ID: 433016
Cookbook: browseurl.jbs
Time: 05:51:48
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

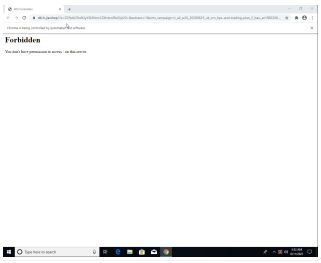
Analysis Report https://pbox.photobox.co.uk/dynclick/p…

Overview

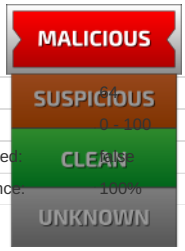
General Information

Sample URL:	https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk...8c&p1=db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=%23/my/creations
Analysis ID:	433016
Infos:	

Most interesting Screenshot:



Detection

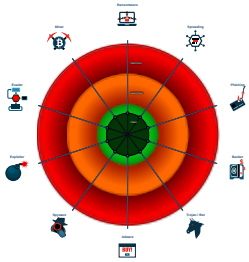


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6664 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_crn_e2_bau_all&uid=67912768&eurl=http://photobox-mkt-prod1-t.campaign.adobe.com/r/?id=h4e5ec0b9,69a17086,5eb6e68f&utm_source=photobox&utm_medium=email&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&_c1v=crm&_c2v=trigger&_c3v=creation&_c4id=1982206&_c5id=1772187782&_c6id=all&_c7id=acc&_cdt=2020-06-23&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&p1=db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=%23/my/creations' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6928 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1588,410492651604263749,13814431910474319796,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1820 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

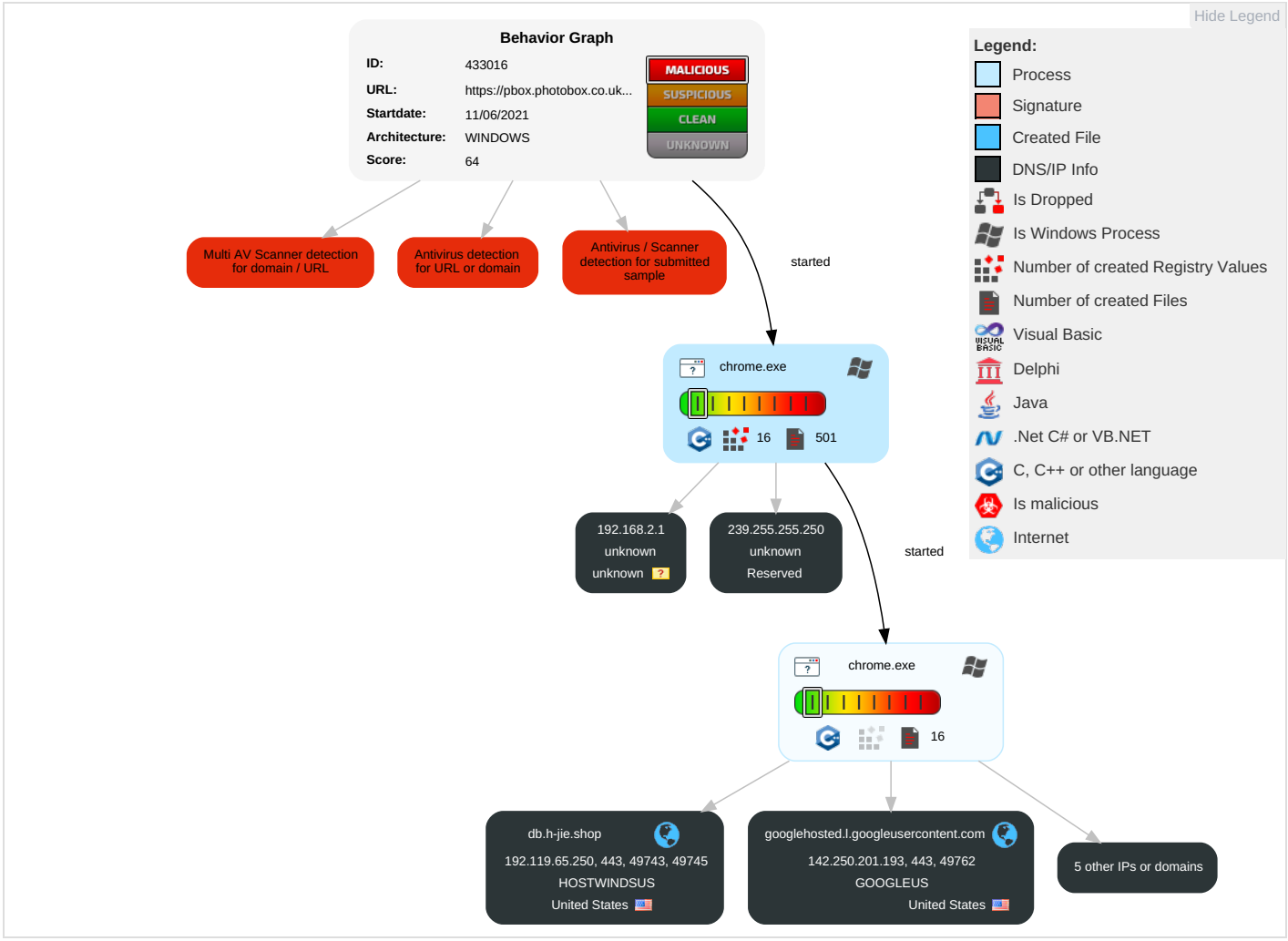
Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

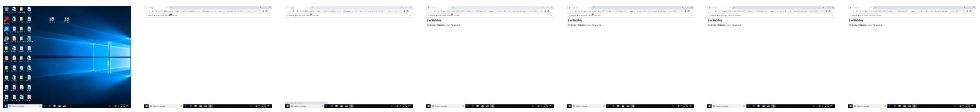
Behavior Graph

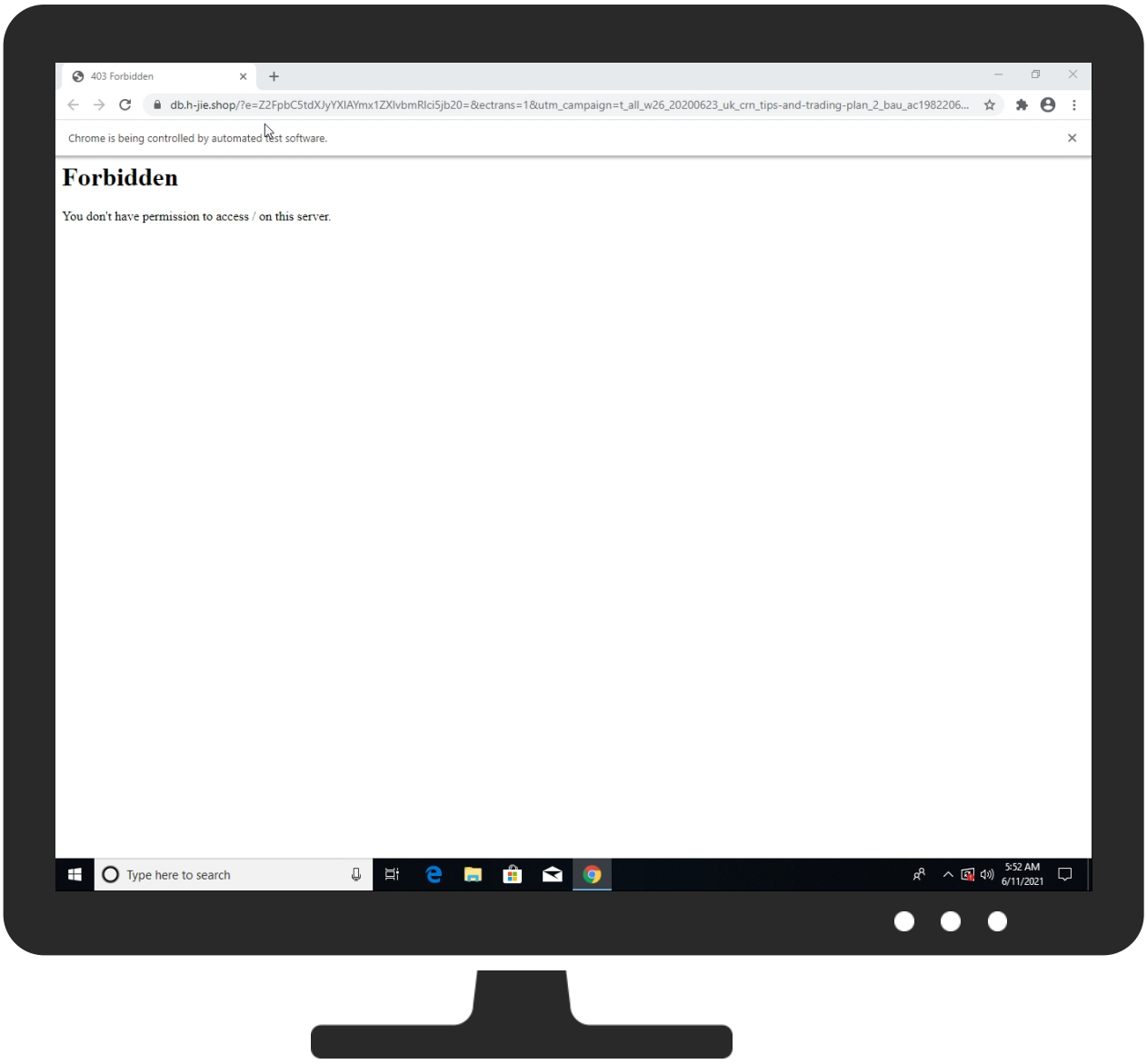


Screenshots

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
http://https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_crn_e2_bau_all&uid=67912768&eurl=photobox-mkt-prod1-t.campaign.adobe.com/r/?id=h4e5ec0b9,69a17086,5eb6e68f&utm_source=photobox&utm_medium=email&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&_c1v=crm&_c2v=trigger&_c3v=creation&_c4id=1982206&_c5id=1772187782&_c6id=all&_c7id=acc&_cdt=2020-06-23&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&p1=db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=%23/my/creations	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
db.h-jie.shop	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
pb.eulerian.net	0%	Virustotal		Browse
pbox.photobox.co.uk	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_cr	7%	Virustotal		Browse
http://https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_cr	100%	Avira URL Cloud	phishing	
http://https://db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=&ectrans=1&utm_campaign=t_all_w26_20200	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
db.h-jie.shop	192.119.65.250	true	false	• 1%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.201.193	true	false		high
pb.eulerian.net	109.232.195.140	true	false	• 0%, Virustotal, Browse	unknown
clients2.googleusercontent.com	unknown	unknown	false		high
pbox.photobox.co.uk	unknown	unknown	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=&ectrans=1&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&utm_medium=email&_c3v=creation&_c2v=trigger&_c1v=crm&_c4id=1982206&utm_source=photobox&_c5id=1772187782&_c6id=all&_c7id=acc&uid=67912768&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cdt=2020-06-23&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c#/my/creations	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.119.65.250	db.h-jie.shop	United States		54290	HOSTWINDSUS	false
142.250.201.193	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
109.232.195.140	pb.eulerian.net	France		50234	EULERIAN-ASFR	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433016
Start date:	11.06.2021
Start time:	05:51:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_crn_e2_bau_all&uid=67912768&eurl=photobox-mkt-prod1-t.campaign.adobe.com/r/?id=h4e5ec0b9,69a17086,5eb6e68f&utm_source=photobox&utm_medium=email&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&_c1v=crm&_c2v=trigger&_c3v=creation&_c4id=1982206&_c5id=1772187782&_c6id=all&_c7id=acc&_cdt=2020-06-23&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&p1=db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=%23/my/creations
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:	17
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.win@39/221@3/6
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\1adc5e77-9b4c-4cc4-ad44-d36de672c81b.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):	164054
Entropy (8bit):	6.050173973069635
Encrypted:	false
SSDEEP:	3072:UZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:UZu7RElMjk71aQw7hbSm7aqfllUOoSiq
MD5:	242127BF6DB7E4DC1E6183F7F182EE0B
SHA1:	0E44C3F7BEDF7B0136D63F5A48F6B3F06DBCDFE1
SHA-256:	80255B51620E77609628879C144268ED14DFB4CD5FFBB963877F563A01424069
SHA-512:	6CD56DC12154542ADE09BD5030BD47820CCB5257862019A05D55CDF4EF27577065025819884BCD6CC090BD26B011CFC4F9F668F2C5CBF3BF30237C8DECC1C0C
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715561360"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\392a2e9b-66c0-4b6b-9d41-fa4012345c42.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751928117300977
Encrypted:	false
SSDEEP:	384:fPheOQLxwUTqtNWrDvqi3ZichHsBGdUrf8qoxR0QEzrL6m38PMu+SdOc4+N31e3X:7W5JiM9FAen0m4oHfGSKECehU
MD5:	089BEC8D533E1CF19F745F45ACA2E0CF
SHA1:	015E378FEAE15AE825628BFE809C9A69DFE8B299
SHA-256:	996B6175FE3215F210208FA4DF38817F5682864EEED6FBDE9B43E18550CB6CB0
SHA-512:	ED8A81AECB1369557398EBF8D879049501327F97CAE0F9357A50062CF9CCF12765E5D3ADB40CD0FE15BDC4D479C9365C21D99CE473214F382D8321AC3FC0E5
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<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\53e802cf-febf-478f-9461-3b5acf1fe55e.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):	172530
Entropy (8bit):	6.079782012647144
Encrypted:	false
SSDEEP:	3072:KzkZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:KkZu7RElMjk71aQw7hbSm7aqfllUOoSt
MD5:	E7A08D814DC1E795FAAB90448B991F5A

C:\Users\user\AppData\Local\Google\Chrome\User Data\53e802cf-febf-478f-9461-3b5acf1fe55e.tmp	
SHA1:	17E6E6C54CDA0C38C7C539A0814E1A0FADA0C872
SHA-256:	05DDD7A7D97B8FCE5D7D4F34C5A90DFE69BC2AD76C15F29CDDCB087175B5E3D5
SHA-512:	0B300C528DFEB29B247F8E0DADE0208853EC904060B64089F71B9673132BBB6BA60087B46E07AC00B1D3165AB425A95D05CD6B10722B3F5B86B217E5D1A1741
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/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\5a61fef0-67f2-4d03-a95b-8f9da48f323f.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):	172530
Entropy (8bit):	6.079780901557343
Encrypted:	false
SSDEEP:	3072:ZzkZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:JkZu7RElMjk71aQw7hbSm7aqfIlUOoSt
MD5:	403C258900BBC67E8E45A37466F16FA9
SHA1:	5DF09C22E232B9EA03155DF76BB2B12A7F9E797B
SHA-256:	36D3D43AA60E0E2729D10EA086A2EA19F6234E1AE277BA3382EF3E37EAFB6F43
SHA-512:	A0AD8627C65CB51621A33EB8D2BFD8F74F1B29E308884C652C6AD2549B85A4848D06C2ED9324DEA9D3B4059263EAC16102B3E2D48407E5D207F68B5D29823A8
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715561360"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\71e04405-c3d4-4417-8bc9-46363ff098c9.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):	172530
Entropy (8bit):	6.079781590353727
Encrypted:	false
SSDEEP:	3072:KqcZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:TcZu7RElMjk71aQw7hbSm7aqfIlUOoSt
MD5:	0DC143312CC38A26CBC946B398389215
SHA1:	28140919FE55C2EBBFB00BB7929F8231E83E9B12
SHA-256:	ACF369387C6C05D909D75D11B152BED54E7D1F35BDC15C5EE304A0D26E6A969D
SHA-512:	034629C3A4AC9D44EE0C9CBA013DBD0543A3FE5C74453E689169CD4044722E2136838971CFA67D83307DE22391083F07E402AC60551D80AE6FB21F6527F4B6BD
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/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\84ff039d-21a6-4085-a928-99bcaacdb52d.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):	172530
Entropy (8bit):	6.079781590353727
Encrypted:	false
SSDEEP:	3072:KqcZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:TcZu7RElMjk71aQw7hbSm7aqfIlUOoSt
MD5:	0DC143312CC38A26CBC946B398389215
SHA1:	28140919FE55C2EBBFB00BB7929F8231E83E9B12

C:\Users\user\AppData\Local\Google\Chrome\User Data\84ff039d-21a6-4085-a928-99bcaacdb52d.tmp	
SHA-256:	ACF369387C6C05D909D75D11B152BED54E7D1F35BDC15C5EE304A0D26E6A969D
SHA-512:	034629C3A4AC9D44EE0C9CBA013DBD0543A3FE5C74453E689169CD4044722E2136838971CFA67D83307DE22391083F07E402AC60551D80AE6FB21F6527F4B6BD
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/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\9c696d35-02b0-4838-9c4b-db2e7a7e1050.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.752566971039097
Encrypted:	false
SSDEEP:	384:RPheOQLxs7UaVDlqtNWrDvqi3ZichHsBGdUrf8qoxR0QEzrL6m3DhPMu+SdOc4+R:ZuW5JiMsFAen0m4oHfGSKECehL
MD5:	0879F9218EDDAECF1650F35E8BA6DDBA
SHA1:	9F2D334E5BA5A74EFD65F90A06DDF376B447D2CA
SHA-256:	433D133A93C0063DEDB850C756195ADCB7C31E69B784E6D220EEF88AAA4DE3A9
SHA-512:	FAA9B18BF87C2142515B77D74E9F5D9A35E694B0F250473CCCDF4B7897969699D005C65B5727D3AC54039963CE946B7B6A5B107416B0C318FE3FD6229FB21A62
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<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\9e69f4f3-f053-4de9-ab5a-1778e2ee5ed8.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):	164252
Entropy (8bit):	6.050766406247824
Encrypted:	false
SSDEEP:	3072:8Zu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:8Zu7RElMjk71aQw7hbSm7aqfIlUOoSiq
MD5:	A4EB428F40269CD3F25F0BF06C2573D7
SHA1:	475797CD7F1BB9CFC8BAB43143A8B284F91698FF
SHA-256:	A53D113094EE323A409A250C3E7EBB4A98E8066ED07BAAB612B64B1A2740C8D4
SHA-512:	69B205046CD0297FB44BECF13148B0FCA21C89689468C3AEDA0FAA9A6C04B19D9D9E3BBF8D8D28ABD92651BA6EDB02F923B5029B90273E121423B849F72326AE
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715561360"},"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):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\09b9f190-d178-4d45-8e10-acd5b6797ae7.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):	1756
Entropy (8bit):	4.851330006474358
Encrypted:	false
SSDEEP:	48:Y2nzMK6qDHGXCtwWsZzRLsDZyKsE53zsDMHUYhbw:JnzMKxDHGXCOXib5eGlhM
MD5:	4A11C08F90CC07D6444285A4375BD24D
SHA1:	6AFC442E802683CA1C7C88C15022FF2BF195B825
SHA-256:	F04E97DAB46B30048270B043A2BCF3C32F18C9C0730A442D2ED6E7354217DC77
SHA-512:	F9AC0743B7088EC0746AF6C4B18AD50D65876929E9D7CFDBBABE626ABB64BD6AEA7B8358E2DEFFE7CADBCC5CCB0C0531E0584F37B40EEC3F15B9D70F6F751ABE
Malicious:	false
Reputation:	low
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://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],"expiration":"13270449152935463","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15847498-bb27-4e73-a62d-98fa5bc712f2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
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\3184508b-e9cc-43f8-9d2b-3e96b802fede.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d71f7c5-ad57-4836-b0c5-a4a04dfb7c6f.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):	5795
Entropy (8bit):	5.188501024236958
Encrypted:	false
SSDEEP:	96:nZLyR2RlYNr5IVvy5k0JCKL8EkOvsrbOTlVuHn:nZLG2ROXI4h4KBkOE1
MD5:	2678F87BC624468960BF228AE980E01B
SHA1:	E20236DF0F33EE43EB0ECB25BEC5B42C8D1AF341
SHA-256:	72B069B4A4D6A96CC5830B9A1E1051CC1833672F8D6C09B4A2B691FED25DECB7
SHA-512:	D0C4DE0083F6B71A5B27CDD94941DDB73E8ED40150889C90DB28C8A177328FDA979F41FA7FF53B08E4F289A2365BC4D987CCD41ACECEAEA9259487CEE47BBA0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267857150562782","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\54c8bc2f-fff0-4ee8-9966-2f4861f30118.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):	1207
Entropy (8bit):	5.575018765611453
Encrypted:	false
SSDEEP:	24:Ym6H0UhsS42bUW+G1KUeiXzkq/HeUe8zUeTkQG7wUJQeRUeiQ:Ym6UUhscUW5KUeiYqPeUekUewLwUJdUg
MD5:	626A09F97ED79D36D49EAA9E3BF26D2F
SHA1:	704B66E00B9487B1BACEF40079A2E646A2C30105
SHA-256:	72743DC91BC2E2C15D5D14BEB28F8BAA15FD04D0CDA714683FED6B11147640DC
SHA-512:	EC10CCD69E27C039A6CEE04FBBD0E0ABA0B7E2266CC305A5B84638A69144143F968987D0CBB3DDCF18C6076E8221C4CE757BDD975655A4F058BBDF3D7991E84
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1623988352.9114,"host":"PgO2hxZ8M4NN0VDnAAB27T8oaIslSdQhqT+pzM9wZp4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623383552.911404},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1654919552.935554,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b29af88-7a51-491d-a6d9-5b297de13fd7.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):	22600
Entropy (8bit):	5.5365340571245705
Encrypted:	false
SSDEEP:	384:AS+1tRLlhMXU1kXqKf/pUZNCgVLH2HfDarUPHGYnZQycq4j:oBLlkU1kXqKf/pUZNCgVLH2HfurU/GYS
MD5:	C7BA8B17F7E0568205BBB4F6FAF65075
SHA1:	B94CED03D192111A7B040CA40F01472CD5291A07
SHA-256:	EC04714E622FB2B142CB1FE8AEA22780B0A8227406542461CA7D394A9699340B
SHA-512:	8FC8A8A376ADDD05CDB74D0904621A9B79C9B29B1744BB6A143BDB5A32ECEDD2745A3F91150FF9BA67D52E8D691EDB9E5A4F315CD41344DEF054F88DBC1A9C7
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267857150273875","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\728ef585-4764-45a4-8036-8f13d214a59c.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):	24064
Entropy (8bit):	5.534354547148771
Encrypted:	false
SSDEEP:	384:AS+1tALlhMXU1kXqKf/pUZNCgVLH2HfDarUkHG0HGYnZgZcq49:oQLlkU1kXqKf/pUZNCgVLH2HfurUoG4X
MD5:	531CEDD7C9FB4D116FFCF00F8C8ADF1F
SHA1:	F4B49B01A29D99EDAA90E370DE6CF380777CC143
SHA-256:	8A88EFDB535A9739363E7A29A7F79A2592210DF434912C0DA48ADC7261933583
SHA-512:	9915C31D06854A11BA6C1630595B6AC6CCCCD72BF73DEC0370CD8D37274BB03731ACEFC8939B36542E09BB5E3EAD1218A1C33599F002001994835F67EFA4936
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267857150273875","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.202902936864267
Encrypted:	false
SSDEEP:	6:mwmEEAq2Pwkn23iKKdK9RXXTZIFUtpDmToZmwPDmVkwOwkn23iKKdK9RXX5LJ:pEAvYf5Kk7XT2FUtp5/PO5Jf5Kk7XVJ
MD5:	2B8BBABA7372C7AA0F2F8A9DA7B127AB
SHA1:	0BB78A44BE5B8B231564F1939AE6A1AC9536C956
SHA-256:	E3A506178C32B693851A9FDB0065F4EA203699C7014CD5BDB7EE725CB866D9A8
SHA-512:	79A225FC53F1994D3CE2364E2B9E061C17305F08621CCD9C1EAF787111E40C4E94A1F5AB7B30EED4850013390DE6665B27125613C07C0C3D4B48F1B956E866C9
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.426 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-05:52:38.430 1ba0 Recovering log #3.2021/06/11-05:52:38.440 1ba0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.1933236445782045
Encrypted:	false
SSDEEP:	6:mwmaq2Pwkn23iKKdKyDZIFUtpDmfIZmwPDmQQkwOwkn23iKKdKyJLJ:HvYf5Kk02FUtpEI/PE5Jf5KkWJ
MD5:	73BC2E76CD786DE7D41EE62DE2263F9C
SHA1:	D0DF1DF001CB4518AD951B8094B7CA79978ECC20
SHA-256:	6C657219007EC1FAF58F07DDA8CDA876E12F0EC8907B64FA6503016A21E632E5
SHA-512:	BB9FB0877A4611D59BBA6F94588D5AA447864636DC3AE653DFADA1C7AF2BA3ECFE381D543C57C02C80F05949AE0EC9A294652DFB29C1AE4CC7912F4B6137DA76
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.422 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-05:52:38.423 1ba0 Recovering log #3.2021/06/11-05:52:38.424 1ba0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.1215123928870596
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06Uwc/JzmfVuFuy9Ix9Kk5p:TekLLOpEO5J/Kn7U1/JYVuFu0ILKk5p
MD5:	77BD126C24EAADF461D29EE152EB6A8A
SHA1:	87678C69AF76286D7A2F53EE88EAFBA76F571A49
SHA-256:	E7694EA54CA1ACD19E86058333152B03BA44955479156557050D060723A58D78
SHA-512:	A5CBF5BC8FB50CB9F1F95F1C4DD4FA74457A13E3BB471C4314C44B2332CD437F393E83C2BEEC443EAA708030507220EF226B50432E331D7DF8C18D24676EB03B
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9730623212757649
Encrypted:	false
SSDEEP:	24:de9H6pf1H1oNqRqLbJLbXaFpEO5bNmISHn06Uwg8:dbfvoNqRq5LLOpEO5J/Kn7Ur8
MD5:	433CE93EA4C7887475215DBEF3ECD803
SHA1:	9227E776CF14E1C6CE35EC7F2DD5622DABC6B930
SHA-256:	1BD72E745A90B3D4196CF79959E1BC8C6E36B46CACD38205CCC1B096C918BA6A
SHA-512:	C0CB0877809416F8B54E7A36BBD37A5D8D33F791B51DFF316F4F86DF8844EA5645B0A5D2915ACF717903578F4D9F100D7C91B8A86F1FE41C3208375A9FB8AB9E
Malicious:	false
Reputation:	low
Preview:	.....K..)..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2904
Entropy (8bit):	4.597216039375315
Encrypted:	false
SSDEEP:	48:34doYxTeiZCK7M7XHCag501ne1nhfruogBIPor:34kW74HCN01ne1n9aogBIPC
MD5:	8B555774411019273 88EF584271C1EAF
SHA1:	0D93606587EE9C98A75DD93B47D50001804A26EA
SHA-256:	FAF2A6DFCFB76029A2696006D16DA70D510096926C4DC78280960A70644C29A6
SHA-512:	E2BDE5DCD9B31B963AD7B5218D2BD68317224E6FEA06D79C8645AEB79280BAB534F482C0DF3D46941F766231EEA79EDAB5013EEDEA0B1AC1E2EFA6290155CED
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...0b35a3de_f03b_497b_aa4f_2be0a1e3d9c7..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....https://db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=&ectrans=1&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&utm_medium=email&_c3v=creation&_c2v=trigger&_c1v=crm&_c4id=1982206&utm_source=photobox&_c5id=1772187782&_c6id=all&_c7id=acc&uid=67912768&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cdt=2020-06-23&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c#/my/creations.....h.....`..... .....i.pu....i.pu...X.....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.162445677624946
Encrypted:	false
SSDEEP:	6:mwmgU+q2Pwkn23iKKdK8aPrqIFUtpDm4XZmwPDmvNVkwOwkn23iKKdK8amLJ:HvYf5KkL3FUtpZX/Pcz5Jf5KkQJ
MD5:	8740609C4829BF7C5D5D76FFD8DBA34E
SHA1:	D2795FAC0DD896CD23E7E4B21513A67851E5B17E
SHA-256:	C1E3C8867CAB844D3E12B2451F589F22CF1E0B6424DCC038D26BAEC2E96A14FD
SHA-512:	F2F1C93A169154D344B4F5953366F99DCBB8B4004FE3EC68332970725B459045A9389FDABD9A65D643F8A2D06B46610D7179C9C1FA15DCC74FFF34B7DCC183E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.566 1ae8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/11-05:52:30.567 1ae8 Recovering log #3.2021/06/11-05:52:30.568 1ae8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Reputation:	low
Preview:	.f.5.................................f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.131348132969166

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Encrypted:	false
SSDEEP:	6:mwmV5q2Pwkn23iKKdK8NIFUtpDmc2ZZmwPDmc2zkwOwkn23iKKdK8+eLJ:WvYf5KkpFUtpk/PE5Jf5KkqJ
MD5:	1720F37A6DDADDDF10A6E6AD4737E9FA
SHA1:	F26FAA7728A7BDA59A7AD1D90C1734EBCA4FFB58
SHA-256:	44E2576E966220C9B88F9DC3D1882129450041B870F7B8C1164DBB04795D4BEB
SHA-512:	275FE3B5DE1A2ED87E8CE66AFAC9285E3CE9BBBBEB048E236E1FB2EFA7A6CF371723C6B6D603805F8709070606600C1C93EFCF0FA772FD774D2A466CB3E8C37C3
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:32.620 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/11-05:52:32.621 1ae4 Recovering log #3.2021/06/11-05:52:32.621 1ae4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_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):	23474
Entropy (8bit):	6.059847580419268

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.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):	5.251811549207524
Encrypted:	false
SSDEEP:	6:mwmDSq2Pwkn23iKKdK25+Xqx8chI+IFUtpDm6ZmwPDmGkwOwkn23iKKdK25+Xqx7:XvYf5KkTXfchI3FUtpv/P95Jf5KkTXfE
MD5:	CCC5A83818560A1021CDF6C3DED171C4
SHA1:	877EC260E7B123831EE02097134AD3CB4853E928
SHA-256:	AE3229D80F6D1288338D264CD742E9D7C5900DCB47081EC4DB95A0E790A1FA06
SHA-512:	F2DA5DF724A863AB1B9FCAC5EF8C6877F32CDEEED3FA8E3E7E39DC11B25D32D773D659F6B72AAA9654B4E4739CD77A3F2DE1F75122269CD14F1CEC9DB79D577
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.417 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/11-05:52:38.418 1ba0 Recovering log #3.2021/06/11-05:52:38.418 1ba0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.200397626843331
Encrypted:	false
SSDEEP:	6:mwmFSq2Pwkn23iKKdK25+XuoIFUtpDmIZmwPDmHxkwOwkn23iKKdK25+XuxWLJ:KSvYf5KkTXYFUtpR/PS5Jf5KkTXHJ
MD5:	6E27D8CD1433FD8E248D594F9CD43C09
SHA1:	C65C223A80A5F7CE76EAADAEE830A47A73E7D2BD
SHA-256:	C5518D08EDAE437613CE20DBB203F2EDD4250CB9F7B31E9AFD3B5D8214935117

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
SHA-512:	1D54B5ED71545663EEB9E60BD48AA9AB03F1A73A6C2FA38C032BAF26CCE1A7A5F80C69C76C29DB19C0FDB289122016B164F0F56F794DD12DA7CC08206CC324 B3
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.411 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/11-05:52:38.412 1ba0 Recovering log #3.2021/06/11-05:52:38.413 1ba0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.258759319657607
Encrypted:	false
SSDEEP:	6:mwmaLOq2Pwkn23iKKdKWT5g1IdqIFUtpDmUbZmwPDmwHUk7kwOwkn23iKKdKWT5i:FOvYf5Kkg5gSRFUtpHb/PF0k75Jf5Kkn
MD5:	ABA19517AE6678A9C52673EA5848EACA
SHA1:	04A62B4FB42F7B5C9C57C0D147D2CC5662EC1D85
SHA-256:	D39CB994C953921B5EF70F8EEFC6E395149699F65A6FB6FECE68E0100EBD1A61
SHA-512:	FCF448388A56C65089BEC2723CD2275B02AF6165B9253F80B16ED361E0FC4A53448EE4BB2509E8B4CE3524EC06AB12EF8B9173FBFA3192475E848363D952DB5E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.377 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/11-05:52:38.379 1ba0 Recovering log #3.2021/06/11-05:52:38.388 1ba0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.1494840122277459
Encrypted:	false
SSDEEP:	48:T9fruogBIvAiJruJg5+Np2AKi+ruJgRfruogBIu:NaogBIvAMaJRT21PaJ8aogBIu
MD5:	F0D8BB7612B16045ECE3D149A2F82D55
SHA1:	2A184B589BFA1C2D44FAC26E719BDD66BA35206D
SHA-256:	6E400F1806871F7E2C957D6D1DD83EEBC6C306992A67DBD52D6D5286E0B685F3
SHA-512:	3C9F81B172AAB96A6DBC7F29DFDC42B0CBD441C290ED1BC703AA9F082C08B5085C48C0B9724DA2FB211063EFEAFE06FA1B56D1CF3578D132B9CFC13107C0AED
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11711264084621417
Encrypted:	false
SSDEEP:	6:U4vzvg4ESsfSM8MkWg9bNFlWCj/lFel3ll4/fMt76Y4QZeS/rG99pG/3qR4EZY4A:psHqLBj/L63ll4nMWQASjG9LpBQZ8fOL
MD5:	ECA9311626355A0A33395A3AB91ECB6D
SHA1:	D7692A0750362D8EBB846DE1F73EC95CBD316AD4
SHA-256:	B205EE6990E519C1DB9A4E0C0174088B5779575B7EEEA18A71C467947EA25BA3
SHA-512:	84B6CCE9F70B63D4132B8B2221B09639E14CEF26696D3E3A9662E49920FF2B4EBEB43584E468C9B1D84644534D18D5DC8B3F43E26628465A9665AC982163359B
Malicious:	false
Reputation:	low
Preview:	.....>.|..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.466015605865162
Encrypted:	false
SSDEEP:	48:kuGx3fa7iM58db1piyybbQSefgGrkNrS0U9RdiN9+:ePa7iM6db7iyobQ5fgGQrS0U
MD5:	6943B8D09B183970FCE0E9DC46FCA7AB
SHA1:	BDF4A8F284021EA9E70F359B9532CBA4762656B2
SHA-256:	5618D8F87EDCC86B35D51B6693340936ED950F2017FBE24784FCD2B4FF91AD03
SHA-512:	3164CE3837CC0D42508BBCFE56A9E9D206B4BB2449D8A9393F97849B407F5930A048B197E6F46129DFC4F984340EC0285B3899416294FCBE6A33C785F247CC08
Malicious:	false
Reputation:	low
Preview:	.7.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..8478000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-11 05:52:40.04][INFO][mr.Init] MR instance ID: 944c5e1c-9c7d-4092-8b2b-7d7a607ee114\n","[2021-06-11 05:52:40.04][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-11 05:52:40.04][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-11 05:52:40.04][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-11 05:52:40.04][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-11 05:52:40.04][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-11 05:52:40.05][INFO][mr.CloudProvider] In

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.183181402811726
Encrypted:	false
SSDEEP:	6:mwmBKQ+q2Pwkn23iKKdK8a2jMGIFUtpDmBtFzgZmwPDmBtFzQVkwOwkn23iKKdKw:mKVvYf5Kk8EFUtp2tJg/P2tJI5Jf5Kkw
MD5:	64A77CCDC14F7809770D2B061D41FE6E
SHA1:	A0BC5D6B9EE54D58EDC760BCA38BFD513C555FD4
SHA-256:	74AD0216252A510766802C976967C4B373B58DC996A3E30D7693120F755E4CBA
SHA-512:	49EAE81499C69D74D84B4C705BC7215C91293D64C6A111B750572F8C681E82C5E1995D00C1AF5139E693FE56ACBA34FFD68F6D2F08AB58C504F0A2DD6BA792F
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.298 1b28 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/11-05:52:30.299 1b28 Recovering log #3.2021/06/11-05:52:30.299 1b28 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.212644030484166
Encrypted:	false
SSDEEP:	6:mwmoAOq2Pwkn23iKKdKgXz4rRIFUtpDmFpZmwPDmAFkwOwkn23iKKdKgXz4q8LJ:aOvYf5KkgXiuFUtpop/PpF5Jf5KkgX2J
MD5:	B11631CB534BEAC7C973170801EA07EF
SHA1:	6A6CB8EC1781D8C64B28470FBA5CDF53A9EDE9F3
SHA-256:	9EAAEFA72EF27997EBA655EF70616CF42396AECD54CF8421607D0F9C4DD26111
SHA-512:	53129C258A436037A3D4FB4F53AC9C98156307BA0993FFCAE7BE3E9C457C9C0D70A16032F1B99CF9ECFDFE1497D00BD6A9D420FE1CEEA776758237FB1F51570
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.589 1b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/11-05:52:30.596 1b50 Recovering log #3.2021/06/11-05:52:30.597 1b50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.1588152159568414
Encrypted:	false
SSDEEP:	6:mwmHQUEU+q2Pwkn23iKKdKrQMxIFUtpDmHfupZZmwPDmHae3VkwOwkn23iKKdKrb:NdpvYf5KkCFUtpAupZ/P+5Jf5KktJ
MD5:	F103E063CD71AF0913A0528528CB5F0F
SHA1:	43103C8B3524F6F2C8D6260F82E50924851C2E75
SHA-256:	C0834C581FBCF9DA8458B363ABC638551BF7DAAF499EA8EA9DF019BB38F4F1E3
SHA-512:	00AACF94C9DA49E1AC1574D22D302A5F25C4AEA4494CF20FD8BB79864EE5C4DE3D17509F9B31F94D589B997516A5323793D7A11A534446B4015FE2B8760B105I
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.487 1ae8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/11-05:52:30.488 1ae8 Recovering log #3.2021/06/11-05:52:30.489 1ae8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.125848607293632
Encrypted:	false
SSDEEP:	6:mwmBHN4q2Pwkn23iKKdK7Uh2ghZIFUtpDmBJ8JZmwPDmBJ8DkwOwkn23iKKdK7UT:mt4vYf5KkIhHh2FUtp2J8J/P2J8D5JfI
MD5:	86F096DB394B5C82F37EA29595D6E769
SHA1:	15430D59FD3D94093D52A92D15DE96FEC55CC295
SHA-256:	786C6E41B1A7B291EE6B41B7EAF46C4680F8A26332BF45F1D58BD082EEB974D9
SHA-512:	9BC842D259500853DBA9862FA0C459327FE516485C0F06EB4557EA6BD0816C76C81B713DDBD19CF8C5CE8CD639E7A14F609F41774F166F8C0DD0CAB6D3C682C
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.260 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/06/11-05:52:30.261 1ab4 Recovering log #3.2021/06/11-05:52:30.261 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\65834b19-8eb1-480a-bf47-dbb856f81491.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:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.215728947172551
Encrypted:	false
SSDEEP:	6:mwmzd3+q2Pwkn23iKKdKusNpV/2jMGIFUtpDmcZmwPDmfVkwOwkn23iKKdKusNp+:UdOvYf5KkFFUtpB/PK5Jf5KkOJ
MD5:	AB497C8BC60474451F3E6648209015D0
SHA1:	F45F64028725C377FECEFE26A6246697F23D3D8E
SHA-256:	DA8DDF5486DE00453ED87570069DF7DB7DB7515F070888645A5717EA1A082761
SHA-512:	D06F9EFC3F35AF81971DD7B8EC122C894288D28B3D4EF7A3AB39D02DE31414F376E8FFE75F847B78CCA0EAB6DEAB8EC1A3D1FF253A83C4D0FB9CE3C461873A8F
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.555 1ae8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-05:52:30.556 1ae8 Recovering log #3.2021/06/11-05:52:30.557 1ae8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.28407455605153
Encrypted:	false
SSDEEP:	6:mwmAq2Pwkn23iKKdKusNpqz4rRIFUtpDmzZmwPDmr2kwOwkn23iKKdKusNpqz4qG:9vYf5KkmiuFUtp2/PZ5Jf5Kkm2J
MD5:	B8105851A286FD2D69A9923BBC2AD380
SHA1:	AB0302C0CA76D003CFCE7A58416E34B3BAC50ACF
SHA-256:	5E2997079ECEB9D543271B9B5B76FCA0921C302B76940A862BCF1683531447A2
SHA-512:	E9F9911A29BECCE196A41F2B16E938AE0154A2402E31EC0A16DF75B36BF2E78DC0177CBAD3E327AF6BB628F2932F684B53CAB20FC7FB63D97646505639597D5
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.591 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/06/11-05:52:30.597 1b40 Recovering log #3.2021/06/11-05:52:30.598 1b40 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.272381393046476
Encrypted:	false
SSDEEP:	6:mwIOq2Pwkn23iKKdKusNpZQMxIFUtpDZtZmwPDZfkwOwkn23iKKdKusNpZQMFLJ:VvYf5KkMFUtpr/Ph5Jf5KkTJ
MD5:	F00AB7903B5E97181D53180306B7C475
SHA1:	998EAF94344EA006A269C062DD6670EE01BACD46
SHA-256:	B9C39F45E4866FBAE3D792E92F0741AB8656B59E24E2DBD4A8627D281193A588
SHA-512:	F767313DA2390856FABEBF7E27759426BABE22AB522CD34B7BBA6186DE95C5A6A2047693586B97BE97489A1C45A6BC89ACCE5CAB49FEFB6E7950E27C89A0E5DF
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:46.882 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/06/11-05:52:46.883 1b24 Recovering log #3.2021/06/11-05:52:46.883 1b24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\65cc1306-712a-4e23-bf15-cee1f91bff9b.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
Reputation:	low
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):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Reputation:	low
Preview:	.'..(.....'..(.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.242449174834344
Encrypted:	false
SSDEEP:	12:qzVvYf5KkkGHArBFUtpFdAg/PFwI5Jf5KkkGHAryJ:yYf5KkkGgPgXdDlJf5KkkGga
MD5:	8FCE2F711A0EB1B9B7A6B1AEB0665D55
SHA1:	83C1B94532DF17735971C32BDC09A98A96388600
SHA-256:	42C92B0E9BBA5D240B9B5E94E702A09A5D7E22AD00D907184C8F73803B190FFA
SHA-512:	F132BF6ACB0E353843A738C75A11F9560955C0FA35FCCD79DAD01A24B7518DC86D9F077C6B193AD998E78B02CBD5F37D32B0F376E76C5A4587603B2FF8A9173
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.738 1b28 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-05:52:38.741 1b28 Recovering log #3.2021/06/11-05:52:38.743 1b28 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.272402293124902
Encrypted:	false
SSDEEP:	12:1dcvYf5KkkGHArqiuFUtpFot/PFV5Jf5KkkGHArq2J:1dmYf5KkkGgCgX4HJf5KkkGg7
MD5:	B0190BEEE0DFD358D5448B42ABDB9003
SHA1:	ACED53E3CFC757AEF8232A5E033460B002F8A01D
SHA-256:	96E7F1D8F632BF18FCBC84F34ADA7F45EE16930FFD43C38742BD3D3AC7546FE1
SHA-512:	B7E8B92C7C151C9632F9EDCB7B0B6E5F3B16C6347E362FEC09DFD59F1C7AAA5076985C7AA1E9BC53FFC049EFBAFE6DC55CFC4B0573F8110246ABC74409FFF 9E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.741 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/06/11-05:52:38.744 1b24 Recovering log #3.2021/06/11-05:52:38.745 1b24 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.245630485878036
Encrypted:	false
SSDEEP:	12:0VvYf5KkkGHArAFUtpkt/PkG5Jf5KkkGHArfJ:05Yf5KkkGgkgS6QJf5KkkGgV
MD5:	F96F8E4C2D68A22DF1D00CF95A0E4B50
SHA1:	008C0EC2F0653C3C38565E12C48B2F3F7D2F99FC
SHA-256:	377A939641B2B1B91F8442394491F37553E97F99EEA72D413481DDD731991D91
SHA-512:	FF04D7F9F5642F024815706E5C0BD93EE8C5A87D71E3979E230D1999E6C246B94FFE2EC391C605D8EF123E91C4567D3125BF0BEEAF0D0F5B019EE9C6353F4F7
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Reputation:	low
Preview:	2021/06/11-05:52:53.975 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/06/11-05:52:53.976 1b24 Recovering log #3.2021/06/11-05:52:53.977 1b24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.231382607194808
Encrypted:	false
SSDEEP:	6:mwmB04q2Pwkn23iKKdKpIFUtpDmB+8JZmwPDmBMDkwOwkn23iKKdKa/WLJ:m04vYf5KkmFUtp2+8J/P2MD5Jf5KkaUJ
MD5:	A6B594AE93B537DE4B4DC4C668D163AD
SHA1:	8A00463C19E48506C819B2DA2AAC876C1F15F39B
SHA-256:	E4E72C81468238CF5F786370A0062D96038AE87050C9EEBF542E9FB06928C7A8
SHA-512:	F149AC2DCF5B62F283EF9AD326B987DB7AA008D5633FC44C790537D9A68131F256A2D6B7C7B140F7CAF7137765F25B2B64FA0BBEB16603B66C490106C599806
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:30.278 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/11-05:52:30.280 1ab4 Recovering log #3.2021/06/11-05:52:30.281 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.29399278063094
Encrypted:	false
SSDEEP:	12:uVvYf5KkkOrsFUtp1g/PMl5Jf5KkkOrzJ:wYf5Kk+gqJf5Kkn
MD5:	4BDF8FCF01135CEAE1A339F731B5C632
SHA1:	B6EF7FCB8E72EF048C709EC83BA09378F0940243
SHA-256:	B0F9CF27E59593962E6BC178F41276A753095D6F605ACA2C2D93F28117B2373C
SHA-512:	5D5BC8DE840754937D93F1B18D0CF16C57FC0506D86A72E81AD3487C230715C990F9CE9D203840F6B503A7D6895AF22CEFCB67DD70DCC908FA98BA44996F2CC
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:40.045 1b28 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/11-05:52:40.046 1b28 Recovering log #3.2021/06/11-05:52:40.047 1b28 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	36

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Entropy (8bit):	4.321888195526177
Encrypted:	false
SSDEEP:	3:9BcMLcXCmly+:9bUlly+
MD5:	4B77884264E6E1440124D24B57A1CE83
SHA1:	DC9A9587F7D2B89CC72B43E672D460DFF33A2EBC
SHA-256:	3CCD8B4E11B879AB7ADFE2D7AC5EC9A4B909F8F4126EC47725D83C2A74A2705D
SHA-512:	74C8CDC1248AD5FD1CC6A6A5BF81E41ABA55F729E7E5D4183C6F4CE4F805B8B97150BE2DA60653F30FA31D06328B1F6AD01EFB3018E26C799F09DAC7DDCAE BDD
Malicious:	false
Reputation:	low
Preview:	....Y.t.....L@y.M.....4.."i.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168 B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\f1b35b14-1384-4911-9a5c-1e4d27c90efe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... ..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H...A...J..;P.....nn p}nnp}.....~~~.....!...!---2---2... .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8b8f414-7f74-41a4-8998-31c3df84765c.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):	22602
Entropy (8bit):	5.536723664013896
Encrypted:	false
SSDEEP:	384:AS+1tALlhMXU1kXqKf/pUZNCgVLH2HfDarUMHGunZgucq4W:oQLlkU1kXqKf/pUZNCgVLH2HfurUAGuD
MD5:	EA815C23633518BC2C99FAB7309889B5
SHA1:	3506C8DEC24A3B3F06BC8919D2B070B3D8D53CB6
SHA-256:	3FFFE8EF93F1F5BE49DC8CFE1DD3C35ACA81E734BA6D2DBD00F7E57DEF187F09
SHA-512:	2A71E871FAD94400334BD5E0B3EEEE2D59F84CF5A603367B832D3F40443766D9B7CD06C81FB7ABE086D4B27441AB87B45F3EA0E9E1A86A387C0EB244D650B7C E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8b8f414-7f74-41a4-8998-31c3df84765c.tmp	
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267857150273875","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\af2e5a16-3e7d-4eaf-b8c5-c73640152a9a.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):	22601
Entropy (8bit):	5.536528471321978
Encrypted:	false
SSDEEP:	384:AS+1tALlhMXU1kXqKf/pUZNCgVLH2HfDarUMHG/nZgycq4I:oQLlkU1kXqKf/pUZNCgVLH2HfurUAG/N
MD5:	CF9BCB7F0B96C12B88C8BFF1AAB6D3A2
SHA1:	BA0A1D9F73E638F02F96C139863083E823ED9A5A
SHA-256:	5BA53F5D733F14D42A6E110CE41CF264734FECB6DBB976ECBE489A6FB18387B3
SHA-512:	ED9BF2305A9C842C479A5690348FE21AE0FB3265D16EEDEAC998B6F5AD4338C83C4B2B83D38A8B357B70A94DDB982ADCC36FD85936D24BAC38BFD331F29FB9F
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267857150273875","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bdd6ff4f-2e87-4cab-89fc-ed4b2640da3d.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):	5739
Entropy (8bit):	5.179323909779663
Encrypted:	false
SSDEEP:	96:nZLPR2RlYNr5IVvy5k0JCKL8/kV1DbOTlVuHn:nZLJ2ROXI4h4KukVH
MD5:	8D05A6FC1BEF8A8A315F909F54B9D444
SHA1:	40D5E7965A9F49D1589EF2880ABEF694EE8A4734
SHA-256:	5F31533B50C8D594A9B66829DD052F61C063AD6C0D90F5AD6342E6660AF859B7
SHA-512:	F219E776921BA109D63847487E7528708250A8177E81C3EDAE907E35A0754005CEEF8DEF7DD9EF978C168CA5F845D55CF983946CD7988083C4F300221DB6AA75
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267857150562782","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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.630350364910836
Encrypted:	false
SSDEEP:	3:tUKUU3WWIEvJZmwv3GU3WZFDhA+1V8sGU3WYnA+1WGv:mwmXEhZmwPDmZASVvDmLStv
MD5:	D8E26257E489C31FC146B135CC688F3F
SHA1:	0DC778D09B43C255B9D0EB658D09D6ECA4E8EE6E
SHA-256:	ADD9C3278D2468344CDB8836848B45EC93F6B07D0A954B0DDC927B0DDAF6A75B
SHA-512:	AD2619C9368CB304EE5155FFB011C9D9DB4D1AFED382554DDFD616830B0F2A51398C64E6A8262AE0A1D2C6884C5F2030EFF945B6DC48CA9A50A6ECE428B266C
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:37.987 1ba0 Recovering log #3.2021/06/11-05:52:38.046 1ba0 Delete type=0 #3.2021/06/11-05:52:38.047 1ba0 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.269211293781373
Encrypted:	false
SSDEEP:	6:mwmi+q2Pwkn23iKKdKfrzAdIFUtpDmhrZmwPDmh7VkwOwkn23iKKdKfrzILJ:6vYf5Kk9FUtpA/Po5Jf5Kk2J
MD5:	4063EB33025F15BA75A4FFB0741250D2
SHA1:	D68B17A8FDF7D9EA6B1379468E6EFAB3A745F203
SHA-256:	5A60F3E0F0F0F6CB9DC77A08F04BDDBD12AEF44F1E1995E59EEB31847590CB4B
SHA-512:	24270EE620F8DA5CC2D9BCB3264F14D2E44A9DAB99A652F18022F521A7A362217D2BC6FBF3064DAB0DF6307F09EC6ACB6498DA1F5A3E108A73F8A68CD87803E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-05:52:38.598 1b48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/06/11-05:52:38.599 1b48 Recovering log #3.2021/06/11-05:52:38.599 1b48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
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
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.27.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6664_1145905860\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197616
Entropy (8bit):	4.955722655128328
Encrypted:	false
SSDEEP:	3072:98Lqy5tdVRpn0eYzR089VDeWLQva3jUmykfftq/3fHn13M+Ya9tKd57s7J4zpd:aLqy5jV70eYzVDYvU0Hnq9
MD5:	715067CF2947DFA3FDABA45D010912D3
SHA1:	71D4506F6DD1BD109F7DA1ECEF70D05BF95CB544
SHA-256:	0F58B5D6F89BFFE34A44803F70AEFD5A435ABD692FDD00D3B1C88575933BA752
SHA-512:	A9216F2839E9F86B4A83770E5E6D9706E788D9ED8EC831CBF51C5F73EC38E03FD96C513601B8A29848B3610D55320DCB44C97F03840657D5E2A50C9EF1CC8C4
Malicious:	false
Reputation:	low
Preview:	.....(.....Q.....p.....P.....,..... .....geips.....K..8.....lgoog.....(D..P.....ozama.....4...h.....onwod.....{..... ..g.bat.....p.....uotpo.....ennab.....q.....nozam.....@T.....<R.....h...L...0.....|.....t...p.....h...d...`...\...\...|...`...P...@...$.....<...8.. .4...0.....(..... .....`...D.....p...T.....(.....\|...x...t...p...l...h...d...`...\...X...T.....L...H...D...@.....8..... 0...,...l...$... .....@..... .....X.....4.....x...t...p.....h.....l...P...X...T...P...L...H...D...@...<...8... 4...0...,...(...$... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\b5a8fc4a-f50d-45f4-a87c-d3ce2a811346.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\b5a8fc4a-f50d-45f4-a87c-d3ce2a811346.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	164158
Entropy (8bit):	6.050493198230393
Encrypted:	false
SSDEEP:	3072:cZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:cZu7RElMjk71aQw7hbSm7aqfIlUOoSiq
MD5:	2ED743A5DC6CB3179AE2D5EE52B00D4B
SHA1:	EA8FCA6C137E198F02C26FF8EB85D08D0441E98A
SHA-256:	E7004C6CA425ABBA109BBBB51246A67FCB860F6676AB9C485A42806399BACEDB
SHA-512:	5CFC66F978D3DB56D768291309F760954B509BD4A27EEEC86D60EC03630110C3C9F2D42C162419CBFF37C450A0AAB2454BF8D3C771B95FDB690868453E5954B
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715561360"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\e61130f8-5f03-415f-8af6-ecda955f0dd7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7523010237759107
Encrypted:	false
SSDEEP:	384:hPheOQLxs7UaVDlqtNWrDvqi3ZichHsBGdUrf8qoxR0QEzrL6m38PMu+SdOc4+Ne:JuW5JiM9FAen0m4oHfGSKECehC
MD5:	0E3C73ED82F5BB7B676CB2AF5D31F78C
SHA1:	BC9F3919141A80EF88AB6B1C4CDE299020D45FA8
SHA-256:	7588A2F1C281854E06C2335DBA7D459529C7A25D8D2755E7B6B6F9B347A4BD90
SHA-512:	C2E80469B5B322AF70311C0D9319AD5EF6784DF0CEAC8D77E1B919A4A6A840F07689672DE49C139D212FFBBFE85B3C68A1CB408A47B3AA1682BFE56B3E3366B7
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<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\f88fb2d0-fb1b-4f9b-a9d8-34e9da8e3a67.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):	164158
Entropy (8bit):	6.050493198230393
Encrypted:	false
SSDEEP:	3072:cZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO8FcbXafIB0u1GOJmA3iuRj:cZu7RElMjk71aQw7hbSm7aqfIlUOoSiq
MD5:	2ED743A5DC6CB3179AE2D5EE52B00D4B
SHA1:	EA8FCA6C137E198F02C26FF8EB85D08D0441E98A
SHA-256:	E7004C6CA425ABBA109BBBB51246A67FCB860F6676AB9C485A42806399BACEDB
SHA-512:	5CFC66F978D3DB56D768291309F760954B509BD4A27EEEC86D60EC03630110C3C9F2D42C162419CBFF37C450A0AAB2454BF8D3C771B95FDB690868453E5954B
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":1.623383553245976e+12,"network":1.623383555e+12,"ticks":299653706.0,"uncertainty":4593756.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715561360"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Temp\2e06bed0-cba8-4432-a2ac-4348cc584a2f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp\2e06bed0-cba8-4432-a2ac-4348cc584a2f.tmp	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\4bd94729-d8b7-448c-b41c-60012b34685f.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6664_1197451410\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):	3.8417538334903507
Encrypted:	false
SSDEEP:	3:SRkGDEzGKb2dGMAz5Bi6QPEA1:SSUVKb2EMcXA
MD5:	C5EB6E81FF20793640FF1368767FE2E4
SHA1:	3838AB9769B8EA3F6F3241504099F6FB2591173C
SHA-256:	DB81C2532D8152C4606833C06B818B1C94FBDB0FBF98F0E89365AD4E7A093529
SHA-512:	3AE2FF526D5908E1B3F4AA5FDBBDF0D0859520CAFFCBF84BFA7D6DC31293CD08243B418533A526015BCF3F1A85E08CEBAB55ADE500D66F962EC8A19D3DA84CD2
Malicious:	false
Reputation:	low
Preview:	1.4302cf764844fc6ca4cd4de8cf5e13481c4dd15b4bd8d667869f9ae2fb54f9bd

C:\Users\user\AppData\Local\Temp\6664_1333044176\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

C:\Users\user\AppData\Local\Temp\6664_1333044176\manifest.fingerprint	
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\8089ee87-c943-415a-b7ec-180f0a2477bb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	7674
Entropy (8bit):	4.625983439498299
Encrypted:	false
SSDEEP:	192:XxPhpq8ILShj4bG4IxkN2K2C282Zp32tBQ3:hPhpq8IwEbRIs2K2C282Zp32tBQ3
MD5:	BAB9CB3FD9DA5A6A74CD6A89E65D1CA4
SHA1:	D71BD45D27B39565369BD1AAF56ED14251FBB39D
SHA-256:	9AEB776800C6FA52EA0B8FD6A7D35CEF5020178DA0093218F5B038F4B288BD08
SHA-512:	37233FF2D6EFCE566513E40DAE9A5E8BCD48B76CCBE7A7B9DD97C19A799ED7AECD76AF631C5520FCCAF18E13637A2D349196FEDAB4EE27CC0FACA894B8D7D9B2
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 57cfc675628524ee4e0821ec94bc92d902b226fb9abbb68d9dcd567647783214 69c3b0aa4376912b377d2555d3eef6fe2 9b87905cfdd10205062b8dec633b15a.SERVER_HANDSHAKE_TRAFFIC_SECRET 57cfc675628524ee4e0821ec94bc92d902b226fb9abbb68d9dcd567647783214 1 f7e85eb5cffb898fb60cf3e086c32e1fd876da45e586d22f1e7670a789fe8ba.CLIENT_HANDSHAKE_TRAFFIC_SECRET 87e96d7211c48116bb74eefa77287bc960 433854d633d8d18e38bf8431224143 c00d37b0e550b910811221f75db7af7dbc1c84d58acbece9a388d6d2101bc9b6.SERVER_HANDSHAKE_TRAFFIC_SECRET 87 e96d7211c48116bb74eefa77287bc960433854d633d8d18e38bf8431224143 e90f629a2e08932da89573e7c2412b8fd16afcaaf13b0e16df847d890b135267.CL IENT_HANDSHAKE_TRAFFIC_SECRET b1060158c742bf7b967e58939d2c8cb78e7a9aac4ef9450ea25fea70893bc5d8 d068a057ca27f370f0321278c3d3810df0b 997712216bd10cf37583f0781f19c23f45f79ea816d20d39fd2d0284c0309.SERVER_HANDSHAKE_TRAFFIC_SECRET b1060158c742bf7b967e58939d2c8cb78e7a 9aac4ef9450ea25fea70893bc5d8 4b60fde21e8859351ddc0703246e70b260fe2723cb21adff88516b3e5db5e

C:\Users\user\AppData\Local\Temp\cd824102-27b0-4dda-90a8-84e6ce3fcdd8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\cd824102-27b0-4dda-90a8-84e6ce3fcdd8.tmp	
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.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.:.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\dbaa0d02-eb9f-48a4-bd7f-d7723b915d0a.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\f2397e70-ae2a-4e31-bbf6-0dd65959504c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\ar\messages.json

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": "......".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .. ..".. },.. "14284488690781267 31": {.. "message": "..... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": "......".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .. ..".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".... ..".. },.. "12139579827238759 20": {.. "message": "..... ....?".. },.. "12827687646031907 5": {.. "message": "..... ....".. },.. "14284488690781267 31": {.. "message": "..... ....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": "......".. },.. "18027627465894571 77": {.. "message": ".....".. },.. "18503975003120203 88": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\ca\messages.json	
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\de\messages.json	
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "H.ngenbleiben".. },.. "12139579827238759 20": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "12827687646031907 5": {.. "message": "Ger.teerkennung".. },.. "14284488690781267 31": {.. "message": "Videowiedergabequalit.t".. },.. "15221406833188603 51": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "15509040647108289 58": {.. "message": "St.rungsfrei".. },.. "16366867476874943 76": {.. "message": "Perfekt".. },.. "18027627465894571 77": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "......".. },.. "12139579827238759 20": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "14284488690781267 31": {.. "message": "......... .....".. },.. "15221406833188603 51": {.. "message": "........ ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": "......".. },.. "18027627465894571 77": {.. "message": "..... ....".. },.. "18503975003120203 88": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. },.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. },.. "12827687646031907 5": {.. "message": "Device Discovery".. },.. "14284488690781267 31": {.. "message": "Video Smoothness".. },.. "15221406833188603 51": {.. "message": "Connection failed. Please try again.".. },.. "15509040647108289 58": {.. "message": "Smooth".. },.. "16366867476874943 76": {.. "message": "Perfect".. },.. "18027627465894571 77": {.. "message": "Volume".. },.. "18503975003120203 88": {.. "message": "Are you able to see your Chromecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\es\messages.json	
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\fi\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "180276274658945717 7": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876 460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6664_1046256250\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276 876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 05:52:33.624581099 CEST	192.168.2.4	8.8.8.8	0xd8c3	Standard query (0)	pbox.photo box.co.uk	A (IP address)	IN (0x0001)
Jun 11, 2021 05:52:34.262211084 CEST	192.168.2.4	8.8.8.8	0xf739	Standard query (0)	db.h-jie.shop	A (IP address)	IN (0x0001)
Jun 11, 2021 05:52:39.271289110 CEST	192.168.2.4	8.8.8.8	0x3594	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:52:33.683934927 CEST	8.8.8.8	192.168.2.4	0xd8c3	No error (0)	pbox.photo box.co.uk	photobox-uk.eulerian.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:52:33.683934927 CEST	8.8.8.8	192.168.2.4	0xd8c3	No error (0)	photobox-u k.eulerian.net	pb.eulerian.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:52:33.683934927 CEST	8.8.8.8	192.168.2.4	0xd8c3	No error (0)	pb.eulerian.net		109.232.195.140	A (IP address)	IN (0x0001)
Jun 11, 2021 05:52:34.323753119 CEST	8.8.8.8	192.168.2.4	0xf739	No error (0)	db.h-jie.shop		192.119.65.250	A (IP address)	IN (0x0001)
Jun 11, 2021 05:52:39.340059996 CEST	8.8.8.8	192.168.2.4	0x3594	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 05:52:39.340059996 CEST	8.8.8.8	192.168.2.4	0x3594	No error (0)	googlehosted.l.googleusercontent.com		142.250.201.193	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 05:52:34.703396082 CEST	192.119.65.250	443	192.168.2.4	49743	CN=db.h-jie.shop CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jun 10 18:53:35 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Sep 08 18:53:34 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 11, 2021 05:52:34.863652945 CEST	192.119.65.250	443	192.168.2.4	49745	CN=db.h-jie.shop CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jun 10 18:53:35 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Sep 08 18:53:34 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6664 Parent PID: 2460

General

Start time:	05:52:29
Start date:	11/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk&eml-name=phx_t_uk_new_crn_e2_bau_all&uid=67912768&eurl=http://photobox-mkt-prod1-t.campaign.adobe.com/r/?id=h4e5ec0b9,69a17086,5eb6e68f&utm_source=photobox&utm_medium=email&utm_campaign=t_all_w26_20200623_uk_crn_tips-and-trading-plan_2_bau_ac1982206_web_1772187782&_c1v=crm&_c2v=trigger&_c3v=creation&_c4id=1982206&_c5id=1772187782&_c6id=all&_c7id=acc&_cdt=2020-06-23&_ceh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&_cleh=b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c&p1=db.h-jie.shop/?e=Z2FpbC5tdXJyYXlAYmx1ZXlvbmRlci5jb20=%23/my/creations'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6928 Parent PID: 6664

General

Start time:	05:52:30
Start date:	11/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1588,4104926511604263749,13814431910474319796,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1820 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly