ID: 452160
Cookbook: browseurl.jbs
Time: 22:13:24
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

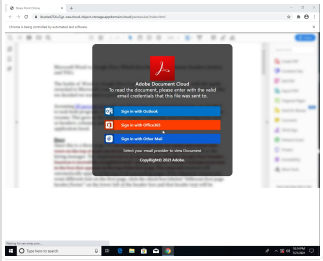
Windows Analysis Report https://ibucket254.s3.jp-osa.c…

Overview

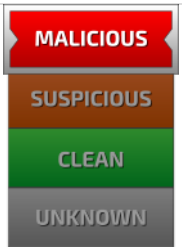
General Information

Sample URL:	http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html
Analysis ID:	452160
Infos:	

Most interesting Screenshot:



Detection



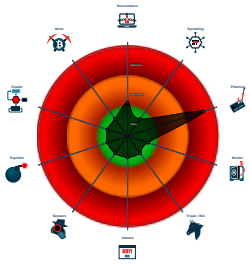
HTMLPhisher

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3180 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5416 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1628,2857767762921153429,2104577615130111225,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain

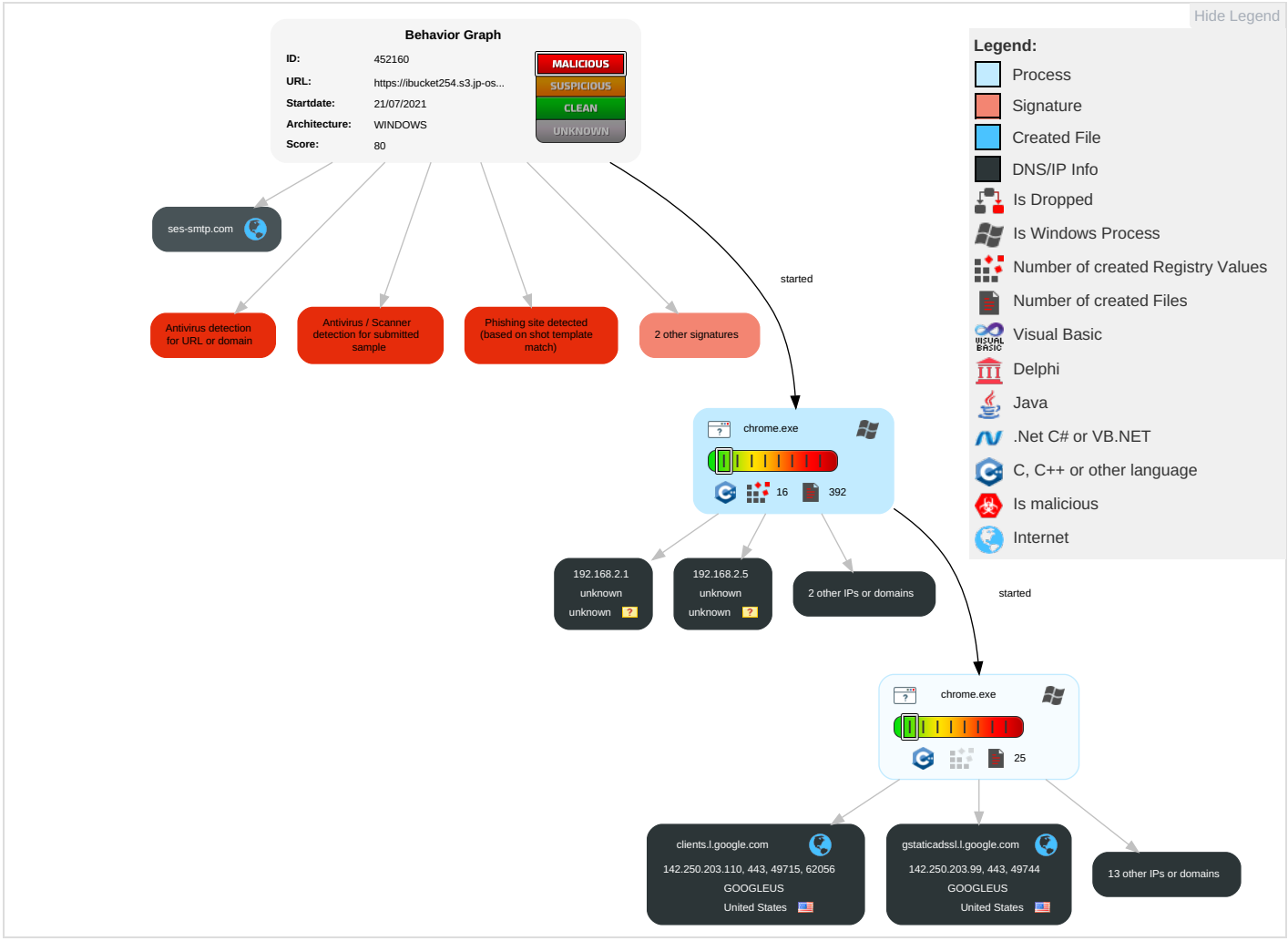
Phishing:

- Phishing site detected (based on shot template match)
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7

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

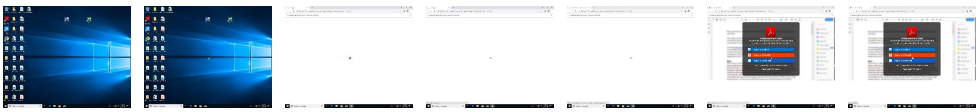
Behavior Graph

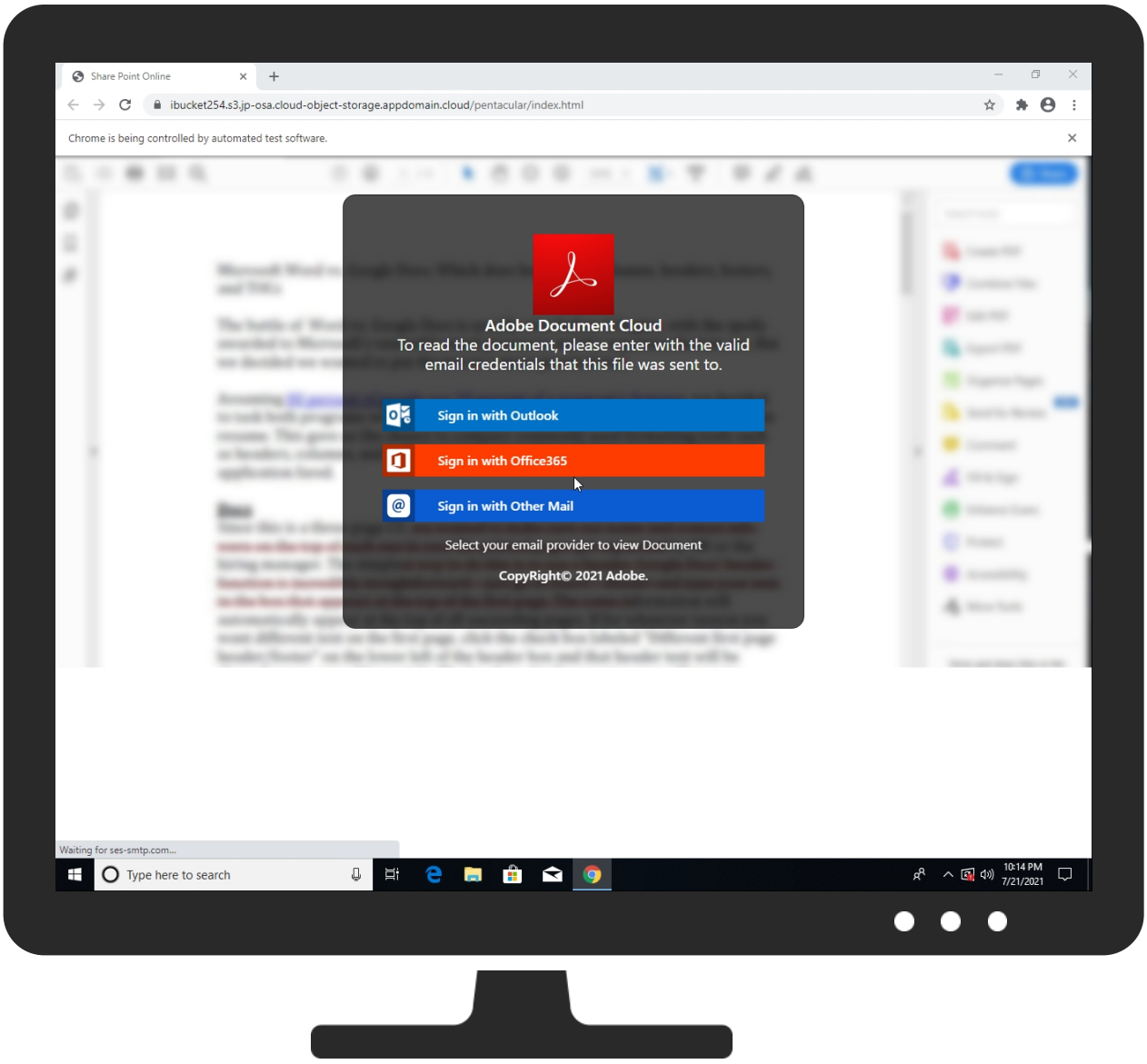


Screenshots

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://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html	0%	Avira URL Cloud	safe	
http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.htmlShare	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html2	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/=F	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://ses-smtp.com	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.203.99	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
ses-smtp.com	104.21.16.61	true	false		unknown
s3.jp-osa.cloud-object-storage.appdomain.cloud	163.68.118.49	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.168.65	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.16.61	ses-smtp.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
163.68.118.49	s3.jp-osa.cloud-object-storage.appdomain.cloud	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.203.99	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.6
192.168.2.5

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452160
Start date:	21.07.2021
Start time:	22:13:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html
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:	14
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:	mal80.phis.win@28/172@12/13
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:14:24	API Interceptor	2x Sleep call for process: chrome.exe modified

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 GM DS.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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	122040
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGm
MD5:	516136E560C1392A28EDFA1A957050D7
SHA1:	BBDF208E48EFC052D332255EF84184BFC946BF5F
SHA-256:	4F812F7C8163C50FE75F441AC6797E18D02B8B66895BC94D0E1153FE24FADEFE
SHA-512:	8F25750E9014F7576E5C81E1A3DE605BB29839A38F0E60D58AB79E034ED1847D9E88A427A834BCA95BF7C4627197AC1194D5A487E0D5E5F88B95E46C4574A425
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f\|.*...'^K`\..e.....j/..\|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1455841969121088
Encrypted:	false
SSDEEP:	12:fD5kPlE99SNxAhUe0eAy5kPlE99SNxAhUe0et:r5kPcUQUfeAy5kPcUQUfet
MD5:	605CB4AB36901E9219D8960F8AD63C26
SHA1:	2194A56FA3E9B57C622CE3B9DBB8C712DF032D64

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-256:	BA6F87798DF0ACFA0B0188419C9268B901876D1324210D3FF63C64386A10E96A
SHA-512:	E6F881E2482B440A33B2ABC3FE7EFB49DD385A57408559D80F9140BF12EA4689F87040729A1CFFA710C3E0AB809EFCFE8E09F5715060043B1533F5202AEF0403
Malicious:	false
Reputation:	low
Preview:	p..... .....Q.o.~..(..... .....T'._.....$.....\...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....j6...~..(..... .....T'._.....$.....\...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\09e80c79-13e8-47b1-bad8-e0517a55384c.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):	376995
Entropy (8bit):	6.049364363276923
Encrypted:	false
SSDEEP:	6144:le98KWPnuw15QgBB/G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinp:lY4j1igBB/GNPUZ+w7wJHyEtAWs
MD5:	881C975423FA4A51D2CAE66F9C6B330B
SHA1:	088ED710553E927C2FEBC2B0272A9868B14FBF4A
SHA-256:	D139B170A26D6927F4F6892EDF28DEC8F3A1E57FD18AA1F2D2DE3C196807140F
SHA-512:	042A77FB427C99D2419134403F5E9D2E897F5ACE999038953622C1AECFFE834C86502381FF3DC450299FDD1BA04F7594C3CBE3A4190963FBB5C11BE85F5455BF
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":1.62693086149198e+12,"network":1.626898464e+12,"ticks":4900751086.0,"uncertainty":4282714.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2f4ee52e-e8f9-4531-b4b3-0367099d2507.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):	376995
Entropy (8bit):	6.04936392152037
Encrypted:	false
SSDEEP:	6144:Ke98KWPnuw15QgBB/G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinp:KY4j1igBB/GNPUZ+w7wJHyEtAWs
MD5:	E050D1FBB61CCA02E7F40DC03297DFEF
SHA1:	45C2EFB243FCFDA0A2A98705641A0387B5E7555F
SHA-256:	286067229B9E7EBA8489BD7B8F20344C3E98B0B5B6E09C6AF6DEFC3D3C1449F9
SHA-512:	E33B0A7A54A6C3CDDE874FE2BD3F434B5EADA7C4FD9A19A91CFB983669DC6E5E1C538BF3DA3E013D6C4EE8886FEBF0CFC506E334BDADBF1FEF383FAAB92BCB10
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":1.62693086149198e+12,"network":1.626898464e+12,"ticks":4900751086.0,"uncertainty":4282714.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488191863"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\575ae279-a432-4bfa-a93d-d76c82ec01f7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743288742493418
Encrypted:	false
SSDEEP:	384:7HvIQa9ru2RcTNgrJvcI3Tw67HGPGnarF6s6xDOiWFrxEmFSJqgIcDOCGQNt1AZR:B+x52KTn8eneIaAn3aEKmwwVQ
MD5:	0AE3AB8DB7A922E17D89607503E7557C
SHA1:	FDF0E35A5F04D869015647AE4333877CB2D627B9
SHA-256:	80FE8ED674EB3C565242DEB25A586692A9D56A9D5F7508D7458D79EA407A96AA
SHA-512:	58B86D57B1BB278C59A68EFCF226E3E8D3426590741667BC144A786EFE7B5FBF72C78509D3E84FA3FF8639B90C6A423864BE86F1F13F47E06BD54E7014EC63C4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\575ae279-a432-4bfa-a93d-d76c82ec01f7.tmp	
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...e@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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C 2
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\023955a4-1890-44cd-b2a3-579a6a319a80.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\20f5d36c-f6b8-4d74-a40a-e0879ff45fed.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):	1377
Entropy (8bit):	5.568365817496754
Encrypted:	false
SSDEEP:	24:YeznWswUv6H0Uhc4BVIUfG1KU+aUe47wUNYxYUBQj3RUeHQ:YkVwUv6UUhc4BeUaKU+aUeuwUNsYUBQk
MD5:	478982383655E95C2FD4C010341E91BF
SHA1:	54900DC67B0019487C5A51B6ED72E64E99836CEF
SHA-256:	751102F609A8A0E74A1C97E87CF9985F6C5AB66854946FEAF9BA09982A8A2FE2
SHA-512:	A1815D7192B4AC2F4C9365A8E0E50FE86A81C358E9A008392C783F75B19DFB4A70C9F2625313455B052E21A8D75FE08E0910536E1A7E971BE6FAB995E163DB82
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642710864.317082,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1626930864.31709},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_in clude_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1658466864.474661,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXlu9G3fM8KGQt4xie4=","mode":"for ce-https","sts_include_subdomains":false,"sts_observed":1626930864.474669},{"expiry":1658466864.367689,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2 OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626930864.367693},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVX gho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1658466861.264293,"host":"8/R rMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b42fbd1-fcac-44e5-aca0-81593344ad3b.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ecb4b9b-3989-47c5-a19e-475591c9a136.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):	22596
Entropy (8bit):	5.535795456326217
Encrypted:	false
SSDEEP:	384:/QrtxLlUPXs1kXqKf/pUZNCgVLH2HfDhrUIAHG5fnTPC414A:eLlKs1kXqKf/pUZNCgVLH2HflrUPGFnv
MD5:	653BC4D9F8C81134CEB8F84348096F19
SHA1:	EEDE0F39ACEBDC99C4B33B333163D1580FC1CCB0
SHA-256:	EFD4EA3C46AA1F278C46F116275C8958C7CB8096D4B57C8584E8633A988F619C
SHA-512:	01E5F40BB1C2B4BDA4FF9439A9BF43737C7E5CC04E6FB8122CCAC8CCD5CFBF2CCBA17ECE644D8483EAB4B200B760AC99F40CF20EEA90065666DB7433ADFCCA51
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":"13271404457167064","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.198969462810183
Encrypted:	false
SSDEEP:	6:m1GSVq2PN723iKKdK9RXXTZIFUtpPJgZmwPFpIkwON723iKKdK9RXX5LJ:NSVvVa5Kk7XT2FUtpPJg/PTI5Oa5Kk73
MD5:	FB0BAE165AC5CCAC0842AC8E9A1FF5A2
SHA1:	CFB3E06AA4A25F9F5284D9ADC4983776B9131E1D
SHA-256:	4055B88D86F7EBEDE862C04E647F4ADB5D316E02E04A3CF35F6C58F02BE163DF
SHA-512:	35B924DE041666EF1DCEB3B6F146C9526600EACB786DF7F54949C1A4C039D1A9BFC7557C29CF9F2E87C091BB52796BAC81D716785F6117CAC366265BC3237C8
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.599 1bc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/21-22:14:26.604 1bc4 Recovering log #3.2021/07/21-22:14:26.606 1bc4 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):	324

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Entropy (8bit):	5.191388614270867
Encrypted:	false
SSDEEP:	6:mtpVq2PN723iKKdKyDZIFUtp6YgZmwPpSIkwON723iKKdKyJLJ:EpVvVa5Kk02FUtpNg/PpSI5Oa5KkWJ
MD5:	DC7303554A6EF2BF6BBF520D448E78EB
SHA1:	D0E177A06D0976456D9822132C5B30AC675A96D2
SHA-256:	9EB533B90C7C5FE55A47B21FD8935F6CC790550F80B09C4B7C4909637CF48E96
SHA-512:	D9AA0A55E04BF9E7FC015D6A9629D400B52CCC8915FC8AFA1B2CF5CB8A758F9F3676ED51CFAFF51054E2BF0931BFBB3258F945587EB875778FC8BD33F0986BI A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.533 1bc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/21-22 :14:26.550 1bc4 Recovering log #3.2021/07/21-22:14:26.551 1bc4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\057a1b3eaa2d474e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.921090269449263
Encrypted:	false
SSDEEP:	6:mIbVYSHT8NWQAlKPUQyrSuXVwwIg/3hWK6t9vvFjZj7tQ0urzTUtIg/3hm:T7z8NWQCUUUmwwIg/2LRZj7i0YzYtIg/
MD5:	4BE191C847A5BED25B50926DE570C811
SHA1:	8C2109CA6972939318ED04B24BAA01C855FC9223
SHA-256:	3ACB9AB01AB923762ECA6701036AB91A7CC1A372A2B11876FE1A1156228AE72B
SHA-512:	528223DC430A8779A615184C25110A1B2E60950061FE54931BC1633C7AD7440C2817FEBE825ED4334C88E2AA0D79C03B6A2EF80B4F20BBD06CCEB437E3E0757
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^.....y....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://appdomain.cloud/.5.E&/.....}.....>.U1Rug..m./.....A..Eo.....yv .....A..Eo.....5.E&/. }..2794FFE9F7F3EA0CA8634F2C44853E0E20D8DF49A6F9C558940872A28BBD1A60.....>.U1Rug..m./.....A..Eo.....1.$L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b6b31cd20412ec5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.417542104515111
Encrypted:	false
SSDEEP:	6:mnrY68E9xEEUgLErySV2YVcXgYp+E3jbr1K6t:yYgqV2Qcrfr
MD5:	18D5C7F965A4A9709A294D3F065475C4
SHA1:	DA6F92253FC35868A11BF5E513C2AD16B7920921
SHA-256:	A33AB1BC2A0E1BBDBE69B7BD9D081506071B1D5EBC6B4F1277D75E25979871B3
SHA-512:	9CE95EC2538DDBAF6A9CBBF90A42A2195961B2CC1FEE80999054B92CFFB5FB07A9A8425A741DA804AF02F7192E27D603E8BACFC88738B5F8E728CDF1CB04E3 78
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...1....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://appdomain.cloud/...E&/.....A.U... S.[w.[.iA2w.B.$.u..T6.A ..Eo.....k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ce82e9cbd7524dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.510064319003701
Encrypted:	false
SSDEEP:	6:mwOYlNYpSVkpSDxVwGiYNZSShvP4LhK6t:dWpSVHfwGlNBNPk7
MD5:	A5B9505270B37D1DD83DB66B39BF64C3
SHA1:	27727E18A281812DD9DA07F9D2051BCBB1BD1895
SHA-256:	B68F4F873DC719F3DD04DC945561459F0E07F0E0C7A0B4EBBEC8CA1F8A737937
SHA-512:	D13D689307759249EF4C750C73D7EDC7B384911A6B30A8F3D4C9BCAF16A3395B02E762D576A309E74559752388E51DF50A5AC91B59E0D1B73F7D6575CC592F5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ce82e9cbd7524dd_0	
Preview:	0\r..m.....G...@..B...._keyhttps://kit.fontawesome.com/585b051251.js .https://appdomain.cloud/=F.E&/.....,.....R..x...N#..`.c.Uw3...5a"!..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ec825d44a6985793_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97736
Entropy (8bit):	5.785754133962089
Encrypted:	false
SSDEEP:	1536:LR8vdaOoiJkmlryICZzzoeVTvLu9etWO5pOgjyWcNJvB6RkXUWXvnfXjAdqF9G1J:OVfJzXCV9nu9W5pOLNh0RYUUfXYj1qi
MD5:	9B9C747362624B63F2D2A972DE532428
SHA1:	CB470FADC18AD127DF8884B87358F43972E240CA
SHA-256:	82888CC94B2D8C739301E9B6273EC7FDA6BD6A57358424D6AC45697855F7074D
SHA-512:	1523D4AEED20CF0696A51B9BC413175DFD15063A92E6583A5C93EF12CAF5545F07A8D576BAE95DC008DE3DC0B3628BBADDE2C80FC6FAD7DD7C7A8B3880E59CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....,.....2794FFE9F7F3EA0CA8634F2C44853E0E20D8DF49A6F9C558940872A28BBD1A60.....'.JN....O!...p|..._".....!.....L.....(.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@.....module....Q.@.....exports...Qc.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa.....D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M....Qb..nJ....d.....Qb../....e.....Qb.v.....f.....Qb.Nxd....h.....S...Qb.x.....j.....Qb..v.....k.....Qb.q.....l.....Qb*..}....n.....Qb.2.V....o.....Qb.....p.....Qb.t.....q.....QbV.....r.....Qb.....s.....R....Qb.0.T....v.....Qb.....w.....Qb&W-.....x.....Qb.[.j.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fcbeb72be584479d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.5181994893674835
Encrypted:	false
SSDEEP:	6:mcSYET08NaYWbVOqZySJiHV6kjrbhal75kJRK6t:og8NaY8ZXQ6kj/MO
MD5:	B78FB847FE2FC884C81806BF2E98C9B9
SHA1:	CBC5A50343CE00C7111259361F6E225FE88A69AF
SHA-256:	C169B1F4D49CFB87F1A0BBBA6762D382613899F86678E132E7969E55BA548CB7
SHA-512:	E0E50A5DE4FB629DC35610D8097DA6209D7B1AB60098702F872B3A7107431FF450DC6ABA3EB19D76D7029E5BB2D92B2ED1C0E3E89FF1D034AFAC7DCCEA0B3AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://appdomain.cloud/...E&/.....H...@u?.[PN?.F...._.N....9....A..Eo.....(*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	4.535717025066104
Encrypted:	false
SSDEEP:	3:7Oxl/llYdlVhoJ2E+T+6OqkopKnyNrkpb/paBgio77Pl6jlhl/llIhB+lmllN:4opaJ0KnyNrkpbMBnAlczkm/N
MD5:	87BAC8E5CAB77FF9C2068EF66600B389
SHA1:	BFE7E1CBAE7F2E0737D4B507CBC4A070126DC982
SHA-256:	B7655A00AF2156B576F34FA5EB8BA67D7926D0DDE6CA83AF5754968137135F57
SHA-512:	39254F4769EF344F66EC442F5634C8D033EF4A39A034364D55BC9D9794A281BF113365CE26CD401EB7DFFF41ACC0C52D2520A4C2431A253D3FD01A4112C02A0
Malicious:	false
Reputation:	low
Preview:	.....oy retne.....W..D]...L..E&/.....A .1kK.L..E&/.....G..+....L..E&/.....$u....l.L..E&/.....NG-.>.z..L..E&/...../...3.^j.../.....^}.Np...^j.../.....3.E&/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	0.9646122626246045
Encrypted:	false
SSDEEP:	24:H6plvJn2QOYiUG3PaV/qLbJLbXaFpEO5bNmISHn06UwDa8:H6plvZXC/alq5LLOpEO5J/Kn7UGa8
MD5:	BD4ACDF321DF40B3774C1D50F7348834
SHA1:	F5EA7C387C283B59B26B0593124BF74B60BC200D
SHA-256:	C949F8D112ABD8E6D18224254B1F801FCCDA22C59AC9B7A82E23EFF5B231FD10
SHA-512:	20A6582CB9F8E36895CEA6E11E0E57CD79ADE1EAF97EF73AFEF1B0951433F38A25FA4BF9E059913DBC6246B65CA11451641A2E5D3E4E7301FA84C044E3E6C744
Malicious:	false
Reputation:	low
Preview:	.....f.c..... ....

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):	2380
Entropy (8bit):	3.5402718647747777
Encrypted:	false
SSDEEP:	48:34LlYrxo6SGAmMoLOszE/GAmlWgEGAk+BfOszEc3SGGAmlWuWOL:34LmAmMWzJAmljAtdzYfAmlzt
MD5:	59BA51E01C76ECFC4EF8734808D73FB3
SHA1:	75B1A99D674449FCBCAB7492AFA777CD27117EDD
SHA-256:	30BEDE92A97600D7C5E6F426DEEEFC5AB924B002ED7E24CE7A7EB07E11F66EE7
SHA-512:	D777DA32DFA72EBC8179EFC54D3901E8DDA1A5D17F6E975E9F95DCD823B57B9256A8F06FCC89F1A3FC0C17D5E1FE9CA4C5297810DD3DCF934F6D77792EF8604
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...d4555645_e5f0_4f0e_aa5e_3a6fab91de13.....v..#..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....W...https://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html.....h.....`..... .....!..\....".\....X.....p.....W...h.t.t.p.s.:././.i.b.u.c.k.e.t.2.5.4...s.3...j.p.-.o.s.a...c.l.o.u.d.-.o.b.j.e.c.t.-.s.t.o.r.a.g.e...a.p.p.d.o.m.a.i.n...c.l.o.u.d./.p.e.n.t.a.c.u.l.a.r./.i.n.d.e.x...h.t.m.l.....8.....0.....8..... ....W...https://ibucket254.s3.jp-osa.clo

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..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):	323
Entropy (8bit):	5.19562652174782
Encrypted:	false
SSDEEP:	6:mhF9+q2PN723iKKdK8aPrqIFUtplZmwPJVkwON723iKKdK8amLJ:fvVa5KkL3FUtpl/P35Oa5KkQJ
MD5:	CC202DB679F21112D95613683DA3BB15
SHA1:	41A3326D1B4B0F6BF75EA22D1F2AF62549010125
SHA-256:	71B8364688E7C2862E62639868E99E9AA11FAC2EE8A81B3AF43F2D89A68C453E
SHA-512:	B8D184D587D8D82904115DCB744DE6684FDFD655D7E09E74FA9035957290BE4C05824F6BF0E0662AC61F82674B997FB750EDA968789C186C4E01500BD969867B
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.449 d58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/21-22 :14:17.451 d58 Recovering log #3.2021/07/21-22:14:17.451 d58 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):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
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...............

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Size (bytes):	323
Entropy (8bit):	5.1683035898786205
Encrypted:	false
SSDEEP:	6:mS969+q2PN723iKKdK8NIFUtp/Q+ZZmwP/y9VkwON723iKKdK8+eLJ:vM4vVa5KkpFUtp/JZ/P/yD5Oa5KkqJ
MD5:	2ADD571B625ED8FF47D4FB1FAC18F23A
SHA1:	6EA3D9E2B3B4875666C0392A1183D2819699E3FB
SHA-256:	F3DC4BC9859720CE386E2C92E7B78A77083B89AD1FE45EE43C1200AC1582DEFE
SHA-512:	E4A2395CA91F471A90BD38683025C1F098B7EBD26F6E89265B8A64EACDF56BEB77B79B4BFEC2CFA2F6F26C664DD71B7B9053EF79C6BD8F3E0B40B687E19576D
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:21.154 d58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/21-22:14:21.155 d58 Recovering log #3.2021/07/21-22:14:21.156 d58 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=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	378
Entropy (8bit):	5.233360762218858
Encrypted:	false
SSDEEP:	6:mKVq2PN723iKKdK25+Xqx8chI+IFUtpogZmwPV50IkwON723iKKdK25+Xqx8ch+Q:9VvVa5KkTXfchI3FUtpog/PII5Oa5KkI
MD5:	00A5A73ED779B283B8EFC48A7419E7DD
SHA1:	CE5AC06731AF35D8C7AB496EEE01E5D8D1B79C3E
SHA-256:	788FC5FCB1F6F85EAEC6F47C9CCBC896309C33515DA7D1395077CCFB053AD43A
SHA-512:	F4CB1147DD93448B86274375370D62F329C29D8FF4DA064DAD0428A9E15FBEA1999BE2EB7830AF4504BBBEA12A30A924F55F74EEA6AC5B5389F050544EFAD9E9
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.374 1bc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/21-22:14:26.379 1bc4 Recovering log #3.2021/07/21-22:14:26.388 1bc4 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):	364
Entropy (8bit):	5.178347650266491
Encrypted:	false
SSDEEP:	6:mTVq2PN723iKKdK25+XuoIFUtpZVUJgZmwPZXGSIkwON723iKKdK25+XuxWLJ:0VvVa5KkTXYFUtprUJg/PcSI5Oa5KkTZ
MD5:	075BCDA225173DDD64F606E1761638CA
SHA1:	D8B451B37D23ED5B94B2E7E3A43A7789CA9BDA64
SHA-256:	67568ADDB4C0F14423FA0CED85496DAFE87F6ECE52FF1475DE26740D32232DF6
SHA-512:	7D851784A7D5BBBF8429AE382AF2E3FE4CDAA1971858862789E8DE8CAACD879C384868C927F087FE75A37785E34B425C4E347ACE5FF50F522D43706D5678E63
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.339 1bc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/21-22:14:26.342 1bc4 Recovering log #3.2021/07/21-22:14:26.343 1bc4 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):	336
Entropy (8bit):	5.178914414890442
Encrypted:	false
SSDEEP:	6:m0MJVq2PN723iKKdKWT5g1IdqIFUtpfdGSgZmwPfXm0IkwON723iKKdKWT5g1I3e:OJVvVa5Kkg5gSRFUtpfdpg/PfXm0I5OM
MD5:	E5130A508A4D58C03BF71675986CA88D
SHA1:	109C9607148776F57F14509CC0C6EDA541BD7BF1
SHA-256:	667D300F635A4C7DC7DA488A3302FDB3C4DA5DB28AE80205256BEDC4F48DC2EB
SHA-512:	A122E34B679DB75908AC1E4509662FBCBC734A57790F0FFB4A506EE15512437B1EAB05B914992226AECBD57026BE7AAB37EF5226DC794B83BD7B8B0ACCE8FCDE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Preview:	2021/07/21-22:14:26.300 1bc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/21-22:14:26.321 1bc4 Recovering log #3.2021/07/21-22:14:26.323 1bc4 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):	0.1433041337740756
Encrypted:	false
SSDEEP:	12:TL+A/VjRf7bV3Sr9AhQMRD/0NuQ0GI/xulybV3Sr9AG:TLxZ1xMASMRUuGwxMAG
MD5:	970D6774938CB935CF1455946659591B
SHA1:	5549FD529EE38C84FE1818066072996EEF6E7745
SHA-256:	604225D653E8FAE8B72C31EBDA91E729468FF5E78E5A1B80E540D552757A2148
SHA-512:	9550BDFDBA8DA61D050373D9A6D65E5AEFE14B530436ECDB3C2E8A84980321AF12BC342CB3B9090EA45E5D01DFA745A2362ABEDA313FC23A28D544B57F66C 23
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):	903
Entropy (8bit):	5.362692249312996
Encrypted:	false
SSDEEP:	24:odl3UGYF3Fi1CPKOY+b/oJsCEY78BJgskfa9yBDOxo7hxMAI:Q3UGYFoM7N/+1SUVGAI
MD5:	7EB16228120AAB308B6B49EAEEBB2405
SHA1:	22C4106216C6436F2D79EA246222B880E3E1EA68
SHA-256:	0284BDBB1A94960587CFD99C2B4500ED565D337274AAEC2C1BA88543F0FBF7F1
SHA-512:	5F921FBB94D93F27F9C5A79CF60F3BE9D0EA3AD30864DA45A0E19722F24422591F9C0559E271B0A396E2AC914D11BDFFD5DAF0B040748DA267B05717DE0C7E4
Malicious:	false
Reputation:	low
Preview:	....."t....appdomain..cloud..html..https..ibucket254..index..jp..object..online..osa..pentacular..point..s3..share..storage*.....appdomain.....cloud.....html.....https.....ibucket254.....index.....jp.....object.....online.....osa.....pentacular.....point.....s3.....share.....storage..2.....2.....3.....4.....5.....a.....b.....c.....d.....e.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....x..:.....B..... .....*Whttps://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html2.Share Point Online:.....J.....#*2<BMS.....

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):	0.046930054619497924
Encrypted:	false
SSDEEP:	12:FF/q6F/aNF/dF/zF/uzF/NF/oF/nqLBj/M+t3n:HlyPXZoXGfqLBMM3n
MD5:	27A4A0BEAA15F67BD600DE9443AC7B59
SHA1:	5E195DDFF1801798EF08D48CDF9D094E3837577C
SHA-256:	FB0B1E59FBC71723F974E4661280372979E4F48CC1A315EA480C11FADE510470
SHA-512:	7594F476502230CD2E7EF3233D28FDDD8163B2CEE85235A97A900993EEF6005775B404868711D886C0EF5A6B776BE8D2661C80DD02AD60E36CB3E42814C7BA1
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.475083959933913
Encrypted:	false
SSDEEP:	48:vcL4GNA+2La7PLMj+8dbbV0EibQSefgGCNrS0U9RdiN9a:shj2La7PLMjVdbbV0EibQ5fgGOrS0Y
MD5:	8C9D4509F0CA1381E607222ACD612B87
SHA1:	4BFA1502FCB1844B9EE934D8F4D3EA9DCAA94D08
SHA-256:	6A095F5FAFC48A61435661919DA78C430EC95C7D6E8208C1C646A2F59945B51F
SHA-512:	1BFEAE1781F084FFFFB87AA2F456DF0D3149A5236694582CAF8A405DF3B80FDC52D1B813AE6965559EBE726891E32725BA3B3B6E7DCEA70EE51A733995211D2
Malicious:	false
Reputation:	low
Preview:	JL....*.....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..447405000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-21 22:14:28.55][INFO][mr.Init] MR instance ID: d6b5348b-8dc7-4595-b874-9c5e860eb17a\n","[2021-07-21 22:14:28.55][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-21 22:14:28.55][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-21 22:14:28.55][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-21 22:14:28.55][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-21 22:14:28.55][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-21 22:14:28.55][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):	338
Entropy (8bit):	5.076714322221633
Encrypted:	false
SSDEEP:	6:mTNAVq2PN723iKKdK8a2jMGIFUtpJvAgZmwPxIZAIkwON723iKKdK8a2jMmLJ:yOvVa5Kk8EFUtpL/Pip5Oa5Kk8bJ
MD5:	C2A90E1DE8CE4D9D91C4ACC7D3A05FA8
SHA1:	19C9F1BA7EC71141B1C7AFF54F9030A7AE101A80
SHA-256:	5BB31A597F21C39FA8223AE162F7874830F34F7D22B7847013FB73FC7E877ECB
SHA-512:	758A3288B4CE28567143952E4127B9B3E0A120BEC5AA11E129691B3ADE3CC922FEE8765F2371CCD1E099C6F495DBB8D5D010B1C02A8F6F6F097C74B6E12A7BDC
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.209 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:14:17.211 1440 Recovering log #3.2021/07/21-22:14:17.212 1440 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):	340
Entropy (8bit):	5.173950234153629
Encrypted:	false
SSDEEP:	6:mjH0+q2PN723iKKdKgXz4rRIFUtp2tHZZmwPsVkwON723iKKdKgXz4q8LJ:mHJvVa5KkgXiuFUtp2BZ/PM5Oa5KkgXS
MD5:	2F50868D632E6F160D25FBBD72AB0B58
SHA1:	EA047477F1A133AF62BEAFDDC9772BAA6ACFBDD2
SHA-256:	C63CED5EB4B106BEE59DF2C872E095B05B85BA1B165F7EB1689E29B053938759
SHA-512:	9C25DD634D60E253EB9A5C3D3237575FC6E712B75CC2DA2946B581B637302FF778A0EE550FA578DA6114DCF6B9352B7882BB8E05C5B252BA4C020281A971A5C
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.468 1718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/21-22:14:17.469 1718 Recovering log #3.2021/07/21-22:14:17.470 1718 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\Reporting and NEL	
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):	53248
Entropy (8bit):	1.3886064298818863
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcS+HqVMD2hVMsIElwQF8mpcS68fVM1S23VMu:zHqVMD2hVMb8fVM1S23VMu

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
MD5:	ACDCD7BDF2A5DD85EF02CBF48B7B6B98
SHA1:	03D9E9B82AE7BD9F81B0C65F89BF74E0B814CB8D
SHA-256:	2D704ACBE5D4BDFAE365557C027E7CDB7DAFD4EA770203A7BB3BC515BE860311
SHA-512:	F7F2C3DD476E9EEF9D7C8214CAE9F217A6D69FA276E171C1DF13488F959C155262DC025774D9DEA2ECBDBC45274071C7EDB4A503631B0930FC7FD1DCD64C561
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	54400
Entropy (8bit):	1.0321051037541311
Encrypted:	false
SSDEEP:	192:fpYOWo0nhIElwQF8mpcSf2hVMYHqVMexIElwQF8mpcS5:fpYOWo0n32hVMYHqVMeR
MD5:	DF6C83174EA3AE7DB3AEE6C5DFCCD186
SHA1:	08FD98EC87052A8563EEE6D3698393EEA87397FD
SHA-256:	4E2AF256C787F14C024E4DFE51C3B6C7CAA05E79C52503E72AF77CB8421CD667
SHA-512:	5CC3A4C5613D06704BB90C71A6075DE1032C9A736CD00D3150E3DFBF0A47908A3DE1B718931FA73468513C36B4681E14241E06992CAF76B3CF196823560FE4B4
Malicious:	false
Reputation:	low
Preview:	.....|.O..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
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):	326
Entropy (8bit):	5.119828833224814
Encrypted:	false
SSDEEP:	6:m5N+q2PN723iKKdKrQMxIFUtp6UdXZmwPItVkwON723iKKdKrQMFLJ:PvVa5KkCFUtp6YX/PIT5Oa5KktJ
MD5:	E5E56E7F251029B26E36BA3714FD51C2
SHA1:	4619AA084F12E8E768A43FB6B9A3398640D664CE
SHA-256:	EC536D8975888329030AD42FB534E95BA13D365D3CD681E675B93EDD33E06AD1
SHA-512:	2C7CC18D38CA027278FDD6C6CA9DA7C0B243B270538B22DF50C569CF9110F23A5B2673ADBEC2F631AA8246B2DF4D6AAEEA90F97AD652DEEB0293C18B3DF15A4E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Preview:	2021/07/21-22:14:17.366 1718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/21-22:14:17.367 1718 Recovering log #3.2021/07/21-22:14:17.368 1718 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):	354
Entropy (8bit):	5.118498645911885
Encrypted:	false
SSDEEP:	6:mBG+q2PN723iKKdK7Uh2ghZIFUtpcuZmwPQ6NVkwON723iKKdK7Uh2gnLJ:AvVa5KklhHh2FUtpcu/PQ6z5Oa5Kkl9
MD5:	DC78514AAE97D76ACF18D2F72F7070CE
SHA1:	B0321C6D623B4C91EE13F78E00443CABC9E9959D
SHA-256:	E0A2BEF487C0926D782065DCECA1D00220EF5D8EF0AF6624B5CCB99CB507D557
SHA-512:	31E59DB5E41016C9BA80359727BA5174E1EE5A12CF0EEF8FF76FA6998AE521D53BF53FF77DC0F3EC7A09246890209DFF28E212EE159099ED17CF16532EF9E7D
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.178 1738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/21-22:14:17.181 1738 Recovering log #3.2021/07/21-22:14:17.185 1738 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\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):	433
Entropy (8bit):	5.219243296369506
Encrypted:	false
SSDEEP:	6:mnS3+q2PN723iKKdKusNpV/2jMGIFUtpyHXZmwPyEtVkwON723iKKdKusNpV/2jz:ifvVa5KkFFUtpy3/PyET5Oa5KkOJ
MD5:	76783F491E425292D3AA45D3F949B6C9
SHA1:	4F46F4C8D8A20258E9C7722E802E498A57CEA823
SHA-256:	4AA5428C7B4016BE53A5BB28D45180D451C7278D75419B79BC48393A0C723C52
SHA-512:	67D4D4E22136D4D8580835451CFA0D6FFBE27BD5823147BB445AB69E2F58CE7C9A930A5995B2852DC6D75B3D3AF69B91C7715B058A742FD9403878CD1866A99
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.420 d58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:14:17.421 d58 Recovering log #3.2021/07/21-22:14:17.422 d58 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):	435
Entropy (8bit):	5.274343261928593
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SSDEEP:	6:mG69+q2PN723iKKdKusNpqz4rRIFUtp5ZZmwP4X9VkwON723iKKdKusNpqz4q8LJ:964vVa5KkmiuFUtp5Z/P4XD5Oa5Kkm2J
MD5:	BD8BEF09C6C2738C54083CF51FE1EDC2
SHA1:	AD561A406DB8C733EDC801AA43137367D3CE9087
SHA-256:	08FE68E3DFB42EF43B65B6CC7D25E99380064E40E1A7065B533D52251ACE4B89
SHA-512:	CA6D9F1EE1ACA892332BC6F998591D7D18660F117A358713CEA7E336A430A00F01F8E33BDF8BFA8F86706DDE93F9D5975B3663FB1EE4038BB2E0682447F810A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.474 d58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/21-22:14:17.475 d58 Recovering log #3.2021/07/21-22:14:17.476 d58 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):	424
Entropy (8bit):	5.197723955512171
Encrypted:	false
SSDEEP:	6:mjTjL+q2PN723iKKdKusNpZQMxIFUtpXKWZmwPXLVkwON723iKKdKusNpZQMFLJ:uTjL+vVa5KkMFUtpaW/PXLV5Oa5KkTJ
MD5:	70E927966E352457A0497AEB410DA004
SHA1:	1E5523AE43E42919D24B278E7EECC6BA464D260A
SHA-256:	FC09E824A010CF42F4939808076DB94D807CB1517B188772B8543B93986FEFC2
SHA-512:	B2DA16E9411BB105D0D1B1CFBC78264106D08F5AB686E3A7A35A33E906C9EE879BC4C529E1E7012AA11AFEFD047962F96E6274C94592041555A3B2FF24A915A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:35.212 105c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/21-22:14:35.213 105c Recovering log #3.2021/07/21-22:14:35.215 105c 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\gfdkimpbcpahaombhbimeihdjnejgicl\def\e48a3126-ed8c-44de-bd10-c636b22f7c94.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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\23ac81fb-24fe-451b-9670-b268c2d105bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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):	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\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.187555946237182
Encrypted:	false
SSDEEP:	12:P4vVa5KkkGHArBFUtpf//PfaT5Oa5KkkGHAryJ:PKVa5KkkGgPgZ3aFOa5KkkGga
MD5:	9D76E6A05270375E447891C368D5A4BB
SHA1:	1AEB498E2D2D28C555D049ECF256E5D204B33886
SHA-256:	9F3FFBDFC18F693ADD79EB8F97E66DE302FD1F0196CB6CD47D64A5800F062020
SHA-512:	E08402C9FECA4FD661D3ED053D7EEE817648EBD692350BAFA79FA733D44BD2223D548B3C03DF44B46954429EC2B5D777C3353366B138CC0F6DF67962029652E
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.903 1718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:14:26.905 1718 Recovering log #3.2021/07/21-22:14:26.906 1718 Reusing old log C:\Users\user\AppData\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):	438
Entropy (8bit):	5.1957741930208865
Encrypted:	false
SSDEEP:	12:16+L+vVa5KkkGHArqiuFUtpEW/PbvgjLV5Oa5KkkGHArq2J:16+YVa5KkkGgCgm7DOa5KkkGg7
MD5:	2A86C1190FD6A8E722D4936B16C3E704
SHA1:	8A000918E7761BDB6ECDE6018D3AD638CE30F902
SHA-256:	9CA5584E0C77BECF2CF3EEC308260A9FE78A53E4EA51724091BDFB0C3CBA33C5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA-512:	D502EA2CB57C6C291492C2D4011E4434383848205CB1D9C859B05B4FC4943B2B9B49A6FB81F2BEC533D514369048F4B80470511B4223E495EA85F4BE3B64B8EE
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.923 105c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/07/21-22:14:26.938 105c Recovering log #3.2021/07/21-22:14:26.940 105c 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):	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\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.1472587320878045
Encrypted:	false
SSDEEP:	12:+L+vVa5KkkGHArAFUtpHxW/Pf6SlLV5Oa5KkkGHArfJ:+YVa5KkkGgkgPH+DOa5KkkGgV
MD5:	C50E39DE39C09AE88D091877C063F293
SHA1:	18168241BAA52CD74460AE117B1A28FBF53FDB82
SHA-256:	A03CA9AE45BEC37E6A96577980B213DE01B58D68EDE883F29B40B67B81ECFA05
SHA-512:	F231E68468DAD19A21FF6C39B9F97ABF9290EDB52029229F19C82377F071A98DE99EB5FF65C4F14AE3F868BA057A283CDA4EF32C312B4549C95C75C2E6365766
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:42.283 105c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/07/21-22:14:42.285 105c Recovering log #3.2021/07/21-22:14:42.286 105c 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):	330

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Entropy (8bit):	5.169412741105431
Encrypted:	false
SSDEEP:	6:mDyq2PN723iKKdKpIFUtpX1/1ZmwPd1pRkwON723iKKdKa/WLJ:GyvVa5KkmFUtpl9/Pd1pR5Oa5KkaUJ
MD5:	750F30FB7C23381D04D2557D08EE4912
SHA1:	7A3474CE83B25AB82902569176121D29062E3C01
SHA-256:	021E3B03F936D223C2356758ECE42FAE98833AADCCC728A0752347A4BF7D0264
SHA-512:	EDFAB6241EC5E564DAF2C4D58A73BAA77B6A9CACE2571EE781BDA8A60A29ADE027D2C49AEA9A798D04AB994DCC7FEB9940768F199EB351FFBA4F3F201D432B66
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:17.178 16a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/21-22:14:17.182 16a4 Recovering log #3.2021/07/21-22:14:17.188 16a4 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):	405
Entropy (8bit):	5.274574174010811
Encrypted:	false
SSDEEP:	6:my+q2PN723iKKdKks8Y5JKKhdIFUtpBdFZZmwPBdFNVkwON723iKKdKks8Y5JKKp:0vVa5KkkOrsFUtprX/PrF5Oa5KkkOrzJ
MD5:	859BBEBCD84256432F178F00176D91ED
SHA1:	DADCC4791F9C222E1C66651C049D1BC4FCB30363
SHA-256:	3097365E961EE1E843CC589BCC071123C7E97DA982004424C99E34FC18C13EF8
SHA-512:	AE81FD164C060C834E7E2B229B1E6AD7FF6D4EFCD11DC038C7D571BF6C813DFC9A67690054C314491748286921B0D6F9DFBA4915397CDFE5F40F13785FEB73AD
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:28.523 d58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/21-22:14:28.525 d58 Recovering log #3.2021/07/21-22:14:28.525 d58 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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:6LfY:EY
MD5:	B93B1F67172702221C05C926E90B608B
SHA1:	F05DC73B36E0A21D8658C324292C583D3B2E7522
SHA-256:	43CECF1A3E00DD56D10B2201AB48C3FB25CFEB95BC2FB6940D3AEE341B507B28
SHA-512:	9B3CD5CC605B9C3CAD841D094BA88F78D93590FBF29F926294010A2A1B7D24A9950BA4665952FB4E79C5491C9BDDA184E25CB1B90915567D56F591E28358DF4
Malicious:	false
Reputation:	low
Preview:	.....z.gO:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b6c49102-1995-4b43-8d3b-a3c34ca6199c.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):	5802
Entropy (8bit):	5.1811750284694815
Encrypted:	false
SSDEEP:	96:nqXbz/YMleaAKIU1xk0JCKL8i1kn1flbOTQVuwn:nqXbMMg9a4KZ1knBN
MD5:	2965DCE8222C9B4635B802CBB3768161
SHA1:	0B97921D95212C750514902188493BACF91D8A52
SHA-256:	D2323A82869EEA04C074AC90A4BE26E110C670131593C173F490D2454769F239
SHA-512:	4AD689BDFA8392508F55913A14928758974DB5A32AB522CC9DD40355313E311D25B58D3216795A33D80659BD8720178E1C069EFE9CF547A4DEDF8C3D35263C3E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b6c49102-1995-4b43-8d3b-a3c34ca6199c.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271404457440403","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c659b28c-2fd0-46ce-89ad-06d0cfe26e5e.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):	2649
Entropy (8bit):	4.874374403112788
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qyvTXDHz5swDseRLstTs/gSZ56Nepsy8zsU6qCPYhbG:2lNnOa+TXDHzzT2fa56NsWxCghS
MD5:	027B10700E3856E32DA40DD3FCD2D2DA
SHA1:	62A59C80135B70D017DC6A964930BFEC7E3B4E02
SHA-256:	BF5F07944A9F6E37C8F2F3B889774EF8F6ACC088C3878C0CDCECB42CFA87BEB2
SHA-512:	F1707C24DDAE250359116158DC80F9BDCD080740FAA9332BDE0CDBF24CF0F1EE6D6F9944C3BB56811AED0559CFBA3A3AD3B5AE5326E1A6243EAAB567B3A9B010
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273996461259796","port":443,"protocol_str":"quic"}],"isolation":[],"serve

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d03731cf-551f-4584-a12f-3a36ffae3248.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):	19113
Entropy (8bit):	5.5717857577034735
Encrypted:	false
SSDEEP:	384:/QrtcLlUPXs1kXqKf/pUZNCgVLH2HfDhrUOAHGHsC0+14l:VLlKs1kXqKf/pUZNCgVLH2HflrUBG716
MD5:	B70DFA2660077A0FD90E26CBF71E7004
SHA1:	52D65C250FA34CCBAB183A6D125817D3FF78D4FD
SHA-256:	5010A1F501B0841E6F45366AD1C0F3A12467E5852D9381CEF6676EC7958ED8F2
SHA-512:	1E8B9DB46E6626048874D96710861F4E2034D39D85B479A2E91D695EF64403332A08FEBDA3705638F38998005637D904212D494E8A150E66D5B58F36E5AEEF5A
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":"13271404457167064","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.4821051588291345
Encrypted:	false
SSDEEP:	3:tUKBbLARyZmwv3jIUmRbVV8sjGHGbVWGv:mvgZmwPcvhVvntv
MD5:	7E1F38D032D6ADB5B1F8429F63B8C7F6
SHA1:	DF777CCEBE9C671C53C1EA3BF367627A628B1EFC
SHA-256:	34DF53ADE92545EAE942E0C425BA08EBBD0FDAF9F8DF91AD26922B47CA4AF020
SHA-512:	69849BA2B8538863893391BAAEDF2BA1AE1B3C0283921A89BE5DCE161A3FFF9B695FB524D6CA25FD3497588C62983B0769A7B697E1EC9F41192DC892EEFB4EE 3
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:25.714 1bc4 Recovering log #3.2021/07/21-22:14:25.793 1bc4 Delete type=0 #3.2021/07/21-22:14:25.794 1bc4 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db7eb458-4a2e-493c-a239-44b02def5972.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):	5206
Entropy (8bit):	4.982998557499149
Encrypted:	false
SSDEEP:	96:nqXbzzYMpaAKIU1xk0JCKL8i1kn1flbOTQVuwn:nqXbIMp9a4KZ1knBN
MD5:	07CC769FC7CDB3FAD866F8DDC6048C7C
SHA1:	329096D652388197636206669E3D3EF70A83A623
SHA-256:	B3842DA22C7A30746747E38D7B09B0CFFFCF71D2181A0E787659E388B9FE4250
SHA-512:	FFEEA5D3B8E937B83C915F392F1BA0D4059519804E6E0DC6BD47DCC3FBB6C66763A87E1EA8B7933853352A1625E40BDC8DF203A811721E28B86659F529893E2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271404457440403","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ed050ba2-67b7-4c73-8c9a-eed76388ef8d.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):	5.5359010764223475
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ed050ba2-67b7-4c73-8c9a-eed76388ef8d.tmp	
SSDEEP:	384:/QrtxLlUPXs1kXqKf/pUZNCgVLH2HfDhrUIAHGKfnTPCv14La:eLlKs1kXqKf/pUZNCgVLH2HflrUPGKnc
MD5:	A94AC72832E1BDB7B258882C188AEBB5
SHA1:	56D2DB5AAA9ECA38FE5C54E2BA4957AC53ABADBC
SHA-256:	B447E3BF401C7967E3398275D1D736DC0FA9666E24376879987E5C0A966DD286
SHA-512:	72DC47ADBCBB4579BD33063B9A387CB571CF9E90E774B483946428853E3868CA31E860D07769D7AF5CE8640CA766C84F11EC198D203B1574A2C3ADE5AC17D1 7
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13271404457167064","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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):	341
Entropy (8bit):	5.197638920603904
Encrypted:	false
SSDEEP:	6:mzAq2PN723iKKdKfrzAdIFUtp3yJZmwPeDskwON723iKKdKfrzILJ:2AvVa5Kk9FUtp3M/P55Oa5Kk2J
MD5:	5BFE4C1F9B9EF14C431E1732E217DB3E
SHA1:	6F7E3277DD8358E204734377225AC495FC8F324A
SHA-256:	1FECDE61E26DD8D5BF4BE749FA8C298B078A9D293A29A65862FAC8B560729060
SHA-512:	102017445A13D99A316A6CE04134CE943492ED1C7FFE3A0170B69A05CCD4F14831234038275E7817D31F7B5563B37EA159384EE1CD05164DD48A152694768BE9
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:14:26.753 f50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021 /07/21-22:14:26.755 f50 Recovering log #3.2021/07/21-22:14:26.756 f50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_d b\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\cffb87c4-831d-45ae-a80c-7d001370ad32.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):	376995
Entropy (8bit):	6.04936393010301
Encrypted:	false
SSDEEP:	6144:we98KWPnuw15QgBB/G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinp:wY4j1igBB/GNPUZ+w7wJHyEtAWs
MD5:	2E96CE71023167E7661ECE30B500EF37
SHA1:	C25724D482008923B8A703B30301C09CF17A0871
SHA-256:	A5ABB7747895440F4B6096E991963F135AEBA4604056688931A0B9CF853C1F08
SHA-512:	9E2DC7F401E669750CD854CED4133CC2AA13ADE0510C92D76380FE2C858BA636BC383D7D4039C99CF5D3AB88BB2F4767FE8844BEC3A691211F192F7F02F873(
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":1.62693086149198e+12,"network":1.626898464e+12,"ticks":4900751086.0,"uncertainty":4282714.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\19c69566-4fb2-49b8-901d-c1b7b7e33413.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\856ef141-f8d5-4abc-bedc-ba8c4888a5e3.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\91d06bc0-84b5-496c-a50b-e2437be995b6.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

C:\Users\user\AppData\Local\Temp\91d06bc0-84b5-496c-a50b-e2437be995b6.tmp	
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."I...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\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	17838
Entropy (8bit):	4.649861281493671
Encrypted:	false
SSDEEP:	384:DFjGClCgCoCGqCygv3464jLtaJqP4gT4N4Lm4M7xslKUH7uva:DFjEBjLtaJg8eLm4M7xsVuva
MD5:	DFD4502FA02C444ADC8911138179DF8D
SHA1:	EB9ABEA700852B16EC98AA993039164C4DA8B294
SHA-256:	F07459B5CCC2C260042939542503151025ACB42C2C30B15E7FFB3E481E9F39BA
SHA-512:	55B8C6D72FB3C5419BCF1F8E78A52068046AEE96412EBEDA4F6773C9FA1AE9D8E69CD31827D8E2E1B74EFFA347B8B0FB7D3DB82DB90F6D3514E7332DA6844C7B
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 74771cebcaf25c53c04b366778d2a8a3505a3d14f4682faa57b6145b4e03f269 70c9fc07594dcc3dad8867ac0ea4e6ece fc964b6a8bfee131f64fa61eab0362f.SERVER_HANDSHAKE_TRAFFIC_SECRET 74771cebcaf25c53c04b366778d2a8a3505a3d14f4682faa57b6145b4e03f269 e ae618b3030c4ed9d25a421eb429d1d70f9e77e3f3010f6b88e85344ff6923e2.CLIENT_HANDSHAKE_TRAFFIC_SECRET d2410756122a09cff8f641bcfe82bcddf6 7cd4defd833f619ad61bb818707efc 87c6534c8457736607dc3690bc5e3037a06a90d5a8d9ff14a66ed3b1f0b20695.SERVER_HANDSHAKE_TRAFFIC_SECRET d2 410756122a09cff8f641bcfe82bcddf67cd4defd833f619ad61bb818707efc 1fe282ba3917f05f39eb4a3b01ecc4b3c44f2baa467b7e916f35bce3b50e8734.CLIENT_HANDS HAKE_TRAFFIC_SECRET 5cbe46d4b6a46e4fed5e9a175fdc2ed78bc3c7b987c82afec1c56e15324bde7b 9e5f7763edd468fd91d82a9c1dc86b976404844cf0483 ac0505540e6b7462927.SERVER_HANDSHAKE_TRAFFIC_SECRET 5cbe46d4b6a46e4fed5e9a175fdc2ed78bc3c7b987c82afec1c56e15324bde7b 495249f9439cd d2a96c61d54d87e978afa7b365d20299bbb3af221e6bd887544.CLIENT_TRAFFIC_SECRET_0 7477

C:\Users\user\AppData\Local\Temp\e2586e41-a733-41d7-bd75-2b55bb230204.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
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.;.lpr..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.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\am\messages.json	
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "12827687646031907 5": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": ".... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874943 76": {.. "message": "... ...".. },.. "18027627465894571 77": {.. "message": "...".. },.. "18503975003120203 88": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SlwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".......".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "......... .. ..".. },.. "14284488690781267 31": {.. "message": "......... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": "......".. },.. "16366867476874943 76": {.. "message": ".......".. },.. "18027627465894571 77": {.. "message": ".... .. ..".. },.. "18503975003120203 88": {.. "message": "....... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\bn\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\da\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "1428448869078126731": {.. "message": "......... ......".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\en\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chromecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fa\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050321
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C8202343738 91BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C000
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\fr\messages.json	
Preview:	{.. "10189845614885205l7": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "1636686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....."".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....."".. },.. "1802762746589457177": {.. "message": "....."".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....."".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... ....."".. },.. "1522140683318860351": {.. "message": "..... ...."".. },.. "1550904064710828958": {.. "message": "....."".. },.. "1636686747687494376": {.. "message": "....."".. },.. "1802762746589457177": {.. "message": "....."".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "1636686747687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351" : {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376" : {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": " $1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8C D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140 683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir3180_1456837572\CRX_INSTALL_locales\ja\messages.json	
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "...".. },.. "128276876460319075": {.. "message": "......".. },.. "1428448869078126731": {.. "message": "......".. },.. "1522140683318860351": {.. "message": "...".. },.. "15509040 64710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "18503975 00312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_ LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

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
Jul 21, 2021 22:14:22.040082932 CEST	192.168.2.6	8.8.8.8	0x3b26	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:22.040827990 CEST	192.168.2.6	8.8.8.8	0x9a8f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:22.041652918 CEST	192.168.2.6	8.8.8.8	0xb300	Standard query (0)	ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.138660908 CEST	192.168.2.6	8.8.8.8	0x74ac	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.138709068 CEST	192.168.2.6	8.8.8.8	0xb4b5	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.140836954 CEST	192.168.2.6	8.8.8.8	0xca7c	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.140867949 CEST	192.168.2.6	8.8.8.8	0xd352	Standard query (0)	ses-smtp.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.164623022 CEST	192.168.2.6	8.8.8.8	0x7a36	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.994451046 CEST	192.168.2.6	8.8.8.8	0x479d	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:26.190433025 CEST	192.168.2.6	8.8.8.8	0xc3aa	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:27.100132942 CEST	192.168.2.6	8.8.8.8	0x8cfc	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:27.302284956 CEST	192.168.2.6	8.8.8.8	0xac69	Standard query (0)	ses-smtp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 22:14:22.066437960 CEST	8.8.8.8	192.168.2.6	0x3b26	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:22.068850994 CEST	8.8.8.8	192.168.2.6	0x9a8f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:22.068850994 CEST	8.8.8.8	192.168.2.6	0x9a8f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:22.083091974 CEST	8.8.8.8	192.168.2.6	0xb300	No error (0)	ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud	s3.jp-osa.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:22.083091974 CEST	8.8.8.8	192.168.2.6	0xb300	No error (0)	s3.jp-osa.cloud-object-storage.appdomain.cloud		163.68.118.49	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.158102989 CEST	8.8.8.8	192.168.2.6	0x74ac	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:25.163929939 CEST	8.8.8.8	192.168.2.6	0xb4b5	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.163929939 CEST	8.8.8.8	192.168.2.6	0xb4b5	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.164017916 CEST	8.8.8.8	192.168.2.6	0xca7c	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:25.165510893 CEST	8.8.8.8	192.168.2.6	0xd352	No error (0)	ses-smtp.com		104.21.16.61	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.165510893 CEST	8.8.8.8	192.168.2.6	0xd352	No error (0)	ses-smtp.com		172.67.166.169	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.191236019 CEST	8.8.8.8	192.168.2.6	0x7a36	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.191236019 CEST	8.8.8.8	192.168.2.6	0x7a36	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:25.509202957 CEST	8.8.8.8	192.168.2.6	0x13a1	No error (0)	gstaticadssl.l.google.com		142.250.203.99	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:26.015949965 CEST	8.8.8.8	192.168.2.6	0x479d	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:26.216744900 CEST	8.8.8.8	192.168.2.6	0xc3aa	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:26.216744900 CEST	8.8.8.8	192.168.2.6	0xc3aa	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:27.127240896 CEST	8.8.8.8	192.168.2.6	0x8cfc	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:14:27.127240896 CEST	8.8.8.8	192.168.2.6	0x8cfc	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.65	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:27.315715075 CEST	8.8.8.8	192.168.2.6	0xac69	No error (0)	ses-smtp.com		104.21.16.61	A (IP address)	IN (0x0001)
Jul 21, 2021 22:14:27.315715075 CEST	8.8.8.8	192.168.2.6	0xac69	No error (0)	ses-smtp.com		172.67.166.169	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 22:14:27.382770061 CEST	104.21.16.61	443	192.168.2.6	49757	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 10 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sun Jul 10 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 21, 2021 22:14:27.830235958 CEST	104.21.16.61	443	192.168.2.6	49760	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 10 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sun Jul 10 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3180 Parent PID: 492

General

Start time:	22:14:16
Start date:	21/07/2021
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://ibucket254.s3.jp-osa.cloud-object-storage.appdomain.cloud/pentacular/index.html'
Imagebase:	0x7ff7c15e0000
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: 5416 Parent PID: 3180

General

Start time:	22:14:17
Start date:	21/07/2021
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=1628,2857767762921153429,2104577615130111225,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8
Imagebase:	0x7ff7c15e0000
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