 fd fd fd 71 4c fd fd 69 fd 58 7e 3e fd 6c 33 76 fd fd fd fd 27 fd fd 10 2d fd 2b 2d 1d fd fd 6f fd 06 fd fd 33 54 64 fd fd fd 31 48 1c fd fd fd fd 6b 2b 06 15 5f fd 2e fd 7c fd 30 5c fd fd 0b fd fd fd fd fd fd e1 13 fd 1d 12 1e 41 fd 24 02 1b fd fd fd fd 32 fd 1d fd 54 1e fd 5d fd 6c 23 fd 65 47 fd 28 7a fd fd 7b fd 33 fd fd fd 34 44 26 04 fd 3b 72 fd fd 3b 06 fd 49 c7 2c fd fd fd 30 fd 2a 34 fd 38 fd fd 6f 2e 29 fd 18 5f fd fd 0e 2b fd 17 70 fd 55 fd 86 fd fd fd fd 30 fd fd fd 67 fd 77 fd fd fd fd 05 8c fd fd 18 fd fd 59 fd 78 75 fd 0c fd 7f 58 fd fd fd 40 59 4b 6b 4c 1d fd 69 fd 0e fd fd 3b fd 6a 6c bc 23 37 fd 66 28 28 fd fd 9c 33 fd 27 5f fd fd 04 fd bf 4d 7d fd 00 22 fd fd 55 fd fd 7e 2f fd fd	!qLiX~>l3v'-+-o3Td1Hk+_.|0\A$2 T]l#eG(z{34D&;r;l,0*48o.)_+pU0 gwxuX@YKkLi;jl#7f((3'_M}U~/	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	1026	256	fd fd 2b fd 45 fd 35 4d fd fd 0c 6d fd 75 2d 42 3c 7e 7e ae 59 fd fd 36 fd fd 6c 71 fd 47 fd 3e fd 73 fd 55 69 61 fd 54 13 fd 3b 2d fd 57 1b fd fd 23 4e fd fd fd fd fd 63 48 fd fd 55 78 fd 64 fd fd 38 5d 21 fd fd 35 fd 69 45 fd 7e 7f 7e fd 5d 37 0e 65 6c 22 fd fd 03 fd fd fd 72 fd 7f fd 59 33 fd fd fd 78 6a bd b9 11 1d 18 41 19 5d fd fd 0f fd fd fd fd fd 5d fd fd 28 53 1f e8 0f fd fd 20 fd 4c 25 25 fd 49 21 10 78 fd 59 49 fd fd 76 20 fd 57 7a fd 45 1f fd 59 08 7b fd fd 24 4b 56 64 4e 5e 35 28 fd 18 fd fd fd fd d5 5c 0e fd 7c fd 06 fd fd 69 fd 58 2a fd 3b 2c fd 15 72 fd 79 fd fd fd 02 fd 69 fd fd fd 7b 17 fd fd 17 0c 6c fd fd 18 44 fd 5c 6e 78 fd fd 0d fd 19 fd 50 6a fd 7f 71 18 38 fd 5b 0f fd 2d 3d fd fd fd 3c 2e 6f f6	+E5Mmu-B<~~Y6lqG>sUiaT-W#NcHUx d8]!5iE~~]7el"rY3xjA]](SL%%lxYIv WzEY{$KVd^5(\\iX*;,ryi{lD\nxPjq8[-=<.o	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	5	1021	06 0c 0f fd fd 21 fd fd 4b 08 66 fd 33 fd fd fd 46 fd fd fd 63 fd 53 fd 20 fd 31 61 fd 06 fd 0b 78 fd 5c 04 f9 fd 0e fd 01 32 fd 73 31 fd 40 fd fd 61 fd 65 fd fd 00 59 28 7b 22 fd 43 fd 7e 04 fd 28 42 71 fd fd 24 fd fd fd 37 fd fd 4f fd fd fd fd fd 30 7e 05 35 75 5e 01 5d 21 57 16 11 11 fd 2e 7e 3b 38 30 6c 23 97 0d 25 58 fd fd 19 fd 28 fd 7e 0c 18 fd 10 fd 2e fd fd 2a fd 20 37 fd fd fd 74 fd 63 0b 7e 17 fd 60 35 76 56 fd 12 54 fd 60 fd 60 fd 6b 51 fd 1d 7b 69 3a 57 fd 12 7a 4a 1a fd fd fd 0b 25 2e fd 30 31 7b 4e 61 1e 45 fd fd 3a fd fd 45 fd fd 75 fd 5c 1d 57 02 fd 5e fd fd 6f 32 76 fd 78 5b fd 5e 0a 73 fd fd 60 fd 5b fd fd fd 12 25 fd 02 22 fd fd 21 3b fd fd fd 5c fd fd 2a fd 0c 3e 1a fd fd fd 25 fd 34 fd fd 40 fd fd fd	!Kf3FcS 1ax\2s1@aeY({"C~ (Bq$7O 0~5u^]!.~;0l#%X(~.* 7tc~`5vVT` `kQ{i:zJ%.01{NaE:Eu\W^ o2vx[^s`[%"!;*>%4@	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	1026	256	fd 47 fd 4b fd fd 1a 25 fd 02 51 41 fd 58 fd 77 fd 75 52 fd 46 49 fd 6b fd 14 fd fd 7c fd 3e fd 67 0f fd fd fd 29 fd 33 fd 0a fd fd fd 3c 4d 2c 22 fd 31 68 fd 36 57 0e fd 5c 77 fd 18 20 73 5a 1c fd 4d 5f 49 fd 69 29 fd 5e 1a fd 3f 72 fd fd 03 fd 3b fd 79 77 46 0c fd 0a 4b 65 fd 77 7d 02 fd fd fd 78 e6 fd fd fd 4d 2f 01 fd 3b fd 40 5c 3a fd 21 fd 5a fd 6d fd 16 15 01 fd fd fd 08 fd 07 fd 5e fd fd 36 fd fd 35 1b 6d fd 2e fd 37 fd fd 48 fd 0f fd 33 31 6f fd 3d 4c fd 06 0b fd fd fd 28 fd fd 52 33 fd 45 fd 61 0c 08 fd fd 3d fd 0e ba 05 55 fd fd 55 1c 72 4e 1c 19 fd fd 46 fd fd fd fd fd fd fd 4e 31 02 2e fd fd fd 77 4e fd 2b 67 0a 74 67 69 fd 6d fd fd fd fd 32 16 fd 92 fd 71 38 28 fd fd 5a fd fd 6b 7f 55 44 5b fd 08 4a fd	GK%QAXwuRFIk|>g)3< M,"1h6W\w sM_Ii)^? r;ywFKew}xM/;@\:!Zm^6 5m. 7H31o=L(R3Ea=UUrNFN 1.wN+tgim2q8(ZkUD[	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	5	1021	65 43 4f fd 2a fd 4d 79 fd 2a 5c fd fd fd 32 fd fd fd 27 fd fd 54 5a 52 4b 4f fd fd fd 73 18 fd 43 fd fd 76 fd 74 6a 6b fd fd 37 fd d2 08 fd fd 07 fd 28 2b fd 2c fd 6f 5e fd fd fd fd 47 fd fd fd 57 03 fd fd fd 74 fd 13 64 fd fd fd 13 fd 56 fd 3b fd 42 fd 6d 63 fd fd fd 48 4f 5c 57 fd fd fd fd 77 41 a8 58 7e fd fd 78 fd 78 1b fd fd fd fd 74 38 2e 7a 30 fd 41 53 fd fd 55 21 fd 1f fd fd 2e 7e 0e fd fd 31 12 76 54 fd fd eb 12 fd 4c fd 76 fd 16 04 fd 3b fd fd fd 41 21 a3 fd fd 6f fd fd 63 0d 03 4b 0e fd 4e fd 39 14 7c 5a fd fd 5b fd 1e e2 fd fd 1e 5a 55 fd 0d fd 60 fd 0b e4 fd 5f 40 2f fd 49 fd 23 4b 2d 2b fd 74 7a 67 55 fd fd 42 fd fd 2d 53 fd 4c 3b fd 1e fd 18 4a fd 7e 68 59 fd 0b 79 fd 43 11 fd fd 52 fd 0b fd 49 fd fd	eC*My*\2'ZRKOsCvtjk7(+,o^GWtdV ;BmcHO\WwAX~xxt8.z0 ASU!.~1vTLv;A!ocK9| [ZU`_@/l#K-+tzgUB-SL;J ~hYyCRI	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	1026	256	fd fd 6c fd 19 45 fd 63 11 7b 5b fd 47 fd 19 fd 1a 6d 31 72 fd 30 fd 05 0c fd 7c fd fd 53 fd fd 47 fd fd 2e fd 61 02 fd fd 12 fd fd 3d 4f fd fd fd 0e fd fd fd fd fd fd 67 fd fd 7d 7f 33 5c fd fd 4c 2f fd fd fd 63 34 12 fd fd 53 1a fd fd 5b 5b fd 49 fd 50 fd fd 61 38 fd fd 44 28 fd fd fd 49 fd fd 5c fd 3b 29 fd fd fd 40 06 fd fd 45 fd fd fd fd fd 1f 23 fd 76 4a fd 3e 0a fd fd 6c fd 5f 34 fd 4a 4f fd 61 13 fd fd 13 fd fd 5e fd 62 32 6e fd 49 0d 49 57 0f 2f 1a 4d 3c fd 66 fd fd fd 56 39 2c fd 49 fd 54 4a fd 72 33 6e fd 0c fd 51 40 fd 1f 16 fd fd 4c 53 fd fd fd fd fd fd 73 fd fd 42 0a 53 fd 03 fd fd 5c fd 31 34 fd 29 42 2a 5d 4c 03 4a 14 fd fd fd 79 38 9a fd fd 4c 6e 1d 38 fd fd fd fd 54 fd fd 0b fd fd 7d fd fd 20 45 fd 34 fd 6a fd fd	lEc{[Gm1r0|SG.a=Og}3\L /c4S[[IP a8D(I\;)@E#vJ>I_4JOa^b 2nIIW/M< fV9,ITJr3nQ@LSsBS\14) B*]LJy8Ln8T} E4j	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	5	1021	fd fd fd c9 fd 54 fd 6b fd fd 6f 29 64 fd fd 4b fd fd 64 fd fd 2a fd fd fd fd 1a fd 35 57 50 49 fd fd fd fd cc 32 1e 47 fd 0f fd 0f fd 12 fd fd 4c fd b8 30 6c fd fd 18 fd 30 09 3a 2d fd 0c fd fd fd fd 5c fd fd 11 fd a0 fd fd fd 10 fd fd 62 30 7e 73 47 fd 0a 08 31 70 fd 5e fd 3e fd fd fd 5a 36 fd fd 0d fd fd 4c fd 12 0b fd fd fd 4a 74 61 2e 06 22 fd 63 64 2c 51 d0 fd 33 71 16 fd 7e 13 7e fd 36 1c fd 41 fd 3d 68 fd 77 62 fd 21 5e 04 fd fd 66 10 2e fd fd fd 40 33 fd fd fd 5f 5c fd 3d fd 3e 08 54 fd 4b 73 68 fd fd fd 1b 78 16 19 fd fd 68 fd fd fd 68 fd 69 09 6b 21 72 fd 73 75 fd 78 fd 39 fd fd 22 54 74 fd 19 14 07 fd 12 fd 27 73 07 fd 1f 67 fd 16 28 fd fd fd fd 3c fd 22 fd fd 0f fd 24 39 7b fd fd 00 fd fd fd	Tko)dKd*5WPI2GL0l0:-\b0~sG1p^>Z6Lta."cd,Q3q~~6A=hwb!^f.@3_\=>TKshxhhik!rsux9"Tt'sg(<"$9{	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	1026	256	fd fd fd 68 68 40 fd fd 53 5c fd 4e 46 43 09 fd 5f fd 29 5d fd 2b fd fd fd 55 c5 fd d5 55 39 fd 7e 45 43 fd 0f fd fd 52 50 fd 1f fb fd 4d 18 1c fd 43 fd fd fd fd fd 42 fd fd 74 fd 56 5c fd 59 fd 1c fd 43 1c 50 4d d2 08 28 fd 40 62 fd 3b fd 63 fd 5d 88 fd fd 21 5d fd 7f fd 74 40 67 61 fd 46 fd fd 53 fa 7a fd 2d fd fd 41 fd fd 20 fd fd fd 4c fd 34 23 56 fd 06 3b fd 1a 28 4f 6d 5a 49 fd fd fd 07 19 fd fd fd fd fd 24 38 fd fd fd 6f fd 01 fd 1a 62 53 06 70 fd 6e fd 4e fd 5b 41 fd fd 14 fd 49 fd fd fd fd fd 25 fd 15 74 fd 25 fd 01 fd fd 73 43 fd 61 fd 03 fd 5b fd fd fd 12 fd fd fd fd 05 25 6f fd fd fd 05 fd 0c fd 24 58 61 fd fd 77 68 fd fd 42 fd fd 20 fd fd fd 6e 14 45 fd fd 3b 45 66 4f 3f fd fd 6d 03 14 fd 8b 40	hh@S\NFC_)]+UU9~ECRPCBtV\YCPM(@b;c]!]t@gFSz-A L4#V;(OmZI$8ob SpnN[AI%t%sCa[%$XawhB nE;EfO?m@	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	5	1021	61 fd fd fd 0a fd 26 fd 2d fd fd 78 fd 69 3a fd 00 48 fd fd 29 00 65 fd 43 0f 27 fd 24 46 fd fd 68 48 79 fd fd 60 fd 59 fd fd fd 37 30 7a 03 19 6d fd 7d fd 01 fd 0e 4e fd 4c fd fd 2c 2a 3f 2b 01 fd fd 35 6a fd 01 0b 25 fd fd 10 fd fd fd 40 fd 7f 14 4b fd fd fd 24 62 fd 44 5a fd fd 04 fd 02 3f 14 fd 2d fd fd 40 fd fd fd fd fd fd fd 1f 3b fd fd fd 31 fd fd 61 fd 62 fd 31 fd 62 fd 71 fd fd db f2 30 58 54 44 31 0f fd 4c 53 40 fd 76 75 69 fd 57 fd fd fd fd 2b 09 58 fd fd 6c 09 fd 78 21 fd 3d 52 fd fd fd f5 3f fd 07 6e fd 14 2c fd fd fd fd fd 75 fd 7b 51 fd 69 fd fd fd 0f 46 fd fd fd 74 fd 12 fd 0d fd fd 13 3c fd 56 2b fd 23 fd fd 66 fd fd 57 fd fd 11 fd fd fd 1c 29 4e 5b 4b ab fd fd 8c 70 75 65 fd fd 4b 2e 76 fd fd 51 04 3e	a&- xi:H)eC'$FhHy`Y70zm}NL ,*?+5j%@K$bDZ?- @;1ab1bq0XTD1LS@ui W+Xlx!=R? n,u{QiFt<V+#fW)N[Kpue K.vQ>	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	1026	256	fd 7e 28 fd fd fd 22 fd fd 5b 2c 5b 69 05 66 fd fd 45 fd fd fd 6c fd fd 6f 54 fd 65 44 fd 25 37 fd 65 6a 1d fd fd fd 5b fd a8 52 09 fd 07 fd 2d 0c fd fd 5e fd fd 50 fd fd 25 fd 16 3a 17 3e fd fd 00 23 5f fd 2b 24 fd e3 fd fd 71 45 7f 5b 70 fd 62 6a fd 2d 24 fd 33 58 fd 46 83 fd fd 70 fd 53 fd 7e 7e 33 fd fd 49 fd fd fd 10 fd 51 fd 3f 08 7a fd fd fd fd 24 34 39 fd fd 08 fd 70 1f fd fd 3a 5c 15 fd 1f 6e 5b 3a fd fd 44 23 0c fd fd 5f 39 73 51 fd 01 f5 fd 40 fd 7c c8 7a fd 66 fd fd 15 fd 18 fd fd 3d fd fd 59 fd 0f fd fd fd 31 fd 5c fd 65 fd 47 fd c4 fd fd 1f 53 24 fd 3e fd fd 3e fd fd 58 74 7c fd fd 1c 08 fd 27 fd fd fd 1b fd fd fd 60 75 55 6e fd 05 fd 43 6f fd b0 fd 27 fd 3a 46 61 49 fd 51 03 fd	~("[,[iEloTeD%7ej[R- ^P%:>#+$qE[pbj- $3XFpS~~3lQ? z$49p:\n[:D#_ 9sQ@\|zf=Y1eG$>>Xt|`u UnCo':FaIQ	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	5	1021	fd 6c fd fd fd fd fd fd fd fd 57 fd 27 fd 17 15 fd 76 76 fd 23 fd 15 0f fd 43 fd 04 47 00 fd 57 fd 26 5b 46 5f 56 19 fd 29 87 2b fd 2e fd fd 58 fd 02 3f 08 78 48 1d 47 55 fd fd fd fd fd 5f 38 71 74 fd 4d fd fd fd 2c 57 52 fd fd fd 06 fd 22 fd fb fd 37 fd 0d fd fd 06 fd 0e e8 4e 11 1e fd 4f fd 3b 03 fd 2d 50 fd 5a 5d fd 32 6f fd 0c fd fd 34 5f fd fd 17 fd 0d fd fd 72 fd 4b fd 58 1b 54 fd fd 2f 23 fd 14 fd fd fd 0f 67 28 62 5c fd fd 79 fd 3e fd 36 2d fd 6a 48 97 fd 52 44 fd 23 fd 25 fd 31 fd fd fd 77 fd 55 fd 00 fd fd 6b fd 6b 69 fd 21 72 fd 51 fd fd fd 49 3d 04 45 fd 5d fd fd fd 14 1a fd 32 32 0b 79 fd fd 38 6e fd fd 73 fd 40 50 29 fd fd 60 6e 05 fd fd 00 66 fd fd fd 31 21 48 31 fd 1f 0f 3b fd 48 fd 3b 11 fd	lW'vv#CGW&[F_V)+.X?xHGU_8qtM,WR"NO;-PZ]2o4_rKXT/#g(b\y>6-jHRD#%1wUkki!rQl=E]2y8ns@P)`nf1!H1;H;	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	1026	256	fd 3b 38 fd fd 69 7d fd fd 02 30 3f fd 71 43 fd fd fd fc 7e 5a 39 6e fd 29 4a 79 fd fd 5d fd 56 fd fd fd 0c fd 70 fd 67 fd 05 0e 54 fd 39 61 fd fd 57 01 fd fd 69 7e 5a 11 fd fd 47 50 fd 5e fd fd 0e fd fd 21 62 fd 7b fd fd 06 03 06 fd 08 5b 2c 5d fd 12 fd 14 1d 46 fd 19 67 04 29 fd 43 fd fd fd 62 fd fd 05 76 0f 01 5b fd fd 66 30 2e fd 26 fd 59 fd 63 70 fd 56 fd 10 5c fd fd 7f fd 4f 7f 74 32 fd 0b fd 14 fd fd 0a 39 45 fd 67 fd 00 fd 1b fd fd fd 1f 26 7e 3c 2d 95 0f fd 1d fd 2b fd fd 66 7d fd 62 fd 3a fd fd fd 22 1a fd 61 fd fd 01 fd 1e 5e 5b fd 48 67 7e 7c fd fd fd af 10 32 fd fd 36 fd fd 18 fd 1f fd 47 7b 55 fd 07 7a 02 fd 02 29 14 fd fd 73 40 fd 22 22 fd fd 26 fd 36 fd 17 fd 20 41 5d 24 2f fd 56 52 39 fd 40 3f fd fd	;8i}0?q~Z9n)Jy]VpgT9aWi~ZGP^!b{[.]Fg)Cbv[f0.&YcpV\O29g&~<-fb:"a[Hg~|26G{Uz)s@""&6A]$/VR9@?	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	5	1021	fd 44 fd fd fd fd 6e fd fd 02 fd 43 63 fd 24 fd fd 35 fd fd 06 5c 3c 6c 71 fd fd 5b 68 fd 56 fd fd ed fd 76 0d fd fd 59 33 fd 23 fd 48 fd 5b 7d fd fd 69 66 25 fd 2a 1f 4f fd 69 38 b8 27 fd fd fd fd 10 39 21 12 fd 6d 30 fd 2f 1b fd fd 62 fd 23 3c fd fd fd fd 20 fd fd fd fd fd 07 fd fd 4d 7c 68 fd 5e fd 73 4e 79 fd fd 31 1e fd 18 00 fd 63 7d fd 0e fd 4f fd 55 2d 06 fd 75 fd fd 24 fd fd 54 fd e8 fd 41 20 12 79 45 fd 37 fd 23 fd fd 74 fd fd 08 fd fd fd 4f fd fd 3c fd fd 63 10 3a 1e 79 5c fd fd 29 59 fd 4f 35 fd 65 49 53 3d 4d fd fd 53 31 66 20 2a 7f fd fd 2c 40 fd 11 3d 0c fd fd 55 fd 36 fd 7b 31 fd 20 6f 51 47 fd fd 68 55 3e 47 fd 3b fd 1c fd 11 65 fd fd fd fd 6c fd fd fd fd 48 77 fd 8d fd 23 c7 17 65 30 09 ad 28 fd 10 0a fd	DnCc$5\<lq[hVvY3#H[}if%*Oi8'9!m0/b#< M\|h^sNy1c}OU-u$TA yE7#tO<c:y\)YO5eIS=MS1f*,@=U6{1 oQGhU>G;elHw#e0(	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	1026	256	04 48 66 a3 fd 66 64 3e fd be fd fd 20 34 45 fd 5c fd fd 47 67 fd fd fd 2f bf fd 5b 5e 04 49 fd 57 5d 70 3c 4b 32 fd fd 4b 32 1d fd 0f 33 6d 60 2c 7a 63 fd fd 5b 64 41 64 5d 6e 1c fd 2d 4b 38 fd fd 07 75 fd 27 2a fd fd fd fd 0d 1f fd 3a 2a 1c 11 fd fd 1c 60 39 18 7d 2f 3e 74 70 fd 48 fd 7a 06 fd fd fd 7b fd fd 6c fd 26 fd 45 37 11 fd fd 22 fd 0e 67 fd 4e fd 0e 29 39 66 fd fd 09 13 31 55 7e fd 66 17 33 5f fd 50 42 fd fd fd 1f 7a 4e fd 14 5c fd 57 37 10 43 fd fd 10 0a 47 fd fd 1f 69 54 9e 26 71 fd fd 78 00 fd 3d 1d fd fd 38 7f fd 19 fd 2c 45 29 2b fd 04 4d 12 fd 53 28 fd 8d 54 fd 3e 77 fd 2c fd fd 26 63 fd fd 47 08 59 57 36 fd 76 03 32 3e fd fd fd 2e 48 fd 09 2d fd 64 33 fd 6c fd fd 0f fd 4d 0f 6b 15 08 fd 19 fd fd fd	Hffd>4E\Gg/[^IW]p<K223m`,zc[dAd]n-K8*:`9}/>tpz{l&E"gN)9f1U~f3_PBzN\W7CGiT&qx=8,E)+MS(T>w,&cGYW6v2>H-d3lMk	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	5	1021	5f 72 39 fd 4e fd 03 fd 35 66 5a 1d fd 75 3e 1f fd 7b 7b fd 17 fd 74 fd 0f fd fd fd 52 fd fd 75 24 fd fd 76 fd 18 0d 4c fd 73 fd 64 35 58 06 4f 40 fd fd fd fd 06 fd 0a 64 79 53 64 fd 77 fd fd 53 fd 15 25 fd fd fd fd 16 5a 1b fd 46 32 fd 18 78 fd 0c fd fd fd fd 0b 51 fd 04 fd fd 5d fd 70 16 fd 5f 73 fd 79 fd 47 fd fd 58 fd 15 fd fd 7c 46 fd 54 fd fd 6b 33 0a 5f fd 0d fd 12 58 77 46 03 22 fd fd 79 59 51 fd 79 fd 29 4d 4d 65 fd fd 2e fd 2e 50 7e fd 14 54 fd 77 fd 56 1f fd ff 31 66 fd 3a 10 24 fd 4f 48 fd 1b fd 2b 40 0b fd 48 fd 2f 38 06 1c 38 fd 41 71 74 fd 0a 38 47 fd fd 09 fd fd fd 19 12 fd 40 1b fd 08 fd fd 29 fd 7f 4b fd 4f fd 11 76 5a 05 fd 07 67 0e fd fd fd 53 fd 31 4d fd fd 68 62 29 5b 0f 54 36 5a 2e fd 76 fd 49 04 fd	_r9N5fZu>{{Ru$vLsd5XO@dySdwS%Z F2xQ]psyGX\|FTk3_XwF"yYQy)MM..P TwV1f$OH+@H/88Aqt8G@)KOvZgS1Mhb)[T6Z.vI	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	1026	256	fd 6d 74 fd fd 37 7e 1a 3e 23 fd 00 10 fd fd fd fd fd 5c fd 57 6b 79 fd 02 17 fd 11 35 61 58 fd 2b fd 09 2b 17 fd 4f 7d fd 07 fd 7c fd fd 1c fd 65 fd 7d 69 fd fd fd fd fd fd fd fd 16 fd 1c fd fd 31 fd fd 2a 1c 00 34 3e 5b fd fd 4e fd 14 fd 4b fd 6b fd fd 1e 12 58 fd fd 5f fd 7c 0b 0c fd 7d 58 00 37 fd 02 06 57 fd 16 55 fd 72 36 44 fd 6e 71 3e fd fd 03 1b fd fd 45 fd fd fd 1d fd 12 56 fd fd fd 02 fd 07 06 fd fd fd 62 0a 08 fd fd 4a 6b fd 31 0d fd 63 fd fd 4c fd 60 fd 33 2b 6c 48 66 3e fd 66 fd 32 31 fd 4f 06 fd fd fd fd fd 2e 33 fd 12 fd 1e c0 05 56 fd 6d fd fd 67 06 fd 09 13 5b fd fd 2b 75 60 fd 7c fd fd 48 79 77 7d fd fd 41 e5 fd fd fd 3f 17 06 0f 2c fd 75 fd 68 2f fd 54 fd 95 fd fd 56 4e 42 47 5f fd fd 17 71 fd	mt7~>#\Wky5aX++O}|e}i 1*4>[NKkX _|}X7WU6Dnq>EVbJk1c L`3+lHf>f21 O.3Vmg[+u`|Hy}A?,uh/TV NBG_q	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	5	1021	18 78 fd 01 fd fd fd 5b 5c 56 fd 28 2c fd 5c 42 fd fd 73 66 fd 09 fd 4d fd 74 3c fd fd fd fd 16 fd 48 7c fd fd 26 fd 4c fd 24 54 19 21 65 fd 7d 48 fd fd 4c 61 2c 00 fd 6d 7e fd 0d fd 4d 51 06 32 42 1f 40 fd fd 34 53 70 fd fd fd fd fd 5f 1f 2a fd d5 22 27 bb 70 50 fd fd fd fd 1a fd 23 5e 3e 1e 7e 15 51 a8 20 fd fd fd 53 59 fd fd 67 fd fd 10 4f 4a fd fd 2a 28 7f 72 fd fd 68 fd 1b 38 fd 37 fd fd 2b 5f fd 5b 42 25 fd fd fd fd fd fd 71 fd fd 0f fd 6e fd 7f 6d 3e fd 03 52 fd 74 fd fd fd 58 3f 21 fd 2c 27 41 fd 1e fd 10 fd 49 fd 52 fd 65 fd fd 66 fd fd 4d 1d 71 7b fd 23 6d 2f fd 4e fd fd fd 59 fd 23 62 fd 1e 7a fd fd fd fd 48 fd 42 1a 77 fd 41 1a fd fd 11 55 fd 3e fd fd 49 fd fd 3c 24 ab 55 fd fd 24 55 fd 15 63 fd 32 fd 02 fd 15 67 37 38	x[\V(,\BsfMt<H|&L$T!e}HLa,m~MQ 2B@4Sp_*'"pP#^>~Q SYgOJ(rh8+_B %qnm>RtX?!,'AIRefMq{#m/NY#bzHB wAU>l<U$Uc2g78	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	1026	256	7d 2e fd 2d fd fd 22 78 48 1a fd fd fd fd 44 3c fd fd 08 fd 13 fd fd 64 fd fd 48 63 43 28 1c fd fd 4b fd fd fd fd fd fd fd fd fd fd 0f 4d fd fd 0f 1f 37 65 fd 79 46 0f fd 10 20 41 0e 74 4b 13 e9 78 fd fd 28 1d 22 fd fd 50 16 fd fd 63 57 5e 7f fd 6c fd 5c 34 fd fd 65 18 3d fd 37 fd fd fd 0f 07 2e 47 5e 35 fd fd 01 fd fd 25 fd 0e 6f fd 44 76 5e fd 13 fd fd 3b 47 fd fd 41 fd c2 1a 6d 21 fd 01 2e fd fd 5c 6b 0c fd 4d fd 67 fd 14 11 3f 49 fd 63 61 fd fd fd fd 30 04 fd 40 fd 18 7c 0d fd 52 fd fd 3c fd 4f 33 5f fd 11 fd 0d fd fd 2f fd 05 37 fd fd fd 5a 32 fd fd 5b 5f fd fd fd 0b fd fd fd 10 68 fd 26 5a fd 0f fd fd 38 44 29 77 18 1d fd fd 20 2a 4d fd 3e fd fd 7e fd 24 fd 5c 77 fd fd 11 28 61 fd 0a fd fd 0e fd 37 5f 5e 51 fd 5e	}.-xHD<dHcC(KM7eyF Ax("PcW^|\4 e=7.G^5%oDv^;Gm!.\kM g?lca0@R<O 3_/7Z2[_hZ8D)w *M>~$\w(a7_^Q^	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	5	1021	2c 62 4c fd 3a 79 7c fd 73 fd 53 3c fd fd fd 1b 27 68 97 7c fd 67 7b fd fd 69 6c fd 0a 1a fd fd fd 50 6b fd fd fd 65 22 69 7f 35 1d 01 fd fd fd 5b fd fd fd fd 33 28 fd 67 fd 0d fd 3a 68 fd fd 4c fd fd fd 2f fd 72 46 30 fd 25 fd 6d fd fd 1f 36 fd 2a fd fd 7f 5d fd 30 14 d7 fd 44 1e 16 6b 79 fd 6a 58 fd 29 fd 66 70 fd fd 55 40 fd 47 24 0f 2b fd fd fd 6b 45 fd 40 6c fd fd 45 fd 35 4b fd 76 5c 7e fd ee fd 02 32 09 3e fd 69 1b fd 79 fd fd fd fd 71 fd fd fd 31 4e 1e fd fd 5c fd 72 6f fd 08 00 fd 18 5a 02 fd 44 3e 1b 50 fd fd 04 fd fd fd fd fd 3f 7b 3d 7b 2d 51 fd fd fd 3c fd 12 fd 08 13 1e 48 fd 32 fd 65 fd fd 0c 39 5e 52 2a 27 fd 5b 1e 47 7c 06 4c fd fd 22 23 2b 3c 2a fd fd fd 42 d0 fd fd 15 38 fd 6e fd f6 fd fd 53 18 1c fd	,bL:y|sS<'h|g{ilPke"i5[3(g:hL/ rF0%m6*]0DkyjX)fpU@G $+kE@IE5Kv \~2>iyq1N\roZD>P?{= {Q<2e9^R*'[G|L"#+ <*B8nS	success or wait	1	411859	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	1026	256	fd 73 24 4c fd 5d a7 19 fd 4d 06 7a fd fd 16 32 29 2a fd fd fd 7d 1d 17 1e 37 fd fd 15 39 10 d3 fd fd 2d fd fd 24 fd 0f 5d 55 07 fd fd 19 29 fd 0d fd 5a fd 7b fd fd d2 ce 52 77 fd 7d fd fd 35 2a f4 fd 3c fd 6f fd fd 6f fd fd fd fd fd fd 15 fd 18 53 3e 0a 59 4c 1b 56 61 56 39 fd fd 50 52 fd fd 05 17 fd 42 0f fd 10 76 15 fd fd 0e 0e 07 16 fd 65 11 fd 03 fd 7a 53 fd fd 44 fd 0d fd 2f 7c 25 fd fd 1c 2a 1c 14 fd 31 fd fd 7d 5b 5f fd 31 fd fd d4 fd 28 fd fd 39 fd 6f fd 46 25 fd 44 fd fd 04 fd 13 fd d3 38 64 fd fd 45 7a 7b 35 00 fd fd 61 02 fd b2 fd 0e fd 08 43 7c fd d5 fd 20 3a fd 56 6e fd 0a 3e fd 4e fd fd 39 13 fd fd fd 67 fd 2a b7 47 76 54 fd 31 fd 0c fd fd 22 fd fd fd 26 fd fd 69 fd fd 1e 0f fd 6b fd	s$L]Mz2)*}79- $]U)Z{Rw}5*<oo>YL VaV9PRBvezSD/|%*1} [_1(9oF%D8dEz{5aC| :Vn>N9g*GvT1"&ik	success or wait	1	4115FA	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	5	1021	fd 6e 3d 66 31 15 fd 5a 09 4a 32 5c fd fd 13 60 06 5d fd 77 7f 11 96 fd fd 7f 55 5a fd fd fd 59 1c fd 59 fd 54 fd 63 12 fd 0f 1f 1a 38 2c 31 fd 7d fd 38 fd 01 1a 54 fc 38 79 fd 18 31 53 fd 60 1f 48 2a fc fd 7f fd fd 67 36 fd 12 7e 5a 1e 09 4d fd fd 49 28 69 fd 4b fd fd 08 4e fd 17 78 1c fd 27 fd fd 3c 43 fd fd 0e fd fd 77 fd 5a 17 fd 69 6d 4f 11 fd bd 06 c3 fd 34 0c fd 61 fd fd fd 2b cf fd 7b 09 56 fd 77 fd fd fd fd 39 29 fd 03 5f 72 fd fd 28 fd 1e 2b 53 47 31 35 2a fd fd fd 3d fd 0d 47 73 fd 63 fd 4d fd 1a 60 3e fd ef fd 2d fd fd fd 24 fd ec fd fd 47 4e 07 0c 53 17 fd 2d fd fd fd fd fd 58 14 fd 1a 3d fd fd 41 34 fd 6d 49 66 fd 1e 4c fd fd 52 fd fd fd 3c 7e 58 fd 05 fd 15 2c 66 2d 19 fd fd 04 4b ca 11 03 4a fd 17	=f1ZJ2\`]wUZYYTc8,1}8T8y1S`H*g6~ZMI(iKNx'<CwZimO4a+{Vw9)_r(+SG15*=scM`>-$GNS-XA4mIfLR<~X,f-K	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	1026	256	fd fd 5f 7c 0b 54 2a fd 74 23 3a fd 5d fd fd 67 32 48 29 33 0b 28 fd fd 1f fd 72 62 47 02 2c fd 5b 79 fd 6d 08 5e fd 13 fd 4b fd 2a fd 6b fd fd 4f fd fd 00 74 fd 13 33 fd 59 fd fd 27 2b fd fd 54 fd 10 fd fd fd 7a fd 5d 66 76 fd fd 12 7f 22 79 fd fd fd 38 fd fd 6c 34 2d fd 16 fd 73 fd 12 fd 6f 70 66 52 2b fd 39 7c fd 14 fd fd fd 33 fd fd 2c fd 67 fd fd fd d9 fd 53 fd fd fd 35 69 15 2d 0c 6f fd fd 2b fd 20 fd 46 47 fd fd 2f fd 6b fd fd fd 0f fd fd 6c 18 56 fd fd fd fd fd 50 21 0e fd 74 fd 51 fd 7e 67 40 7e fd fd 33 fd fd fd 0b fd fd fd 27 fd fd fd fd 00 fd 06 39 fd fd fd fd 09 11 fd fd fd 5d 3d 26 fd 32 15 4e fd 61 fd 45 50 21 fd 09 fd 77 fd fd 54 51 fd 33 69 fd fd 6d 48 fd 61 fd fd fd fd 4f fd fe 27 55 53 2c 34 70 fd	|T*t#:]g2H)3(rbG,[ym^K*kOt3Y'+Tz]fv"y8l4-sopfR+9|3,gS5i-o+ FG/klVPtQ~g@3'9]=&2NaEP!wTQ3imHaO'US,4p	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	5	1021	fd 59 fd fd 75 6c fd 68 90 0c fd fd fd 16 49 fd fd 28 fd 5b fd 9d fd 7e 2d fd 02 fd 45 fd 16 71 fd fd 1f fd fd fd fd 21 0e 11 2b 0a 1a fd fd 59 fd 4a 1a fd fd 60 46 fd 7d fd 43 14 fd fd 4e 66 19 02 fd fd 5e 63 25 4d fd 1d 30 3b 55 fd fd 51 fd 2a 1c fd 13 71 fd fd 45 5f 43 fd fd 37 fd 31 69 49 38 fd fd fd fd 4d fd 5a fd 0a fd 1d 67 fd 27 fd 10 fd fd fd fd 78 5c 1f 71 15 fd fd fd 69 fd 90 6f fd fd 60 0c fd fd 21 fd fd 0d 41 0b fd 6a 45 76 fd 51 fd 04 fd fd fd fd 6a fd 30 fd 7e 5e 69 fd 3d fd 47 65 4a 09 3f fd 06 5f 73 fd 69 fd 16 fd fd 31 fd 7c 02 7d fd 7e fd 4f fd 50 45 17 3a fd 4e fd 7e 10 7e 65 fd fd 70 fd 4e 31 5f fd fd fd fd fd 45 fd fd 69 20 76 fd fd fd 50 7f 16 fd fd fd 17 4f 36 34 c8 50 fd fd 2a 4b fd 67 70 fd fd fd fd 22 fd	YulhI([~-Eq!+YJ`F}CNf^c%M0;UQ*qE_C71iI8MZg'x\qio`!AjEvQj0~^i=GeJ?_si1|}~OPE:N~~epN1_EiPO64P*Kgp	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	1026	256	0e fd 72 3b 15 fd 48 fd fd fd 3c fd fd 57 0c fd fd fd 51 3b 55 3b 78 fd fd fd fd 40 67 fd 07 fd 3f 7e 1b 44 63 fd 23 fd fd fd 47 fd fd fd 26 fd fd 15 69 fd 4d fd 77 fd fd fd fd fd 54 1c fd fd 29 fd 17 ae 78 65 4e fd fd 0a fd 6d fd e2 3e fd 6b 0b 4e 3b 47 69 01 47 fd 45 70 47 fd 3f fd fd 5b fd 6d 6d 42 fd 84 fd 4f fd fd e4 2c fd 59 fd cb fd fd fd fd fd 79 fd 1c 56 fd 66 fd fd 63 fd 56 fd 15 1a 33 fd fd fd 08 fd fd fd 7a fd 20 61 32 fd fd 58 fd 47 39 7d fd 28 fd 50 5e fd fd 5d 31 fd 15 fd fd fd 6a 51 57 ad fd fd 64 fd 31 fd 7f 5f fd 66 60 fd fd 61 29 42 3d 77 20 fd 77 19 2a 57 fd fd fd 4b fd fd 4a 7e fd 2e 79 aa 1d fd 6d 08 fd 08 fd 3f fd fd 26 17 6f fd 09 31 07 68 fd fd 14 44 5d fd 4a 2c 6c 15 fd fd 64 fd 2a fd fd	r;H<WQ;U;x@g?~Dc#G&iMwT)xeNmkN;GiGEpG?[mmBO,YyVfcV3za2XG9}(P^]1jWd1_f`a)B=ww*WKJ~.ym?&o1hD]J,ld*	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	5	1021	fd 5b 4a fd 6d fd fd 36 fd fd 1e fd fd fd fd 13 fd 18 07 fd fd 4c 6f 63 42 40 12 4e 13 5a 62 fd 78 5f 4f fd fd 52 36 fd fd 72 71 68 24 51 26 20 7f fd 14 fd 39 75 fd 4f 75 fd 1f fd 1f 01 fd fd fd fd 00 30 6e fd fd 44 10 17 2b fd fd fd 6c fd 51 fd 42 0c fd fd fd 25 fd fd 54 fd fd fd 53 fd 5c 31 fd fd 73 fd 25 2e fd 7a fd 58 fd fd 6e 06 76 70 fd fd fd e8 fd 08 60 fd 5a 26 64 fd fd fd fd fd 30 fd 0c 27 43 0c 0e 19 56 72 1a fd fd 72 fd 3c fd 00 fd 79 fd fd fd fd fd 78 71 69 fd 0a fd fd fd 5c 3d fd fd 0e fd fd 15 57 46 fd 6a 92 fd fd fd fd fd fd 65 fd e1 fd a7 7a fd fd 44 fd 17 fd fd 74 2e 7f 4a fd 2c fd fd fd 50 59 63 fd fd 22 4e fd 48 43 2f 51 1d 5b fd fd 3c fd fd fd 70 fd 00 fd 5a 70 44 37 fd fd fd 3b 33 fd	[Jm6LocB@NZbx_OR6rqh$Q& 9uOu0n D+QB%TS\1s%zXnvp`Z &d0'CVrr<yxq i\=WFjezt.J,PYc"NHC/Q[<pZpD;3	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	1026	256	fd fd fd 44 23 fd 58 27 fd fd fd fd 2b 36 fd 12 fd 30 fd fd fd 7f 3e fd fd 0c fd 22 fd 0d fd fd 4e fd 65 fd fd fd fd 1c 0e fd 6d 56 35 fd 2f 2c 57 55 fd fd 6b 5e fd fd fd fd 68 22 7f 51 fd 15 0a fd 0f 5e fd 43 fd 1c fd fd fd 1c 7f fd fd 57 15 12 18 24 42 06 fd 78 fd fd fd 7d 0a fd 5d 4d 31 1f 50 fd fd 46 fd 3e 74 74 7f 74 fd fd fd fd 6f fd 51 27 52 fd 27 20 fd fd 29 fd 64 fd fd fd 61 fd fd 0b 79 fd 54 1d fd fd 74 0d fd 21 fd 71 fd 18 fd 6b 1f fd 1b fd 57 fd 33 fd fd fd 71 29 fd 2b fd 6b fd fd fd 7a 4e 39 fd 2b fd fd fd 0f 73 30 5c 1d fd fd fd 3c 04 fd fd 13 fd 36 50 fd fd fd fd fd fd 43 32 fd 67 fd 07 67 44 0b 72 6e fd 00 7d 64 5f fd fd 7f 25 fd 53 09 fd fd 53 fd fd 66 fd 69 fd fd 6a ab fd 58 1e 5b fd 37 fd fd 03 fd fd 4b fd 0c fd 15 66 30	D#X'+60>"NemV5/,WUk^h"Q^CW$Bx}]M1PF>tttoQ'R')dayTt!qkW3q)+k zN9+s0<6C2ggDrn}d_% SSfijX[7Kf0	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	5	1021	46 72 fd 37 fd 27 24 fd fd 38 fd 4f 14 fd 62 fd fd 11 fd 18 c7 fd 52 fd fd fd 5a 44 5a fd fd 49 fd fd fd 0f 09 fd 10 2c 68 b0 fd 09 fd 03 fd fd 0f fd fd 59 17 5f fd 2e fd 00 fd fd 5f 51 fd 51 7e fd fd 6a fd 1a 4a fd 07 fd 78 fd 3c 6f fd fd fd 52 4e 0d fd 7e 05 fd fd fd fd 4f fd 0f fd fd 10 fd fd 63 fd fd 33 fd fd fd 21 fd 52 28 00 fd fd 5b fd fd fd fd fd 7f fd fd 53 fd 5a fd fd fd 5a f1 fd 3d fd fd 30 3d 01 7e 10 fd bc 43 59 fd fd 7d 20 69 fd fd 32 fd 1f fd 31 fd fd 4c 3f fd fd fd 05 fd 76 62 fd 1c 1f fd fd 71 fd 1b fd fd 45 50 fd fd 29 fd fd 32 fd 18 78 79 56 5a 16 e9 fd 7e 5a fd 23 00 fd fd 2f 0f 2e 25 0f 5a 66 68 68 33 fd 0f 3a 3a 03 71 6d 41 fd 58 fd 54 11 fd fd 14 fd fd fd fd fd fd 78 7c 34 fd 5e 9d fd 21 25 fd fd 01	Fr7'$8ObRZDZI,hY_._QQ ~jJx<oRN~ O3!R([SZZ=0=~CY} i21L?vbqEP)2x yVZ~Z#/.%Zfhh3::qmAXT x|4^!%	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	1026	256	18 fd 69 05 fd 4f fd 18 75 27 12 69 fd fd 03 23 48 59 19 06 1d 4d fd 7e 52 fd 6f fd 65 fd 11 5e fd fd 99 4d fd fd fd fd fd 2a 5d 28 5a fd 76 fd fd 23 fd 71 3e fd 71 3a fd fd 74 74 22 fd 31 fd 5e fd fd 24 33 fd 69 6b 68 52 fd 75 07 2e 3b fd 3c 3c 13 fd fd 41 fd fd 0b fd 4c fd fd 79 fd 3f fd fd fd 17 21 fd 43 41 fd fd fd 0c 7a fd fd 10 72 67 fd 5a 6b fd 4a fd fd fd 7a fd 12 2a fd 1d 42 4c 51 72 fd 60 fd 39 fd 46 fd fd fd 3f 7f 02 25 76 58 19 78 64 fd 3f 59 fd fd 57 1e fd fd fd 2d fd 66 fd fd fd 28 fd fd 93 fd 26 fd 67 19 fd fd fd fd 08 64 46 fd 76 4c 4b 2d fd fd fd fd 40 68 74 fd 7f 34 fd 13 fd fd 2b 35 7d 40 2d fd 29 42 fd 73 4e fd 4b fd 0a 3f 27 fd 18 fd 44 3d fd 40 fd fd fd 62 fd 01 55 fd fd 04 36 51 06 4d 7e 1a fd fd 09	Ou'i#HYM~Roe^M*] (Zv#q>q:t"1^$3ikhRu.; <<ALy?!CAzrgZkJz*BLQr `9F?%vXxd?YW- f(&gdFvLK-@ht4+5}@-)BsNK?'D=@bU6QM~	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	5	1021	2e 4f 0a 57 2d 68 7c 26 fd 19 11 65 fd 22 21 fd 40 fd 94 fd fd fd 2c fd 6b 2a fd 1e fd fd fd 41 01 67 24 6a 3c 29 04 59 12 fd 65 5b 2b 07 fd fd fd 0d 64 fd fd 2c 1f 4e fd fd fd 1d fd 5c fd 20 52 7f 75 fd 18 56 50 70 fd fd 12 fd 5b 55 06 51 c9 28 fd 34 1b 2c 38 40 fd fd fd fd 3f fd 19 fd 77 1f 3b 13 18 fd 6f 6e 16 05 fd 09 0d 63 25 fd 21 fd fd fd fd 1b fd d2 fd c6 fd fd fd 78 16 65 fd 0e c8 65 fd 71 fc 1d fd 5c 79 08 54 fd 64 fd fd 44 5f fd 1f da 1f fd 2b fd 07 10 3a 30 fd 09 fd fd 3f 44 00 fd 27 fd fd fd 2e fd fd 42 fd 67 fd 01 fd 15 65 fd fd 2f fd 59 fd 24 2f fd fd 47 fd 65 fd fd b4 57 7e fd 64 2e fd fd 57 54 fd 7e fd 37 fd fd 20 fd 20 19 fd 33 3d fd 1d 3d 03 29 fd fd 69 04 fd 51 68 fd 4e 2d 62 3f fd fd	.OW-h|&e"!@,k*Ag$j<)Ye[+d,N\ RuVPp[UQ(4,8@?w;onc%!xeeqyTdD_+:0?D'.Bge/Y$/GeW~d.WT~73==)iQhN-b?	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	1026	256	fd 5f 77 fd fd fd 26 12 2b 7a 28 fd 58 7d 7d 74 4a fd fd 24 67 fd 53 6a fd 5d 5d 61 31 fd 1e 05 7b 46 fd 99 20 fd fd 15 60 78 fd 1b fd fd 4d 13 3e fd 65 dc 44 fd 78 1c fd fd 29 fd fd fd 5c fd 0b fd 7f 16 16 72 06 22 2b fd 56 27 fd fd 71 59 2c fd fd 21 41 fd 76 37 fd 16 fd fd 69 fd 69 fd fd 06 5a 41 fd fd fd 22 fd fd 51 1c fd 65 5d fd 5c fd fd fd fd fd 54 fd 1a fd fd 42 52 fd 31 59 7a 48 6c 62 1a 9e fd fd fd 6b fd 09 52 fd 04 05 fd fd 82 0c 03 fd 15 fd 35 fd 6c fd 55 24 6f fd 0b 7d 19 fd 27 fd fd 42 17 6f fd 0f fd fd fd 41 fd 44 32 fd 6c 45 fd 0f fd fd 4c fd 14 60 54 16 fd 6b fd 52 7c 1d fd 6c fd 76 fd fd fd 3e 59 2b fd 77 fd 3e 7f fd fd 3b 6b fd 27 35 0c 03 2f 4f 1a 0e 49 61 78 7d fd 7c fd 36 3d	_w&+z(X}}t$gSj]]a1{F`xMeDx\r"+V'qY,!Av7iiZA"Qe]\TR1zHlbkR5lU$o}'BoAD2lEL`TkR|lv>Y+w>;k'5/OIax}|6=	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	5	1021	65 fd 6c 21 fd fd 02 fd 65 fd fd 4b fd fd fd 1a 23 fd fd 09 6f 38 fd 27 fd 16 15 fd 1e 01 fd 77 fd 0f fd 01 fd fd 4e fd 65 7b fd 6d 00 21 fd fd fd 12 fd 7f 65 32 fd fd 1f fd 3f fd fd 0c fd 0f 48 fd fd 91 fd fd fd fd 7e fd 11 6a fd fd fd 20 fd fd 6d 19 fd fd 7a fd 02 fd fd 31 fd fd 5d 58 fd fd 38 fd fd 1b fd 00 7a fd fd fd 1f 4f 61 fd 52 06 7a fd 6d fd fd 6c fd 49 18 fd 22 21 6c fd 42 fd fd 54 23 fd 67 fd 35 fd 40 77 25 2d fd 7d 7f 16 fd 70 fd 02 fd fd 5f fd 19 74 25 86 14 95 fd fd 15 12 40 5e 19 fd fd fd 23 fd 70 0d fd 0a fd fd fd fd 7d fd 3e fd 71 19 7a fd fd fd 5b 71 e0 fd 1b 5b fd fd fd 6a 63 fd fd 4b 26 fd 0c 41 6d fd fd 7d fd 3f 6c fd fd fd fd fd fd fd fd 65 fd fd fd 47 62 fd fd fd fd fd 41 15 1f 28 64 4a	l!K#o8'wNe{m!e2H~j mz1X8zOaRzm ll"!lBT#g5@w%- }p_t%@^#p}>qz[q[jcK&Am}?eGbA(dJ	success or wait	1	411859	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	1026	256	fd 13 fd 30 30 fd fd fd 7b fd fd fd 10 fd fd 39 a8 fd 17 fd 2b 0d 44 05 fd 00 36 fd 72 fd fd fd 6f fd fd fd 24 76 12 fd 42 fd 20 4a fd 64 12 5d 06 64 46 55 34 4e 5f 2c 26 fd 0e 1c fd 55 fd 51 fd 02 fd fd 5d 37 fd 5c fd fd 14 fd fd 6f fd fd 3c 7d 59 fd fd 14 07 30 5e 3b 58 2d fd 5d fd 1b fd fd fd fd fd fd 13 20 3c 66 fd 54 49 fd 6d fd 5c 1c fd fd 38 2f fd fd fd fd fd fd fd fd 66 fd bb 11 fd fd fd 51 fd fd 02 1a fd 49 13 fd 0f 14 fd fd 05 08 63 00 87 2e fd 6d fd fd fd 78 52 fd 23 fd 0e 74 32 77 fd 40 00 0d 6e fd fd fd 72 fd fd 00 fd 1c fd 3d 01 fd 76 df fd 4e 4f fd aa 44 fd 4c 50 b0 fd fd 5f 7d 2a fd 0f 49 fd fd fd 63 3b 49 05 3a fd fd 6e fd fd fd 2c 0d fd fd fd fd fd 58 fd 22 15 1a 3b 0d 23 37 fd fd fd 45 76 fd fd	00{9+D6ro$vB Jd]FU4N_,&UQ]7\o< }Y0^;X-] <fTIm\8/fQIc.mxR#t2w@ nr=vNODLP_}*Ic;I:n,X";# 7Ev	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	5	1021	27 7b fd 5a fd db fd 5a 2e f0 28 fd 6e 61 30 01 24 fd 6f fd fd 7f 2e fd 2d fd fd fd 7a 52 fd 0f 44 1e fd 05 fd 43 0c fd fd 6f 4c fd 77 66 fd 5f fd 36 28 30 07 fd fd 59 fd fd 43 fd fd f2 16 63 fd 00 4a 12 21 67 6a 3d 46 fd 70 fd 62 4f fd fd 76 fd 02 44 3c fd fd 66 2c fd 59 fd 1f 58 fd 06 47 fd fd 72 5a fd 3d fd 14 49 fd 7f 20 fd fd fd 7d 75 fd fd 13 56 fd fd 55 fd 25 fd 13 fd 2f fd 13 fd fd fd 62 68 fd 47 73 fd 94 21 fd fd fd fd fd 78 fd 39 7e fd 38 fd fd 15 fd 20 fd 44 7f fd 5e fd 58 44 79 66 51 fd 21 fd fd 1d 77 fd 69 0d fd 7f 60 74 fd 4f 78 fd fd fd fd 01 24 0d fd fd fd 07 fd 3e 6f 5f fd fd 5c fd 3a 01 fd fd fd fd 31 fd fd 1f 12 74 fd fd fd 53 09 0d 17 44 fd 37 75 43 5a fd fd 75 3e fd 0c fd 57 fd fd 61 fd 55 fd fd	'{Z.(na0$o.-zRDCoLwf_6(0YCc!gj=FpbOvD<f,YXGrZ=I}uVU%/bhGs!x9~8D^XDyfQ!wi`tOx$>o_\:1tSD7uCZu>WaU	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	1026	256	43 60 09 70 fd 6f fd 6b 43 07 85 fd fd 7d 9b fd fd fd fd 6c fd fd 14 38 13 56 fd fd fd 6e 63 fd 10 fd 2a 20 55 fd 7f 65 fd 45 fd b7 4b 06 fd fd fd 00 17 45 44 27 61 10 fd 02 33 3c 7c fd fd 06 56 17 7d 1b fd fd 4c 2a 4c 61 77 fd fd 5a 3d 72 09 fd 41 fd 6e 6d 18 77 fd 6e fd fd 07 fd fd fd fd fd 5c 7f 1d fd 5a 38 fd fd 7f 31 fd 22 fd 31 3b fd fd 54 6d 70 5d fd fd fd 3b fd 65 fd fd 56 64 fd fd fd fd fd fd 73 bb 28 2a 1f 5a 0d 5f fd 2d 2b fd fd 2a fd fd fd 61 fd 72 fd fd fd 45 00 fd fd 30 5d 01 fd fd fd 20 fd 7d 0f 1b 30 fd 7e 08 fd fd 42 fd 00 7f fd fd fd fd 62 fd 44 fd fd 50 00 fd fd 0c fd fd 69 0a 32 fd fd 1a 1f fd fd 6f 2c fd fd 1d fd fd 64 24 fd 65 fd fd 53 fd fd 55 1d fd 57 fd 2a 6b 4e fd fd fd 3c 6c 1b fd fd 53 35 fd	C`pokC}l8Vnc*UeEKED'a3<|V}L*LawZrAnmwn\81"1;Tmp];eVds(*Z_-+*arE0]}0~BbDPi2o,deSUW*kN<IS5	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	5	1021	fd 5e 6a fd fd fd 67 fd fd fd fd 72 fd 31 fd 7d fd 5c fd fd fd 7d 5a 18 5b 7d fd 06 1c fd 4d 5f 0f fd 39 fd fd fd fd 02 7f 0a fd 36 75 4d 3f 4d 3a fd 06 02 fd 16 00 3b 19 19 fd fd 20 3b fd 38 fd fd 73 49 3e 00 0f fd fd 0e 3a 24 fd fd 24 fd fd 06 12 fd fd 6e 91 fd 15 37 fd 4f fd 2f 0e fd 22 fd 3b 5b fd 48 fd 54 65 fd fd 7c fd 52 fd 6f fd 1b fd fd fd 74 21 26 fd 59 fd fd 5c 4f fd 73 fd 2a fd 2a fd fd fd fd 07 fd 49 fd 49 02 fd 45 59 40 77 fd 15 fd fd 06 fd 05 fd 1f fd 08 dc 1f fd 45 fd 44 fd fd fd 4e 59 10 fd 0e 34 fd fd 75 fd 7a 01 2a 45 72 04 fd fd 6f fd 14 fd 58 11 6c fd 38 fd fd 10 57 3c 47 2f fd 78 28 2e fd fd fb 2a 06 fd 0b 32 fd 3d 79 fd 5d fd fd fd 56 fd 04 fd fd 0c 77 fd 0d 57 fd fd 58 fd fd fd fd 54 fd 57 36 fd fd	^jgr1}\}Z{}M_9uM?M:;;8I>:$$n7O/";[HTe|Rot!&Y\Os*IIEY@EDNY4uz*EroXl8W<G/x(.*2=y]VwWXTW6	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	1026	256	23 61 2e fd 66 58 79 44 06 fd 12 56 fd 17 67 fd fd 11 2f 69 fd fd fd fd 41 5e fd 3e fd fd 5e fd fd 7a 73 fd 4b 9a 0a fd 19 fd 45 fd 30 7b fd 40 fd 3d 5a 47 fd fd fd 1d df fd fd 29 fd 13 fd 48 fd 2d fd fd 53 64 fd 32 fd fd fd 16 b2 fd 30 fd 28 10 09 fd 2d 0f 76 58 fd fd fd 71 63 fd 6b fd 07 fd 36 fd 31 fd fd 3e fd 53 fd 45 11 3f fd fd 19 01 41 fd 4d fd 08 35 fd 22 68 b2 fd 7e fd 17 4b fd 02 35 fd fd 42 45 23 fd fd 5b 2f 39 0b fd fd 40 1d 7d 10 1a fd 7c fd fd 75 64 55 fd 1a 09 07 61 13 5c 19 58 52 34 1c fd fd 51 fd fd fd 2c 2e fd fd 00 c7 fd fd 7d 00 22 fd fd fd 60 fd fd 49 fd 1d fd fd 41 fd 24 fd 16 fd 6b fd 28 15 fd fd 53 7e 3a fd 3d 25 5b 39 94 78 fd 1f 62 fd fd 4e 62 6c fd fd 1a fd 1c 51 04 08 fd fd fd fd fd fd 35 00 fd	#a.fXyDVgiA^>^zsKE{@=ZG)H-Sd20(-vXqck61>SE?AM5"h~K5BE#[/9@}|udUa\R4Q,.}"`IA$k(S:=%[9xbNblQ5	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	5	1021	3e 24 7a fd fd fd fd fd fd fd 54 fd 12 fd 0c fd fd 6d fd fd 3a fd 7e fd 0e 5a 35 57 42 fd 77 fd 70 6b 5f 10 fd 4a fd fd 2a 42 fd fd 39 fd fd fd 17 33 0f 68 1c 35 fd 6f 25 fd fd fd 27 fd fd fd 8b 10 fd 3f fd 4e 2a fd 37 fd 06 2d fd 13 fd fd 0f fd 09 96 0e fd fd 1b 13 59 fd fd 29 fd fd b7 fd fd fd 3f 0b 5a 54 fd 30 6e 20 fd 65 fd fd d5 fd fd 70 fd fd fd 1e 3e fd fd 39 fd fd 4d fd fd 2e 5e fd 63 fd fd fd 0c 42 fd fd 71 fd fd 4e 51 fd 48 06 fd 35 fd fd 13 fd fd 05 fd fd 6c bb 3c fd 47 10 49 fd fd fd 36 4a fd 1b 37 76 fd fd 6f 37 6d fd fd 31 fd fd 76 95 fd 70 fd fd 1a 39 fd 68 fd fd 4d 05 fb 15 13 3a 7b 04 fd fd fd fd 2e 5e 4f 09 fd 37 fd fd 61 fd 62 78 15 fd 0d 6a fd 19 6b 2d 73 fd fd fd fd 49 fd 2e fd 43 7f	>$zTm:~ZWBwpk_*B93h5o%'?N*7-Y)?ZT0np>9M.^cBqNQH5l<GI6J7vo7m1vp9hM:{.^O7abxjk-sIC	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	1026	256	fd 2e fd fd fd fd 57 45 fd 21 4a b1 fd fd 06 65 2c fd fd fd fd fd 66 2c fd fd 20 48 fd 2f 74 fd 5d 52 6f fd 15 74 fd fd fd 67 45 2f fd 49 43 1a fd fd 39 fd 00 20 6f 08 57 fd 2c 89 fd 5c 44 5d fd 7e 5c 47 2c fd 51 fd 3c 21 03 40 60 fd 0c fd 30 fd 35 3d fd 30 73 35 53 20 0c fd 3a fd fd 28 7b 51 6a 66 3a 3a 3d fd 16 31 36 5e fd 63 1f fd 57 fd 74 73 65 7a fd fd fd 2c 30 fd fd fd 53 48 2c ed fd fd 00 fd fd fd 7e fd 1b 75 16 fd 78 fd fd fd 2e 0f 00 41 fd 66 fd fd fd 25 3b 2b fd fd 4e fd fd fd 22 6b a7 78 07 fd fd fd 42 05 fd 51 55 fd 4c 3e 1a fd 3d 7e fd 35 79 5b fd 77 fd fd 76 fd 0c 7f fd fd fd fd 6d 58 4f 10 48 fd 5a 31 fd 5c 52 51 fd fd fd fd 5d fd fd 75 fd fd 11 6c 52 7c 3c 47 fd fd fd fd 27 fd fd 0e fd 2d 19 52 54 2d 12 6b fd	.WE!Je,f,H/t]RotgE/IC9oW,\D]~\G,Q<!@`05=0s5S :({Qjf::=16cWtsez,0SH,~ux.Af%;+N"kxBQUL>=~5y[wvmXOHZ1\RQ]ulR|<G'-RT-k	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP3iHx1cFFHBUeguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	5	1021	fd 59 2d 28 17 6c 07 fd 40 fd fd 82 5e 37 fd 10 fd ed fd fd 13 21 fd 62 5c 4e 7b fd f8 fd fd fd 31 0e 62 01 fd 7c 23 32 52 fd 66 61 5c fd fd fd 25 3e 63 45 17 fd 79 fd fd 2b 25 fd fd 12 fd 0e fd 48 fd fd fd fd 6b 6d 51 7c fd 3b fd 7e 3e 56 fd 78 09 fd 09 5b 35 fd 5d fd 76 7c fd 5b 25 4f 04 27 fd fd 51 fd fd fd fd fd 5c 59 fd 67 4a 7d 21 fd 67 3b 16 75 34 fd 55 fd 3b 21 fd fd 04 04 3f 07 49 fd d9 6c fd fd fd 73 fd 32 00 33 44 fd fd 3a fd 5d fd fd fd fd fd 28 30 fd fd 03 57 14 3e 34 12 ed f2 fd 7e 37 4e 62 10 fd 19 fd fd fd 72 fd fc fd 41 1e 0d 7e fd 7c fd fd fd 69 36 3a 35 fd fd fd 1f fd fd 6a 03 26 54 fd 1d 4c fd 21 44 00 fd 06 00 70 26 fd 34 fd fd 7b 44 fd fd fd fd fd fd 05 fd 42 fd fd fd 32 fd 25 fd 10 56 12 fd	Y- (l@^7!b\N{1b|#2Rfa\%>cEy+%HkmQ|;~>Vx[5]|[%O'Q\YgJ}!g;u4U;!? lls23D:] (0W>4~7NbrA~|i6:j&TL! Dp&4{DB2%V	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1026	256	fd fd 02 fd 27 fd 5b fd fd 44 26 70 70 0e fd 74 05 3c fd fd 70 77 fd fd 2d fd 12 6a fd 02 3a 46 fd 2c fd fd fd fd 7b fd fd fd fd 0c fd fd fd fd 52 16 1b 2c 0d 49 fd fd fd fd 70 42 fd 66 52 68 fd fd fd 67 fd 61 fd fd 5c 72 01 fd 36 41 5c fd fd 58 fd fd fd fd fd fd 01 fd ca fd 7c 53 fd 37 61 2b 10 fd 2d 5a fd 73 fd 39 03 6b fd 18 5b 53 8d 70 15 18 fd fd 6e 04 fd fd fd 6d fd 63 1c fd 4f fd 06 59 fd 0e fd 74 32 fd fd 5b 7b 27 55 1a fd fd c3 b8 4a 53 fd fd 47 fd fd 7c fd fd 3a fd fd 2c 4c fd fd 7a 2f fd 5f fd 7b fd fd 38 4c 40 7a fd 4f fd 7d fd 6e 4d 5b 6f fd 73 fd fd 47 fd fd 26 7d fd 3d 26 fd fd 70 67 fd fd 40 1a 65 fd fd 70 7c 38 fd 1a 07 fd fd 0f 59 fd fd fd 2c 48 71 fd 4a fd 6c fd fd 46 6c 3c fd fd 79 51 fd	'[D&ppt<pw-jF, {R,IpBfRhga\r6A\X|S7a+-Zs9[SpnmcOYt2[{'UJSG|: , Lz/_{8L@zO}nM[osG&}& pg@ep|8Y,HqJlFl<yQ	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnIbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	5	1021	fd fd fd 75 2f fd 24 64 38 6e fd fd fd 5e 5d 2e fd 6b fd bb 03 15 fd 3f fd 4f 5c fd fd 31 fd 6c 4d fd 17 34 fd 1e 31 0d 17 fd 07 fd 26 fd fd 49 70 32 fd fd 6a f9 62 fd 03 53 fd 0f fd fd fd 6f 78 2e 23 fd 2a fd fd 74 fd 08 fd fd fd fd fd 6f fd fd fd fd 68 53 fd fd fd 65 61 fd 47 fd 28 fd fd 44 56 fd 51 35 62 48 7e fd 28 3b fd fd 44 fd fd 78 1e fd fd 38 fd fd 20 24 fd 62 fd fd fd fd fd 39 09 fd fd 2a fd fd fd 5f fd fd 16 3e 68 fd fd fd fd 06 fd 71 69 fd fd 30 23 2a 78 7e 07 71 fd fd 5c fd 75 fd 4d fd 19 a1 fd 4b fd 34 fd 13 fd 6a fd fd 31 fd 6a 57 fd fd 27 fd 2e fd fd 78 fd 30 20 70 4a 5b fd 6c 70 2e fd 70 08 21 fd fd 71 fd 58 57 fd fd 38 7d fd 13 fd 25 fd fd fd 26 fd fd fd 05 fd 71 00 fd fd 64 fd fd fd 56 31 34 02 fd fd 5e 57 fd 2e 2b	u/$d8n^].k? O\1IM41&Ip2jbSox.#* tohSeaG(DVQ5bH~(;Dx8 $b9*_>hqi 0#*x~q\uMK4j1jW'.x0 pJ[lp.p!qX W8}%&qdV14^W.+	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	1026	256	6c fd fd fd fd 3f 2d 66 fd 73 fd 63 47 fd fd 30 fd 26 fd 13 fd fd 71 18 08 77 66 0b fd fd 49 fd fd fd 19 32 11 fd 51 fd 20 fd fd 60 fd 42 99 06 55 7a 62 fd fd 16 79 fd ce fd 4d 0c fd 65 4d fd e5 7a 19 fd 64 fd fd fd 7f 47 0f fd 71 fd fd fd 55 2d fd fd 3e 02 09 49 61 fd 5e fd 34 fd 2b 65 5e 18 fd fd 8a fd 47 51 fd fd fd 34 fd 5e fd 64 5c 57 fd 28 fd fd 4f fd fd 24 fd fd fd fd 2e fd 4a fd fd fd 5c 2a 06 fd 3a 3b fd fd 38 fd fd 66 54 fd 2d fd 73 12 fd 11 50 fd 46 fd 70 1c 42 14 fd 77 fd 7b 27 fd fd fd fd 12 37 04 2c fd 51 00 41 fd fd fd fd 10 fd 8f fd fd 7c fd 0e 50 13 fd 48 fd 75 3b 08 fd 79 61 fd 61 15 fd fd 33 6e fd 18 fd 1a fd fd 06 fd 59 fd 2b 3f 1d fd fd 62 7b a7 11 66 fd 1b 77 1c 59 18 54 44 fd fd fd 61 fd 29 39 71	l?-fscG0&qwl2Q `BUzbyMeMzdGqU- >la^4+e^GQ4^d\W(O$.J\ *:;8fT-sP FpBw{'7,QA|PHu;yaa3nY +?b{fwYTDa)9q	success or wait	1	4115FA	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	1282	40	4b 36 74 65 31 59 47 50 6e 49 62 6f 34 47 63 47 4f 45 50 33 69 48 78 31 63 46 46 48 42 55 65 67 75 78 52 47 6d 33 58 53	K6te1YGPnlbo4GcGOEP 3iHx1cFFHBU eguxRGm3XS	success or wait	1	41164B	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	1322	38	7b 33 36 41 36 39 38 42 39 2d 44 36 37 43 2d 34 45 30 37 2d 42 45 38 32 2d 30 45 43 35 42 31 34 42 34 44 46 35 7d	{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}	success or wait	1	41167E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg	5	1021	44 01 fd fd fd 29 58 7b 26 56 fd 0d fd 06 fd fd 27 5f fd fd 6d fd fd fd 66 fd 41 4e fd 2c fd fd 45 3f fd 57 fd fd 45 57 01 23 fd fd 7c fd fd 78 66 fd 55 65 58 c9 5d 07 04 21 fd 69 9c fd fd 0b fd 75 fd 98 fd 34 fd fd 63 fd 74 fd 0e fd 73 02 61 fd fd fd fd fd fd 08 0b fd fd 03 12 2d 7b 35 fd fd fd fb 6a fd 0b 77 fd fd fd 4a 7c fd fd fd fd fd 4c 67 29 44 fd 76 49 fd fd 61 47 1f fd 6f 2c fd 49 b5 3e fd 03 36 fd 43 2c 7d 5b fd 4b 75 39 08 fd 61 59 fd 43 55 21 69 61 28 08 fd 65 5e fd 56 45 fd fd 1b fd 30 fd fd 0b 15 fd 61 fd 7f fd 06 69 fd 66 77 fd 49 3d fd 29 fd 62 6a 30 0a fd fd 62 69 39 5d 43 fd fd fd 60 fd 36 44 fd fd fd 79 0d fd 65 4b 51 42 f5 30 14 3b 1f fd fd 40 fd 4c 05 fd 68 29 12 29 fd fd 41 fd 28	D)X{&V'_mfAN,E?WEW#|xfUeX]!iu4ctsa-{5jwJ|g)DvIaGo,I6C,}[Ku9aYCU!ia(e^VE0aifwI=)bjbi9]C`6DyeKQB0@h))A(	success or wait	1	411859	WriteFile
C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg	1026	256	fd fd 39 fd fd fd fd 15 fd fd 43 fd 06 fd fd fd fd fd fd 04 24 fd fd 42 fd 4c fd fd 48 0d 11 fd fd 06 61 fd 2b fd fd 48 fd 0f 2a fd fd 4c 5c fd 10 63 fd fd fd 38 68 fd fd 5c fd 5b 32 fd fd 34 73 fd 57 6d fd 6f 12 fd 2b fd fd fd fd 78 fd fd fd fd 8e fd 48 31 2c fd 1f fd 39 7a fd 7f fd 12 6e fd fd fd 62 20 fd 33 54 13 fd fd fd 48 fd fd 73 01 39 3f 33 75 fd fd 40 33 fd 5f 1c 43 0f 5c fd fd 6b 07 40 0c fd fd 27 18 fd 20 37 72 01 20 fd 19 03 fd 29 fd 37 39 56 fd fd fd 28 00 34 b3 59 22 5e fd 7b 30 fd fd fd fd 41 12 fd 4c 02 fd 0d 47 6b 5d 23 36 fd fd 7c fd 3d fd fd 4d 0e 12 74 71 fd fd fd fd fd fd 48 fd 13 3c 73 01 fd fd fd 27 0c fd fd fd fd 59 fd 4e 7e fd fd 48 25 fd 67 fd fd 60 e6 33 fd 0e 0c fd 59 49 fd fd fd 7f fd 00 2b 45 fd 48	9C$BLHa+H*L\c8h\[24sWmo+xH1,9znb3THs9?3u@3_C\k@' 7r)79V(4Y"^{0ALGk]#6|=MtqH<s'YN~H%g`3YI+H	success or wait	1	4115FA	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\FENIVHOIKN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\FENIVHOIKN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ.docx	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\NEBFQQYWPS.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\NEBFQQYWPS.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\QNCYCDFIJJ.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\RAYHIWGKDI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\RAYHIWGKDI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SFPUSAFIOL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SFPUSAFIOL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\SQRKHNBNYN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\SQRKHNBNYN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\UOOJJOZIRH.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\UOOJJOZIRH.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WKXEWIOTXI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\ZBEDCJPBEY.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\ZBEDCJPBEY.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\FENIVHOIKN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\FENIVHOIKN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\NEBFQQYWPS.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\NEBFQQYWPS.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\QNCYCDFIJJ.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\QNCYCDFIJJ.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\RAYHIWGKDI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\RAYHIWGKDI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\SFPUSAFIOL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SFPUSAFIOL.mp3	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQRKHNBNYN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\SQRKHNBNYN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\UOOJJOZIRH.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\UOOJJOZIRH.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WKXEWIOTXI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\ZBEDCJPBEY.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\ZBEDCJPBEY.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\ZBEDCJPBEY.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\BPMLNOBVSB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\BPMLNOBVSB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\BPMLNOBVSB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\FENIVHOIKN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\FENIVHOIKN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\JSDNGYCOWY.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\JSDNGYCOWY.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\KZWFNRXYKI.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\LTKMYBSEYZ.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\LTKMYBSEYZ.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\NWTVCDUMOB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\RAYHIWGKDI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\RAYHIWGKDI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\SQRKHNBNYN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\SQRKHNBNYN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\UOOJJOZIRH.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\UOOJJOZIRH.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\WKXEWIOTXI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\WUTJSCBCFX.docx	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\WUTJSCBCFX.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\WUTJSCBCFX.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\WUTJSCBCFX.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\YPSIACHYXW.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\YPSIACHYXW.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\YPSIACHYXW.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\YPSIACHYXW.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\ZBEDCJPBEY.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Downloads\ZBEDCJPBEY.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Amazon.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Amazon.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Bing.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Bing.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Facebook.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Facebook.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Google.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Google.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Live.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Live.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\NYTimes.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\NYTimes.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Reddit.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Reddit.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Twitter.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Twitter.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Wikipedia.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Wikipedia.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Favorites\Youtube.url	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Favorites\Youtube.url	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\IconCache.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\IconCache.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\BPMLNOBVSB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\KZWFNRXYKI.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\NEBFQQYWPS.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFlJJ.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\QNCYCDFlJJ.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\UOOJJOZIRH.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI\WKXEWIOTXI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\JSDNGYCOWY.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\KZWFNRXYKI.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\LTKMYBSEYZ.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ\NWTVCDUMOB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\WUTJSCBCFX.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ\YPSIACHYXW.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\BPMLNOBVSB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\FENIVHOIKN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\KZWFNRXYKI.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\WKXEWIOTXI.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\WUTJSCBCFX.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX\ZBEDCJPBEY.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\RAYHIWGKDI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\SFPUSAFIOL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\SQRKHNBNYN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\WKXEWIOTXI.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\YPSIACHYXW.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Desktop\YPSIACHYXW\ZBEDCJPBEY.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\BPMLNOBVSB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\KZWFNRXYKI.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\NEBFQQYWPS.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\QNCYCDFIJJ.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\UOOJJOZIRH.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\KZWFNRXYKI\WKXEWIOTXI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\JSDNGYCOWY.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\KZWFNRXYKI.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\LTKMYBSEYZ.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\NWTVCDUMOB.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\WUTJSCBCFX.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ\YPSIACHYXW.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\BPMLNOBVSB.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\BPMLNOBVSB.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\FENIVHOIKN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\FENIVHOIKN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\KZWFNRXYKI.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\KZWFNRXYKI.xlsx	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\WUTJSCBCFX\WKXEWIOTXI.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\WKXEWIOTXI.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\WUTJSCBCFX.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\WUTJSCBCFX.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\ZBEDCJPBEY.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\WUTJSCBCFX\ZBEDCJPBEY.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\RAYHIWGKDI.pdf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\RAYHIWGKDI.pdf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\SFPUSAFIOL.mp3	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\SFPUSAFIOL.mp3	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\SQRKHNBNYN.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\SQRKHNBNYN.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\WKXEWIOTXI.jpg	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\WKXEWIOTXI.jpg	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\YPSIACHYXW.docx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\YPSIACHYXW.docx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\ZBEDCJPBEY.xlsx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\Documents\YPSIACHYXW\ZBEDCJPBEY.xlsx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\AdobeARM.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\chrome_installer.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\SetupExe(20200723102007 17D0).log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\SetupExe(20200723102007 17D0).log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCDDA.tmp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCDDA.tmp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Templates\Normal.dotm	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\ngen.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\ngen.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\CR_4BAC1.tmp\setup.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\CR_4BAC1.tmp\setup.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\DismHost.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Temp\F0AA5307-87B6-41CC-8AB9-9D4E70F644BD\DismHost.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\MSIMGSIZ.DAT	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\CameraRoll.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\en-US.1	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\UrlBlock\urlblock_637194112741176080.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\VersionManager\versionlist.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\alertIcon.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\alertIcon.png	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppBlue.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppBlue.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorBlue.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorBlue.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorWhite.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppErrorWhite.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppWhite.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AppWhite.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.gif	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.gif	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\AutoPlayOptIn.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppBlue.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppBlue.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppWhite.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ElevatedAppWhite.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Error.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Error.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ErrorPage.html	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ErrorPage.html	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileCoAuth.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileCoAuth.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncConfig.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncConfig.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncHelper.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\FileSyncHelper.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMHeroToast.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMHeroToast.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMLockedFileToast.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMLockedFileToast.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMScanExclusionToast.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\KFMScanExclusionToast.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\LoadingPage.html	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\LoadingPage.html	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.exe	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.VisualElementsManifest.xml	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDrive.VisualElementsManifest.xml	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveLogo.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveLogo.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveSetup.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveSetup.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveStandaloneUpdater.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveStandaloneUpdater.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveUpdaterService.exe	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\OneDriveUpdaterService.exe	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaCritical.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaCritical.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaError.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaError.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaNearing.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\QuotaNearing.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Resources.pri	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Resources.pri	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\SaveApplicationEventLogs.wsf	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\SaveApplicationEventLogs.wsf	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ScreenshotOptIn.gif	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ScreenshotOptIn.gif	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\TestSharePage.html	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\TestSharePage.html	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ThirdPartyNotices.txt	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\ThirdPartyNotices.txt	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\vaultIntro.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\vaultIntro.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Warning.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\19.086.0502.0006\Warning.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\setup\ECSConfig.json	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	unknown	38	success or wait	1	41134B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\microsoft-skydrive-desktop_16_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\microsoft-skydrive-desktop_16_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_11_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_11_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_17_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_23_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_27_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_27_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_37_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_37_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_38_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_9_0.png	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_9_0.png	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{0A0496DA-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{0A0496DA-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000016.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000a.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000a.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000b.db	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000b.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	unknown	38	success or wait	1	41134B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	unknown	153605	success or wait	1	41140B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db	unknown	153605	success or wait	1	41140B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db	unknown	153605	success or wait	1	41140B	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	SysHelper	dword	1	success or wait	1	40C72B	RegSetValueExW

Analysis Process: U59WtZz2Sg.exe PID: **2312**, Parent PID: **3184**

General

Target ID:	6
Start time:	00:22:15
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe --Task
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000000.323219375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000000.323219375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000000.323219375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.323219375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000000.324169163.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000000.324169163.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000000.324169163.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.324169163.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.321377469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000000.322799276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000000.322799276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000000.322799276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.322799276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000002.364455127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000002.364455127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000002.364455127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000002.364455127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000000.322395529.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000000.322395529.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000000.322395529.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.322395529.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000000.323671151.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000000.323671151.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000000.323671151.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000000.323671151.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\geo[1].json	0	500	7b 22 69 70 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 39 22 2c 22 63 6f 75 6e 74 72 79 5f 63 6f 64 65 22 3a 22 43 48 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 5f 72 75 73 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 33 38 5c 75 30 34 34 66 22 2c 22 63 6f 75 6e 74 72 79 5f 75 61 22 3a 22 5c 75 30 34 32 38 5c 75 30 34 33 32 5c 75 30 34 33 35 5c 75 30 34 33 39 5c 75 30 34 34 36 5c 75 30 34 33 30 5c 75 30 34 34 30 5c 75 30 34 35 36 5c 75 30 34 34 66 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 75 72 69 63 68 22 2c 22 72 65 67 69 6f 6e 5f 72 75 73 22 3a 22 5c 75 30 34 32 36 5c 75 30 34 34 65 5c 75 30	{"ip":"102.129.143.49","country_code":"CH","country":"Switzerland","country_rus":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0438\u044f","country_ua":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0456\u044f","region":"Zurich","region_rus":"\u0426\u044e\u0	success or wait	1	40CFD3	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: U59WtZz2Sg.exe PID: **5900**, Parent PID: **3324**

General

Target ID:	7
Start time:	00:22:23
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000007.00000002.350733876.0000000002105000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000007.00000002.351892792.00000000021A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000007.00000002.351892792.00000000021A0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: build2.exe PID: **1544**, Parent PID: **6132**

General

Target ID:	8
Start time:	00:22:24
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe"
Imagebase:	0x400000

File size:	264192 bytes
MD5 hash:	B9212DED69FAE1FA1FB5D6DB46A9FB76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000008.00000002.350956103.00000000020D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000008.00000002.349827384.00000000004B9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: U59WtZz2Sg.exe PID: **4296**, Parent PID: **5900**

General

Target ID:	9
Start time:	00:22:26
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.343989029.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.345862911.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.345862911.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.345862911.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.345862911.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.344652371.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.344652371.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.344652371.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.344652371.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.347232318.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.347232318.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.347232318.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.347232318.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.345188173.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.345188173.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.345188173.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.345188173.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000000.346399832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000000.346399832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000000.346399832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000000.346399832.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000009.00000002.353616538.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000009.00000002.353616538.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000009.00000002.353616538.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000009.00000002.353616538.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: build2.exe PID: **5364**, Parent PID: **1544**

General

Target ID:	10
Start time:	00:22:27
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build2.exe"
Imagebase:	0x400000
File size:	264192 bytes
MD5 hash:	B9212DED69FAE1FA1FB5D6DB46A9FB76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000000.378213612.0000000000627000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000000.347600742.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000000.369240104.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000000.347031103.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000000.347942903.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000000.347322735.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: build3.exe PID: **5972**, Parent PID: **6132**

General

Target ID:	11
Start time:	00:22:28
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\81bc8e9b-9d47-41ad-b82b-bbc3ff54a6de\build3.exe"
Imagebase:	0xb90000
File size:	9728 bytes
MD5 hash:	9EAD10C08E72AE41921191F8DB39BC16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000000B.00000000.345320617.0000000000B91000.00000020.00000001.01000000.00000007.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000000B.00000000.345320617.0000000000B91000.00000020.00000001.01000000.00000007.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000000B.00000002.347163945.0000000000B91000.00000020.00000001.01000000.00000007.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000000B.00000002.347163945.0000000000B91000.00000020.00000001.01000000.00000007.sdmp, Author: unknown
Reputation:	moderate

Analysis Process: schtasks.exe PID: **5880**, Parent PID: **5972**

General

Target ID:	12
Start time:	00:22:28
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Azure-Update-Task" /tr "C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe"
Imagebase:	0x340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **5968**, Parent PID: **5880**

General

Target ID:	13
Start time:	00:22:28
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mstsca.exe PID: **4536**, Parent PID: **1084**

General

Target ID:	14
Start time:	00:22:28
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
Imagebase:	0xee0000
File size:	9728 bytes
MD5 hash:	9EAD10C08E72AE41921191F8DB39BC16
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000000E.00000000.347198189.0000000000EE1000.00000020.00000001.01000000.00000008.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000000E.00000000.347198189.0000000000EE1000.00000020.00000001.01000000.00000008.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000000E.00000002.564552396.0000000000EE1000.00000020.00000001.01000000.00000008.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000000E.00000002.564552396.0000000000EE1000.00000020.00000001.01000000.00000008.sdmp, Author: unknown • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown
Antivirus matches:	• Detection: 92%, ReversingLabs
Reputation:	moderate

Analysis Process: schtasks.exe PID: **4612**, Parent PID: **4536**

General

Target ID:	15
Start time:	00:22:29
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Azure-Update-Task" /tr "C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe"
Imagebase:	0x340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: U59WtZz2Sg.exe PID: **6096**, Parent PID: **3324**

General	
Target ID:	16
Start time:	00:22:33
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000010.00000002.373204030.00000000020F3000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000010.00000002.378615646.0000000002230000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000010.00000002.378615646.0000000002230000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: U59WtZz2Sg.exe PID: **4756**, Parent PID: **6096**

General	
Target ID:	17
Start time:	00:22:35
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\439dd104-1941-4ae6-af5f-8afc23993f7a\U59WtZz2Sg.exe" --AutoStart
Imagebase:	0x400000
File size:	680448 bytes
MD5 hash:	41001FDD7879CE9EDE214E92C7E492BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.367371233.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000002.378588767.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000002.378588767.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000002.378588767.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000002.378588767.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000000.364650257.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000000.364650257.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000000.364650257.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.364650257.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000000.365343536.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000000.365343536.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000000.365343536.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.365343536.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.363751420.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000000.366169302.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000000.366169302.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000000.366169302.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.366169302.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000000.364114264.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000000.364114264.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000000.364114264.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000000.364114264.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **4712**, Parent PID: **4612**

General

Target ID:	18
Start time:	00:22:36
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIADAP.exe PID: **4296**, Parent PID: **2156**

General

Target ID:	23
Start time:	00:23:58
Start date:	30/11/2022
Path:	C:\Windows\System32\wbem\WMIADAP.exe

Wow64 process (32bit):	false
Commandline:	wmiadap.exe /F /T /R
Imagebase:	0x7ff715590000
File size:	177664 bytes
MD5 hash:	9783D0765F31980950445DFD40DB15DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly