ID: 511702
Sample Name:
Md0q201V1D.exe
Cookbook: default.jbs
Time: 14:08:08
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

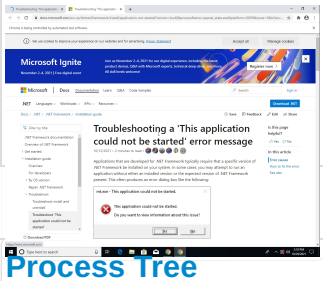
Windows Analysis Report Md0q201V1D.exe

Overview

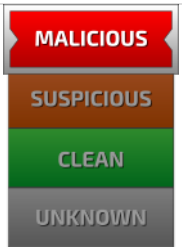
General Information

Sample Name:	Md0q201V1D.exe
Analysis ID:	511702
MD5:	a0bc297d8eaad3..
SHA1:	ac6858536f64ec7..
SHA256:	b06b803c1a6548..
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection



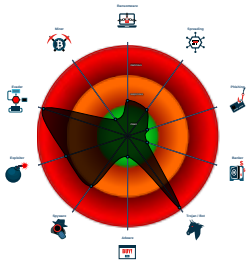
Raccoon RedLine SmokeLoader Vidar

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

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Vidar
- Yara detected SmokeLoader
- System process connects to networ…
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Found malware configuration
- Yara detected UAC Bypass using C…
- DLL reload attack detected

Classification



Process Tree

- **System is w10x64**
- Md0q201V1D.exe (PID: 6304 cmdline: 'C:\Users\user\Desktop\Md0q201V1D.exe' MD5: A0BC297D8EAAD37F1B145D108786E993)
  - Md0q201V1D.exe (PID: 5724 cmdline: 'C:\Users\user\Desktop\Md0q201V1D.exe' MD5: A0BC297D8EAAD37F1B145D108786E993)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 21.exe (PID: 2132 cmdline: C:\Users\user\AppData\Local\Temp\21.exe MD5: A0BC297D8EAAD37F1B145D108786E993)
        - 21.exe (PID: 808 cmdline: C:\Users\user\AppData\Local\Temp\21.exe MD5: A0BC297D8EAAD37F1B145D108786E993)
      - B096.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\B096.exe MD5: F57B28AEC65D4691202B9524F84CC54A)
        - aspnet_state.exe (PID: 4772 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe MD5: 3269806DC450E24113CF4FE03C3AD197)
          - chrome.exe (PID: 6016 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0' MD5: C139654B5C1438A95B321BB01AD63EF6)
            - chrome.exe (PID: 6128 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,3532224147046022434,3796046305070752020,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 1472 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0' MD5: C139654B5C1438A95B321BB01AD63EF6)
            - chrome.exe (PID: 3732 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1512,11815571981665026670,16401458370521835106,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1896 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - ServiceModelReg.exe (PID: 7320 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe MD5: FFF587A66B8D5A50A055B9CD6D632BEB)
          - chrome.exe (PID: 8084 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=ServiceModelReg.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0' MD5: C139654B5C1438A95B321BB01AD63EF6)
            - chrome.exe (PID: 6240 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,13203243795606022941,14762146736583605753,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 5744 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=ServiceModelReg.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0' MD5: C139654B5C1438A95B321BB01AD63EF6)
            - chrome.exe (PID: 7992 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,11199746608983669523,6532242252009539287,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
      - BBE1.exe (PID: 4756 cmdline: C:\Users\user\AppData\Local\Temp\BBE1.exe MD5: 787AF677D0C317E8062B9705CB64F951)
      - CBF0.exe (PID: 6000 cmdline: C:\Users\user\AppData\Local\Temp\CBF0.exe MD5: 73252ACB344040DDC5D9CE78A5D3A4C2)
      - DF3A.exe (PID: 5464 cmdline: C:\Users\user\AppData\Local\Temp\DF3A.exe MD5: 9FA070AF1ED2E1F07ED8C9F6EB2BDD29)
        - DF3A.exe (PID: 6180 cmdline: C:\Users\user\AppData\Local\Temp\DF3A.exe MD5: 9FA070AF1ED2E1F07ED8C9F6EB2BDD29)
      - EBBE.exe (PID: 1140 cmdline: C:\Users\user\AppData\Local\Temp\EBBE.exe MD5: 539C39A9565CD4B120E5EB121E45C3C2)
      - C066.exe (PID: 5604 cmdline: C:\Users\user\AppData\Local\Temp\C066.exe MD5: F0BE69176E592FA1A6345A7090A9EA30)
- gbhudtb (PID: 7044 cmdline: C:\Users\user\AppData\Roaming\gbhudtb MD5: A0BC297D8EAAD37F1B145D108786E993)
  - gbhudtb (PID: 3016 cmdline: C:\Users\user\AppData\Roaming\gbhudtb MD5: A0BC297D8EAAD37F1B145D108786E993)
- gbhudtb (PID: 5332 cmdline: C:\Users\user\AppData\Roaming\gbhudtb MD5: A0BC297D8EAAD37F1B145D108786E993)
  - gbhudtb (PID: 3796 cmdline: C:\Users\user\AppData\Roaming\gbhudtb MD5: A0BC297D8EAAD37F1B145D108786E993)
- bhhudtb (PID: 8080 cmdline: C:\Users\user\AppData\Roaming\bhhudtb MD5: 73252ACB344040DDC5D9CE78A5D3A4C2)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "45.9.20.149:10844"
  ],
  "Bot Id": ""
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://xacokuo8.top/",
    "http://hajezey1.top/"
  ]
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Vidar_2	Yara detected Vidar	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\DF3A.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x20735:$x1: https://cdn.discordapp.com/attachments/ • 0x207e9:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\B096.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7b593:$x1: https://cdn.discordapp.com/attachments/ • 0x7b647:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\DEDC.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7ae95:$x1: https://cdn.discordapp.com/attachments/ • 0x7af49:$x1: https://cdn.discordapp.com/attachments/ • 0x7affd:$x1: https://cdn.discordapp.com/attachments/ • 0x7b0b1:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\BBE1.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x43bf:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\D8D0.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x4443:$x1: https://cdn.discordapp.com/attachments/
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.326584645.0000000004DE1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000027.00000000.489693993.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000013.00000002.400930179.000000000201000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000027.00000000.488918061.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000013.00000002.400697119.000000000580000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
29.3.CBF0.exe.3080000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
39.0.DF3A.exe.ed0000.11.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x20735:$x1: https://cdn.discordapp.com/attachments/ • 0x207e9:$x1: https://cdn.discordapp.com/attachments/

Source	Rule	Description	Author	Strings
31.0.DF3A.exe.a40000.3.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x20735:$x1: https://cdn.discordapp.com/attachments/ • 0x207e9:$x1: https://cdn.discordapp.com/attachments/
24.0.B096.exe.a00000.1.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7b593:$x1: https://cdn.discordapp.com/attachments/ • 0x7b647:$x1: https://cdn.discordapp.com/attachments/
24.2.B096.exe.a00000.0.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7b593:$x1: https://cdn.discordapp.com/attachments/ • 0x7b647:$x1: https://cdn.discordapp.com/attachments/
Click to see the 62 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Exploits:

Yara detected UAC Bypass using CMSTP

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Deletes itself after installation

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

Renames NTDLL to bypass HIPS

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Vidar

Yara detected SmokeLoader

Yara detected Raccoon Stealer

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected Vidar

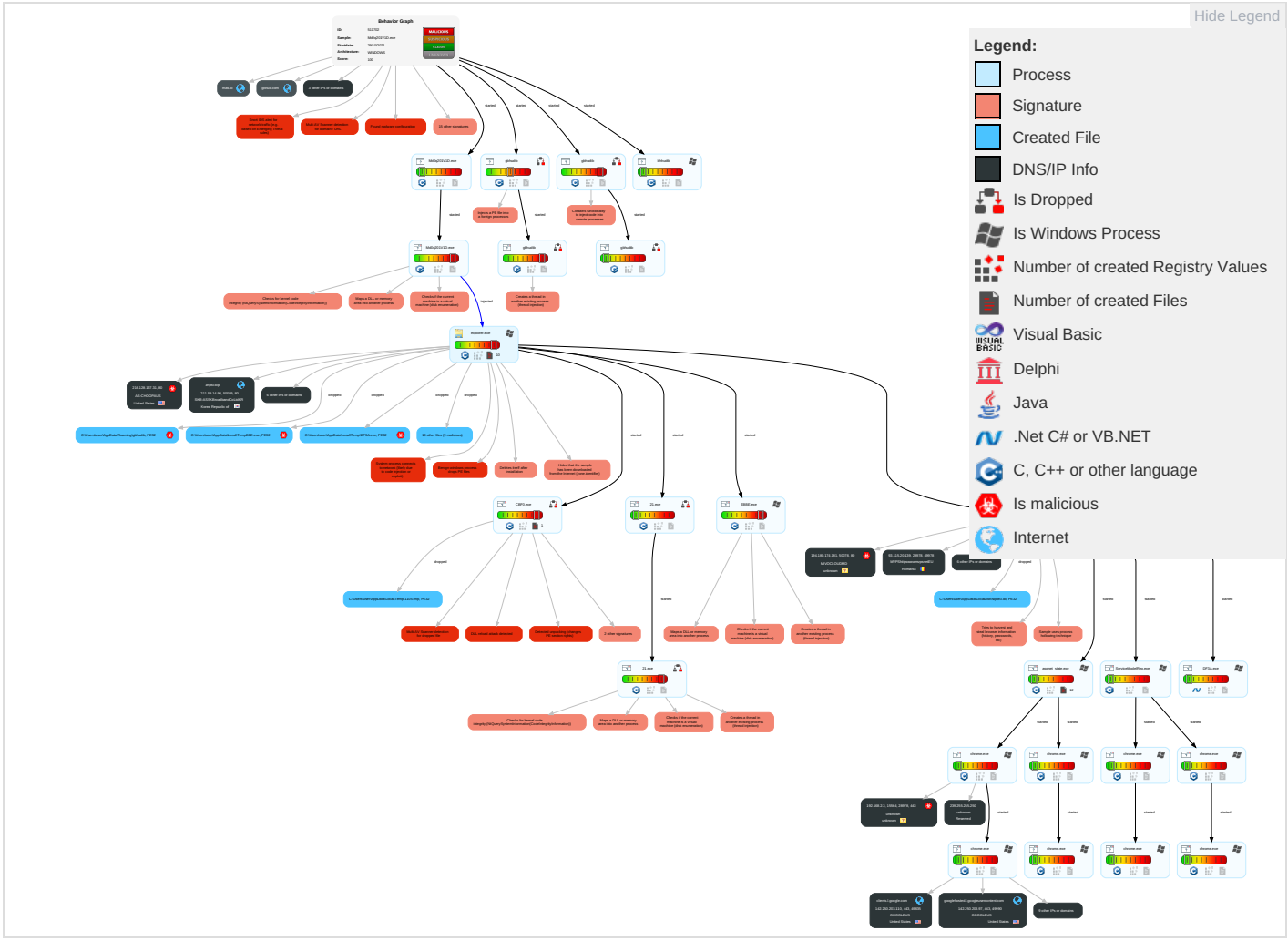
Yara detected SmokeLoader

Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Native API 1	DLL Side-Loading 1 1	DLL Side-Loading 1 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 3 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 6 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoc

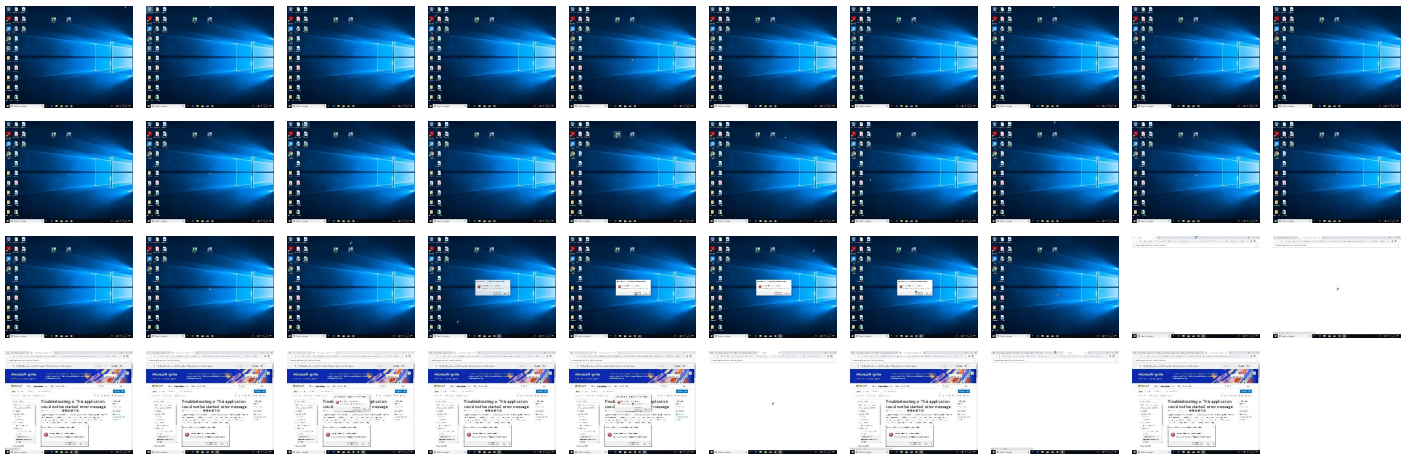
Behavior Graph

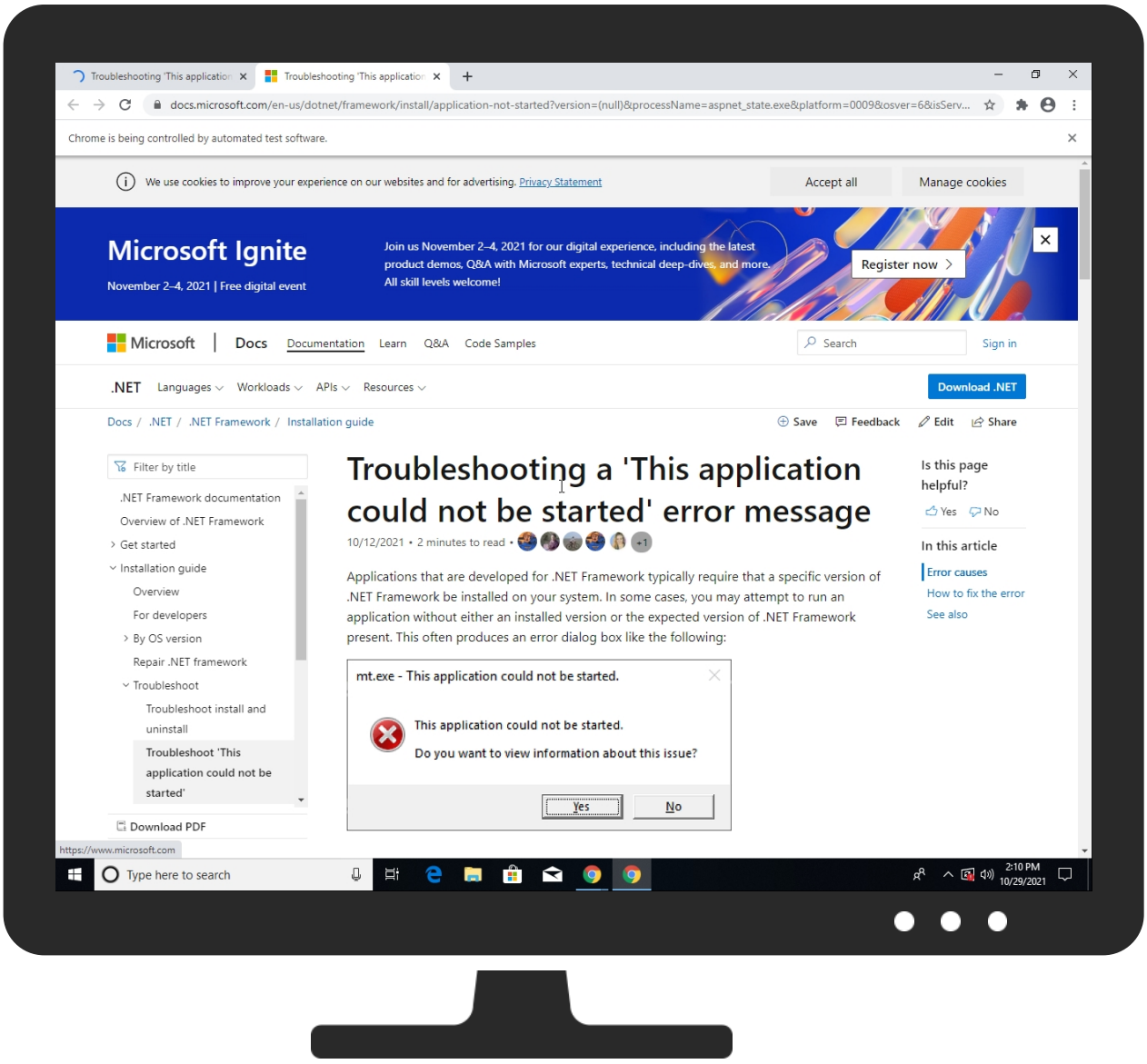


Screenshots

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
Md0q201V1D.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1105.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1105.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\BBE1.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.CrypterX	
C:\Users\user\AppData\Local\Temp\CAC5.exe	55%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\CBF0.exe	80%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\CD17.exe	14%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Local\Temp\D8D0.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\DF3A.exe	43%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.3.EBBE.exe.2d30000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.ServiceModelReg.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
40.0.ServiceModelReg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
19.0.21.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Md0q201V1D.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.gbhudtb.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.21.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.DF3A.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
40.0.ServiceModelReg.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
39.0.DF3A.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
20.1.gbhudtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.gbhudtb.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.EBBE.exe.2d20e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.CBF0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.Md0q201V1D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.DF3A.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
3.2.Md0q201V1D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
45.1.bhhudtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.gbhudtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.CBF0.exe.3070e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.ServiceModelReg.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
29.1.CBF0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.ServiceModelReg.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
3.0.Md0q201V1D.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.EBBE.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.aspnet_state.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
14.2.gbhudtb.2be15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.DF3A.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
0.2.Md0q201V1D.exe.2d815a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.gbhudtb.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.21.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
29.3.CBF0.exe.3080000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.gbhudtb.2cb15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.gbhudtb.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.21.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.gbhudtb.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.gbhudtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.aspnet_state.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
19.0.21.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
30.0.aspnet_state.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
40.2.ServiceModelReg.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
30.0.aspnet_state.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
19.0.21.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.1.gbhudtb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.21.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.0.DF3A.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
20.0.gbhudtb.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.21.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
30.0.aspnet_state.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
30.0.aspnet_state.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1141492		Download File
19.0.21.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.Md0q201V1D.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.21.exe.2cc15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/DetailsDataSet1.xsd	0%	Avira URL Cloud	safe	
http://sysaheu90.top/game.exe	16%	Virustotal		Browse
http://sysaheu90.top/game.exe	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://65.108.80.190/936	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://privacytoolzforyou-6000.top/downloads/toolspab2.exe	100%	Avira URL Cloud	malware	
http://65.108.80.190/mozglue.dll	0%	URL Reputation	safe	
http://65.108.80.190/freebl3.dll	0%	URL Reputation	safe	
http://https://mdec.nelreports.net/api/report?cat=mdocs	0%	Avira URL Cloud	safe	
http://65.108.80.190/nss3.dll	0%	URL Reputation	safe	
http://65.108.80.190/softokn3.dll	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://194.180.174.181//l/f/SZ0UyXwB3dP17Spzhll9/44498d94a24300ea08dae81ac5b8f477f8279a65	0%	Avira URL Cloud	safe	
http://194.180.174.181//l/f/SZ0UyXwB3dP17Spzhll9/cb2d375dd6e8a66a5a24666f2ccf0d937c972efe	0%	Avira URL Cloud	safe	
http://toptelete.top/agrybirdsgamerept	100%	Avira URL Cloud	malware	
http://193.56.146.214/	0%	Avira URL Cloud	safe	
http://xacokuo8.top/	100%	Avira URL Cloud	malware	
http://hajezey1.top/	100%	Avira URL Cloud	malware	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://nusurtal4f.net/	0%	Avira URL Cloud	safe	
http://znpst.top/dl/buildz.exe	100%	Avira URL Cloud	malware	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://65.108.80.190/706	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://194.180.174.181/	0%	Avira URL Cloud	safe	
http://65.108.80.190/	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://65.108.80.190/vcruntime140.dll	0%	URL Reputation	safe	
http://65.108.80.190/msvcp140.dll	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iyc.jelikob.ru	81.177.141.36	true	false		high
accounts.google.com	172.217.168.45	true	false		high
avatars.githubusercontent.com	185.199.109.133	true	false		high
github.com	140.82.121.4	true	false		high
mas.to	88.99.75.82	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
znpst.top	211.59.14.90	true	false		high
nusurtal4f.net	45.141.84.21	true	false		high
privacytoolzforyou-6000.top	5.188.88.203	true	false		high
toptelete.top	172.67.160.46	true	false		high
api.2ip.ua	77.123.139.190	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
hajezey1.top	5.188.88.203	true	false		high
sysaheu90.top	5.188.88.203	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
js.monitor.azure.com	unknown	unknown	false		high
xacokuo8.top	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
telegalive.top	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sysaheu90.top/game.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://65.108.80.190/936	false	• Avira URL Cloud: safe	unknown
http://privacytoolzforyou-6000.top/downloads/toolspab2.exe	true	• Avira URL Cloud: malware	unknown
http://65.108.80.190/mozglue.dll	false	• URL Reputation: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://65.108.80.190/freebl3.dll	false	• URL Reputation: safe	unknown
http://65.108.80.190/nss3.dll	false	• URL Reputation: safe	unknown
http://65.108.80.190/softokn3.dll	false	• URL Reputation: safe	unknown
http://194.180.174.181//l/f/SZ0UyXwB3dP17Spzhll9/44498d94a24300ea08dae81ac5b8f477f8279a65	true	• Avira URL Cloud: safe	unknown
http://194.180.174.181//l/f/SZ0UyXwB3dP17Spzhll9/cb2d375dd6e8a66a5a24666f2ccf0d937c972efe	true	• Avira URL Cloud: safe	unknown
http://toptelete.top/agrybirdsgamerept	true	• Avira URL Cloud: malware	unknown
http://193.56.146.214/	false	• Avira URL Cloud: safe	unknown
http://xacokuo8.top/	true	• Avira URL Cloud: malware	unknown
http://hajezey1.top/	true	• Avira URL Cloud: malware	unknown
http://nusurtal4f.net/	false	• Avira URL Cloud: safe	unknown
http://znpst.top/dl/buildz.exe	true	• Avira URL Cloud: malware	unknown
http://65.108.80.190/706	false	• Avira URL Cloud: safe	unknown
http://194.180.174.181/	true	• Avira URL Cloud: safe	unknown
http://65.108.80.190/	false	• URL Reputation: safe	unknown
http://65.108.80.190/vcruntime140.dll	false	• URL Reputation: safe	unknown
http://65.108.80.190/msvcp140.dll	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
194.180.174.181	unknown	unknown		39798	MIVOCLOUDMD	true
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
162.159.130.233	unknown	United States		13335	CLOUDFLARENETUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
185.199.109.133	avatars.githubusercontent.com	Netherlands		54113	FASTLYUS	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
81.177.141.36	iyc.jelikob.ru	Russian Federation		8342	RTCOMM-ASRU	false
172.67.160.46	toptelete.top	United States		13335	CLOUDFLARENETUS	false
211.59.14.90	znpst.top	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
140.82.121.4	github.com	United States		36459	GITHUBUS	false
216.128.137.31	unknown	United States		20473	AS-CHOOPAUS	true
93.115.20.139	unknown	Romania		202448	MVPShttpswwwmvpsnetEU	false
45.141.84.21	nusurtal4f.net	Russian Federation		206728	MEDIALAND-ASRU	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
5.188.88.203	privacytoolzforyou-6000.top	Russian Federation		34665	PINDC-ASRU	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511702
Start date:	29.10.2021

Start time:	14:08:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Md0q201V1D.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
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.troj.spyw.expl.evad.winEXE@74/167@62/20
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51.1% (good quality ratio 29.2%) • Quality average: 29% • Quality standard deviation: 30.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:09:40	Task Scheduler	Run new task: Firefox Default Browser Agent BF8D87ED27EA04ED path: C:\Users\user\AppData\Roaming\gbhudtb
14:10:34	API Interceptor	7x Sleep call for process: C066.exe modified
14:10:57	Task Scheduler	Run new task: Firefox Default Browser Agent A4EC042678D4669E path: C:\Users\user\AppData\Roaming\bhhudtb
14:11:02	Task Scheduler	Run new task: Firefox Default Browser Agent 621E197CCCA21806 path: C:\Users\user\AppData\Roaming\fehudtb
14:11:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\1ba0d279-1ad8-451e-a70f-de201594af59\C295.exe" --AutoStart
14:11:26	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\1ba0d279-1ad8-451e-a70f-de201594af59\C295.exe" --AutoStart
14:11:27	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\1ba0d279-1ad8-451e-a70f-de201594af59\C295.exe s>--Task
14:11:40	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\TelemetryServices\fodhelper.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\AQNoUsTOxr	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.7814144457324289
Encrypted:	false
SSDEEP:	96:dIQLKnlxKp2LK3IQkKylSK62kK0L62y7z3qU+bDoYysX0uhnydVjN9DLjGQLBE3M:962I+bDo3irhnydVj3XBBE3ud
MD5:	D9EB8022FD3B8EE752008BD119F0FBBB
SHA1:	32B613EFA72902BFB39EA6FF27B0E9F8D3985A33
SHA-256:	69858096A6332A75B2B491B0AB2DFD8359123FB17B794DD7BA84373DC34B1484
SHA-512:	87C58557D1D8E3DAA6053C5D4C7210378ADA090BA3EB22FE5306DFC234A98AB86EF7E212696CA6576072E535ECE3D6F1C44750843B555D773EBA4E29A1B619E7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\chrome_urls.txt	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1429
Entropy (8bit):	5.274877286745222
Encrypted:	false
SSDEEP:	24:MZTRbQJwlnu4EIfoMmQJwlnu4EjH9oMmQJwlnu4GTRbQJwlWu4gIfoMmQJwlWu4W:AlpMIQPM2P+lp9IQP92PE
MD5:	4347CC65785803494752CF2338D19AAB
SHA1:	B68A8009D28D1BC48DA8964FFC446696964058E9
SHA-256:	B217C805BAF5AA4D69E3BC4A51859827E613253E7B55CBCD3B07560D5C2115FA
SHA-512:	FDB0D5A4151C4C26B7E8BEC6A35A16DFAED941C5D3072D830A925EB83DBE731811F8C259BB36284FEC8BD86202DA5BB4E5E681F1819486FECCE7CDC2EF11960
Malicious:	false
Reputation:	unknown
Preview:	URL: http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0..Count: 2..Last visit: 2021-10-29 21:10:29.....URL: https://docs.microsoft.com/dotnet/framework/install/application-not-started?version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0..Count: 2..Last visit: 2021-10-29 21:10:29.....URL: https://docs.microsoft.com/en-us/dotnet/framework/install/application-not-started?version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0..Count: 2..Last visit: 2021-10-29 21:10:29.....URL: http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=ServiceModelReg.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0..Count: 2..Last visit: 2021-10-29 21:10:50.....URL: https://docs.microsoft.com/dot

C:\Users\user\AppData\LocalLow\fPT59QhKSGE.zip	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1841
Entropy (8bit):	7.634695689852965
Encrypted:	false
SSDEEP:	24:9jTO6RC/Ep21CPXRsy8zeRiByTkmKdLzGDz7ytNvN2bEVm3jWzuq1OSdFN5y6v88:9NCsMUXR1niBjjmP62QdzuKOW5y6F
MD5:	2C527C1F4D30880EA86DDE4C0CC1CD23
SHA1:	01FDEBB33BB4E6234DC360A7C895B8DD4AC6EB8F
SHA-256:	C5F7E2C50ADD5B0D058EF07659A7E437B73516D652B7927B2698B64B5C3412B2
SHA-512:	58A4EB7CB8E5B2F2C4BEEE3A2FCF16D5B30B83097638D914B43C422D975F78EAEFD08C9ACE05D65106BED87042AB7F08AC301DCA501DB700580EA971E8C761F1
Malicious:	false
Reputation:	unknown
Preview:	PK.....q]S.....*...browsers/cookies/Google Chrome_Default.txtUT.....|a..|a..|a..Kk.1...2.ox7.....b....FJD.3.Fi0..G.iZ(iR.JH.{.{.....`.0.>..%7..))..%.rY{.....X.....FJ.f8...+c..B.3.K..j..''...b%Z.k.....Vf.V!....!$.R1 ...../O.-h..G.e..VZX.....W.....O...vQ....n.8.Z/@0..+.T.....A^Q".{g.H..9..Km4.....\|..+.='..w.....s._.z..5)..x.:.u).O.`.eK,W.....ZU c.P..jl.RFr-.=..&lF7..F.>.w...4..h..uy].... ..h.x.q.7..R.R.c...C.R.~L...\ .p2.p.z.m...y...Oi7~(.._4-...~HE~.....PK.....q]S.....browsers/chrome_urls.txtUT.....\|a..\|a..\|a..Ok. ...{!.!'....v. ....a.6...Z.1.....<....g..W.>.Wa..y...`.....9....t\L.;J.&...W....}....a.<!%....g.m.\|y\.g.z.....(>.e..2....y+$@.;.88#....2.g....Z.1B..0|{.....^u.YH>&cZ.$....*-..CH...p$..(.2-hEIU .I2.k.a..o..O.....>F<Y....Zc.V.....Y..A6.?'.&..?9/...\.F..}?...|..-..|1..PK.....q]S.....=.....System Info.txtUT.....|a..|a..|auS.n.0.<.@.a.2..$...S.W.6N..A.\.Fbl"2).R^..w..nr.a...p.; ...Ea....HB8x..

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.4334508710755112
Encrypted:	false
SSDEEP:	96:dNwf2WtfkjzS8NhV2Q0Ch32uwnnihkKLdH2Qf2:du5wEkhGhBH
MD5:	4A5E8FB665F7F9C276B38C5CFBD15D10
SHA1:	A0DF8F94A3A67B03A569A25A0658104A7915E029
SHA-256:	E095AE577F462636A5DB3107A1033540E1695071DCC03405422651D391339AA8
SHA-512:	492F3F1350E5F52CC80D62CD26EEE984E6C98444F55CDF75824263CA19EA9FF0834D74394104D655F209DFF88FB49B74BDE3C941978E88AC2A4644498AC14250
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\C066.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."..... @.0@.idata..H.....@.0..CRT.....@.0..tls.... .....@.0..rsrc..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\13c08b90-0c19-4b85-83da-a9c4dd83285c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96740
Entropy (8bit):	3.75005252311946
Encrypted:	false
SSDEEP:	384:2K34dqKZGMX8OPsvvV4+lENtrevx73CV7+Hv6GOxrcfVhxCrD/SrApm4zcb1FlSg:5346K+59CX+Oge7tD3Q3rG/KxPNTr
MD5:	795ADA0AD7DFBD414E443CC12889C188
SHA1:	C5682B9CBEB5489E2B8DA1C0BDD0264CB90880B9
SHA-256:	2FC2EECBF22C8AA6A370CBF0884B1C8627C9A2BEE6AC59FC769DE7E1FA95BB87
SHA-512:	ABE86A19820206AD6431C0758A59C578C5A859FD32AAE0751E5CBD2EFD73CE7AA9D0B6A7156FA0E15568F91C0EC8CE9DECA28B109FFF9B5E415B21D0248D8E0B
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\13c08b90-0c19-4b85-83da-a9c4dd83285c.tmp	
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....I8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\17b6b034-6ccd-4bbe-8ead-8ffd7655270a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185224
Entropy (8bit):	6.0767786021951835
Encrypted:	false
SSDEEP:	3072:h8PLD8n55EtvVAkRNGWr9x39UfkT7RdOAD+FcbXafIB0u1GOJmA3iuRw:aPLD8Qtdf0S39U6TlUaqfIlUOoSiuRw
MD5:	FB20DB9CC2ECCF503196D173C40E506F
SHA1:	31D0BFFF97A8EAD257DAC75A19334A4269CC18EA
SHA-256:	41A240AD71C126200141586D587A7C211542BDD575B038DA91B7DC1AC5C37250
SHA-512:	CE04CF7A66FF3F14C76A76C530E66903DCAB52962979A66B2D280DD19072530282CA9F23B922DB6367D733A4A09583138B24A52F4E97320A55F027E9D543A6D4
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\3366f6f8-0dc7-4d25-b0cb-16ae790a8a61.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7494983911950053
Encrypted:	false
SSDEEP:	384:lK34dqZpX8OPsvvV4+lENtrevx73CV7+Hv6GOxrcfVhxCrD/SrApm4zcb1FlSO/h:k34ZK+59CX+Oge7tD3Q3rG/KxPNBd
MD5:	F24E50A646EF83AE65C4D3C84057E0E1
SHA1:	D0BC925FF3DCA80A088D30368CE65F90469FB451
SHA-256:	93DDEBD8F5655128F26C795AC39A3E6F1BED3A9C18A3CCED0CB758F27532BDA7
SHA-512:	D07C49BFB8036241196E30EC65130BD898F1D19F2B1DF28EFE26A49A0447DBD4787BBFE57EEB3B7A7FDFE440A535E4347323B0A29B201568DDCEF38787861E9
Malicious:	false
Reputation:	unknown
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....I8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3867d940-4f91-4cd9-bedf-1b681a77be65.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87023
Entropy (8bit):	6.102321908149239
Encrypted:	false
SSDEEP:	1536:SUuGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SUuFcbXafIB0u1GOJmA3iuR+
MD5:	04EA3ECF47F46C9AB073A1A8CAE1617E
SHA1:	062C6F716D0EE3126EB4C687FCA4F403DF7657B9
SHA-256:	53BC3171C0A8431E431E2DF17F7001AFD829930A31766D8898A81846A2992FA3
SHA-512:	84DBBDA70C2148B1FEDB2019519D5FF3BA18F4DB3CB7F218F0B9A140B86073C17BB303658132AEB6331682A48B887005C9C78B47755D5707A243465E8C8CC7E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\3867d940-4f91-4cd9-bedf-1b681a77be65.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\5298aac8-1da2-471d-8294-5dab686fcd20.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	176739
Entropy (8bit):	6.047238136544904
Encrypted:	false
SSDEEP:	3072:nLD8n55EtvVAkRNGWr9x39UfkT7RdOAD+FcbXafIB0u1GOJmA3iuRw:nLD8Qtdf0S39U6TlUaqfIlUOoSiuRw
MD5:	0A420CBFE79BE2CEAEAF4E46E41FE083
SHA1:	1B8E2EC3BDD26F1FC6D885F6477EE3970F4DE337
SHA-256:	92EE68E061C0E63F5C2FFAE49B08F8F043D39A755B6534C62EED4C2C36EFF2DB
SHA-512:	0E26A621E1D22EB7EE984D99629D0457199BB2A0C46A49D1C4391B5DD420C5874BD232B84A9D3A027D8FBA6B074661779053564DFE8B1CB5A7652E58E9DFD79
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799845608"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ebd71b0-feab-4966-8817-fc85f426ba9f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185223
Entropy (8bit):	6.076780431502545
Encrypted:	false
SSDEEP:	3072:hgLLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:mLLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	C6253FD173F227E4E7F1D3EE08B8F6E0
SHA1:	E47BBBFAEE3A8AB40D874B80A6567A1F29919548
SHA-256:	75D32CFD112422BB63CB13795D6E93350D085BB509A1DD2E380B202F2A9C32E7
SHA-512:	DC5CD4C2B983686ECF7DCD5A0AB3624AA95F59868B2D2CA23DC983D50576556090AEB3733F6BCA0D50C0962B64A7659321E4BA6055ADE9EE910BDEF0E8484B72
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ffecbc7-f9d0-4765-9d05-d84937d0bf6a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97460
Entropy (8bit):	3.7500740509204293
Encrypted:	false
SSDEEP:	384:sK34dqKZGMX8OPsvvV4+lENtrevx73CV7+Hv6GOxrcfVhxCrD/SrApm4Mqcb1Flm:T346K+59CXIOge7tD3Q3rG/KxPNTw
MD5:	6A8E3D13A5556A0CF18EE6B5E948051D
SHA1:	57301E22657F904D0F48AF9035004AB24AADAA66
SHA-256:	6D838678FA265E00EBDC97F464EC7201EF556914FC2D690088E0B59BC5D7FBC3
SHA-512:	AC6DBB5D4797D30B8191ED7329D46B537BA459E620468650E521D48FDE5DE62DB0DB3EC8D962E0C2C82DB19730A0BE25918BC0AB8B120DC2985C510D635A3F6
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ffecbc7-f9d0-4765-9d05-d84937d0bf6a.tmp	
Preview:	.|.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....I8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8ed402ed-9f0d-4bfa-a526-42c4e63459a4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	185223
Entropy (8bit):	6.076780431502545
Encrypted:	false
SSDEEP:	3072:hgLLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:mLLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	C6253FD173F227E4E7F1D3EE08B8F6E0
SHA1:	E47BBBFAEE3A8AB40D874B80A6567A1F29919548
SHA-256:	75D32CFD112422BB63CB13795D6E93350D085BB509A1DD2E380B202F2A9C32E7
SHA-512:	DC5CD4C2B983686ECF7DCD5A0AB3624AA95F59868B2D2CA23DC983D50576556090AEB3733F6BCA0D50C0962B64A7659321E4BA6055ADE9EE910BDEF0E8484E 72
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RF BBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppN r2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS 1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_man ager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftIE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6 CF
Malicious:	false
Reputation:	unknown
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\01ab4a26-c84a-4892-a73a-1a76565e8bda.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5193
Entropy (8bit):	4.979900818343623
Encrypted:	false
SSDEEP:	96:n8pCFcqX9pcKI1Vok0JCKL8aPQkNNMkZpbOTQVuwn:n8pCFF9pcj04Kukv/
MD5:	F40CC1605A6D5FAD4929C5FEFF714C6B
SHA1:	0D4E880D4BDD0DDF03591242FF448FF9ACB60719
SHA-256:	C70C793088B14C73D04D05D4518B31C5734DF395AA4062D5D07F8E4CD1412D51
SHA-512:	DB058CD1700DAB2993DAC4A4D94E0AABE937A0D43E190C4211F4A6A21D5136AB5B1389A19D71C91EBA86915869739D1B76EF7E4E7101327E5603C1EA1142EC1 2
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\01ab4a26-c84a-4892-a73a-1a76565e8bda.tmp	
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13280015426034104","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5f710deb-912f-40ef-aec8-6dfa68ef8525.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5193
Entropy (8bit):	4.978422207122921
Encrypted:	false
SSDEEP:	96:n8pCFc5I9pcKI1fok0JCKL8aTkjumbOTQVuwn:n8pCF/9pcja4KJkjL
MD5:	EE0754416F54375288C9950DAF72542A
SHA1:	F7EC603343910D680E0A9EE4416F3DF982F79598
SHA-256:	E148266E52AE28915E86890469C01CE201183E6991823382AB0A0FE6681550BA
SHA-512:	74DE81A3F44347423BF756953DF5DD52C4809EA29B7D745541C427131C08D03BE7AB7F200064F56E02557064EE848BD3A27EDE2D7A8A55A1679F00E7374D8E20
Malicious:	false
Reputation:	unknown
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13280015426034104","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d92133c-777e-4084-a984-5737bc2935d0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.57736597591648
Encrypted:	false
SSDEEP:	384:/cTtwLlG7Xk1kXqKf/pUZNCgVLH2HfDPrUdDLo4K:hLlAk1kXqKf/pUZNCgVLH2HfrrUBod
MD5:	C07E3F5EA2C2CC872B66432A983028A6
SHA1:	C5F107707761B9BCACF3F055267CC3FCB303312F
SHA-256:	5578698169AD8171E228B57F50FE7280EEBFE7E4896CC935AAEAFC16B8EB017C
SHA-512:	B59897A29DAD3A1BCB192CB8489825B9532D553C5820256AAA25EFE9B53CF5FFA5423AA0098EFE22C5CEB308A874CE858FAE08CFAB9213A24FB9B52D95C713C2
Malicious:	false
Reputation:	unknown
Preview:	

{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280015424813965","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.2131284716711255
Encrypted:	false
SSDEEP:	6:maEeRmdVOq2PWXp+N23iKKdK9RXXTZIFUtnEeRmdjXZmwBEeRmdQDkwOWXp+N23/:pv+Ova5Kk7XT2FUtnvq/Bv15f5Kk7XVJ
MD5:	24E9100145747BAA4C3889A9C5C206DB
SHA1:	0BB53B2828C801DA97F3BE448D10AFF8D9FB521D
SHA-256:	E9F670384287EAAC2342064D0B8264965BC55F9929700AD54D688A664D172BCC
SHA-512:	FC6F76775DA866E3C19147610B2BB0212899988DBC3C7B833EAF7CE962522402EBC8DFD142D6885AE196EC38BC8F69F2119BB5F59899094BB808CC0EBF39D98
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/10/29-14:10:44.182 8f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/10/29-14:10:44.184 8f4 Recovering log #3.2021/10/29-14:10:44.185 8f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old+. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.2131284716711255
Encrypted:	false
SSDEEP:	6:maEeRmdVOq2PWXp+N23iKKdK9RXXTZIFUtnEeRmdjXZmwBEeRmdQDkwOWXp+N23/:pv+Ova5Kk7XT2FUtnvq/Bv15f5Kk7XVJ
MD5:	24E9100145747BAA4C3889A9C5C206DB
SHA1:	0BB53B2828C801DA97F3BE448D10AFF8D9FB521D
SHA-256:	E9F670384287EAAC2342064D0B8264965BC55F9929700AD54D688A664D172BCC
SHA-512:	FC6F76775DA866E3C19147610B2BB0212899988DBC3C7B833EAF7CE962522402EBC8DFD142D6885AE196EC38BC8F69F2119BB5F59899094BB808CC0EBF39D98
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:44.182 8f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/10/29-14:10:44.184 8f4 Recovering log #3.2021/10/29-14:10:44.185 8f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.217993576664083
Encrypted:	false
SSDEEP:	6:maEeRm/4q2PWXp+N23iKKdKyDZIFUtnEeRmbZmwBEeRmKFkwOWXp+N23iKKdKyJd:pvLva5Kk02FUtnv4/BvnF5f5KkWJ
MD5:	FB49EA72F90C78269BF908408C05B028
SHA1:	C9A4A332D07F5E787841B0EAD9DCB6E0EBFB0F08
SHA-256:	1C9C62B45107367F1CB20F9AE47E8C4C097D314E3726F12E0FE94AD74BFAC518
SHA-512:	251C941212BCD389FE22885345A372F658DEE245AD8F0023FE8AD5350CA75111FD45E5DEABB668D8146C88C7CD81BFE44C8E109FB49DD06E9402C72C1EBB159
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:44.113 8f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/10/29-14:10:44.177 8f4 Recovering log #3.2021/10/29-14:10:44.178 8f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.217993576664083
Encrypted:	false
SSDEEP:	6:maEeRm/4q2PWXp+N23iKKdKyDZIFUtnEeRmbZmwBEeRmKFkwOWXp+N23iKKdKyJd:pvLva5Kk02FUtnv4/BvnF5f5KkWJ
MD5:	FB49EA72F90C78269BF908408C05B028
SHA1:	C9A4A332D07F5E787841B0EAD9DCB6E0EBFB0F08
SHA-256:	1C9C62B45107367F1CB20F9AE47E8C4C097D314E3726F12E0FE94AD74BFAC518
SHA-512:	251C941212BCD389FE22885345A372F658DEE245AD8F0023FE8AD5350CA75111FD45E5DEABB668D8146C88C7CD81BFE44C8E109FB49DD06E9402C72C1EBB159
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:44.113 8f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/10/29-14:10:44.177 8f4 Recovering log #3.2021/10/29-14:10:44.178 8f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Size (bytes):	13448
Entropy (8bit):	3.496787945228552
Encrypted:	false
SSDEEP:	96:34gHv2EhZk9Sly2gLThZk9Q78l4I2gLhhZk9Q78lwg8R2pLchZxo7plWK2pLEhZG:3HnE/DC9PNWStdSG
MD5:	C9C2061CD45FF26018679E016E8F308F
SHA1:	775E768E6E959030005BB9C5766B013037878423
SHA-256:	E1C44F7A439CDBFF47343B478E2DA39FB8C4BFE73D16420BA5A59EAD5F6166E8
SHA-512:	D844220BA9297BE2B1DA3673B058AA466EDB386EDEC17B721586B8DC4FB3CA7D0ED65BE9123FF2290CE4E96E74E0D0FF8C1EA02A81701634F3A1C03EB9E1A0 A7
Malicious:	false
Reputation:	unknown
Preview:	SNSS..!..1..,.......$...4325d4a0_5254_4d0f_a259_2eb450f69d61.....................%... ....5..0.......&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.......................!..1..,.......$...2d3ff34f_df6a_4e93_8e40 _05f7b18759b4......................y.....................................https://docs.microsoft.com/en-us/dotnet/framework/install/application-not-started?version=(null)&processNam e=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0..h.......`...h..A....i..A......... ...(..............................l.......h.t.t.p.s.:././.d.o.c.s...m.i.c.r.o.s.o.f.t...c.o.m./.e.n.-.u.s./.d.o.t.n.e.t./.f.r.a.m.e.w.o.r.k./.i.n.s.t.a.l.l./.a.p.p.l.i.c.a.t.i.o.n.-.n.o.t.-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWe:
MD5:	6C88FEEDEE47B405DCBB87ABEBC47027
SHA1:	C28B0EB68BAB44D7D6F514351A3BDFCD70A3941E
SHA-256:	153DDD24CD5DBCA43DC2071DDF4BE156DCBF32FB3338A2815023358A9740F708
SHA-512:	A78C7A534278ADF5D741C721D7109E0E421C3C43EF0E3E4265E9A9BA9AECD8E1FC14268183CE5CCA79523D1B1554AA29E708DF54023720D37929658359E242A
Malicious:	false
Reputation:	unknown
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5..... ....f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.232662299260004
Encrypted:	false
SSDEEP:	6:maEeXSmSVq2PWXp+N23iKKdK8NIFUtnEeXSYgZmwBEeXSzIkwOWXp+N23iKKdK8n:pvXSJVva5KkpFUtnvXSYg/BvXSzI5f5c
MD5:	E2040ED7DBD41A2D5AF72A9C334618CF
SHA1:	9628732D47A6E8B609562DA46C55E4DC820C891B
SHA-256:	CE2B8B548F018AEDDFD13EB20D76923E2D715239452D5ABC3B882C59C4D12DC3
SHA-512:	18DFC5AB6DBBEC50D6E19865103D8E65A31F315AF62B80A6353BAC950180721A52FA7D5D2F533F6C80C146F825313458C7367EF140477DC3A748094BFDA3DD5
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:27.505 8e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/10/29-14 :10:27.506 8e4 Recovering log #3.2021/10/29-14:10:27.507 8e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.232662299260004
Encrypted:	false
SSDEEP:	6:maEeXSmSVq2PWXp+N23iKKdK8NIFUtnEeXSYgZmwBEeXSzIkwOWXp+N23iKKdK8n:pvXSJVva5KkpFUtnvXSYg/BvXSzI5f5c
MD5:	E2040ED7DBD41A2D5AF72A9C334618CF
SHA1:	9628732D47A6E8B609562DA46C55E4DC820C891B
SHA-256:	CE2B8B548F018AEDDFD13EB20D76923E2D715239452D5ABC3B882C59C4D12DC3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
SHA-512:	18DFC5AB6DBBEC50D6E19865103D8E65A31F315AF62B80A6353BAC950180721A52FA7D5D2F533F6C80C146F825313458C7367EF140477DC3A748094BFDA3DD5
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:27.505 8e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/10/29-14 :10:27.506 8e4 Recovering log #3.2021/10/29-14:10:27.507 8e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	unknown
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.259827089317539
Encrypted:	false
SSDEEP:	6:maEeRWvUf4q2PWXp+N23iKKdK25+Xqx8chI+IFUtnEeRWlJZmwBEeRWlDkwOWXpi:pvv4va5KkTXfchI3FUtnvkJ/BvkD5f5G
MD5:	647AC9965A71591C224C5EFF662A5EC4
SHA1:	566B28A50B3159789A62B811842500274A9D3611
SHA-256:	AD79970F9BECA6486DDEBB9AEDD6139F616433DF2B6A39DAEA4C559CF6AFF6EA
SHA-512:	29F8F13DBF8D7AB3E51C39A390866C7B5728B7FBD12E275ED27679D8536205292A974DD368FDD690D59003DDCF2A52EF343865D0F53B49FCA6DBED8DA4A0A8B
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.804 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/10/29-14:10:43.805 1f24 Recovering log #3.2021/10/29-14:10:43.805 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.259827089317539
Encrypted:	false
SSDEEP:	6:maEeRWvUf4q2PWXp+N23iKKdK25+Xqx8chI+IFUtnEeRWlJZmwBEeRWlDkwOWXpi:pvv4va5KkTXfchI3FUtnvkJ/BvkD5f5G
MD5:	647AC9965A71591C224C5EFF662A5EC4
SHA1:	566B28A50B3159789A62B811842500274A9D3611
SHA-256:	AD79970F9BECA6486DDEBB9AEDD6139F616433DF2B6A39DAEA4C559CF6AFF6EA
SHA-512:	29F8F13DBF8D7AB3E51C39A390866C7B5728B7FBD12E275ED27679D8536205292A974DD368FDD690D59003DDCF2A52EF343865D0F53B49FCA6DBED8DA4A0A8B
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.804 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/10/29-14:10:43.805 1f24 Recovering log #3.2021/10/29-14:10:43.805 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.235089548406038
Encrypted:	false
SSDEEP:	6:maEeRWmT4q2PWXp+N23iKKdK25+XuoIFUtnEeRWmtJZmwBEeRWjSDkwOWXp+N23B:pv94va5KkTXYFUtnvjJ/BvDD5f5KkTXp
MD5:	56EF95D882EBCEC3586A7B36280E7B1D
SHA1:	69BA65F59A0BAF574B0B5C9D8C9722FACB9F1AC8
SHA-256:	FEA122246C951A3D386C8D328ED6D651438CFFF449AA2900EF4C17B593DBB35A
SHA-512:	A21F8E1F6A9BA052541739087B1CBDE98AB372239186D83863347AD29B618EBF3ED23ECA32AD6BBED4B67BE62265523468C699C34283180FD8C2CCC3DE6540A 0
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.796 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/10/29-14:10:43.798 1f24 Recovering log #3.2021/10/29-14:10:43.800 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.oldMS (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.235089548406038
Encrypted:	false
SSDEEP:	6:maEeRWmT4q2PWXp+N23iKKdK25+XuoIFUtnEeRWmtJZmwBEeRWjSDkwOWXp+N23B:pv94va5KkTXYFUtnvjJ/BvDD5f5KkTXp
MD5:	56EF95D882EBCEC3586A7B36280E7B1D
SHA1:	69BA65F59A0BAF574B0B5C9D8C9722FACB9F1AC8
SHA-256:	FEA122246C951A3D386C8D328ED6D651438CFFF449AA2900EF4C17B593DBB35A
SHA-512:	A21F8E1F6A9BA052541739087B1CBDE98AB372239186D83863347AD29B618EBF3ED23ECA32AD6BBED4B67BE62265523468C699C34283180FD8C2CCC3DE6540A 0
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.796 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/10/29-14:10:43.798 1f24 Recovering log #3.2021/10/29-14:10:43.800 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.270914232365926
Encrypted:	false
SSDEEP:	6:maEeRWfL4q2PWXp+N23iKKdKWT5g1IdqIFUtnEeRW6LJZmwBEeRWBbDkwOWXp+N4:pve4va5Kkg5gSRFUtnvZJ/BvUbD5f5Kg
MD5:	0FB81C78FB820C8320909DCF5CF3B43A
SHA1:	35E57E72C84512466ADB1506D2B65BAEB551E023
SHA-256:	2A37399DBE5FE2AEC984D072696CA3688A7A90EB125D3348B6BBBD67163F920C
SHA-512:	65A641930907EBF8217B1A7A1FE42CBF5CD796658D8B32F34D0AAB01A870302D79E17FBD16A8BAF9DD5A647FF2DB592507EB46B8CE4BE2A6005C8C8DE94A9C 6E
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.696 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/10/29-14:10:43.697 1f24 Recovering log #3.2021/10/29-14:10:43.698 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.270914232365926
Encrypted:	false
SSDEEP:	6:maEeRWfL4q2PWXp+N23iKKdKWT5g1IdqIFUtnEeRW6LJZmwBEeRWBbDkwOWXp+N4:pve4va5Kkg5gSRFUtnvZJ/BvUbD5f5Kg
MD5:	0FB81C78FB820C8320909DCF5CF3B43A
SHA1:	35E57E72C84512466ADB1506D2B65BAEB551E023
SHA-256:	2A37399DBE5FE2AEC984D072696CA3688A7A90EB125D3348B6BBBD67163F920C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
SHA-512:	65A641930907EBF8217B1A7A1FE42CBF5CD796658D8B32F34D0AAB01A870302D79E17FBD16A8BAF9DD5A647FF2DB592507EB46B8CE4BE2A6005C8C8DE94A9C6E
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:43.696 1f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/10/29-14:10:43.697 1f24 Recovering log #3.2021/10/29-14:10:43.698 1f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3007
Entropy (8bit):	6.085856219048523
Encrypted:	false
SSDEEP:	48:MYtYS6542D/rUPgdiGpqbZ7xPbD4wXesKsSPwm3Ublpu4KinJIQPu4KWx0HP2PuM:nt/6542D/UgojjPTeAMDUbl1KyJIQrKu
MD5:	99FE901287E08CE0B86EC5CE26DCCC49
SHA1:	AFAB5CB3FFCB646B38EE78D1918C89321E368EBD
SHA-256:	2AB9B6FF7AA534DEF87345363536C6FAF9B6E01A67739294870D5FAE4AB5A54B
SHA-512:	7EF515D3AF1524831706645DF9A2181440067BA10FC43770F6E5F497BE5060525C69438F234F0A48E240384FD3950E27521776259E70B8924693C348870E04E6
Malicious:	false
Reputation:	unknown
Preview:	....."......0..0009..0x409..11324..4.0.30319.0..4.5..6..applaunch2..application..aspnet..be..com..could..docs..exe..found..framework..fwlink..go..http..isserver..microsoft..net..not..noversion..null..o1..osver..platform..plcid..prd..processname..pver..sbp..shim..shimver..started..state..this..troubleshooting..version..dotnet..https..install..en..us*.....0.....0009.....0x409.....11324.....4.0.30319.0.....4.5.....6.....applaunch2.....application.....aspnet.....be.....com.....could.....docs.....dotnet.)....en.,....exe.....found.....framework.....fwlink.....go.....http.....https.*....install.+....isserver.....microsoft.....net.....not.....noversion.....null.....o1.....osver.....platform.....plcid.....prd.....processname.....pver. ....sbp.!....shim."....shimver.#....started.$....state.%....this.&....troubleshooting.'....us.-....version.(2.....0.....1.....2.....3.....4.....5.....6.....9.....a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	0.3283577581710296
Encrypted:	false
SSDEEP:	6:xQ94/fMt76Y4QZVRtRex99pG/VTqR4EZY4QZv8fO1:A4nMWQA9L/BQZ8fO1
MD5:	790A5E6E8A4AD043F767BCCE64D5E13F
SHA1:	4FCF9A7FAD71EBD6F5CF6D85FBD8EC846D305DDF
SHA-256:	84A0564FE257C6F916767D3334607B8425BDF7D8BDAC729519AB3D7AAF7832F2
SHA-512:	1E741C52BA7858118F0D8FBEB41D5FE88BB88464C8FF2D6B752113620412D3499A3A5DD9419E5059DC717142F354C0D62B84DDEE5DCAAE70BCDC6C4722C8942
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessiono (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13448
Entropy (8bit):	3.496787945228552
Encrypted:	false
SSDEEP:	96:34gHv2EhZk9Sly2gLThZk9Q78l4l2gLhhZk9Q78lwg8R2pLchZxo7plWK2pLEhZG:3HnE/DC9PNWStdSG
MD5:	C9C2061CD45FF26018679E016E8F308F
SHA1:	775E768E6E959030005BB9C5766B013037878423
SHA-256:	E1C44F7A439CDBFF47343B478E2DA39FB8C4BFE73D16420BA5A59EAD5F6166E8
SHA-512:	D844220BA9297BE2B1DA3673B058AA466EDB386EDEC17B721586B8DC4FB3CA7D0ED65BE9123FF2290CE4E96E74E0D0FF8C1EA02A81701634F3A1C03EB9E1A0A7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessiono (copy)	
Preview:	SNSS.....!.....1.,.....$...4325d4a0_5254_4d0f_a259_2eb450f69d61.....%..... .....5..0.....&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.....!.....1.,.....$...2d3ff34f_df6a_4e93_8e40 _05f7b18759b4.....y.....https://docs.microsoft.com/en-us/dotnet/framework/install/application-not-started?version=(null)&processNam e=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0.....h.....`.....h..A....i..A..... ...(.....l.....h.t.t.p.s.:./.d.o.c.s...m.i.c.r.o.s.o.f.t...c.o.m./.e.n.-.u.s./.d.o.t.n.e.t./.f.r.a.m.e.w.o.r.k./.i.n.s.t.a.l.l./.a.p.p.l.i.c.a.t.i.o.n.-.n.o.t.-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	0.5102847836765736
Encrypted:	false
SSDEEP:	48:Tbw/qALihje9kqL42WOT/9FUT+BwSfCAczwjDOIk:fOqAuhjspnWOvUT+BHKAcz5Ik
MD5:	383CFA774C903C6DC227EAD7C33DE1A8
SHA1:	C0EBB3958A3DD564A65FA5F543B162C76620F1A9
SHA-256:	B2320C476448462DC6006CC1F08ECA3DD30744943905CA32A6B9BC942C12138C
SHA-512:	095E2A8543DE9474A60A7CFCC08CE64610AB54C19E69EDF86EB7E62316061A17EEAAACFC738C82229A2A1CF70395288DA3862B3601054D67E10A2C224EA9BF8 7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>...,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5193
Entropy (8bit):	4.979900818343623
Encrypted:	false
SSDEEP:	96:n8pCFcqX9pcKI1Vok0JCKL8aPQkNNMkZpbOTQVuwn:n8pCFF9pcj04Kukv/
MD5:	F40CC1605A6D5FAD4929C5FEFF714C6B
SHA1:	0D4E880D4BDD0DDF03591242FF448FF9ACB60719
SHA-256:	C70C793088B14C73D04D05D4518B31C5734DF395AA4062D5D07F8E4CD1412D51
SHA-512:	DB058CD1700DAB2993DAC4A4D94E0AABE937A0D43E190C4211F4A6A21D5136AB5B1389A19D71C91EBA86915869739D1B76EF7E4E7101327E5603C1EA1142EC1 2
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280015426034104","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	36864
Entropy (8bit):	0.7701922072347449
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU1cEB/AlIoTRs5:wIElwQF8mpcSas/Al7sW53Cdfv1
MD5:	4C839CB756F3977AE4919050136908C0
SHA1:	37E09C0373575A74B728DBA090B91FD9D509DB30
SHA-256:	4ADCD04D296DD666A40878C409AF87E3489CDAD195C56880B45BCF0F1904A020
SHA-512:	03395D8245570BD9788D0078F27D888FD7BC9993518CCA9FB5CBF8C251018E74B3040226CD6310D248146D3E7C087919C8A28E25188EDE9E281637BC3E89C68A
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3......@ ....C..........g...^.........j.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.57736597591648
Encrypted:	false
SSDEEP:	384:/cTtwLlG7Xk1kXqKf/pUZNCgVLH2HfDPrUdDLo4K:hLlAk1kXqKf/pUZNCgVLH2HfrrUBod
MD5:	C07E3F5EA2C2CC872B66432A983028A6
SHA1:	C5F107707761B9BCACF3F055267CC3FCB303312F
SHA-256:	5578698169AD8171E228B57F50FE7280EEBFE7E4896CC935AAEAFC16B8EB017C
SHA-512:	B59897A29DAD3A1BCB192CB8489825B9532D553C5820256AAA25EFE9B53CF5FFA5423AA0098EFE22C5CEB308A874CE858FAE08CFAB9213A24FB9B52D95C713 C2
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280015424813965","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17092
Entropy (8bit):	5.583181891141964
Encrypted:	false
SSDEEP:	384:/cTtpLlG7Xk1kXqKf/pUZNCgVLH2HfDPrUPDLWo4h:WLlAk1kXqKf/pUZNCgVLH2HfrrUuoO
MD5:	FBB21F03F922068D76A443D7681BC18A
SHA1:	559BEFF9C85046840A57211712D2F54AE125D95B
SHA-256:	B20A825A2AF7FB06E581B754DCAD60260DD1329A2A6A355B8A0687D00D810F7A
SHA-512:	1C19F702C12476ED0DCD5FB569CF9A185C6818C878C3C5D8321D6D430B81B39AF5CB9BCED104A95AAA1279E236317D61A76301F6779E9B5449BE211CD10CE5 B
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.. (copy)	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280015424813965","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I58
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	unknown
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.265905370390252
Encrypted:	false
SSDEEP:	6:maEeRUyAq2PWXp+N23iKKdKusNpZQMxIFUtnEeRUbZmwBEeRU4kwOWXp+N23iKK+:pvyyAva5KkMFUtnvyb/Bvy45f5KkTJ
MD5:	D4586C20AA021CDF26D8393D5FDFC9A3
SHA1:	B10541B4CA058DB10D427CB68B0815C76CE652E5
SHA-256:	A9793BD0271D2953FA1F44CEB74A349F5384644528FC346AB141BD42D0BDDA2C
SHA-512:	4E8C83708D7AFEF6B59488A106CE3CF2C389E5EC11495BA113DEFECA9087E8A6CCD85C36F871A9D14FA412C617E54EECA6797AC00680FDA0CB59251F94D2E/ 09
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:41.764 df0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/10/29-14:10:41.765 df0 Recovering log #3.2021/10/29-14:10:41.766 df0 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldos (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.265905370390252
Encrypted:	false
SSDEEP:	6:maEeRUyAq2PWXp+N23iKKdKusNpZQMxIFUtnEeRUbZmwBEeRU4kwOWXp+N23iKK+:pvyyAva5KkMFUtnvyb/Bvy45f5KkTJ
MD5:	D4586C20AA021CDF26D8393D5FDFC9A3
SHA1:	B10541B4CA058DB10D427CB68B0815C76CE652E5
SHA-256:	A9793BD0271D2953FA1F44CEB74A349F5384644528FC346AB141BD42D0BDDA2C
SHA-512:	4E8C83708D7AFEF6B59488A106CE3CF2C389E5EC11495BA113DEFECA9087E8A6CCD85C36F871A9D14FA412C617E54EECA6797AC00680FDA0CB59251F94D2E/ 09
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:41.764 df0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/10/29-14:10:41.765 df0 Recovering log #3.2021/10/29-14:10:41.766 df0 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\f3f072f8-9740-417a-a88b-dfe93adcb8b1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac7d1c27-d7ae-4dfb-862c-070a5827ea1e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	17092
Entropy (8bit):	5.583181891141964
Encrypted:	false
SSDEEP:	384:/cTtpLlG7Xk1kXqKf/pUZNCgVLH2HfDPrUPDLWo4h:WLlAk1kXqKf/pUZNCgVLH2HfrrUuoO
MD5:	FBB21F03F922068D76A443D7681BC18A
SHA1:	559BEFF9C85046840A57211712D2F54AE125D95B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac7d1c27-d7ae-4dfb-862c-070a5827ea1e.tmp	
SHA-256:	B20A825A2AF7FB06E581B754DCAD60260DD1329A2A6A355B8A0687D00D810F7A
SHA-512:	1C19F702C12476ED0DCD5FB569CF9A185C6818C878C3C5D8321D6D430B81B39AF5CB9BCED104A95AAA1279E236317D61A76301F6779E9B5449BE211CD10CE5B
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280015424813965","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.460609817731167
Encrypted:	false
SSDEEP:	3:tUKj5U5MfRUcF30yZmwv2S5U5MfRXVNFWSV8tS5U5MfRXVNFWSWGv:maEeRUIZmwBEeRMSVhEeRMStv
MD5:	ED595A3BDACDE073C1297DF727DBC4D0
SHA1:	0D273E01F6A8B0C77892ADAD1909650E61A9EF77
SHA-256:	56550BDC600F9DD8BB9134E4F954A9D1FC0939DA04F22FDD38B110BFB0866D6E
SHA-512:	2A40594973C8947C63CFDB071F266413747CF19C424EFC121C5EDD6854C34D373950446D8301FDFFBECF2FF4F621CC25BEDE0EE948E4160B1C7AF7D9FF8BBAB
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:41.124 8f4 Recovering log #3.2021/10/29-14:10:42.682 8f4 Delete type=0 #3.2021/10/29-14:10:42.682 8f4 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.460609817731167
Encrypted:	false
SSDEEP:	3:tUKj5U5MfRUcF30yZmwv2S5U5MfRXVNFWSV8tS5U5MfRXVNFWSWGv:maEeRUIZmwBEeRMSVhEeRMStv
MD5:	ED595A3BDACDE073C1297DF727DBC4D0
SHA1:	0D273E01F6A8B0C77892ADAD1909650E61A9EF77
SHA-256:	56550BDC600F9DD8BB9134E4F954A9D1FC0939DA04F22FDD38B110BFB0866D6E
SHA-512:	2A40594973C8947C63CFDB071F266413747CF19C424EFC121C5EDD6854C34D373950446D8301FDFFBECF2FF4F621CC25BEDE0EE948E4160B1C7AF7D9FF8BBA B
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:41.124 8f4 Recovering log #3.2021/10/29-14:10:42.682 8f4 Delete type=0 #3.2021/10/29-14:10:42.682 8f4 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	unknown
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e693ec52-2d0e-4227-8774-954423d894b9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	unknown
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ee68a962-742b-43eb-93af-8db2e86d8ed6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5193
Entropy (8bit):	4.977948195597817
Encrypted:	false
SSDEEP:	96:n8pCFc5I9pcKI1fok0JCKL8aTkjuzbOTQVuwn:n8pCF/9pcja4KJkjA
MD5:	403C2C47933957AA76729FEE38AAC01B
SHA1:	5A82E7091A8D5BFC88A4B52F309D5165A5203B2E
SHA-256:	8BFECC26C3A718F73B8D4EEA149967FF700177190CC8A1F4304286A337C348F6
SHA-512:	2DABEEC46ECDC95366EFEAEDD6A676B71FAD3605DC851839DA9434A4F48D302DBDAA7934219910F3F623273DAC59488A22F1A269E54F3E29F2B700F599185AI F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ee68a962-742b-43eb-93af-8db2e86d8ed6.tmp	
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280015426034104","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f13931a8-f7f2-4c5b-8012-fa5bd2fcc868.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2151
Entropy (8bit):	4.89628161613295
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qz5sCGsQRLsC2HZrsysAMyKs4MHKsmMHgzYhbD:JTnOCXGDHazpCmZrsOM9GIG9hH
MD5:	906A257501BB067F8C7EC0583389BD7E
SHA1:	3EB950BD6BBE5D2BD5BBF5AAB211A306295062FF
SHA-256:	E3221CD0FCEA91239BC8428F5F1661EDFCC2D8E4E019212552E4D5487FE824B3
SHA-512:	DE030BD9541604557042C7CC3CF3DCF0DDEA5FF00D0CF7198D2AA4CD1F0829D791E22D75B41C05BA23AC23ADFCE39712A6E2F4E2958A73C1E4A41A5352D49 B
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation": [],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.c om","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[50],"expiration":"13282607428238388","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"}, {"alternative_service":[{"advertised_versions":[50],"expiration":"13282607428244406","port":443,"protocol_str":"quic"}],"isol

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f4c1d6ea-25cd-46c1-a120-5b8b54342841.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.126205610080349
Encrypted:	false
SSDEEP:	6:maEeR2q2PWXp+N23iKKdKfrzAdIFUtnEeRsBZmwBEeRsbkwOWXp+N23iKKdKfrzS:pvkva5Kk9FUtnvqB/Bvqb5f5Kk2J
MD5:	BC3D75492A9CEDB07489A2B2AA0896C0
SHA1:	4571A89962260C4A10B0054E3E1235507887E42D
SHA-256:	2B82B394BCCEB5A449A994A8AC220A776B1D42CAD16D41A8CFBA9D18ADDA97B9
SHA-512:	BB625611546CAD40183386B96C2A256DC84A25F91937E1CD4F9BE40824CF2FDA6A12AB7AD2C7BD066432B46417E0F154703C3EA132C40C2D087EFED559A0014
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/10/29-14:10:44.200 df0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/10/29-14:10:44.201 df0 Recovering log #3.2021/10/29-14:10:44.201 df0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old8f (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.126205610080349
Encrypted:	false
SSDEEP:	6:maEeR2q2PWXp+N23iKKdKfrzAdIFUtnEeRsBZmwBEeRsbkwOWXp+N23iKKdKfrzS:pvkva5Kk9FUtnvqB/Bvqb5f5Kk2J
MD5:	BC3D75492A9CEDB07489A2B2AA0896C0
SHA1:	4571A89962260C4A10B0054E3E1235507887E42D
SHA-256:	2B82B394BCCEB5A449A994A8AC220A776B1D42CAD16D41A8CFBA9D18ADDA97B9
SHA-512:	BB625611546CAD40183386B96C2A256DC84A25F91937E1CD4F9BE40824CF2FDA6A12AB7AD2C7BD066432B46417E0F154703C3EA132C40C2D087EFED559A0014
Malicious:	false
Reputation:	unknown
Preview:	2021/10/29-14:10:44.200 df0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/10/29-14:10:44.201 df0 Recovering log #3.2021/10/29-14:10:44.201 df0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\GrShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018238520723782249
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zELqCjtl:/M/xT02zSBl
MD5:	4D6A87B837034502A12B3821F7C67DB9
SHA1:	2D9AEFD5997E23FA1AC4FCD4F3BEF29FB8514207
SHA-256:	774273543D373714C0F766A844038E50D14A69C70281883599D0EF65F7E10D92
SHA-512:	599B9EF531293B6AE2D99E2F105E0A5ECE1AD8CF998FD0F14B812A62080527B0AC4BB67970E761D05B6CB5C1ED5AC3D313E05812E7BEF20AFD1FAC7394B797D8
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	unknown
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4(
Malicious:	false
Reputation:	unknown
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185223
Entropy (8bit):	6.076780072694005
Encrypted:	false
SSDEEP:	3072:hrFLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:pFLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	9A3435BB2916D49F5662DF2DF9B0234A
SHA1:	7FB511EA0AB19F8497578647E031083111A67A9C
SHA-256:	BFD8A4F5CCA6D59405E9D0E4FFDB32E8A37EAFBAF1855AE9F4FD57DABD10CCBA
SHA-512:	9CE8ECCD4AF9E34CC3FAF9F8BE21E3B591140366FC947FDB8238AD2C0808C8AEA7FD0FB91B67A1F2F50F644793DC6A328EEC02D4E9C8C12BA6DE2F0B997B9BB2
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State2. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87023
Entropy (8bit):	6.102321908149239
Encrypted:	false
SSDEEP:	1536:SUuGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SUuFcbXafIB0u1GOJmA3iuR+
MD5:	04EA3ECF47F46C9AB073A1A8CAE1617E
SHA1:	062C6F716D0EE3126EB4C687FCA4F403DF7657B9
SHA-256:	53BC3171C0A8431E431E2DF17F7001AFD829930A31766D8898A81846A2992FA3
SHA-512:	84DBBDA70C2148B1FEDB2019519D5FF3BA18F4DB3CB7F218F0B9A140B86073C17BB303658132AEB6331682A48B887005C9C78B47755D5707A243465E8C8CC7E5
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185223
Entropy (8bit):	6.076780431502545
Encrypted:	false
SSDEEP:	3072:hgLLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:mLLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	C6253FD173F227E4E7F1D3EE08B8F6E0
SHA1:	E47BBBFAEE3A8AB40D874B80A6567A1F29919548

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
SHA-256:	75D32CFD112422BB63CB13795D6E93350D085BB509A1DD2E380B202F2A9C32E7
SHA-512:	DC5CD4C2B983686ECF7DCD5A0AB3624AA95F59868B2D2CA23DC983D50576556090AEB3733F6BCA0D50C0962B64A7659321E4BA6055ADE9EE910BDEF0E8484E 72
Malicious:	false
Reputation:	unknown
Preview:	 {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statet (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87023
Entropy (8bit):	6.102321908149239
Encrypted:	false
SSDEEP:	1536:SUuGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SUuFcbXafIB0u1GOJmA3iuR+
MD5:	04EA3ECF47F46C9AB073A1A8CAE1617E
SHA1:	062C6F716D0EE3126EB4C687FCA4F403DF7657B9
SHA-256:	53BC3171C0A8431E431E2DF17F7001AFD829930A31766D8898A81846A2992FA3
SHA-512:	84DBBDA70C2148B1FEDB2019519D5FF3BA18F4DB3CB7F218F0B9A140B86073C17BB303658132AEB6331682A48B887005C9C78B47755D5707A243465E8C8CC7E
Malicious:	false
Reputation:	unknown
Preview:	 {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5c47e94-90e2-4413-9940-476700670340.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185224
Entropy (8bit):	6.076777172710909
Encrypted:	false
SSDEEP:	3072:h9cLD8n55EtvVAkRNGWr9x39UfkT7RdOAD+FcbXafIB0u1GOJmA3iuRw:vcLD8Qtdf0S39U6TlUaqfIlUOoSiuRw
MD5:	C005E1F8BBDB08BD8E31B8EFD5A481E3
SHA1:	CEF1835073662B631533BBBF9FD323D877FF6F4C
SHA-256:	4D12801559358F65B0327E9C6A83479734B92E8FC3002A6C2EA17711D5A577ED
SHA-512:	C4DB8A3CF32103BCD2EB3AB86B5F9FE24A82CD495751DE273A987894CFC401139DD6D506DD21BF09750A69B5E285746EE20BE48AD9B597C5FA2EF1ABFCD72 74
Malicious:	false
Reputation:	unknown
Preview:	 {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ba54649f-ae69-496b-a2e4-8ef3e2285261.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749334477100088
Encrypted:	false
SSDEEP:	384:7K34dqZpX8O7vYlENtrevx73CV7+Hv6GOxrcfVhxCrD/SrApm4zcb1FlSO//VNMp:W34o+59CX+Oge7tD3Q3rG/KxPNBm
MD5:	B737DC295F256C510B59268D288E2D10
SHA1:	8B19D8F23BE9C56F483DC60E34B43420A076358E

C:\Users\user\AppData\Local\Google\Chrome\User Data\ba54649f-ae69-496b-a2e4-8ef3e2285261.tmp	
SHA-256:	6BE0B7FE791BEEC2CDAEDFF948422F2047D5B982D70ABA87D52BB08E4649203C
SHA-512:	34256F525C39C13A1002FD6B99DC2E20B278059041D061D4741672F7ED1E6F803616EAD3FC36F17640B3C115AEC0920D992E7F679B3EC31E0552EE7D049AADA(
Malicious:	false
Reputation:	unknown
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....I8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\d1bea835-ec0c-4c85-9e15-c8ec6c7cb00a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185224
Entropy (8bit):	6.0767786021951835
Encrypted:	false
SSDEEP:	3072:h8PLD8n55EtvVAkRNGWr9x39UfkT7RdOAD+FcbXafIB0u1GOJmA3iuRw:aPLD8Qtdf0S39U6TlUaqfIlUOoSiuRw
MD5:	FB20DB9CC2ECCF503196D173C40E506F
SHA1:	31D0BFFF97A8EAD257DAC75A19334A4269CC18EA
SHA-256:	41A240AD71C126200141586D587A7C211542BDD575B038DA91B7DC1AC5C37250
SHA-512:	CE04CF7A66FF3F14C76A76C530E66903DCAB52962979A66B2D280DD19072530282CA9F23B922DB6367D733A4A09583138B24A52F4E97320A55F027E9D543A6D4
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d6c3685d-5a55-4a4c-bd1c-94d6754e56bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	185223
Entropy (8bit):	6.076780072694005
Encrypted:	false
SSDEEP:	3072:hrFLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:pFLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	9A3435BB2916D49F5662DF2DF9B0234A
SHA1:	7FB511EA0AB19F8497578647E031083111A67A9C
SHA-256:	BFD8A4F5CCA6D59405E9D0E4FFDB32E8A37EAFBAF1855AE9F4FD57DABD10CCBA
SHA-512:	9CE8ECCD4AF9E34CC3FAF9F8BE21E3B591140366FC947FDB8238AD2C0808C8AEA7FD0FB91B67A1F2F50F644793DC6A328EEC02D4E9C8C12BA6DE2F0B997B9BB2
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\df341cd3-d32d-4701-b328-329dc38280ff.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185224
Entropy (8bit):	6.076780174978916
Encrypted:	false
SSDEEP:	3072:t8PLD8n55EtvVAkRNGWr9x39UfkT7RdOAD+FcbXafIB0u1GOJmA3iuRw:mPLD8Qtdf0S39U6TlUaqfIlUOoSiuRw
MD5:	EA18642CBF5A149F2E28A60525572442
SHA1:	AC404D749E66CBEA45827B1C4734DE3053239B05
SHA-256:	FAEF55D41AC6DE200EDBD4EEA543F1332850256A91304CAFD4ED152C325DD06F

C:\Users\user\AppData\Local\Google\Chrome\User Data\df341cd3-d32d-4701-b328-329dc38280ff.tmp	
SHA-512:	72EF0293DED469C529E0F93334B6202AF370FAC88A945F3C3543C59A3D246318A432C6868AA451350342CCE9191C5943D6EB0F41CACFFD61F4375FC80AE8DE4
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799845608"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e8e32cf2-a584-474e-8e3a-c19f2984814d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	87023
Entropy (8bit):	6.102321908149239
Encrypted:	false
SSDEEP:	1536:SUuGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SUuFcbXaflB0u1GOJmA3iuR+
MD5:	04EA3ECF47F46C9AB073A1A8CAE1617E
SHA1:	062C6F716D0EE3126EB4C687FCA4F403DF7657B9
SHA-256:	53BC3171C0A8431E431E2DF17F7001AFD829930A31766D8898A81846A2992FA3
SHA-512:	84DBBDA70C2148B1FEDB2019519D5FF3BA18F4DB3CB7F218F0B9A140B86073C17BB303658132AEB6331682A48B887005C9C78B47755D5707A243465E8C8CC7E
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	unknown
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\fe69df42-7940-45ca-ad99-1bfbbf7f932b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185223
Entropy (8bit):	6.076780072694005
Encrypted:	false
SSDEEP:	3072:hrFLD8n55EtvVAkRNGWr9x39UfkT7RdOADfFcbXafIB0u1GOJmA3iuRw:pFLD8Qtdf0S39U6TltaqfIlUOoSiuRw
MD5:	9A3435BB2916D49F5662DF2DF9B0234A
SHA1:	7FB511EA0AB19F8497578647E031083111A67A9C
SHA-256:	BFD8A4F5CCA6D59405E9D0E4FFDB32E8A37EAFBAF1855AE9F4FD57DABD10CCBA

C:\Users\user\AppData\Local\Google\Chrome\User Data\fe69df42-7940-45ca-ad99-1bfbbf7f932b.tmp	
SHA-512:	9CE8ECCD4AF9E34CC3FAF9F8BE21E3B591140366FC947FDB8238AD2C0808C8AEA7FD0FB91B67A1F2F50F644793DC6A328EEC02D4E9C8C12BA6DE2F0B997B9BB2
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635541827385395e+12,"network":1.635509428e+12,"ticks":217354275.0,"uncertainty":3694755.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B096.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\B096.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84jE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvKvjHKs
MD5:	AE8CFF33270358D6EC23793128B3EF2F
SHA1:	5E6B156157EDEA4222A5E0C258AE9ADEBB8CB7CE
SHA-256:	498EAB9F855E7CE9B812EAD41339A9475127F0C8E7249033B975071D2292220C
SHA-512:	473111AD332D5E66724AFB0CE5A1E1C97890D60484A818D1DB8C2386A99C05BAE6C9D5C535DDFB6790BF5707C153502B938BE201393A3D70342A62902E0A3C9
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BBE1.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\BBE1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2388
Entropy (8bit):	5.316698480382997
Encrypted:	false
SSDEEP:	48:MxHKXwYHKhQnoPtHoxHhAHKzvKvDfHK7HKhBHKdHKBSTHvmHKAHKoLHG1qHqHAHJ:iqXwYqhQnoPtlxHeqzyLq7qLqdqsOqAL
MD5:	5A67F45FC45A5C358BA694BE7D6FDE4A
SHA1:	5670BA980A3F52150C0D41B819A60AB7E0620567
SHA-256:	485DCB4FFCD317D66CAB28BC902D252C440AEE78067C651AEFA124D46073FECF
SHA-512:	0C7AFCB6CFF807B4514447019FED5BC398B488E3D7BBD332CE85AD774FB05C84AB5C5B99EC0BF48CB56CC8E8C52BEA1AA31459182F1D40234F663ECC279F67C
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DF3A.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\DF3A.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84jE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvKvjHKs
MD5:	AE8CFF33270358D6EC23793128B3EF2F
SHA1:	5E6B156157EDEA4222A5E0C258AE9ADEBB8CB7CE
SHA-256:	498EAB9F855E7CE9B812EAD41339A9475127F0C8E7249033B975071D2292220C

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DF3A.exe.log	
SHA-512:	473111AD332D5E66724AFB0CE5A1E1C97890D60484A818D1DB8C2386A99C05BAE6C9D5C535DDFB6790BF5707C153502B938BE201393A3D70342A62902E0A3C9
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Temp\0faa7aea-12bb-4849-8fa9-815fe14274fd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	unknown
Preview:	.

C:\Users\user\AppData\Local\Temp\1105.tmp	
Process:	C:\Users\user\AppData\Local\Temp\CBF0.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1622408
Entropy (8bit):	6.298350783524153
Encrypted:	false
SSDEEP:	24576:hNZ04UyDzGrVh8xsPCw3/dzcldJndozS35IW1q/kNVSYVEs4j13HLHGJImdV4q:dGrVr3hclvnqzS35IWk/LvRHb0
MD5:	BFA689ECA05147AFD466359DD4A144A3
SHA1:	B3474BE2B836567420F8DC96512AA303F31C8AFC
SHA-256:	B78463B94388FDDB34C03F5DDDD5D542E05CDED6D4E38C6A3588EC2C90F0070B
SHA-512:	8F09781FD585A6DFB8BBC34B9F153B414478B44B28D80A8B0BDC3BED687F3ADAB9E60F08CCEC5D5A3FD916E3091C845F9D96603749490B1F7001430408F711D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L!y>.@.m.@.m.@.m...l.@.mg$.l.@.mg$.lN@.mg$.l.A.mg$.l .@.mg$.l.@.mg$.m.@.mg$.l.@.mRich.@.m.....PE..L...s<s.....!.....P....(K.....@A.....&.....8.....h...Y.. .....N..`l..T.....text....).....*..... ..`RT.....@..... ..`.data...dW...P.....0.....@....mrdata.h#.....$...>..... ....@....00cfg.....b.....@..@.rsrc...8.....d.....@..@.reloc...N.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\21.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346624
Entropy (8bit):	6.008556977987189
Encrypted:	false
SSDEEP:	3072:rwrBNjy106UX1gBXf8fVzu3kkGwSQ46yyZ4AX/cpM0p2a4sqOD06zWusdImyJLiT:0VT1fVzBnKyyH/cKy4sqOlwyy
MD5:	A0BC297D8EAAD37F1B145D108786E993
SHA1:	AC6858536F64EC7113F1CD10B248430DA8510DB8
SHA-256:	B06B803C1A654849E7B0310B0B590CA574568AB9EBA41858E8CAAFF5DBBEACBA
SHA-512:	8C18514C5D43497B5711131B0328CBF7C6ECD51F04A60F421175786C7431B999E30BD5B16FE9345C38FD3E0C26A682A611602A1B2FE657488485246B3BA3B541
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\21.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L...._.....p..... .....@.....t.....J.....d....`s..<.....s.....0.....@..... .....text..... ..`.data....io.....@....pale.....Ps.....@....rsrc....<...`s..<.....@..@.reloc...#....s..$...&..... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\5b81b21e-8488-49fb-af11-a55e6b006d71.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	unknown
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\B096.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	512512
Entropy (8bit):	7.846723941917503
Encrypted:	false
SSDEEP:	12288:Tw86shtDE09VgbshnKMstp7eylszgTDzLTDaMqvK8J+LF:TVhdLVg2Zep7njXzPDxC+J
MD5:	F57B28AEC65D4691202B9524F84CC54A
SHA1:	F546B20EB40E3BC2B6929BA0F574E32422CED30C
SHA-256:	87D86132095541ED3B5FE05EB06692E1712287B6FFD9832A28EB85F52B55F0A5
SHA-512:	1A773186B0A15F743F8D9681036A9ECA45E2DD5F7944725498E929C5438ACFFCD753061EB475383E5759FC41A8ADE4EB717F3D3529313C3C0D48C659B5E36F09
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\B096.exe, Author: Florian Roth
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. .....@..... .`.....S..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... . .....@..B.....H.....u...p.....HZ..X.....MZ.....@.....!....!This program cannot be run in D OS mode....$.....PE....." ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\BBE1.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	22528
Entropy (8bit):	5.395556088889033
Encrypted:	false
SSDEEP:	384:ezekc2D26R7pXha5eglsu2tiP39n+NDr7vGuywqFGc1QzOQslg:qJcMnacgl6Q10rSuywCZ1QO
MD5:	787AF677D0C317E8062B9705CB64F951
SHA1:	41BF391CE44004A22BA7F18E5FDCDCFCEA73E38F
SHA-256:	7CFA3F3EBB7DCE336E24DF02D5BA0FDBC081927892D597986113FB11EDF1702E
SHA-512:	8A9BF2D0DF12926F3253DCF5F2B5186928107C36189F404C50C69B67BC09DDA267FACD53E3259ABF3934DE6682BC3B0E49D1D5ACCFA5D4A5B702F4F9EF8D8E 5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\BBE1.exe, Author: Florian Roth
Antivirus:	• Antivirus: ReversingLabs, Detection: 22%

C:\Users\user\AppData\Local\Temp\BBE1.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..N.....nl.. .....@.. .....P.... .`.....I..S.....Z..... ..... ..H.....text...tL.. ...N..... ..`.rsrc.....P.....@..@.reloc..... .....V.....@..B.....PI.....H.....PK... .....MZ.....@.....!....!This program cannot be run in D OS mode....$.....PE.....' ..P.....Z8.. ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\C066.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	601600
Entropy (8bit):	7.082709411162039
Encrypted:	false
SSDEEP:	12288:ZYr2Nn9c+v4tOOc7JMZim3+sKQS4Kwp6vHOZjV1:OrCZSyUimTTwHC
MD5:	F0BE69176E592FA1A6345A7090A9EA30
SHA1:	CF56A6E67759A06B2681170AF52902FA9CFB9128
SHA-256:	28D82936CA3150866022F80B28D5422D66F54FB6FD81321A3E853CE29FAF74FF
SHA-512:	D8E1CA5BF558DD0DC1F6281F0970FC7E7E192110315D2F275C0A49FF0CB6F65EB7217C2024FC596A29AD3D1036B51D42A622F39672BC1F0C17ABCECC3122D6
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L.....Q_.....p..... .....@.....x.....zL.....d....@w..<.....w.....0..... ...@.....text..... ..`.data....io.....@....ruxat.....0w.....@....rsrc....<...@w..<.....@..@.reloc...#....w..$..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\C295.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	877056
Entropy (8bit):	7.462302194895007
Encrypted:	false
SSDEEP:	24576:yYuSM7Gp8zSjQLCV9ibUqyuziiM95BxXEr:yv7i8zSjbVwB1ZM910r
MD5:	B79D3399603938A695A98A75DCFBAB91
SHA1:	AF9A85F2CC85CD3B040536C988AAB45C237A22D9
SHA-256:	934690E391745FCA58CA0DF6D41952D6F58ED7B18AB8FDDA22484B01EB262BE8
SHA-512:	5499156CB77B33218077A690AF2EC89D9E9C2AC20796BB2F0A889DD97E569DDD84FDEC0F7C9332523A95D47081235E1BD2240D2971CDD5153CFA906C39BFA0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L....._.....p..... .....@.....|....ja.....d....{..<.....{.....0.....@..... .....text..... ..`.data....io.....@....vuci.....p{.....@....rsrc....<...{..<.....@..@.reloc...#....{..$...>..... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\C8FE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604160
Entropy (8bit):	7.081312542094628
Encrypted:	false
SSDEEP:	12288:zUq737aTz5aNquRVgE6/kEObrF5d/WYN4t88+wGOjsyDR:Aq7rwa0uRm8brF5LupDs
MD5:	DE692F1B4D4C63FED395BE25E878858E
SHA1:	16F5B74E898FB0CD30F127CB1E03DA79E481158A
SHA-256:	6ED753E5B9A7AC5D89A6F9749E24C5BEB7483C6FDA2057E81E1EB3ED5A32AB21
SHA-512:	24227BBCD1451E7F6A2B6C16637987B1388BE398A88005851AF24805BFD7B57AE39AE7B70E69DE3B424EE48E4FB65EF0CABD710692EBC9393F2A1542E6D8E067
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\C8FE.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.>.T.m.T.m.T.m."2m.T.m.".m.T.m."3mqT.m.,.m.T.m.T.m .T.m."6m.T.m.".m.T.m.".m.T.mRich.T.m.....PE..L.....*_.....v.....@.....@.....~.....4.....d....P}..I.....}..... ....@.....text..... ..`.data...H.u.....@....rsrc....I...P}..J.....@..@.reloc...#....}..$.....@..B..... ....

C:\Users\user\AppData\Local\Temp\CAC5.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	7.390894610588505
Encrypted:	false
SSDEEP:	6144:IdQPlt1M8RJNHUMb62VCDuy1DzJDGLkjNVlZeJjuzbgwuA7ITsq:Ialt6mJN0x2VmlhtawtcjunnF7
MD5:	FA00DF47BCC5F9AD16ED71856FB6F4D6
SHA1:	561D89B6384A44E6D47AC4B68D04FFFFF3DE3558
SHA-256:	B2F5636B2E78B3F60EA53FD0C7C95656E11C08FAC59869B38A165C7BF39CF1E5
SHA-512:	3A6ACB14B041B341C979F233D881225615B225DAC9E84F0CD62DAEC69818212A9620AE82E4B61BA5547E3A0EB9D1D8442EF52CE86BF093918203D33DDF3283C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 55%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....`.....6....._%.....@.....(....`..H/.....@.....p..... .....text..... ..`.rdata...E.....F.....@..@.data....<.....@....xoj....r....P.....@..@.rsrc...H/...`...0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\CBF0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	212992
Entropy (8bit):	6.734269361613487
Encrypted:	false
SSDEEP:	3072:UJ+Dg6a/6BO0fFI4+uX67vtk4nNcDxzyuEpuVMO6P2+BwvHJ3/RA:FDy/6BOSFI48v2dxzyuEpynVP
MD5:	73252ACB344040DDC5D9CE78A5D3A4C2
SHA1:	3A16C3698CCF7940ADFB2B2A9CC8C20B1BA1D015
SHA-256:	B8AC77C37DE98099DCDC5924418D445F4B11ECF326EDD41A2D49ED6EFD2A07EB
SHA-512:	1541E3D7BD163A4C348C6E5C7098C6F3ADD62B1121296CA28934A69AD308C2E51CA6B841359010DA96E71FA42FD6E09F7591448433DC3B01104007808427C3DE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 80%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....^.....V.....,.....p....@.....q.....\...<.... ..8.....q.....@.....p..x..... .....text....U.....V..... ..`.rdata...G...p...H...Z.....@..@.data...DB.....@....cipizi.r.....@..@.rsrc...8.... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\CD17.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	262248
Entropy (8bit):	7.344044114091331
Encrypted:	false
SSDEEP:	6144:7Zd5yNguYYTkxcNQoF8KzJugf/vTvN9KQqJlo:7Zd5yNguPQyNQYJuSvDLKXIo
MD5:	EDE62358EA39643E43992E9068E03CA2
SHA1:	0F73E8F96C01135A91D4E1BFECA139AD31C72C15
SHA-256:	187CB817751D6871EB7BE566DD9D9A98A46EDB11391220B69E4FAD695F31E605
SHA-512:	552B31EDA2131C8326996DEBA1812C6A6B23D892DDABDD17C3182FCD43B9019CFC863EED1FF67FA2EC21297E98F61502D3E095972D2C6710D08B3F27EA82 1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\CD17.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{a.....0..... .. ....@.. .....@..... ..@.....(...W.....XH.....h.... ....H.....text..... ....`.rsrc...XH.....J.....@..@.reloc..... .....@..B.....d.....H.....I...."..... .....?.....?.....?.....?..... .....?..... .....@..... .....@..... .....@..... .....

C:\Users\user\AppData\Local\Temp\D8D0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	27576
Entropy (8bit):	5.969933955399239
Encrypted:	false
SSDEEP:	384:bekc2D26R7pXha5eglsu2CfQG9kyf4ZZK61TEYFGc1QzOQs42Aghgn:bJcMnacgl6EWlXzZ1QO4khgn
MD5:	FA6D8115D2266A121FE7C1552C0DDDFD
SHA1:	9166433A1F42AE7A623F26341DD9BBED91A045B3
SHA-256:	237E9E25B4DADE7BD2CCD0F6D59C9D607EEED8E60C1041F10BE3D4C50B37A459
SHA-512:	58825BAF9D243279393A635AEE9E7493682F18105D24CFAAF270BFAE54CB2FFDFE12734D7E3EB34983C554F3599BB73D523029871F28D8AFBF25CD27798C2368
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\D8D0.exe, Author: Florian Roth
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....".."...0..N.....I... .....@.. .....G... .`.....I..O.....,.....X..... ..... ..H.....text....L... ...N..... ..`.rsrc...,.....P.....@..@.reloc..... .....V.....@..B.....I.....H.....PK..L!.....MZ.....@.....!...!This program cannot be run in DOS mode....$.....PE....." ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ..... .. ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\DEDC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	510976
Entropy (8bit):	7.850749525333838
Encrypted:	false
SSDEEP:	12288:Iw86shtDE09VgbshnKMstp7eylszgTDzLTDaMqvK8J+W:IVhdLVg2Zep7njXzPDxC+W
MD5:	B0A956B96769AA21A44206DD528C5B39
SHA1:	30CF20E67DFA3FC38C6E80B761AD0D523C5AF43A
SHA-256:	37B78E9A50830B88E97F6048F90EA0AFE925E0C6E4F0E9A1CF3C7849787D9C4C
SHA-512:	5B6D8707FA2D4B7D41D7B1733409A34645DF2B42FF064D9E7643A8F4AE7076A798B2012959AF6F8B30E44D60B28EF4B1761E0CB3287448329C9144AE9FD9CE9F
Malicious:	false
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\DEDC.exe, Author: Florian Roth
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....N.... ....@.. .....@.....yq... .`.....K..... ..... ..... ..H.....text...T.... ..... ..`.rsrc.....@..@.reloc..... . .....@..B.....0.....H.....u..hk.....@Z..X.....MZ.....@.....!....!This program cannot be run in D OS mode....$.....PE....." ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\DF3A.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	161280
Entropy (8bit):	5.163359140538006
Encrypted:	false
SSDEEP:	3072:hj1+ax5s9jVultxyIAMzTjSMzTjoIe1UhCp:hJqjVoeN
MD5:	9FA070AF1ED2E1F07ED8C9F6EB2BDD29
SHA1:	6E1ACD6CB17AB64AC6DBF0F4400C649371B0E3BD
SHA-256:	08D67F957EC38E92301EEAAAF2759EF2A070376239EAD25864C88F3DD31EAB8C
SHA-512:	14A1CD1090A2ECCEA3B654EEE2B7D4DE390219F8C3C200D97D2AB431311BDF24B1B40F2F38E78804AD286654CD33DFB515704C9B863DAF0786A0D633F05C9B2
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\DF3A.exe	
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\DF3A.exe, Author: Florian Roth
Antivirus:	• Antivirus: ReversingLabs, Detection: 43%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0.wa.....P..l..... .....@.. ..... @.....O.....x..... ....H.....text....k... ...l..... ..`.rsrc.....n.....@..@.reloc..... .....t.....@..B.....H.....(u..t.....A...HL...(.....M...Z.....@..... .....!.....L.....!...T...h...i...s... ...p...r...o...g...r...a...m... ...c...a...n...n...o...t... ...b...e... ...r...

C:\Users\user\AppData\Local\Temp\E64F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	791552
Entropy (8bit):	7.368824467033047
Encrypted:	false
SSDEEP:	12288:uDMkBTpEvda0f6dSctc54lTQazT6A/9Or+ilw8lCW0k7ro8R3D3INLf3:QMk+dV6dS6KazZ4rPlw8lCWYQi
MD5:	7917305400EE899130B1D5B7AFA0A159
SHA1:	D45E1A34FE773040D7034A80BBEBB3DBD3EA4252
SHA-256:	80C4B12305B41D2FDCD9DCCD53D2414C3AEA2188198F3D79AF262709C1E2DAC9
SHA-512:	417DECA0BEEE73B6EA8379B85726A9DAAF4DC32721D7A658BA42B9D359A6739F7478D3E0068C8B110497CB222956A1AFA5E1BF28C202965DEDE7A659EB824EF6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.....^.....Rich..... ...PE..L...m;._.....v.....@.....P....0...I..... .....~..@..... .text..... ..`.data...H.u.....@....rsrc....I...0...J.....@..@.reloc..8$.....&.....@..B.....

C:\Users\user\AppData\Local\Temp\EBBE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348672
Entropy (8bit):	5.997778327285649
Encrypted:	false
SSDEEP:	6144:0BbSn3n6QHUKl3hINRqdhUm6b8mCcNebxCg1:Eu3n6UUKlxS2Um6b8mCcNej
MD5:	539C39A9565CD4B120E5EB121E45C3C2
SHA1:	5E1975A1C8F9B8416D9F5F785882DFB0CC9161DC
SHA-256:	C673B8408DB0EB515651E6A6F3361C713903001011C6E13A1825C0376A83D1DD
SHA-512:	3CC343A53051BE34B4CAD9AA9A9AE68D6B5A978B2ECD10516E4934452D29A9455A6CEB5EB7C7B691B2D08F1781BFB7B1E3627CB2823DD4F60860861F2202BAF
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.>.T.m.T.m.T.m."2m.T.m.".m.T.m."3mqT.m.,.m.T.m.T.m .T.m."6m.T.m.".m.T.m.".m.T.mRich.T.m.....PE..L....8?`.....v.....`.....@.....z.....f.....$...d....py..l.....y..... ....@.....text..... ..`.data...H.u.....@....rsrc....I...py..J.....@..@.reloc...#....y..$.....@..B.....

C:\Users\user\AppData\Local\Temp\F11E.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1111994
Entropy (8bit):	7.9252602794269915
Encrypted:	false
SSDEEP:	24576:4CRVwOoPzND9TI7RUGb+89w4ZFLkAPLYLSeUr:hOhJGTIAAcns
MD5:	27E7D6FAA08A1A69CB7C62D199B1B4F6
SHA1:	507F02D50BA701760A6D2303A648563030FB3ECD
SHA-256:	3896AD778346B9D5B04331410015969F2AF655B6277DBF612721027B73173E50
SHA-512:	7100ED807C5C1C56D5A3FCB4E69BE326F5D14BC44076E2E35355E6B8E3A175ED1B9FF4BC9C82FBCB1C19D1DD552E1D9242CD17CD5C44F9320C067ACA301D159
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\F11E.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j@...!.R.!.R.!.R'Y.R4!.R'Y.R.!.R'Y.R=!.R.!.R.!.R'Y.Ry!.R'Y.R/! .R'Y.R/!.R'Y.R/!.RRich.!.R.....PE..L....ALV.....~.....\.....@.....`.....3.....xE..... ....@...@.....(.....text...)..... ..`.rdata...F.....H.....@..@.data...(.... .....@....rsrc...xE.....F..".....@..@..... .....

C:\Users\user\AppData\Local\Temp\F1AC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3904000
Entropy (8bit):	7.959244774483495
Encrypted:	false
SSDEEP:	98304:zvl5DY66TDyQmymjivZkn7ikGqoa2+GEm:LY1TmlGv2nm2oa2+G
MD5:	3D0D60FAAE1EDD40DBF2CC9906FE2EC4
SHA1:	53B3CFBF2EBFFFD09932EF3DDC54BD993F2AD921
SHA-256:	D5758DC0615523F537C19BC7D9C6D7C530AAF3749C57147D6264EEA0DD24522A
SHA-512:	38F8701FC34D1FDD32B74EB3941180D542E859E2B3A2630767C2D0E3F992B4F5199DE38CEA6B67FC570FFE2C83F010F1DA4028519616272F36D01D887339103D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....ya.....".....T...:9.....`8...@..... .....:.....`<. ..`...@.....@..... .....:.d.....`8.H.....Cgw(.O~.$+8.. ...,8.....@....text....S...`8..T...08..... ..... ..`.rsrc...d.....:.....:.....@..@..... ....

C:\Users\user\AppData\Local\Temp\FD36.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	516536
Entropy (8bit):	7.850812641211313
Encrypted:	false
SSDEEP:	12288:qw86shtDE09VgbshnKMstp7eylszgTDzLTDaMqvK8J+ymtE:qVhdLVg2Zep7njXzPDxC+TE
MD5:	C55C023A1BEA32E71A99614D39DC4DD6
SHA1:	44809A18A01B2647C9A80AF0EF9CA131EEF34E97
SHA-256:	D7241A7DA97FDEFE199F23605BFAB8F878728A71F4B1B12F26AA83F775AE2FC5
SHA-512:	5A4A071A5CE5EB921738324AF71A8434DF5AF2219016006A0002D6918DCADAD8580BEF6D4973F05ACD9FF68C23DE6B8C3F6308709294DAD03D024068C9F4266
Malicious:	false
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\FD36.exe, Author: Florian Roth
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....~.... .....@.. .....@.....'... .`.....$...W..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... . .....@..B.....`.....H.....t..<k.....Y..X.....MZ.....@.....!....!This program cannot be run in DOS mode....$.....PE.....".....P.....Z8.. ...@..... .....@.....8..O....@..x.....`.....7..... ....H.....text..`.... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.008556977987189
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:	Md0q201V1D.exe
File size:	346624
MD5:	a0bc297d8eaad37f1b145d108786e993
SHA1:	ac6858536f64ec7113f1cd10b248430da8510db8
SHA256:	b06b803c1a654849e7b0310b0b590ca574568ab9eba418 58e8caaff5dbbeacba

General

SHA512:	8c18514c5d43497b5711131b0328cbf7c6ecd51f04a60f421175786c7431b999e30bd5b16fe9345c38fd3e0c26a682a611602a1b2fe657488485246b3ba3b541
SSDEEP:	3072:rwrBNjy106UX1gBXf8fVzu3kkGwSQ46yyZ4AX/cpM0p2a4sqOD06zWusdImyJLiT:0VT1fVzBnKyyH/cKy4sqOlwyy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>...m...m...m..2m...m...m...m..3mq..m...m...m...m...m..6m...m...m...m...m...mRich...m.....PE..L....._.....

File Icon

Icon Hash:	aedaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x41cb20
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5FA116E2 [Tue Nov 3 08:37:54 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	e522cb867082e04c7a4b61561f8516ce

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3cb18	0x3cc00	False	0.598652906379	data	6.98974133443	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x3e000	0x26f69c8	0x1600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pale	0x2735000	0x2e5	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2736000	0x3c00	0x3c00	False	0.746940104167	data	6.42028876467	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x273a000	0x123f0	0x12400	False	0.0812553510274	data	1.05090954457	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Paraguay	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 14:09:40.249532938 CEST	192.168.2.3	8.8.8.8	0xc836	Standard query (0)	xacokuo8.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:40.372556925 CEST	192.168.2.3	8.8.8.8	0xff0c	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:40.629740953 CEST	192.168.2.3	8.8.8.8	0x5478	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:40.880671978 CEST	192.168.2.3	8.8.8.8	0xbc14	Standard query (0)	privacytoo lzforyou-6000.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:43.668574095 CEST	192.168.2.3	8.8.8.8	0x9db3	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:44.010621071 CEST	192.168.2.3	8.8.8.8	0x8a09	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.299552917 CEST	192.168.2.3	8.8.8.8	0x9567	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.549968958 CEST	192.168.2.3	8.8.8.8	0x947a	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.831943989 CEST	192.168.2.3	8.8.8.8	0x562	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:01.170274973 CEST	192.168.2.3	8.8.8.8	0x1495	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:01.426273108 CEST	192.168.2.3	8.8.8.8	0x91d9	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:03.559824944 CEST	192.168.2.3	8.8.8.8	0xb9c4	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:03.810604095 CEST	192.168.2.3	8.8.8.8	0x1c0b	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:04.063611031 CEST	192.168.2.3	8.8.8.8	0xffeb	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:04.738146067 CEST	192.168.2.3	8.8.8.8	0xaa7b	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.089852095 CEST	192.168.2.3	8.8.8.8	0x7901	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.929352045 CEST	192.168.2.3	8.8.8.8	0x26e2	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:08.174237013 CEST	192.168.2.3	8.8.8.8	0xf2b4	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:09.930037975 CEST	192.168.2.3	8.8.8.8	0x4ec3	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:11.287599087 CEST	192.168.2.3	8.8.8.8	0x1089	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:11.535811901 CEST	192.168.2.3	8.8.8.8	0xf6e9	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:11.784204960 CEST	192.168.2.3	8.8.8.8	0x524a	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 14:10:12.428087950 CEST	192.168.2.3	8.8.8.8	0xe2ab	Standard query (0)	iyc.jelikob.ru	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:12.735543966 CEST	192.168.2.3	8.8.8.8	0x614c	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:12.990253925 CEST	192.168.2.3	8.8.8.8	0xe0e1	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:13.261889935 CEST	192.168.2.3	8.8.8.8	0xfe4b	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:13.544400930 CEST	192.168.2.3	8.8.8.8	0xc420	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:15.586174965 CEST	192.168.2.3	8.8.8.8	0xd0bf	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:15.862766027 CEST	192.168.2.3	8.8.8.8	0x7c2a	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.132903099 CEST	192.168.2.3	8.8.8.8	0x2b2c	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.393680096 CEST	192.168.2.3	8.8.8.8	0xb9bf	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.650090933 CEST	192.168.2.3	8.8.8.8	0x6ef3	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.816096067 CEST	192.168.2.3	8.8.8.8	0xc1c0	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:19.878665924 CEST	192.168.2.3	8.8.8.8	0x7415	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:20.138806105 CEST	192.168.2.3	8.8.8.8	0xfda9	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:20.468445063 CEST	192.168.2.3	8.8.8.8	0x77e	Standard query (0)	sysaheu90.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.111479998 CEST	192.168.2.3	8.8.8.8	0xa277	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.389888048 CEST	192.168.2.3	8.8.8.8	0x97af	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.389945984 CEST	192.168.2.3	8.8.8.8	0x48f4	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:29.239370108 CEST	192.168.2.3	8.8.8.8	0xa8d1	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:29.573542118 CEST	192.168.2.3	8.8.8.8	0xa6e9	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:30.214529037 CEST	192.168.2.3	8.8.8.8	0x3598	Standard query (0)	avatars.githubusercontent.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:31.983638048 CEST	192.168.2.3	8.8.8.8	0xa3c2	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.245552063 CEST	192.168.2.3	8.8.8.8	0xab43	Standard query (0)	avatars.githubusercontent.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:34.801071882 CEST	192.168.2.3	8.8.8.8	0x63a	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:37.919708014 CEST	192.168.2.3	8.8.8.8	0x9d28	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:41.363266945 CEST	192.168.2.3	8.8.8.8	0x26e8	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:44.169285059 CEST	192.168.2.3	8.8.8.8	0x59b	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:44.604974985 CEST	192.168.2.3	8.8.8.8	0x7156	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:48.412956953 CEST	192.168.2.3	8.8.8.8	0x45dd	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:51.762058020 CEST	192.168.2.3	8.8.8.8	0xe31b	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:51.895178080 CEST	192.168.2.3	8.8.8.8	0x51b2	Standard query (0)	toptelete.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:57.205171108 CEST	192.168.2.3	8.8.8.8	0x4151	Standard query (0)	nusurtal4f.net	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:57.765567064 CEST	192.168.2.3	8.8.8.8	0xed61	Standard query (0)	znpst.top	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:09.428842068 CEST	192.168.2.3	8.8.8.8	0x4603	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.175357103 CEST	192.168.2.3	8.8.8.8	0x5091	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.704349995 CEST	192.168.2.3	8.8.8.8	0xed15	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:17.404216051 CEST	192.168.2.3	8.8.8.8	0x9631	Standard query (0)	mas.to	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 14:11:20.502801895 CEST	192.168.2.3	8.8.8.8	0x14c7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:22.049130917 CEST	192.168.2.3	8.8.8.8	0x1f6	Standard query (0)	mas.to	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:41.048815012 CEST	192.168.2.3	8.8.8.8	0x5be6	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:45.143712044 CEST	192.168.2.3	8.8.8.8	0xa4e4	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 14:09:40.349797010 CEST	8.8.8.8	192.168.2.3	0xc836	Name error (3)	xacokuo8.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:40.389902115 CEST	8.8.8.8	192.168.2.3	0xff0c	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:40.648988008 CEST	8.8.8.8	192.168.2.3	0x5478	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:41.235708952 CEST	8.8.8.8	192.168.2.3	0xbc14	No error (0)	privacytoolzforyou-6000.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:43.688175917 CEST	8.8.8.8	192.168.2.3	0x9db3	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:09:44.030148983 CEST	8.8.8.8	192.168.2.3	0x8a09	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.318998098 CEST	8.8.8.8	192.168.2.3	0x9567	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.569439888 CEST	8.8.8.8	192.168.2.3	0x947a	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:00.851335049 CEST	8.8.8.8	192.168.2.3	0x562	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:01.189889908 CEST	8.8.8.8	192.168.2.3	0x1495	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:01.445811987 CEST	8.8.8.8	192.168.2.3	0x91d9	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:03.579739094 CEST	8.8.8.8	192.168.2.3	0xb9c4	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:03.829663992 CEST	8.8.8.8	192.168.2.3	0x1c0b	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:04.354789019 CEST	8.8.8.8	192.168.2.3	0xffeb	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:04.758182049 CEST	8.8.8.8	192.168.2.3	0xaa7b	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.112236023 CEST	8.8.8.8	192.168.2.3	0x7901	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.112236023 CEST	8.8.8.8	192.168.2.3	0x7901	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.112236023 CEST	8.8.8.8	192.168.2.3	0x7901	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.112236023 CEST	8.8.8.8	192.168.2.3	0x7901	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.112236023 CEST	8.8.8.8	192.168.2.3	0x7901	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:07.948779106 CEST	8.8.8.8	192.168.2.3	0x26e2	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:08.648478031 CEST	8.8.8.8	192.168.2.3	0xf2b4	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 14:10:09.950828075 CEST	8.8.8.8	192.168.2.3	0x4ec3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:09.950828075 CEST	8.8.8.8	192.168.2.3	0x4ec3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:09.950828075 CEST	8.8.8.8	192.168.2.3	0x4ec3	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:09.950828075 CEST	8.8.8.8	192.168.2.3	0x4ec3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:09.950828075 CEST	8.8.8.8	192.168.2.3	0x4ec3	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:11.306994915 CEST	8.8.8.8	192.168.2.3	0x1089	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:11.555179119 CEST	8.8.8.8	192.168.2.3	0xf6e9	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:12.161859035 CEST	8.8.8.8	192.168.2.3	0x524a	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:12.493707895 CEST	8.8.8.8	192.168.2.3	0xe2ab	No error (0)	iyc.jelikob.ru		81.177.141.36	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:12.754959106 CEST	8.8.8.8	192.168.2.3	0x614c	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:13.009208918 CEST	8.8.8.8	192.168.2.3	0xe0e1	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:13.281296968 CEST	8.8.8.8	192.168.2.3	0xfe4b	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:13.564043045 CEST	8.8.8.8	192.168.2.3	0xc420	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:15.605772018 CEST	8.8.8.8	192.168.2.3	0xd0bf	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:15.882200956 CEST	8.8.8.8	192.168.2.3	0x7c2a	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.153029919 CEST	8.8.8.8	192.168.2.3	0x2b2c	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.413116932 CEST	8.8.8.8	192.168.2.3	0xb9bf	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:16.670523882 CEST	8.8.8.8	192.168.2.3	0x6ef3	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.838687897 CEST	8.8.8.8	192.168.2.3	0xc1c0	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.838687897 CEST	8.8.8.8	192.168.2.3	0xc1c0	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.838687897 CEST	8.8.8.8	192.168.2.3	0xc1c0	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.838687897 CEST	8.8.8.8	192.168.2.3	0xc1c0	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:18.838687897 CEST	8.8.8.8	192.168.2.3	0xc1c0	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:19.898004055 CEST	8.8.8.8	192.168.2.3	0x7415	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:20.157886028 CEST	8.8.8.8	192.168.2.3	0xfda9	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 14:10:20.488089085 CEST	8.8.8.8	192.168.2.3	0x77e	No error (0)	sysaheu90.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.131249905 CEST	8.8.8.8	192.168.2.3	0xa277	No error (0)	hajezey1.top		5.188.88.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.417649031 CEST	8.8.8.8	192.168.2.3	0x97af	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:27.429796934 CEST	8.8.8.8	192.168.2.3	0x48f4	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 14:10:27.429796934 CEST	8.8.8.8	192.168.2.3	0x48f4	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:29.266856909 CEST	8.8.8.8	192.168.2.3	0xa8d1	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 14:10:29.274403095 CEST	8.8.8.8	192.168.2.3	0x7d5f	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 14:10:29.594722033 CEST	8.8.8.8	192.168.2.3	0xa6e9	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:30.233423948 CEST	8.8.8.8	192.168.2.3	0x3598	No error (0)	avatars.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:30.233423948 CEST	8.8.8.8	192.168.2.3	0x3598	No error (0)	avatars.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:30.233423948 CEST	8.8.8.8	192.168.2.3	0x3598	No error (0)	avatars.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:30.233423948 CEST	8.8.8.8	192.168.2.3	0x3598	No error (0)	avatars.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.007085085 CEST	8.8.8.8	192.168.2.3	0xa3c2	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.264583111 CEST	8.8.8.8	192.168.2.3	0xab43	No error (0)	avatars.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.264583111 CEST	8.8.8.8	192.168.2.3	0xab43	No error (0)	avatars.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.264583111 CEST	8.8.8.8	192.168.2.3	0xab43	No error (0)	avatars.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:32.264583111 CEST	8.8.8.8	192.168.2.3	0xab43	No error (0)	avatars.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:34.820704937 CEST	8.8.8.8	192.168.2.3	0x63a	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:38.020772934 CEST	8.8.8.8	192.168.2.3	0x9d28	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:41.382754087 CEST	8.8.8.8	192.168.2.3	0x26e8	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:44.196780920 CEST	8.8.8.8	192.168.2.3	0x59b	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 14:10:44.196780920 CEST	8.8.8.8	192.168.2.3	0x59b	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:44.624536991 CEST	8.8.8.8	192.168.2.3	0x7156	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:48.432509899 CEST	8.8.8.8	192.168.2.3	0x45dd	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:51.781487942 CEST	8.8.8.8	192.168.2.3	0xe31b	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:51.918087006 CEST	8.8.8.8	192.168.2.3	0x51b2	No error (0)	toptelete.top		172.67.160.46	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 14:10:51.918087006 CEST	8.8.8.8	192.168.2.3	0x51b2	No error (0)	toptelete.top		104.21.9.146	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:57.240221977 CEST	8.8.8.8	192.168.2.3	0x4151	No error (0)	nusurtal4f.net		45.141.84.21	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		211.59.14.90	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		222.236.49.123	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		118.221.132.200	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		115.88.24.203	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		89.201.145.218	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		92.62.104.245	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		211.169.6.249	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		179.178.42.164	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		31.166.170.180	A (IP address)	IN (0x0001)
Oct 29, 2021 14:10:58.028448105 CEST	8.8.8.8	192.168.2.3	0xed61	No error (0)	znpst.top		123.213.233.194	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:09.448448896 CEST	8.8.8.8	192.168.2.3	0x4603	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.197093010 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.197093010 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.197093010 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.197093010 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:11.197093010 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.723599911 CEST	8.8.8.8	192.168.2.3	0xed15	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.723599911 CEST	8.8.8.8	192.168.2.3	0xed15	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.723599911 CEST	8.8.8.8	192.168.2.3	0xed15	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.723599911 CEST	8.8.8.8	192.168.2.3	0xed15	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:12.723599911 CEST	8.8.8.8	192.168.2.3	0xed15	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:17.423815966 CEST	8.8.8.8	192.168.2.3	0x9631	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:20.522248030 CEST	8.8.8.8	192.168.2.3	0x14c7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:20.522248030 CEST	8.8.8.8	192.168.2.3	0x14c7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 14:11:20.522248030 CEST	8.8.8.8	192.168.2.3	0x14c7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:20.522248030 CEST	8.8.8.8	192.168.2.3	0x14c7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:20.522248030 CEST	8.8.8.8	192.168.2.3	0x14c7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:22.069711924 CEST	8.8.8.8	192.168.2.3	0x1f6	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:41.068432093 CEST	8.8.8.8	192.168.2.3	0x5be6	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)
Oct 29, 2021 14:11:45.163240910 CEST	8.8.8.8	192.168.2.3	0xa4e4	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hdytesri.org
  - hajezey1.top
- hxpkekj.com
- privacytoolzforyou-6000.top
- glmgx.com
- yuwnqq.com
- bhitjmrc.com
- dignolmjwo.com
- uhgju.org
- vumfxrbs.com
- npvevaeyy.net
- jqgngasfhc.org
- fjibch.net
- yvypqbsdmc.com
- knelfvrqfb.com
- mgtlhphal.com
- iouiiivyis.org
- pblfggd.net
- qrhhbxdcks.net
- tdgnneuj.com
- fvlfqoywa.com
- ymejogxekm.net

- cfgober.net
- weiifp.org
- cwqkqbcdy.org
- rxaxe.net
- auuomlb.com
- hhqcogw.org
- uuocrqwp.org
- eqvwckh.com
- fvfjwsqv.org
- sysaheu90.top
- rowqyedjmp.org
- toptelete.top
- 194.180.174.181
- nusurtal4f.net
- znpst.top
- tnjhdjy.org
  - 193.56.146.214
- rfjetdallh.org
- hndhvvubql.org
- potfqvj.org
- qpxove.net
- oftpi.net
- ussig.org
- ddmqcj.org
- swmkrkh.net
- 65.108.80.190

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Md0q201V1D.exe PID: 6304 Parent PID: 5100

General

Start time:	14:08:56
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\Md0q201V1D.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Md0q201V1D.exe'
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Md0q201V1D.exe PID: 5724 Parent PID: 6304

General

Start time:	14:09:01
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\Md0q201V1D.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Md0q201V1D.exe'
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.338103224.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.338316447.0000000001F91000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3352 Parent PID: 5724

General

Start time:	14:09:08
Start date:	29/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
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: 0000000A.00000000.326584645.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: gbhudtb PID: 7044 Parent PID: 664

General

Start time:	14:09:40
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\gbhudtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gbhudtb
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 21.exe PID: 2132 Parent PID: 3352

General

Start time:	14:09:42
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\21.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\21.exe
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 21.exe PID: 808 Parent PID: 2132

General

Start time:	14:09:49
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\21.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\21.exe
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
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: 00000013.00000002.400930179.0000000002061000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.400697119.0000000000580000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: gbhudtb PID: 3016 Parent PID: 7044

General

Start time:	14:09:51
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\gbhudtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gbhudtb
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: gbhudtb PID: 5332 Parent PID: 664

General

Start time:	14:10:01
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\gbhudtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gbhudtb
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: B096.exe PID: 6404 Parent PID: 3352

General

Start time:	14:10:02
Start date:	29/10/2021

Path:	C:\Users\user\AppData\Local\Temp\B096.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B096.exe
Imagebase:	0xa00000
File size:	512512 bytes
MD5 hash:	F57B28AEC65D4691202B9524F84CC54A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.503371064.0000000003E09000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000018.00000003.442159115.00000000065DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000018.00000002.520563950.0000000006381000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000018.00000002.519980779.0000000005F90000.00000004.00020000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\B096.exe, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: BBE1.exe PID: 4756 Parent PID: 3352

General

Start time:	14:10:06
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\BBE1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BBE1.exe
Imagebase:	0x790000
File size:	22528 bytes
MD5 hash:	787AF677D0C317E8062B9705CB64F951
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\BBE1.exe, Author: Florian Roth
Antivirus matches:	• Detection: 22%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Analysis Process: gbhudtb PID: 3796 Parent PID: 5332

General

Start time:	14:10:08
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\gbhudtb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gbhudtb
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	A0BC297D8EAAD37F1B145D108786E993
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: 0000001C.00000002.449845582.0000000000561000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001C.00000002.449446646.0000000000530000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: CBF0.exe PID: 6000 Parent PID: 3352

General

Start time:	14:10:09
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\CBF0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CBF0.exe
Imagebase:	0x400000
File size:	212992 bytes
MD5 hash:	73252ACB344040DDC5D9CE78A5D3A4C2
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: 0000001D.00000003.438106147.0000000003080000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001D.00000002.453324146.00000000031C1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001D.00000002.453199313.0000000003090000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 80%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: aspnet_state.exe PID: 4772 Parent PID: 6404

General

Start time:	14:10:10
Start date:	29/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe
Imagebase:	0x960000
File size:	47208 bytes
MD5 hash:	3269806DC450E24113CF4FE03C3AD197
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001E.00000000.439226875.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001E.00000000.438304869.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001E.00000000.439894383.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001E.00000000.440496476.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001E.00000002.466743057.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: DF3A.exe PID: 5464 Parent PID: 3352

General

Start time:	14:10:14
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\DF3A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DF3A.exe
Imagebase:	0xa40000
File size:	161280 bytes
MD5 hash:	9FA070AF1ED2E1F07ED8C9F6EB2BDD29
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: EBBE.exe PID: 1140 Parent PID: 3352

General

Start time:	14:10:17
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\EBBE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EBBE.exe
Imagebase:	0x400000
File size:	348672 bytes
MD5 hash:	539C39A9565CD4B120E5EB121E45C3C2
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: 00000021.00000002.481901309.00000000048F1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000021.00000002.480747015.0000000002D30000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: chrome.exe PID: 6016 Parent PID: 4772

General

Start time:	14:10:20
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: C066.exe PID: 5604 Parent PID: 3352

General

Start time:	14:10:23
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\C066.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C066.exe
Imagebase:	0x400000
File size:	601600 bytes
MD5 hash:	F0BE69176E592FA1A6345A7090A9EA30
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000023.00000003.479598454.0000000004960000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: chrome.exe PID: 6128 Parent PID: 6016

General

Start time:	14:10:24
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,3532224147046022434,3796046305070752020,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 1472 Parent PID: 4772

General

Start time:	14:10:25
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=aspnet_state.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 3732 Parent PID: 1472

General

Start time:	14:10:28
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1512,11815571981665026670,1640145837052183510 6,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1896 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: DF3A.exe PID: 6180 Parent PID: 5464

General

Start time:	14:10:28
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\DF3A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DF3A.exe
Imagebase:	0xed0000
File size:	161280 bytes
MD5 hash:	9FA070AF1ED2E1F07ED8C9F6EB2BDD29
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.489693993.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.488918061.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.488076798.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000027.00000000.487377447.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: ServiceModelReg.exe PID: 7320 Parent PID: 6404

General

Start time:	14:10:31
Start date:	29/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe
Imagebase:	0xae0000
File size:	221800 bytes
MD5 hash:	FFF587A66B8D5A50A055B9CD6D632BEB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.483819247.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000002.507631653.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.480873861.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.483001107.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.484896100.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: chrome.exe PID: 8084 Parent PID: 7320

General

Start time:	14:10:42
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=ServiceModelReg.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 5744 Parent PID: 7320

General

Start time:	14:10:46
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=ServiceModelReg.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 6240 Parent PID: 8084

General

Start time:	14:10:46
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,13203243795606022941,14762146736583605753,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8
Imagebase:	0x7ff6225d0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7992 Parent PID: 5744

General

Start time:	14:10:50
Start date:	29/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,11199746608983669523,6532242252009539287,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: bhhudtb PID: 8080 Parent PID: 664

General

Start time:	14:10:57
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\bhhudtb

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\bhhudtb
Imagebase:	0x400000
File size:	212992 bytes
MD5 hash:	73252ACB344040DDC5D9CE78A5D3A4C2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis