ID: 433212
Cookbook: browseurl.jbs
Time: 13:11:07
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

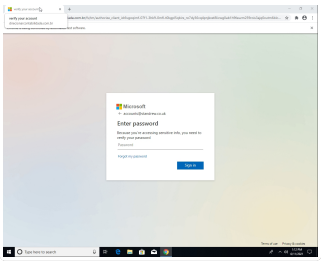
Analysis Report https://pbox.photobox.co.uk/dynclick/p…

Overview

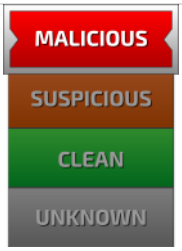
General Information

Sample URL:	https://pbox.photobox.co.uk/dynclick/photobox-uk/?eml-publisher=photobox-uk...irecionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=
Analysis ID:	433212
Infos:	

Most interesting Screenshot:



Detection



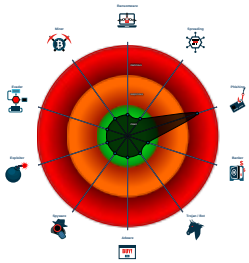
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5508 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=direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5380 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,5330392758278265500,18383578165368118498,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1860 /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

Phishing:

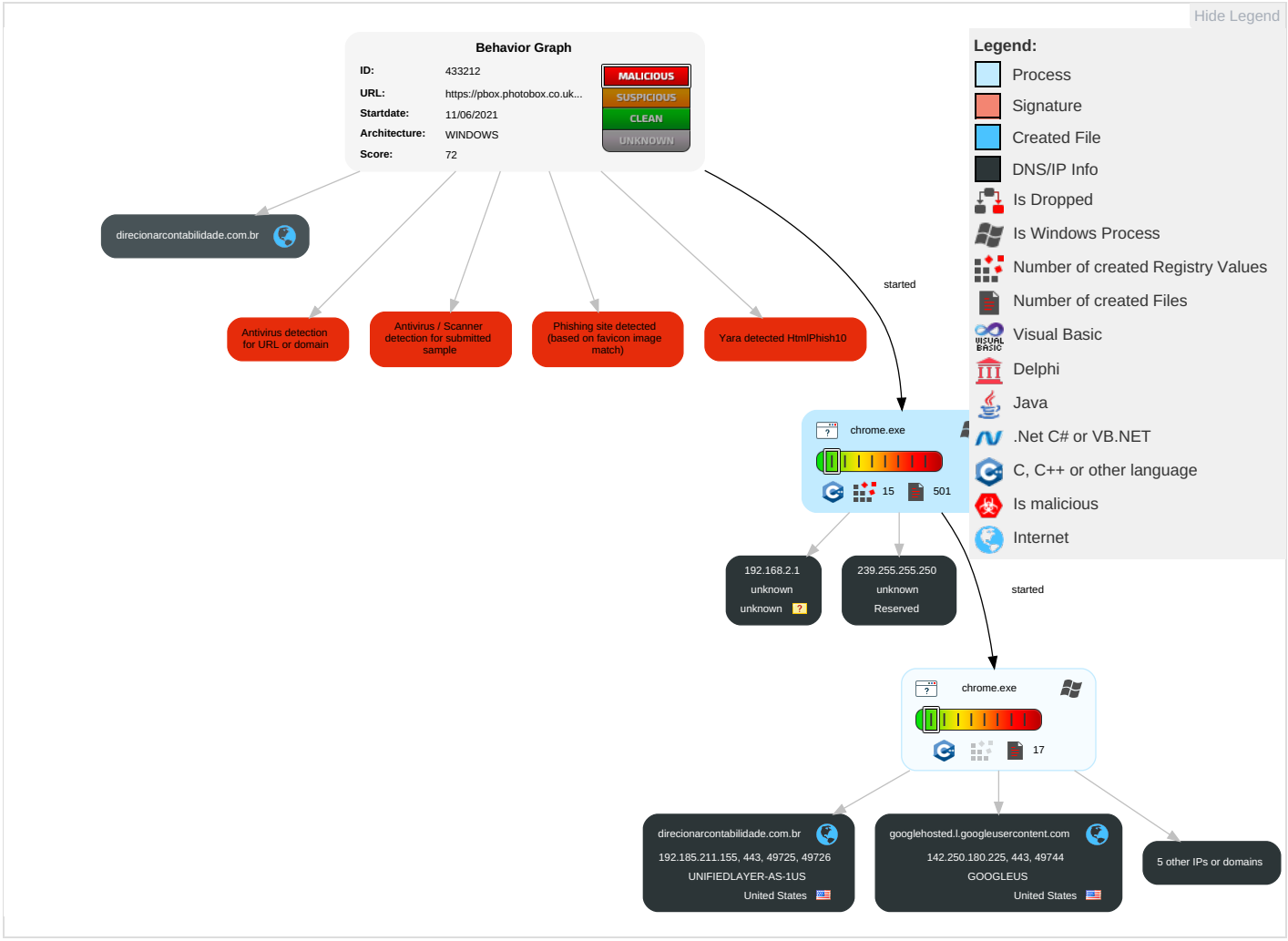
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

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 3	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

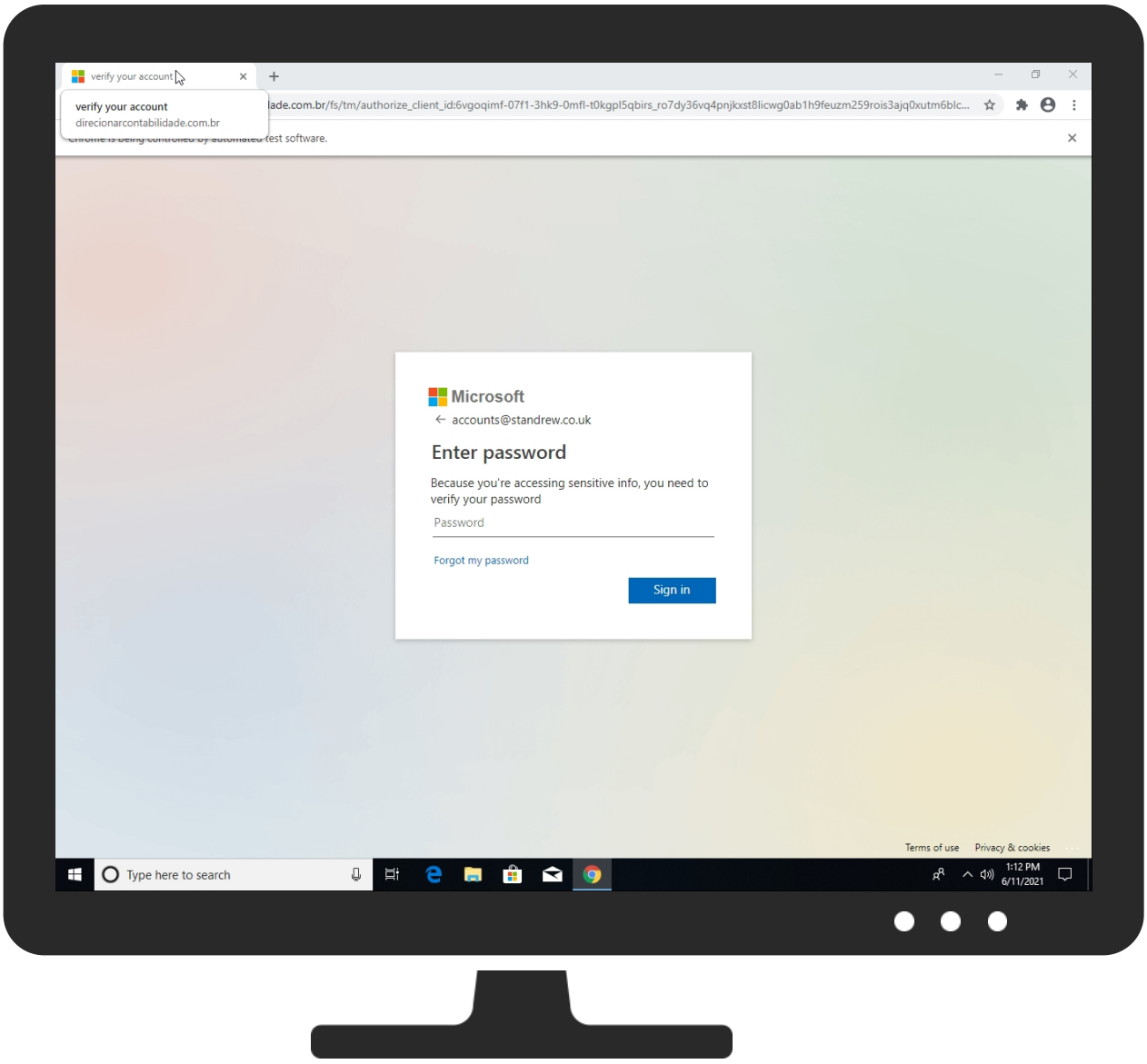
Behavior Graph



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=direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=	100%	Avira URL Cloud	phishing	
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=direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://direcionarcontabilidade.com.br/fs/tm/authorize_client_id:6vgoqimf-07f1-3hk9-0mfl-t0kgpl5qbirs_ro7dy36vq4pnjkxst8licwg0ab1h9feuzm259rois3ajq0xutm6blckyzh8pevn7wfdg2451kdr3o4wy1a7zhj5ugpcxn0t6l8siqmf29bve?data=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://direcionarcontabilidade.com.br/fs/tm/authorize_client_id:6vgoqimf-07f1-3hk9-0mfl-t0kgpl5qbir	0%	Avira URL Cloud	safe	
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://direcionarcontabilidade.com.br/fs/tm/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=&ectrans=1&utm_c	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
direcionarcontabilidade.com.br	192.185.211.155	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.180.225	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://direcionarcontabilidade.com.br/fs/tm/authorize_client_id:6vgoqimf-07f1-3hk9-0mfl-t0kgpl5qbirs_ro7dy36vq4pnjkxst8licwg0ab1h9feuzm259rois3ajq0xutm6blckyzh8pevn7wfdg2451kdr3o4wy1a7zhj5ugpcxn0t6l8siqmf29bve?data=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
192.185.211.155	direcionarcontabilidade.com.br	United States		46606	UNIFIEDLAYER-AS-1US	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:	433212
Start date:	11.06.2021
Start time:	13:11:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
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=direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=
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:	16
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:	mal72.phis.win@34/212@4/6
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:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\2ee06de9-d779-4b26-afc4-5ad961d2cce1.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):	172394
Entropy (8bit):	6.079978753390114
Encrypted:	false
SSDEEP:	3072:P4TdLgVDqfsAtDzQFU36fdYPL8JP4FcbXafIB0u1GOJmA3iuRg:gpgIRXv6fWPL8VmaqfIlUOoSiuRg
MD5:	704DCD7D8C95EB166240CEF4955566B7
SHA1:	CE32F1D18C7A8A76BDB342D9DECDD525E0AB19C4
SHA-256:	E42AECB6D7F5017178CF80A6E910C349DC7AFDE7F833CAABA8634CEBC6E819DE
SHA-512:	CB1727F8E290BFE7C9AF46495DE345F4C51A67B9B3EE3CD4C546B7D01E5B889EDCEEF0DAAADE8823559F4AA3E5F79361BBD9421BC60FAF24D5DB4C82CD1CBDB
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623442316770073e+12,"network":1.623409918e+12,"ticks":95771354.0,"uncertainty":4564002.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5a88546b-d6db-4f6c-93bb-88a22ff96173.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7517831258957637
Encrypted:	false
SSDEEP:	384:zj43/F6opJu7KNTrIvvF3g/5YHBUGEDrup/HxY5ld0rODmO5q1LfrYO5JXN21D6W:I611aFgAEe7D9BknLOVKb1vhg
MD5:	D2E57DEC88DCAA4345EB97D28F203DCE
SHA1:	0BFE9B0EF9F399C99AC90A345F114E3286AF4D97
SHA-256:	CED0C04CE6482CE11BB9643E9BEF45071BFA1AD3390137510A9A492E70028C88
SHA-512:	25908E23D985D31442B9B0831EFCDAF32BA5F1A2B8B3F80CA05E3E43E3F01B6AE7F18F4AC96B7990EF4F380B09F29E4D50A4FC7C591FC0A0E73FCB99B2A55ABB
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\95f66b07-734d-4da2-856b-2ff6f004284a.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):	172394
Entropy (8bit):	6.079979278353393
Encrypted:	false
SSDEEP:	3072:PRfdLgVDqfsAtDzQFU36fdYPL8JP4FcbXafIB0u1GOJmA3iuRg:Z9gIRXv6fWPL8VmaqfIlUOoSiuRg
MD5:	8C31F72BF856993117308ECFFF6F507E
SHA1:	A0B95DC5465E84D00895C92423C3E84104589ABA
SHA-256:	743A5B2C1BD26ADC2B1A0084504C20D8DCA3409B7C1629502BD7607DAC3DF89B
SHA-512:	CC258FF88BEA2A6969AAABF18BDF8C566F32964F3F76558417ED032CB7AFD5887BC94C8B980502681E0068A1447580C2F6849FBBC607DC0743411F10AC6E37E
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623442316770073e+12,"network":1.623409918e+12,"ticks":95771354.0,"uncertainty":4564002.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0b2cd3c0-169f-40df-924c-916765608447.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):	5730
Entropy (8bit):	5.1864568701420755
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0b2cd3c0-169f-40df-924c-916765608447.tmp

SSDEEP:	96:njChoD2RaiAXcVaok0JCKL8Slk+16bOTQVuwn:njCs2RFQcb4Klk+S
MD5:	62F1EA80FF6E01680301DEF0C49A845E
SHA1:	043DDF8640C3C54EEE3A5D043B8CCBBC4CE0AEAE
SHA-256:	BB6CA276474D47369BCE001E213EAF077F5710767BE77B6FBE83F15EF6FBF4B3
SHA-512:	6153075CFD129721E1910B20EFE2EBDEC7BD696F760837337C0003B302ECC67C26D61E348634C0DBBD2F812228E55543EB803192BCB266BF487067B66A5C48D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267915914133040","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\355af998-f745-456d-8e22-7628dcfaefb2.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):	5134
Entropy (8bit):	4.9868871513765605
Encrypted:	false
SSDEEP:	96:njCh2D2pcVaok0JCKL8Slk+16bOTQVuwn:njC62pcb4Klk+S
MD5:	46160D18D1656A40A73BC5700C29488F
SHA1:	CDB0A19854AFAFC17F0B4F2147E63FC90FF3B01A
SHA-256:	A009BEE8FB7AFF358525BD0DC3577A358309D7336306CB00F214BB0C38BC6EC7
SHA-512:	DC00B13B60124DDD1D16374A7A641B5079AD6503A67A32A0D1C9C05B8B85CE2F5915F9C6CBCBAE4786C77CD88928057020732DA7E71241A80EC3148B3540A3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267915914133040","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55f859b1-f9e5-4579-92a4-8ae57930d6dc.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ad032af-39f9-4f27-a512-899016544d88.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):	22595
Entropy (8bit):	5.536171320463521
Encrypted:	false
SSDEEP:	384:/hatyLlckXv1kXqKf/pUZNCgVLH2HfDJrU6HG3nT8T4QoEt4U:bLlzv1kXqKf/pUZNCgVLH2HflrUKG3n8
MD5:	F27AAB925FB3056D1864C21F46C87DFB
SHA1:	80A0FD0F47DA53FBAAEE373125F1EDC7BC354599
SHA-256:	2AFC9FEE990F6515EC3E85D0A02832ADEECEDDBD31545987C6DF5989DE34DA4F
SHA-512:	781EEE64EC5629EAD7B551F0B3F39A77E4682023D5E760940691A6F969C40F1FE167F05739CC6661365FCD3FA4C23155F727C9923E96213C874C29B40A384B28

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ad032af-39f9-4f27-a512-899016544d88.tmp	
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":"13267915913873603","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\99ef0c3c-2cbd-4cba-8488-636b95164b6e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.1753185264863415
Encrypted:	false
SSDEEP:	6:mw4JSN+q2PWXp+N23iKKdK9RXXTZIFUtpD4lucZmwPD4Hw3VkwOWXp+N23iKKdKT:p+va5Kk7XT2FUtpsuc/PBV5f5Kk7XVJ
MD5:	0FA4E979180C94A2FC916E44CAA0483F
SHA1:	659B2470ACE8AC9F87D54A3148FC399709C916F7
SHA-256:	41D4B3DFB54BC69DBDC898ED3052924E6563EDFD9790D31227EF39AA6E65E8E9
SHA-512:	E0B75BBC14B9428E1862FD53EA12F881CD29070467AA383C22874CB672C09397B86F0F8E2366AFF5DD466F18B53C7BC04E3E83C8A3BC03D3429EBFA48AE18E02
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.157 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-13:12:02.165 1dc Recovering log #3.2021/06/11-13:12:02.166 1dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.1433832353059294
Encrypted:	false
SSDEEP:	6:mw4Mi+q2PWXp+N23iKKdKyDZIFUtpD4ymZmwPD4gVJVkwOWXp+N23iKKdKyJLJ:G+va5Kk02FUtpxm/PnV5f5KkWJ
MD5:	CB45198D6BDF7E70CBDA00D5F479E860
SHA1:	991903FC9DB96C594072E4E930A2968CC4467C92
SHA-256:	CF26FA0FBA95B98ABE2E6BF24C3BC9A1153588134749F8CCAC58D14FDF39BA1C
SHA-512:	9876210EFAA5BAE3D7D75EDDE7625D7E7D83CCA1F6D9A4DDE89ECBA833D10A1AF0BCC066CDC8A8B7F2A50D8E8B38D96D78DA3F0B97065599FF4EB08BB0D5BE3C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Preview:	2021/06/11-13:12:02.082 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-13:12:02.088 1dc Recovering log #3.2021/06/11-13:12:02.090 1dc 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:	modified
Size (bytes):	12288
Entropy (8bit):	1.2799978028733963
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7Uq4zR7+ARKn1XIZdMo:dNw2QQn1YTMo
MD5:	8A7DA5C74603B468846F046D5529AE65
SHA1:	0670096266D41DC21B2B485F8BFD0C8604BC0776
SHA-256:	5563F88881ED4FDCF18B0CCA8AA56E7874297E718B480F636EEE7C43729FC214
SHA-512:	D523B810C4FE519935510BE0E4CF7356574062D6392AABB7AE58E6F8FBB9786BAB67FC78E72C8B25ADE99DC9F9F06B7359D7D6B4132B5B4124CF404A86022C0
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):	0.9690588496875637
Encrypted:	false
SSDEEP:	24:LCcLgAZOZD//qLbJLbXaFpEO5bNmISHn06Uw68:LC8NOZ/q5LLOpEO5J/Kn7Ut8
MD5:	78591566EB668F8FAE58B05A20EF730F
SHA1:	E12D4CD554C8737278A26C4ADC0798B848A14BE1
SHA-256:	0DBC99DFC5622CA73131852BBA23163CDCC6DF004B97FB5CECEC4CB1948238EF
SHA-512:	0F481D122DDBDB3C62FAFC29224627F0042BF1A042CE1A187B6641D0224F6C215C59E0B4271082E6C7D170DB42C7D2EA2A4B1EBBAFF3FDEC46F5CAB5AF4D9FA
Malicious:	false
Reputation:	low
Preview:	....

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):	2195
Entropy (8bit):	4.75381431664196
Encrypted:	false
SSDEEP:	48:34Jdxit2lTbU73n8c4syxux8B2FP79GppWfruogB2nz:34ZS8mVNFPUpYaogBMz
MD5:	013C5C081ECD73A0112A4C8D2A1584B3
SHA1:	05CDAD25FDABE42CADAB6AAB57BF8784D083B7F8
SHA-256:	344F906E7862130D0E700DE0FEF6F56E5B44B350836C8FD13E3D89ABFD9671BE
SHA-512:	684AE4581EC7A272CEBE1EBCC2F5972B4C056BE6C41BDD93CB512AEBBC91513AC8C0BCC9FB95DED2BF727B6B440E69B6AB4231514243902452835O7E6CA30C9
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...2256de56_8c02_49c0_8d00_7e8a453463d4.....g..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....1.,.....https://direcionarcontabilidade.com.br/fs/tm/authorize_client_id:6vgoqimf-07f1-3hk9-0mfl-t0kgpl5qbirs_ro7dy36vq4pnjkxst8licwg0ab1h9feuzm259rois3ajq0xutm6blckyzh8pevn7wfdg2451kdr3o4wy1a7zhj5ugpcxn0t6l8siqmf29bve?data=YWNjb3VudHNAc3RhbmRyZXcuY28udWs=....<...8.....0.....h.....`.....X.....`.....X.....i.....j.....h.t.t.p.s.:.//.d.i.r.e.c.i.o.n.a.r.c.o.n.t.a.b.i.l.i.d.a.d.e...c.o.m...b.r./.f.s./.t.m./.a.u.t.h.o.r.i.z.e._.c.l.i.e.n.t._.i.d.:.6.v.g.o.q.i.m.f.-.0.7.f.1.-.3.h.k.9.-.0.m.f.l.-.t.0.k.g.p.l.5.q.b.i.r.s

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
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):	5.212889952862088
Encrypted:	false
SSDEEP:	6:mwGQL+q2PWXp+N23iKKdK8aPrqIFUtpDFRESG1ZmwPD1QLVkwOWXp+N23iKKdK8h:ryva5KkL3FUtpJREX/PeR5f5KkQJ
MD5:	7828A8E2A34345ED5D2EEF819057F675
SHA1:	FEB5C854AD0AF52B885843149FFD3DCAED575338
SHA-256:	0D98C3AEBB4F0858DA1B09BD9663DBBA55EB4FC03E26A8A68E3041000FA0D324
SHA-512:	ACFE7AC9DF9D2C409035A0DEA90D16F45F0CD064D3B5E626EF10DF3A0A6B5AF166FA8667B2EC2A546C9056B13FF20334A6D04FC955045F07996A7BDD29650E8
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:54.168 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/11-13:11:54.169 1418 Recovering log #3.2021/06/11-13:11:54.170 1418 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:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Malicious:	false
Reputation:	low
Preview:	.f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f. 5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5.. ....f.5...............f.5...............f.5...............f.5...............f.5...............f.5..............

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):	5.197779752826246
Encrypted:	false
SSDEEP:	6:mwhipQL+q2PWXp+N23iKKdK8NIFUtpDhouGKWZmwPDheQLVkwOWXp+N23iKKdK8n:2Q+va5KkpFUtpeuGKW/PgQV5f5KkqJ
MD5:	163E38EFD861E6F9A54539AB75402382
SHA1:	363C6F4C7FEDBEA684010C02F2565F9422C07995
SHA-256:	E531FDE752F78D57296D7C7D3B9AA27040EE3D2DCC35E20043144F14F78354F0
SHA-512:	0F22BB3A0843BB762167A3021DC0DCE8391DFBBC4FE8E71ED5ECA736CD6DF2146BCEE28412F07B121961FDE619F998257F3EABE01721A01D9680835E2F40582 B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:56.177 15ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/11-1 3:11:56.178 15ec Recovering log #3.2021/06/11-13:11:56.179 15ec 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:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/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=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5 n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","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:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/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
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\Favicons	
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):	20480
Entropy (8bit):	2.7657715693104175
Encrypted:	false
SSDEEP:	48:0Bmw6fUN7mfruogB212lTbU73LllruprBzdnw1Ok0STXUBdsxxjmfruO2lTbU73g:0BCHaogBNEapldwsnSTkvuOaBpaBZB
MD5:	844CB0B06759F676E8DD226DA7BAA4F2
SHA1:	74FCD323314E316420E70D8C9482B06900ABED81
SHA-256:	A762945333AF4A05F55928403E9291D5765CB4723E766DD1201EA5F8DC4696D7
SHA-512:	5293379DB20CA9CE2DFDB7D4FD562428C985137F660AD33DFB88DD49CD1C8DDFE28DA8AE50BBA9ECE22072FE30CD1BBAE7A4E9495EA83AFBAA62E1851167821
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.778375471873636
Encrypted:	false
SSDEEP:	24:g2gArMJyyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwn2emM3n:g2drMJydBmw6fU22emM3n
MD5:	E4D43CE34CB30BA79DF7FE590C40B528
SHA1:	30866E339DBD1CCF86FA6C852AC351806A6D4EE9
SHA-256:	31A2E2EB09EB202D8B73D5DC3CF5466C387BD307EFEE3265AC686D817D0A3D64
SHA-512:	44ECEB090941C1EAC5A35588B62A67ACA4A1F023A73715FDC1514FB945EEB8BA23BD4EC7FD48CBF2567EE0E2CF9FEE6ED7BDAC0F1E6C574F6BAF681A472D7947
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Reputation:	low
Preview:	....

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):	369
Entropy (8bit):	5.234961155475281
Encrypted:	false
SSDEEP:	6:mw4k3+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpD4xcZmwPD4WcVkwOWXp+N23iKKN:J+va5KkTXfchI3FUtpj/PbcV5f5KkTXc
MD5:	4AE104009D8708872FB293F3A10C4C0F
SHA1:	AC6DBC6B012E66AB30345A35E4F85871DDA5FEDA
SHA-256:	17C2DCE30DE8AFA2BB8EEE91B62A35E4EE7A48C7D88BFC47E1E9ED057FC9C63E
SHA-512:	AE86B7DEC51F1D51D1DB7C82A887D996C73A54775E5C47530C1DE8CE738356CB4E9CB412D6DF100A07554492945F1A6A40008A0E031CF80380A2D9FDBC86F8D
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.045 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/11-13:12:02.047 1dc Recovering log #3.2021/06/11-13:12:02.048 1dc 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):	355
Entropy (8bit):	5.126580112999325
Encrypted:	false
SSDEEP:	6:mw4qe+q2PWXp+N23iKKdK25+XuoIFUtpD4qXOmZmwPD4qsVkwOWXp+N23iKKdK28:he+va5KkTXYFUtpxV/PxsV5f5KkTXHJ
MD5:	401E2EA983E78E17BDD28C220C844B06
SHA1:	1B019BEA4D27997576B65F8D9C8AB8281CF1597F
SHA-256:	9317F06B5C53A366C769F66BFA0C3ACE35D142953E024967C7340AAEC8DCF844
SHA-512:	8FA4D3C583FE8110CEFF39306A2B69DE9ADB7201B371162D7A1D6353412ADE193280C7EBA67418CB0CE20688E947D4E363B72BFFF682928E8359FD977081AAE
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.031 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/11-13:12:02.032 1dc Recovering log #3.2021/06/11-13:12:02.033 1dc 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Entropy (8bit):	5.183978075453867
Encrypted:	false
SSDEEP:	6:mw4Myq2PWXp+N23iKKdKWT5g1IdqIFUtpD4az1ZmwPD4wVARkwOWXp+N23iKKdKn:uva5Kkg5gSRFUtpnz1/P65f5Kkg5gS3e
MD5:	21777B35DDCE01FA2382AA7BA3FBBDE3
SHA1:	7E3101C3DAA9AB167F87E7A0D4C178874D2E6880
SHA-256:	513916750A21C88B2BC3B577B2513BA53692E33638C515199E920C00885E0ACB
SHA-512:	8710BB21129DB5353B5E5319F4F20599A951A79429A3F6EDF296673A77A0D2742572E2CA5410F946EC3CBE5C65AF8CADEF40C361DC907FCD935D509F1B1191B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:01.960 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/11-13:12:01.966 1a14 Recovering log #3.2021/06/11-13:12:01.970 1a14 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):	1.330249183084777
Encrypted:	false
SSDEEP:	48:TCtfruogB2KlJm2lTbU73glATyruprBAh92uDRsUwk2lTbU73wl+ruprBNAfruon:uxaogBrl/s+apO32SaUwDaapvAaogBs
MD5:	C0C0600CC92709FAFE1DDDE5DFCBCFE0
SHA1:	1F3EAB1C6E07244886EE638956D024ACC15C3D39
SHA-256:	BCFBA3365494628007D6E999945EAAE159B7A8AE2FCC8E74614C7EE1BBF17C31
SHA-512:	EEA20B544CA3A651F6BDACA2DBE7CDD74139C203EBFF82EA2D52266F24B58410998C8D1AB298C915C5AE97F313AC911328A10AA88ED8A95B68501ED1F007A35C
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5818
Entropy (8bit):	6.202729137189418
Encrypted:	false
SSDEEP:	96:rK74ZGvcrjpgL/jed4wVGF7bsFih2aogB2apktv4e:rK7zvcrjpg7j24wVK7Ie2aka6t1
MD5:	ADE45B0407D777A4C80C7CD04F5DFDAF
SHA1:	89FF01378867E13B59927C911C3F8CD18E0D40D8
SHA-256:	C8DA59AE6C3AE53F7D7C59124E658646FF5B06A0FC4F1CBDA71AE6A4DB305D72
SHA-512:	9089FDEC6ED0C02E80EAF99759C4D58B56FC5DDABE0F6CA0D4A401D5A4F2F766428210B7C948C542DC22A37F4B6CE4458E326AA27D0050596075B739506A5AB9
Malicious:	false
Reputation:	low
Preview:	....."...Q..06..1772187782..1982206..2..2020..20200623..23..67912768..ac1982206..acc..account..adobe..all..and.@b79bed2958568ab17f18979440690c16a1c6f09f5afc870aacd7ecb1e408488c..bau..br..c1v..c2v..c3v..c4id..c5id..c6id..c7id..campaign..cdt..ceh..cleh..co..com..creation..crm..crn..direcionarcontabilidade..dynclick..e2..email..eml..eurl..fs..h4e5ec0b9,69a17086,5eb6e68f..http..https..id..medium..mkt..name..new..p1..pbox..photobox..phx..plan..prod1..publisher..r..source..t..tips..tm..trading..trigger..uid..uk..utm..verify..w26..web..your..ywnjb3vudhnac3rhbmryzxcuy28udws..1..ectrans..07f1..0mfl..3hk9..6vgoqimf..authorize..client..data.lro7dy36vq4pnjkxst8licwg0ab1h9feuzm259rois3ajq0xutm6blckyzh8pevn7wfdg2451kdr3o4wy1a7zhj5ugpcxn0t6l8siqmf29bve..t0kgpl5qbirs*...Q....06.....07f1.H....0mfl.I....1.F....1772187782.....1982206.....2.....2020.....20200623.....23.....3hk9.J....67912768.....6vgoqimf.K....ac1982206.....acc.....account.....adobe.....all.....and.....authorize.L.D.@

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):	33356
Entropy (8bit):	0.047616568017834
Encrypted:	false
SSDEEP:	3:gln3llu/fllW/NllFl/fll//Nll2XFllFl/fllMXFllH0pMRgSWbNFl/l/4ltNl2:g99x/oXeBg9bNFlWCj/lEW/l3n
MD5:	1A038B07528E85A5BE4024BFE2BF3923
SHA1:	E246A0271FED539BFA76C42CED57E0D05B6C3586
SHA-256:	EF12580E4A9DE18CE91C5CB2594AF146E23D42835A47FAEB73A552388C430995

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
SHA-512:	407B96A8209232EB6360FA2851D97685C457BD6CF3E5F071C17DC8998357EE91D53264D738484D7202D2997C0C71219E803BEA27B183D4E55DA109BD2F1EE63C
Malicious:	false
Reputation:	low
Preview:	.....DPz..... ....

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):	2954
Entropy (8bit):	5.456755235785031
Encrypted:	false
SSDEEP:	48:nZgTJxGHJIzsa7tsM5D8dbRWr7jbQSefg8NrS0U9RdiN976:n6Tua76Mydbcr7jbQ5fgcrS0V6
MD5:	E198A8547AC3F54C195261409D2A5BDB
SHA1:	DB6681A6497343BCFF9FF807B5620DC97D69C4F9
SHA-256:	D566DB1276A3F4B667A34CB173E5862BCC298F46E0C2A2835BD6F4D7A815D552
SHA-512:	A35479362F1ADA3FB020682579E9BAF05857BF34DCCB75149B46AA58F9D9CD7E6336DFC93B17BE0091558EC3BE0EE9309648E15D74A3BDC2F691DA09DDA923E
Malicious:	false
Reputation:	low
Preview:	..~...*.....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..309342000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-11 13:12:03.82][INFO][mr.Init] MR instance ID: ee4bb815-156e-415c-8a6e-a3df4055cef6\n","[2021-06-11 13:12:03.82][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-11 13:12:03.82][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-11 13:12:03.82][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-11 13:12:03.82][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-11 13:12:03.82][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-11 13:12:03.82][INFO][mr.CloudProvider]

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):	329
Entropy (8bit):	5.209035989301693
Encrypted:	false
SSDEEP:	6:mwbS9+q2PWXp+N23iKKdK8a2jMGIFUtpDdXZmwPDhtVkwOWXp+N23iKKdK8a2jM4:Hlva5Kk8EFUtpF/PdT5f5Kk8bJ
MD5:	C86422592FCB08D9AE669821E1382CB3
SHA1:	1B9EF6F01EF66A6EEB74038DC601A605626AF03B
SHA-256:	7974D050CD86E235B6E4FB635C7E100EAC82C6C877D33B62D76DE5C245A634B9
SHA-512:	1B42D414336BEEB5011D4883E6C185C1319F524F8D6A3F29AB27530A2C34E177704EFC030F7BB57E3EB7113F7C2A0D2FD236E19D9A90904D73FC0B1479FCE50(
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:53.909 728 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/11-13:11:53.913 728 Recovering log #3.2021/06/11-13:11:53.915 728 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):	331
Entropy (8bit):	5.214662735023354
Encrypted:	false
SSDEEP:	6:mw4IN+q2PWXp+N23iKKdKgXz4rRIFUtpDl1ZZmwPDl1NVkwOWXp+N23iKKdKgXzW:zIva5KkgXiuFUtppH/PpV5f5KkgX2J
MD5:	F31042F4A08FD7B0CE569DEB423BE918
SHA1:	07F5E255F900859D2339C13FC6FCC19C737F6718
SHA-256:	CC45553E069A2A38F3F388ECBB1701A0C3C267CA4BFEF01392C0E3342C455FFD
SHA-512:	3CD41566377E9C191978C98F51FB9C3B804F651920CC21A5AFA149D15B65C9749F5D31F53571D53D94E2690005E1AD21F05070AFCA9966A1873527395EDAE782
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/06/11-13:11:54.198 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/11-13:11:54.200 508 Recovering log #3.2021/06/11-13:11:54.200 508 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:5ljljljljl
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):	317
Entropy (8bit):	5.181251522688807
Encrypted:	false
SSDEEP:	6:mwtU+q2PWXp+N23iKKdKrQMxIFUtpD1ZmwPDHQnVkwOWXp+N23iKKdKrQMFLJ:jva5KkCFUtpx/Pj05f5KktJ
MD5:	B43B3671CF6FF80B8AB7E8EC6B1170E0
SHA1:	E8D9FCB02E807FA05EDC12D2C7F6798280A393BB
SHA-256:	1CEA18EC219713657CD8E5E53DF156B70C576D987C4A2577B805923D8641C5BB
SHA-512:	6E45F43B48AC504F0C1B306A6FE61F3992B8C21B20351927A3CD58E7B5D45186A03837E19B9A9A1D98D9F4C40823B2FB255435F0B57D5217395480F7FD8DEA5B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:54.085 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/11-13:11:54.086 508 Recovering log #3.2021/06/11-13:11:54.087 508 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):	5.2088212568699035
Encrypted:	false
SSDEEP:	6:mw+wOq2PWXp+N23iKKdK7Uh2ghZIFUtpDU9ZmwPD7VFckwOWXp+N23iKKdK7Uh2w:awOva5KkIhHh2FUtpo9/PHvc5f5KkIh9
MD5:	782568CDF0276D22EB340C0DA4C3AD93
SHA1:	C695FF155B79C1AC7CA86FCD71E35C15923D6161
SHA-256:	8511BA8E1259045DD2D305C3842E14DE73EBDD91A2775D90BEA04C409C6E499B
SHA-512:	D0562B96CEDC850A8A16A7F8F55F6D21F9C02BC7CE3490FA935B80C9A874BB7646EF64F0FA2342D3C69613C4A3D87B1B2E8DAADE311384D6A1240795F659044
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:53.876 12f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/06/11-13:11:53.879 12f4 Recovering log #3.2021/06/11-13:11:53.880 12f4 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\1cf3a28d-ccca-4a09-a2ba-4a88eb543005.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\1cf3a28d-ccca-4a09-a2ba-4a88eb543005.tmp	
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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):	427
Entropy (8bit):	5.252180712135989
Encrypted:	false
SSDEEP:	6:mwZt+q2PWXp+N23iKKdKusNpV/2jMGIFUtpDvIZZmwPDvINVkwOWXp+N23iKKdKK:9ova5KkFFUtpkZ/Pkz5f5KkOJ
MD5:	7325684E8C58DFE8F87903939B69BFA6
SHA1:	6BCE4B1F6FA908B35D6D06F3DBD1E853AE2F49D3
SHA-256:	67DBEBD3A2D42B24C16379E8132D95ABD6F7CFCC250CBB10C1573EDEFFEFE7AD
SHA-512:	7E2FFF23E2315E3127AE1DAE22591AA0AACDE743C132306A98322BC2EBF2DE08FDB88879DBED669C7EB1AD7F313C1B9C342F5C3A00872F59577B8E20E76EE428
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:54.141 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-13:11:54.142 508 Recovering log #3.2021/06/11-13:11:54.142 508 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):	5.269688601944261
Encrypted:	false
SSDEEP:	6:mwdUQQL+q2PWXp+N23iKKdKusNpqz4rRIFUtpDbG1ZmwPDbQLVkwOWXp+N23iKKi:JUFyva5KkmiuFUtpY/P4R5f5Kkm2J
MD5:	58379CB7591F7CF3928D81CB572BED01
SHA1:	6C235A8F38D3F799AFB72A6B1A40060D314A22E9
SHA-256:	6081E39BCF2F98F190AD52A1A3D6F5D16B9615BD9C752F6542D1E3D91FE9E66B
SHA-512:	C66F3B4E9F2ED287F46DEBBB6D88AE893B63334873BA4F942664E1FCE8DF137BBC30A4BF6806AEB940FB41F2A348711313ABAE4C3262EB7E417D9E50B9E576BD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Preview:	2021/06/11-13:11:54.202 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/06/11-13:11:54.204 1418 Recovering log #3.2021/06/11-13:11:54.204 1418 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
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):	415
Entropy (8bit):	5.223198713310842
Encrypted:	false
SSDEEP:	6:mw4EI+q2PWXp+N23iKKdKusNpZQMxIFUtpD4En5ZmwPD4EntVkwOWXp+N23iKKd0:7va5KkMFUtp15/P1T5f5KkTJ
MD5:	A8427648AF06DF183B2E517E37E6DFF0
SHA1:	A21934A37F415D2DAB0B1281023F8DAFFEBAA935
SHA-256:	D3C1CFE049C9452F132426243C5B0A291F4DED40135CF827EBC19675269DB710
SHA-512:	E1FCF0EF190400F9FCDE4F0EB034DA60FAB399940E416E0E3031A74D0750CFBD7144C13688B82045B4B1BCCD940E26B054B64E606D0EED12DB9C904764D4A1 4
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:10.214 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/06/11-13:12:10.215 dd8 Recovering log #3.2021/06/11-13:12:10.215 dd8 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\8c591ad7-c12e-4405-8317-1c5b4525818b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.175828742819958
Encrypted:	false
SSDEEP:	12:XIva5KkkGHArBFUtpO/PBF5f5KkkGHAryJ:X6a5KkkGgPgIf5KkkGga
MD5:	9860AD4111F40C51BB5757A829F21EF1
SHA1:	A9BE12BED05AF9F23D965FE10EBC777B93665E6A
SHA-256:	D876A2DB721C21C3F264F319004B40A23A21EBC9734683ECAFC1D1BC4CC61041
SHA-512:	F2AE3C67EA4656AA0B2151DB821C74010DD652F3AD9DA14BD0877FD326E37BB6CEF2C6D0455C2151321AF4694A2ECEB1F21FF615EB55DEED4CF85418E62BA8
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.114 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-13:12:02.117 508 Recovering log #3.2021/06/11-13:12:02.118 508 Reusing old log C:\Users\user\AppD ata\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):	429
Entropy (8bit):	5.171535808109863
Encrypted:	false
SSDEEP:	12:Eva5KkkGHArqiuFUtpg/P75f5KkkGHArq2J:ua5KkkGgCgaf5KkkGg7
MD5:	4A30A90BD643BA715786427F2A1A56B1
SHA1:	C5DF174E433A6CDC529C67CAA661EB79AC7CC4F1
SHA-256:	838D7DFE9FC47F288AF39CB142EDA9195ACEDF3B9C963E4A34AF7EFB8BC42498
SHA-512:	4261F12405CBD561E62C4EAA9ECC02DF250BABA320897059C421619EC2748F2A15B631035D00F58F9BB4D67AB09B71A392CB3B9D7A12468B717E5E1F808D5603
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.115 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/06/11-13:12:02.118 dd8 Recovering log #3.2021/06/11-13:12:02.119 dd8 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
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):	415
Entropy (8bit):	5.168928268119745
Encrypted:	false
SSDEEP:	12:Iyva5KkkGHArAFUtp3Z/P3z5f5KkkGHArfJ:ha5KkkGgkgVRlf5KkkGgV
MD5:	EA018C243AB9F79ABBDD556DE5E22A3C
SHA1:	151EE701B2A69D3F42DCAAF1C5363521F930A8FF
SHA-256:	A4C1441E73F19CBF83C4A8B3E3B9B4BCFEF45F7CC4B2A7E5AA6218EB1B6CAD91
SHA-512:	EED66894CEE4119A4730DF91125B6D46D6BE6673FE7A032576C57AB266F9F5189A8A86F6B5B025844FE42CC3274C8684E912F9FBF37F8FAF64D8DBDED55C238
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:17.336 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/06/11-13:12:17.337 dd8 Recovering log #3.2021/06/11-13:12:17.337 dd8 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
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):	321
Entropy (8bit):	5.2781768713288395
Encrypted:	false
SSDEEP:	6:mw7hA4q2PWXp+N23iKKdKpIFUtpD7MJZmwPD7RFxFkwOWXp+N23iKKdKa/WLJ:3hA4va5KkmFUtpHMJ/PHjxF5f5KkaUJ
MD5:	A1DAF13CFC3653EA26EFD464D3A4BDE8
SHA1:	EF23316E1B1751F1E6242BB9CE1586A65FE1F36A
SHA-256:	7D4A9F869750D7EC790A1B542932498F879BB028C95CC47A1A8897D5F988E482
SHA-512:	B4C9371208915C1FBCE02F7544C43938D7EC1743BAE7E2B71004A59239B8C14EF693F7F8B00EE42B5036DBAEEBFAD86C67BA6DD7357D9CAEB34D1BACBA749 87
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:11:53.881 574 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/11-13:11:53.883 574 Recovering log #3.2021/06/11-13:11:53.884 574 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):	399
Entropy (8bit):	5.302455852196152
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
SSDEEP:	6:mw46QFt+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpD46jZmwPD46S3VkwOWXp+N23iC:GOva5KkkOrsFUtph/PI5f5KkkOrzJ
MD5:	812EDE011E3D532A12DCBD4E5FC05582
SHA1:	1DC2D043239ECCB9F966241221B6B5E911AA943D
SHA-256:	FC047DBCB33F7FB1EE069A74691B222AA9219B586DD9D3E308DB6DA6394B288D
SHA-512:	CD45E4F292D4198B1F519590005536BAF00191DEBB8FC486F512CE9412850663D230838D32351C293AC47B04BD8A568E6CB647E47FAE7B9985C20F4018BD2060
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:03.805 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/11-13:12:03.806 dd8 Recovering log #3.2021/06/11-13:12:03.807 dd8 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):	48
Entropy (8bit):	4.522055208874201
Encrypted:	false
SSDEEP:	3:37uJWHV72/:35HZW
MD5:	DC6F9AD59CD557C95936F18BAA2BC5A9
SHA1:	3BAE5019CCFB53C598C0C0627B2379311AD01015
SHA-256:	25EAF79CBAB9F43E7E9853108BAE7834E09EC7ACC7E8D5EEF1BD3619986240A1
SHA-512:	06C1D8172D307B0E87E3A2DB4A86E957D0FC878F865A7422D9664CF7BC90E2D6B3180D3B9273D2423B602CA76CA277AC66E63213DD5C9D58BFF5D98A04F11A
Malicious:	false
Reputation:	low
Preview:	.....R?l.....P.....k.....;k...=..

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:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\af67d7f8-6353-42df-b607-a187e641d822.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\af67d7f8-6353-42df-b607-a187e641d822.tmp	
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\a0c4e483-0a17-436f-96e7-67c40907d63c.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):	24055
Entropy (8bit):	5.5338928717368825
Encrypted:	false
SSDEEP:	384:/hatyLlckXv1kXqKf/pUZNCgVLH2HfDJrUiHGJHGMnT8T4Q6SEt4Z:bLlzv1kXqKf/pUZNCgVLH2HflrUiGtG5
MD5:	7C60DADA7B222204A29EB73085D74122
SHA1:	A43F519662CFA4A4B630ED849B94296B579DDBEF
SHA-256:	ECF0F8EFEF8A8C1ACA6A49A1FA60F760975E0D09CCD39A05CEDC6E827EFC8FB0
SHA-512:	8F8065C0E65CE3D27F10CAF09ADBB6D9D40BB6A316DB50E0C53D727C17994A44109C805103F89870712F5F73B6506456E417A0476042D130656685BAB7BEBFB3
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":"13267915913873603","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\ce76418a-d515-451a-9160-edaf8a0cb7e9.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):	22594
Entropy (8bit):	5.536179540622254
Encrypted:	false
SSDEEP:	384:/hatfLlckXv1kXqKf/pUZNCgVLH2HfDJrUQHGMnTmT4QpEt4/:YLlzv1kXqKf/pUZNCgVLH2HflrUUGMnW
MD5:	9181F9F68701760F1EAB1C7A2F7C8E2C
SHA1:	3EEAABCBB0815A3F10A92F4863D51F6215A388B5
SHA-256:	47A2AACDD958090C7B479D95497CB1BEDFE65FF4BC3165E84356BF25265EF9AF
SHA-512:	3E6BE8E87742F5C3C4D1E11FD7923853CEF85B5A081DECED8D2B9D988F978FB401AB82F9F96870755A92A4D844A07165D529E8FD192F7734E4006E02953DCD5
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":"13267915913873603","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	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):	136
Entropy (8bit):	4.488312225339183
Encrypted:	false
SSDEEP:	3:tUKUUFGG11Zmwv3GUFGUrASV8sGUFGUrASWGv:mw4GXZmwPD4UUSVvD4UUStv
MD5:	721F67A4B8E3FEC549F2259AD32332B1
SHA1:	1B5C3C9836D59AE41AA8107CF05E5F88E71F0632
SHA-256:	BD3269E9182327DD5E82FF476041ACF070EB01B1D38DB8C83F067D8D18FCAA5B
SHA-512:	D9ABB210CE295112D47DBD40BF937E0600BB8995FE49AE36F7F167057905E1BD7DD8FEE2614EBBC1D274A443005A3304211C3F7038CDA1DC580DD34B2193F0E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:01.488 1dc Recovering log #3.2021/06/11-13:12:01.574 1dc Delete type=0 #3.2021/06/11-13:12:01.574 1dc Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dbffaa0b-102c-4946-adb0-ed7dfac53cb0.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):	1206
Entropy (8bit):	5.576303470925583
Encrypted:	false
SSDEEP:	24:YI6H0UhUoR2bU5sTG1KUerkq/HeUeXby2qUeXvX7wU/z9RUenHQ:YI6UUhUgcU5seKUewqPeUer2UefLwU/2
MD5:	65C0F4ABF0DF5A05F1CE08F8A0F974BB
SHA1:	00D26AAB75076E3D3A45FC298AE69F90B425563B
SHA-256:	D6922B927A8BA8FDD6745C5779C96A4AE0EA93D0E7A77C419713D952F313CA91
SHA-512:	FA5CBCE09B37ADD8214E22B9ECBC67D9340B4AFD802F14FD2750E3F31300D0CC6487BED8A237CBA38C42E517FCE0A96EE36017CF196E16DCD7F88557F64B285
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1624047116.523563,"host":"PgO2hxZ8M4NN0VDnAAB27T8oaIslSdQhqT+pzM9wZp4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623442316.52357},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1654978316.548615,"host":"8/RrMmQICD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Entropy (8bit):	5.161873379205375
Encrypted:	false
SSDEEP:	6:mw4H+q2PWXp+N23iKKdKfrzAdIFUtpD4uZmwPD4fd3VkwOWXp+N23iKKdKfrzILJ:Dva5Kk9FUtpf/PcT5f5Kk2J
MD5:	BCBA9076CD574FC00720DEFB8A37A704
SHA1:	39B924BA709DB87C96CB2C85AA5D507C42C14193
SHA-256:	3987B1C7FE7B0FD015BF32CC7A9549F42F5AD686C78C0E0DD7B033B0D782AEBD
SHA-512:	F7DA87F0935174F52AFDD34AA99AF3FCFFC0663EAB2A06D37059F491E2E5037826FBBD43F9656609A32F4502C4B0B96D1B93371A1BF917597050468BBCE925ED
Malicious:	false
Reputation:	low
Preview:	2021/06/11-13:12:02.314 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021 /06/11-13:12:02.315 dd8 Recovering log #3.2021/06/11-13:12:02.316 dd8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shar ed_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
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
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\b1e6142e-57c4-49b3-bcb5-3f8e17742bc5.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):	172394
Entropy (8bit):	6.079979278353393
Encrypted:	false
SSDEEP:	3072:PRfdLgVDqfsAtDzQFU36fdYPL8JP4FcbXafIB0u1GOJmA3iuRg:Z9gIRXv6fWPL8VmaqfllUOoSiuRg
MD5:	8C31F72BF856993117308ECFFF6F507E
SHA1:	A0B95DC5465E84D00895C92423C3E84104589ABA
SHA-256:	743A5B2C1BD26ADC2B1A0084504C20D8DCA3409B7C1629502BD7607DAC3DF89B
SHA-512:	CC258FF88BEA2A6969AAABF18BDF8C566F32964F3F76558417ED032CB7AFD5887BC94C8B980502681E0068A1447580C2F6849FBBC607DC0743411F10AC6E37E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\b1e6142e-57c4-49b3-bcb5-3f8e17742bc5.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623442316770073e+12,"network":1.623409918e+12,"ticks":95771354.0,"uncertainty":4564002.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\13489708-e2f3-4135-99f7-05f15f20db00.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...I5....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\143f4401-6c2b-4ac6-b5f4-84721c765b82.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...I5....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\4c88130a-8823-4f7a-8187-d38148913625.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\4c88130a-8823-4f7a-8187-d38148913625.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.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.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\79042fa7-9d59-4e4f-b51e-9b8991eaf17d.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\a5d96ea2-d2bd-45c2-bc9a-8b0c804ba2f3.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):	9198
Entropy (8bit):	4.620912761644036
Encrypted:	false
SSDEEP:	96:sFTjBN+yz1zBfDCcr8JEhqiF4xZLli5jGUIUUvHzMDzzyQ4HOJoucpnGNjHQLtSt:s1jL+m1lD78kqKA1lgGxuuQoBp482
MD5:	3F2DF0B185A844FE921F1C86283204CC
SHA1:	FC08C91F2A9B7752B6D23B9AF1D18125EB7C6AD4
SHA-256:	DB7DEDD500E2451034335E09811475B25AABF56FD5D7E06E9867485644C87317
SHA-512:	2D3A6B02F0382859375B09ACCDA1022BFAE462AE32924BF8203F955201CB874FC24503878276542664678 7D7F236AFA576852569C410EEDFA35CC6A4AA1092E0
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 00f348c1c3988071b958c02ba9b8039e455f3482702bae5fa07cd08f57eb801c 9e62e133d965455c7d5111bc2b73a08ff f5c148a285fa5768cbd5da44c7df3ec.SERVER_HANDSHAKE_TRAFFIC_SECRET 00f348c1c3988071b958c02ba9b8039e455f3482702bae5fa07cd08f57eb801c 1 3836908047170b3a33c55cbf0bfdf9951b807d612cd8fd33565c7ec073623e6.CLIENT_HANDSHAKE_TRAFFIC_SECRET 3ebf8030b3ff64aefe8e2afda267a51517 7506073ee7a9e8db739ee618728be7 260fd4fb36ab93656db9a012e46afd8eafaa8bb0023f3f58ac6f0f589aa3c50e.SERVER_HANDSHAKE_TRAFFIC_SECRET 3e bf8030b3ff64aefe8e2afda267a515177506073ee7a9e8db739ee618728be7 80d34a2ebd1c33caf967eb11c51a70f34fde9ab99b18f236b6ffb500c1fd93a9.CLIENT_HANDS HAKE_TRAFFIC_SECRET 5586ee5626d83bd1ec2b3adc47b8853697a0a01b77c8603ba142e4467aa28f35 7664f818ab213f70969d62c9a69786f229d87240a53af 184aca534b27bac2cde.SERVER_HANDSHAKE_TRAFFIC_SECRET 5586ee5626d83bd1ec2b3adc47b8853697a0a01b77c8603ba142e4467aa28f35 4d2bf9ec634c6 e126b98b22ce14102ab8a6da32d9e269fc3988965fb8cb5a3fb.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\f83e1990-c308-4668-bac7-12a3015f2367.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\f83e1990-c308-4668-bac7-12a3015f2367.tmp	
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_dir5508_1967848061\13489708-e2f3-4135-99f7-05f15f20db00.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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\ca\messages.json	
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885 B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\de\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\es\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\fi\messages.json	
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34lTQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\hi\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D03 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\it\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... .."... },.. "app_name": {.. "message": "Chrome . ... .."... },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....."... },.. "iap_unavailable": {.. "message": ".. .. .."... },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\lt\messages.json	
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\nl\messages.json	
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5508_1967848061\CRX_INSTALL_locales\pl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

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 13:11:56.237677097 CEST	192.168.2.3	8.8.8.8	0x6b48	Standard query (0)	pbox.photobox.co.uk	A (IP address)	IN (0x0001)
Jun 11, 2021 13:11:56.904490948 CEST	192.168.2.3	8.8.8.8	0x8007	Standard query (0)	direcionarcontabilidade.com.br	A (IP address)	IN (0x0001)
Jun 11, 2021 13:12:01.207192898 CEST	192.168.2.3	8.8.8.8	0xc3c6	Standard query (0)	direcionarcontabilidade.com.br	A (IP address)	IN (0x0001)
Jun 11, 2021 13:12:01.821882963 CEST	192.168.2.3	8.8.8.8	0x9de6	Standard query (0)	clients2.googleusercontent.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 13:11:56.296098948 CEST	8.8.8.8	192.168.2.3	0x6b48	No error (0)	pbox.photobox.co.uk	photobox-uk.eulerian.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:11:56.296098948 CEST	8.8.8.8	192.168.2.3	0x6b48	No error (0)	photobox-uk.eulerian.net	pb.eulerian.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:11:56.296098948 CEST	8.8.8.8	192.168.2.3	0x6b48	No error (0)	pb.eulerian.net		109.232.195.140	A (IP address)	IN (0x0001)
Jun 11, 2021 13:11:57.305038929 CEST	8.8.8.8	192.168.2.3	0x8007	No error (0)	direcionarcontabilidade.com.br		192.185.211.155	A (IP address)	IN (0x0001)
Jun 11, 2021 13:12:01.402879000 CEST	8.8.8.8	192.168.2.3	0xc3c6	No error (0)	direcionarcontabilidade.com.br		192.185.211.155	A (IP address)	IN (0x0001)
Jun 11, 2021 13:12:01.883558035 CEST	8.8.8.8	192.168.2.3	0x9de6	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:12:01.883558035 CEST	8.8.8.8	192.168.2.3	0x9de6	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	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 13:12:01.736016035 CEST	192.185.211.155	443	192.168.2.3	49743	CN=direcionarcontabilidade.com.br 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.	Fri May 21 07:50:45 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 07:50:45 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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 13:12:01.736481905 CEST	192.185.211.155	443	192.168.2.3	49742	CN=direcionarcontabilidade.com.br 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.	Fri May 21 07:50:45 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 07:50:45 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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: 5508 Parent PID: 4232

General

Start time:	13:11:52
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=direcionarcontabilidade.com.br/fs/tm/?email=YWNjb3VudHNAc3RhbmRyZXcuY28udWs='
Imagebase:	0x7ff77b960000
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

Analysis Process: chrome.exe PID: 5380 Parent PID: 5508

General

Start time:	13:11:54
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=1504,5330392758278265500,18383578165368118498,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1860 /prefetch:8
Imagebase:	0x7ff77b960000
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

Disassembly