

ID: 452272
Cookbook: browseurl.jbs
Time: 03:06:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
Private 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 39
No static file info 39
Network Behavior 39
Network Port Distribution 39
TCP Packets 39
UDP Packets 39
DNS Queries 39
DNS Answers 39
HTTPS Packets 40
Code Manipulations 41
Statistics 41
Behavior 41
System Behavior 41
Analysis Process: chrome.exe PID: 3384 Parent PID: 992 41
General 41
File Activities 41
Registry Activities 42
Analysis Process: chrome.exe PID: 4752 Parent PID: 3384 42
General 42
File Activities 42
Registry Activities 42
Disassembly 42

Copyright Joe Security LLC 2021

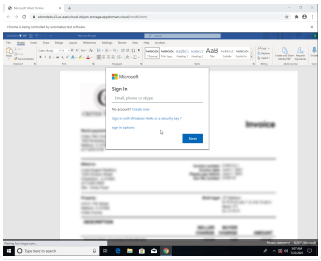
Windows Analysis Report https://sdsmdsds.s3.us-east.…

Overview

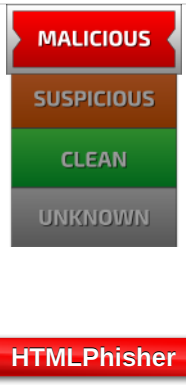
General Information

Sample URL:	http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html
Analysis ID:	452272
Infos:	

Most interesting Screenshot:



Detection



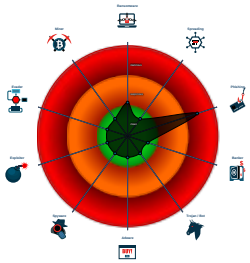
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3384 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4752 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1640,1593597631044081880 6,8945249272788690503,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /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

Copyright Joe Security LLC 2021

AV Detection:



Antivirus / Scanner detection for submitted sample

Phishing:



Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

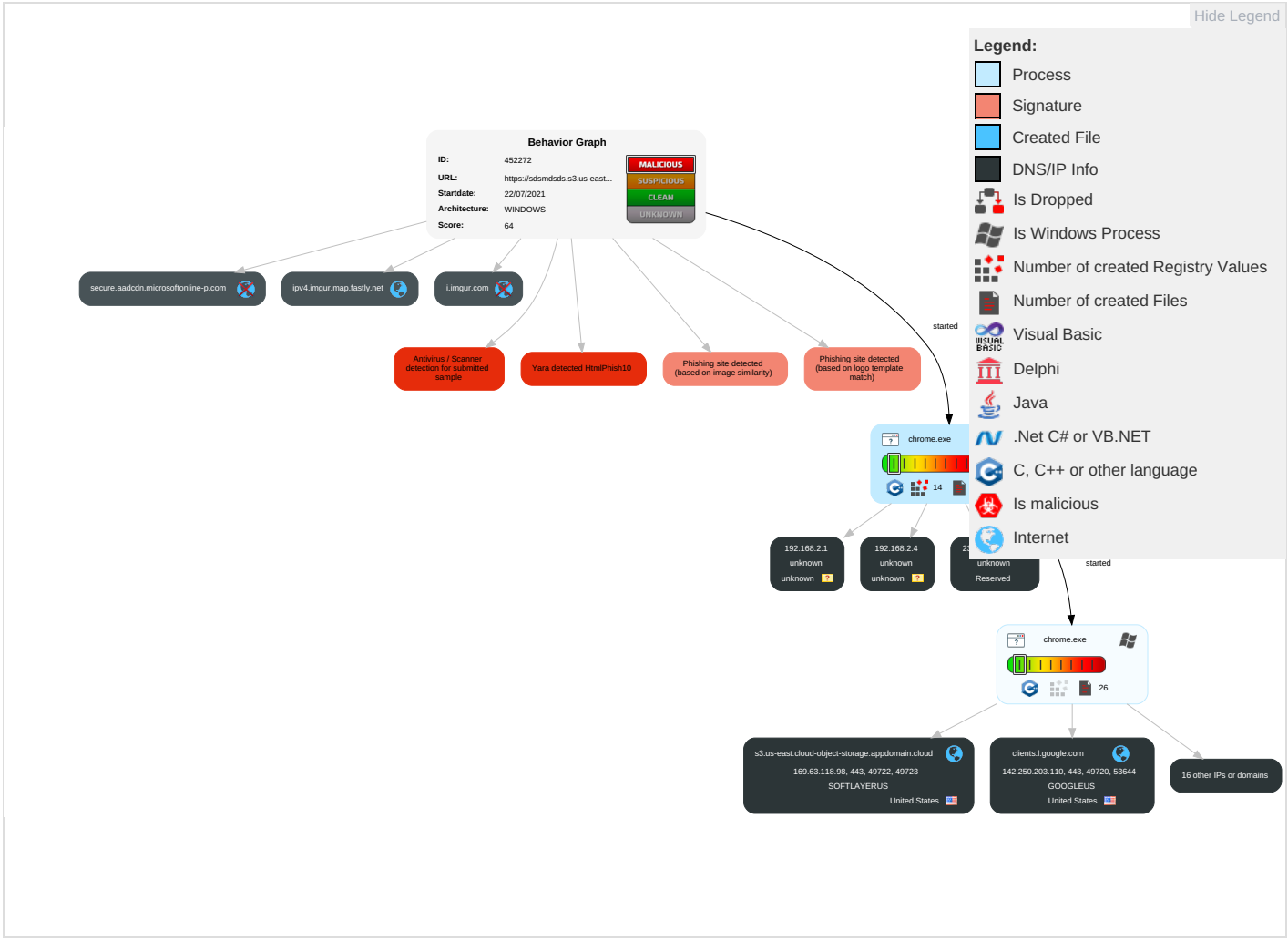
Phishing site detected (based on logo template match)

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

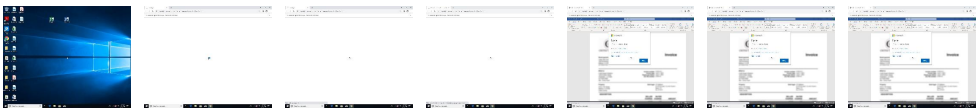
Copyright Joe Security LLC 2021

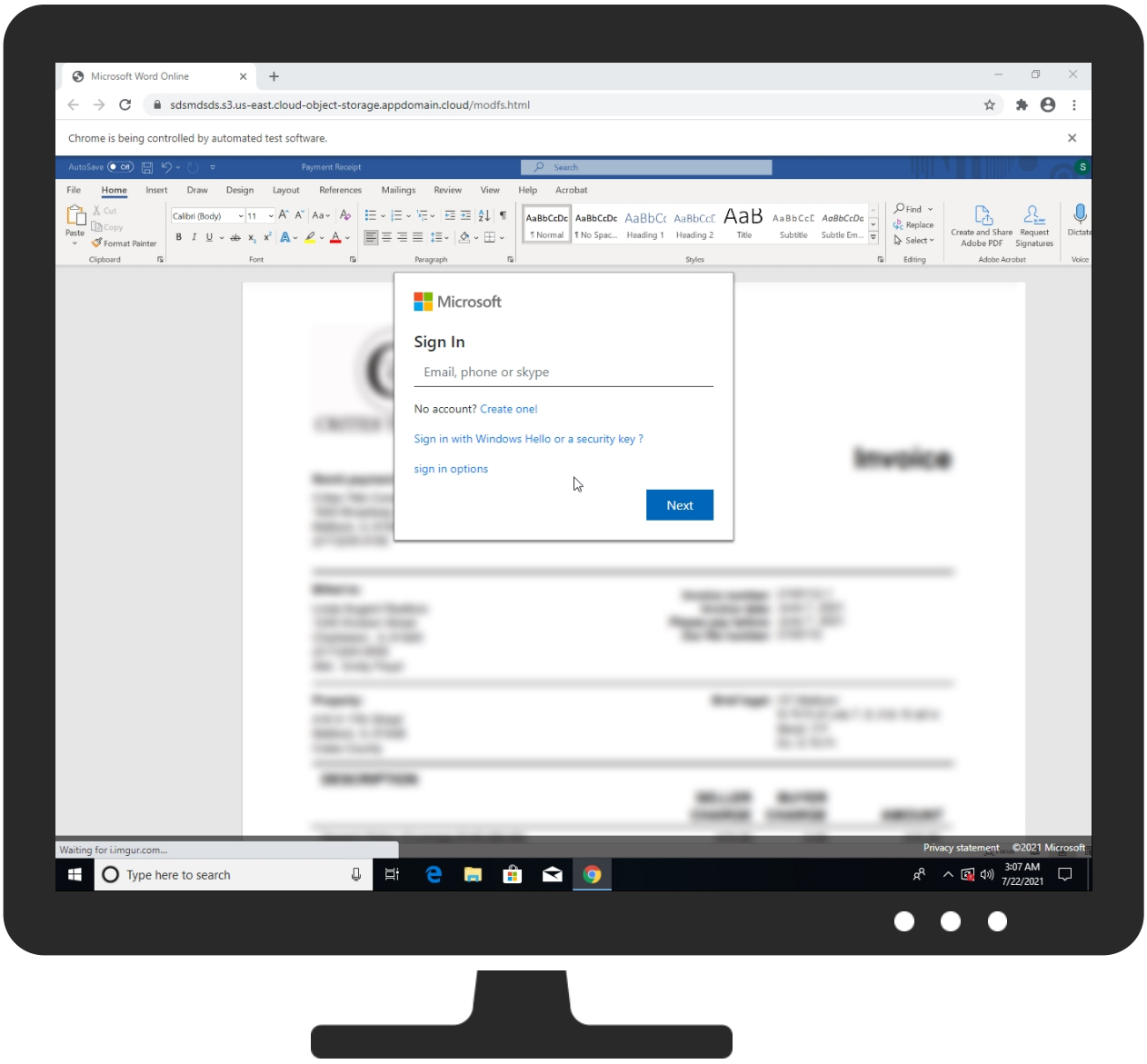


Screenshots

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://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html	0%	Avira URL Cloud	safe	
http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html2	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://appdomain.cloud/GL	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/;)	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.htmlMicrosoft	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/-i	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
s3.us-east.cloud-object-storage.appdomain.cloud	169.63.118.98	true	false		unknown
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
i.gyazo.com	104.19.143.111	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
ipv4.imgur.map.fastly.net	151.101.112.193	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown
kit.fontawesome.com	unknown	unknown	false		high
i.imgur.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.143.111	i.gyazo.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
169.63.118.98	s3.us-east.cloud-object-storage.appdomain.cloud	United States		36351	SOFTLAYERUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452272
Start date:	22.07.2021
Start time:	03:06:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@32/185@14/13
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:07:10	API Interceptor	1x 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):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2A0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....l.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.l.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.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.145340414441777
Encrypted:	false
SSDEEP:	6:kKq3PqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:S3O5kPlE99SNxAhUe0et
MD5:	049C00D55231AC82EE83E15AE4266493
SHA1:	9BA1BFC9C595635A524550888856C7DE7F61E982
SHA-256:	3F6D0F9A68B305F5C48F54AC580A3960B6492063FE59BE8BE99B1D1A210B76AA
SHA-512:	B0F14574B4A275122FA015949A97B64ECD15275B15E361CA61D1CDC697648CF3C4E8991E8BBEE50D2D263FD9E4568112513DC1AC36A66CB7D17184C44D5B196
Malicious:	false
Reputation:	low
Preview:	p..... .....U.~..(..... .....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\0fa001ba-a932-4b6b-adfb-da9f331f6cf2.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):	174418
Entropy (8bit):	6.07917638838986
Encrypted:	false
SSDEEP:	3072:UUbkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:3aExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	F64C8BD0B9BD09C9F0849042148A285C
SHA1:	16EDFB0F049D09386F3E821779D2BF37BA62D265
SHA-256:	FFD5843AF931C0DF85052F1B986390E7BB55D6026E13882EACBE3EB543C8DACB
SHA-512:	916595653B68B349F5648AB68AE3B326E605D7202B3CCEC90F2A1EBEE2BC0D698B96CDC078EE984E699DCE9D423694C35FD33D5FD5BE9C9EBF67E56C3D967(87
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016465124"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\29cae7cf-6470-48f0-b89c-5b65d4d0ff81.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):	166054
Entropy (8bit):	6.04967169974803
Encrypted:	false
SSDEEP:	3072:EZkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:nExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	ADA8B31D4942BA64AFF1425E6949C6E1
SHA1:	3598FA06C3A22B16353EDD5DEE1A50B715273183
SHA-256:	4A1EFDC3F4888171F37D4D06CA959F6830612CF3165325B9D2BA7F3E160E4A82
SHA-512:	52F43C1AB1055F468EB5DCECF928091CC7D0DF2178BD85895C5C801A4645F0EF76B7E205DA6F3E274409AA175047E0000DD1212B0C5D4EC8DB1E2A4F82D2F9
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016465124"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\4445659c-dffb-4958-ac3c-53b63805fdd2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7511473537902464

C:\Users\user\AppData\Local\Google\Chrome\User Data\4445659c-dffb-4958-ac3c-53b63805fdd2.tmp	
Encrypted:	false
SSDEEP:	384:nDqNVrw+zXQx8NhrKvFf3uBreHP2GyVrgDFFx+/L7qrI5mA7A/h15aOr7NNw1pwH:6KNFOPa2we7ZbXEHrCjKZf1l3
MD5:	A818990E6F6D8F59BD3BF8F7993DD42E
SHA1:	8DC11BC2941C63CB0BA4FEBBC404FCD8F98CDE90
SHA-256:	3C9329751B79F527BF589B01B08A7A64A77308C03542B258BF04A907DFDF21C5
SHA-512:	1BD73138284B0E9EA8A349280C2F06E938057D6F01733C5B0C6E905E9DEF9D610C0B57BFA82DB4D906E1416B871596198CE8757FC1F832BBA990706E4544884B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j@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\49ee52f3-dbc1-4106-9b89-b7b2ae0de228.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):	166054
Entropy (8bit):	6.04967169974803
Encrypted:	false
SSDEEP:	3072:EZkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:nExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	ADA8B31D4942BA64AFF1425E6949C6E1
SHA1:	3598FA06C3A22B16353EDD5DEE1A50B715273183
SHA-256:	4A1EFDC3F4888171F37D4D06CA959F6830612CF3165325B9D2BA7F3E160E4A82
SHA-512:	52F43C1AB1055F468EB5DCECF928091CC7D0DF2178BD85895C5C801A4645F0EF76B7E205DA6F3E274409AA175047E0000DD1212B0C5D4EC8DB1E2A4F82D2F9
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016465124"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ab8e060-0164-402b-bbb7-bc2ae9874894.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751404082520592
Encrypted:	false
SSDEEP:	384:5DqNVrw+3IXXV8ix8NhrKvFf3uBreHP2GyVrgDFFx+/L7qrI5mA0CA/h15aOr7No:Z+KNFOPw2we7ZbXEHrCjKZf1li
MD5:	DDD890BD20DCB704EBB1E8F85F848E63
SHA1:	E72C383CC6CDC5C625541D6047DA8B8EAF229A33
SHA-256:	1B3B1E8D029D57CCD121339A6ABADAC62BAB067C024E923E61D89E030131F657
SHA-512:	18FE99980E1644F7CFC4E49BB00893EC1265C1BD46CB6E406FAD481DD047E050045AD7E05F38F6D574EC22A5F47DD6EC59D8BA55B159B0201827E246F5B7F14
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j@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\652a3a7f-5a33-41d1-8db1-0afc18965b05.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):	165960
Entropy (8bit):	6.049393371502024
Encrypted:	false
SSDEEP:	3072:AZkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:rExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	CB365FDE7BD63E6FD995F9EC243B7662

C:\Users\user\AppData\Local\Google\Chrome\User Data\652a3a7f-5a33-41d1-8db1-0afc18965b05.tmp	
SHA1:	B5BBB859EFCE51AF0E3BAB0A1ACDB7792E09CC07
SHA-256:	428D9FE238AEAC95BEC9708B4EB97146DE46215252FFF667639B471953A1637F
SHA-512:	4F98651076F8E45CF3F7B77F8FEC4042739E07FDF842F99FFA5E274B0B8FF51924859C9B9FB86450553D08B85410623A1739F7009E95D7D87C239BB39BDF1864
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016465124"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f31125c-f03e-4755-bc2a-2974488fd57f.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):	165960
Entropy (8bit):	6.049393371502024
Encrypted:	false
SSDEEP:	3072:AZkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:rExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	CB365FDE7BD63E6FD995F9EC243B7662
SHA1:	B5BBB859EFCE51AF0E3BAB0A1ACDB7792E09CC07
SHA-256:	428D9FE238AEAC95BEC9708B4EB97146DE46215252FFF667639B471953A1637F
SHA-512:	4F98651076F8E45CF3F7B77F8FEC4042739E07FDF842F99FFA5E274B0B8FF51924859C9B9FB86450553D08B85410623A1739F7009E95D7D87C239BB39BDF1864
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016465124"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0e4abc9f-77ac-426e-b570-d9743e691843.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):	5794
Entropy (8bit):	5.190954907618103
Encrypted:	false
SSDEEP:	96:nlCTbT+MNlXiQNcKIvok0JCKL8RGks1zbOTQVuwn:nlCyM/PNcQ4KsGksh
MD5:	44DFBD57E43832881CE27C69C4F8A8EC
SHA1:	F1060FC189CAACBDB775F2A8ADB3B71D64367BEF
SHA-256:	70A2A6122CB5E7E6860E495936194ACAA2521C21CF062C11A51D5C1C8DC71416
SHA-512:	DE1294E04C5A30B92DB1D7F06C15A5342A650952E26DC983AFFD42EB3A7BA1628C9F64989E11626EA805CA7B636B61DDBF1FA293D83F11BBB93A28028219A11B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0e4abc9f-77ac-426e-b570-d9743e691843.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271422024750308","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\81e9a38e-1855-4acc-930d-b3c95f6f9ab2.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):	5172
Entropy (8bit):	4.986707505005809
Encrypted:	false
SSDEEP:	96:nlCTGXMpcKIvok0JCKL8RGks10bOTQVuwn:nlCgMpcQ4KsGks8
MD5:	29BB97E2B587D2DDB58D62C18F7A3887
SHA1:	C75084251AF3E1166B998A3D11C29F22D4BE64AF
SHA-256:	72263A2C4EAC0D1089E0FA5031AB376D1D3DABA8FEB4B813ED7C4CCE5A0F7FE4
SHA-512:	6B3031E03477C32D205781860CA32B579D534A6FD65B927C0738445E2E94FE5750375AC224B4E6464D74A9B5E9292F0441B01140A9ABA43ECDA434EDF9BCE990
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271422024750308","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9bf091da-24ad-4d46-ae19-a6997dead82b.tmp	
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535929685574232
Encrypted:	false
SSDEEP:	384:tr6tJLlHxfXv1kXqKf/pUZNCgVLH2HfDdrUFHG8nTkCLI4z:cLlRPv1kXqKf/pUZNCgVLH2HfxrUZG8F
MD5:	778B4642B1474A42239459436CC0FB7B
SHA1:	29327F7A936ABA637855A59EA339F84173B1C9E6
SHA-256:	551CDD926B7ECF233219D073E4FC75BA5C71E5AC4B9B5C558D07FAB445589FBF
SHA-512:	1D03ABCD8E7A4BC11311A53541DBEE15EDD6F3D71878963A62FF46F48A0CC838CED718B69CC1B0081049F7D004DF70A616A110C633D7DEFF82C5C2AF9D3792D
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":"13271422024475459","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.185088022548264
Encrypted:	false
SSDEEP:	6:mLZFIq2PWXp+N23iKKdK9RXXTZIFUtpqfuuZZmwPqt2kwOWXp+N23iKKdK9RXX5d:cOva5Kk7XT2FUtpUjZ/P+25f5Kk7XVJ
MD5:	889A77F6EC8827B86965571ADCF03777
SHA1:	681AA907AA52802BD3671FAC5F2943209D082BC1
SHA-256:	E1163B276994A6D60381BEE6A1A563C725C6658537733768A98E236DAA3A51D3
SHA-512:	3A43D7A6DD23E1CF26645E2CE23E91CF4FEBFE5D24180A1600A6A6E91AC492CAB7766540DAD94BDCCCC094797514FA06173C2D8CBED129780E20D2D1486219
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.138 1a64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-03:07:20.141 1a64 Recovering log #3.2021/07/22-03:07:20.142 1a64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.148984339479655
Encrypted:	false
SSDEEP:	6:mL/Oq2PWXp+N23iKKdKyDZIFUtpqQZZmwPqQzkwOWXp+N23iKKdKyJLJ:bva5Kk02FUtp/Z/P/z5f5KkWJ
MD5:	F08968D6DB25C4BF38664E2574173172
SHA1:	61CA89721FE355F118AA08239737073503759FC7D
SHA-256:	EAA1C5DD34958698DCCAF3627301BAE23B2E80B45F3811497988095815A2CADC
SHA-512:	3553C00B3D0B7545DC7EEBCF5157D64280AA799340E08E7E620874CB968302869647950E61580B0F594979B829FAE8DEE6C0CECD8C13FEA61842C634886D450D
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.132 1a64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-03:07:20.133 1a64 Recovering log #3.2021/07/22-03:07:20.133 1a64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\057a1b3eaa2d474e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.930991690980454
Encrypted:	false
SSDEEP:	6:mIbVYSHT8NWQAlKPUQyrSTztVK/wIg/3hyK6tUKb1hVmZzVQMMWkgCaRg/3hpL:T7z8NWQCUUUHcwIg/W1brVmZOxWpZRgj
MD5:	F75DD88EB54037157F0B1B4419BCCB9F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\057a1b3eaa2d474e_0	
SHA1:	FC9BC2A2142D708626ADDEBF9CC49252C3D6856A
SHA-256:	C477E529384646B3E805667B004FE207CED4F948933A1470F89F9A56255A6B58
SHA-512:	A49C37E5B5BE09907BA1637D7FBCACB685939C3C70CA2E46429BD629C869F2AD2DEA379D6F2254C1530B3BD73C9C69D0E151CDF6601894346F8B05942E8C61 F
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/-i.I&/.....W.....>.U1Rug..m./.....A..Eo.....p.. 5.....A..Eo.....-i.I&/.Po..331BC30303AEABCDE2CC45EFCF32DBD5C9BDA8A10527897F0CF608D3BAEB5724.....>.U1Rug..m./.....A..Eo.....L.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):	5.438305805397921
Encrypted:	false
SSDEEP:	6:mnrY68E9xEEUgLErySZsi1tV6Yp+E3jbrWRK6t:yYgqSO1fq
MD5:	30035028C7EBE8DD06D68F47A8430E81
SHA1:	42E4CF5C8F825F3BDCF6002958ACAB71CF659590
SHA-256:	117030D75EE95068895CFD0AA61251099EDA180ECCFE2F0C8634FF938ED852A9
SHA-512:	3113A90E0AC3FFFE78134FBF20F930590FD8B1A54FE6B543E74EB856A2A65077642F1F8CDC34EF6C7D4B2F8AD9F57F0AF509C0FE001365D94F23BD09AE0D183
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/GL..I&/.....P.....A.U... S.[w.[.iA2w.B.$.u..T6. A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e646c241401bf71_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.485528147274547
Encrypted:	false
SSDEEP:	3:m+leRla8RzYP2FycyGYWCULLuFvDL85Ka1T1Kl//lPD+lhmRw5qb5foyRm5XlpK+:m1YerCU6STQtVSEVonFK6t
MD5:	BCB352F46E0CA5E5E5C8E4C63A2CA048
SHA1:	74E521CB792995CB87DBE3A0AADA76750BA8F9D5
SHA-256:	E3B70524BF8F9B4DFA4DB3363697F4A1916A0E712A12AC839A76D17DDCE70BF0
SHA-512:	C672CCEF65056685BCCC904CA5168FCAC9D8F6ED151B33E956EA98D9AF0724E927CFCA5D18EC25BCF199B250118DE0C37018F154485F8B88864B92A4CAAA6E AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....I....._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://appdomain.cloud/\...I&/.....L.....P.....v..jgy.zW.O.xj.]... .`..A..Eo.....N.....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):	5.480015720628775
Encrypted:	false
SSDEEP:	6:mwOYlNYpSVkpSFspvtVCLiYNZSShvP4UVnK6t:dWpSVHFsv3GlNBNP9p
MD5:	8124008C7E2DFDAE973AF24BCEC288AE
SHA1:	FE5E3DF37480E10FC99E9D07FC551757324E6427
SHA-256:	1E4CEA2E5427789C916F3EAFCB342CD9DE324F2E24208B19276A8F20A1D3A61E
SHA-512:	932D44E91E190AF33A5C1965F3A455D354C80F75819089A97BD1800A4A4231D5847E070A2B17483D38B7CE71BFA728C34728AD5B5B2304D4321E514C997B6281
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...@..B...._keyhttps://kit.fontawesome.com/585b051251.js .https://appdomain.cloud/;).I&/.....R..x...N#..`.c.Uw3...5a"!..A..Eo.....p.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c6f62b67bce83557_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c6f62b67bce83557_0	
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.7727989751338935
Encrypted:	false
SSDEEP:	1536:WvsIsBp3MT67ky9jg2zKUjMIkjBvs2NWyx1pee0Agru4OH9G1qvSPL:0s73Mhy+nsklvs/q1pD0dDJ1qg
MD5:	CEDE2F2C78DD7484261C302FD73F150F
SHA1:	495775CEDC0C3C7D053332514B2890349BAD332D
SHA-256:	48224B54BCCEB2E385AF6DBB86E28C03C234800578F6319BE8ED4512948C94B7
SHA-512:	7D12D1F75F3A909A1B6A0D7961DE8B6B66B190F3C6C51E8B2A9FBB0D47D5848EE368F7ED3B798975134108D9F2770C901C91FEE4633D6F9C26DD04F9371A0F1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....>.....331BC30303AEABCDE2CC45EFCF32DBD5C9BDA8A10527897F0CF608D3BAEB5724.....'.JN....O ....n.....S.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@zq>.....module....Q.@..o....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.....Qb2:.7....d.....Qb...n....e.....Qb..I....f.....Qb"".....h.....S...Qb..|....j.....Qb._6....k.....Qbz{ j.....l.....Qb..%(....n.....Qb..".....o.....QbR.T.....p.....Qb.....q.....Qb6UGD....r.....Qb.....s.....R....QbZ..i....v.....Qbf2.3....w.....Qb... ....x.....Qb.....y....

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):	5.52462406385398
Encrypted:	false
SSDEEP:	6:mcSYET08NaYWbVOqZyS6Vprbhal75kKZK6t:og8NaY8ZXmp/MxT
MD5:	18840A9CA52C24885F9505AD049FEBBD
SHA1:	DCD859DA8254307CF807BFE3324C6E3093BA1F41
SHA-256:	4E7DDD01390560AD3DF4AA9BDF9102CC795D6E602602D6F8D12323AC463C57EF
SHA-512:	0F8688E6FEB736DDB37216449B1142E9C9DD3230E781141758330C0C50CD7EE18A07632B49CCD2ECCD4CC0FD02600BD0AFD8251234BAE4987B57DCFEA47CB 1
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/....I&/.....F.....H...@u?.[PN?.F...._.N... .9....A..Eo.....S.....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:	zlib compressed data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	4.971918350277683
Encrypted:	false
SSDEEP:	6:xaX/9/UMWs/KiK/YKK/ENSbFzQ3zbn3pHkQ+IRwHT+:xaX8FYzyz7V4hT+
MD5:	8397CDABADA3824946687617F567601A
SHA1:	C6B85A23105645A01E95099621CF0CC58214D218
SHA-256:	76212D4B395A04302D47BD128E7698969A3D5E433ACDECCCC2BE8FC2BA90B972
SHA-512:	85C6311288A0C798CBE8CCDC2B23D40CEFDDE05F32E46AA2A62774B6C5FCF32C55C1F88EAF19677659F24CED39E20949B4D51C0FFB1B1D3B5DE6889A993D4 EE
Malicious:	false
Reputation:	low
Preview:	x.....~.oy retne.....W5.g+...q.I&/..q.....A .1kK.q.I&/.....G..+....q.I&/.....q...$ld^.q.I&/.....$u....I./.I&/.....NG-.>.z../.I&/.....^}.Np..@ikt../.....-..0..x@ ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....D..I&/.

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):	0.8206109577734338
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06Uwfb4+z6lR9:TekLLOpEO5J/Kn7UibbulR
MD5:	F5E05BF052F4F7A79082640B6F580B6D
SHA1:	1ED62B6BAACA003FCE989C08C1DA176DC7888D3B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA-256:	B3D127C511551E921A7568D2657AD207A2D8988A386928AD194CFA54E2FD5881
SHA-512:	804787D492847599891202F1E802A8755A340E500493A8DD5C093B45334AC4307171CE82176F2ADF28E440131825F6F6E2499CD575D02A671010A2AA242A3739
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):	0.9681432311423015
Encrypted:	false
SSDEEP:	24:RrcLgAZOZD/tqLbJLbXaFpEO5bNmISHn06UwX8:18NOZtq5LLOpEO5J/Kn7U48
MD5:	9DD3266FB593C2DBD3DA8BEEAD30C221
SHA1:	8500EE435040CEA71A804DA31E8A999EF657CC6B
SHA-256:	BB5A1798FA64668F8FEC8ACCDF82CFD833CD229C8F0F1402A1B4982F486B552B
SHA-512:	5E78D7926A11ED9D6BDAAEA678F5248177936D96542D11D1E9007E55EAD637C6A03B173814B41F029EBA48E81A7727C13421622B86C9D6A4EEB85BCB0B03BDF 0
Malicious:	false
Reputation:	low
Preview:	.....I.&..... ....

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):	2260
Entropy (8bit):	3.3902945387376104
Encrypted:	false
SSDEEP:	48:34KXYxi3KE7EgHpszVYKE7MKEi/pszVhvKE7mL:34GEE7mzvE7REBzqE7m
MD5:	BF76AADB5067DF172AFEB4A7BA1D3642
SHA1:	B39EAAE0C73E3C13B380D3C1D8E18645AB49F782
SHA-256:	3CC879D676F3D2D1896E4DCD9E6471FE165B7D9E19045F8B5C2B8D5008635ABE
SHA-512:	903FE383290C4BEE7216C45AE4F1A2F0B79663FD93831C396780FEBB20CD4E09385FB401CD1D0FE1F6145DF0566C5322A47468896E42492E38F700B8B01C5E5C
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...dfcc7365_4c17_4e33_a36c_ef52229b3b29.....:+'h..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....K...https://sdsmdsds.s3.us-east.cloud-object- storage.appdomain.cloud/modfs.html.....h.....`.....w:s.....w:s....@.....X.....K...h.t.t.p.s.:./ ./.s.d.s.m.d.s.d.s...s.3...u.s.-.e.a.s.t...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./.m.o.d.f.s...h.t.m.l.....8.....0.....8..... ....K...https://sdsmdsds.s3.us-east.cloud-object-

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
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):	317
Entropy (8bit):	5.214742053532449
Encrypted:	false
SSDEEP:	6:mLeAQL+q2PWXp+N23iKKdK8aPrqIFUtpqgAG1ZmwPqgAQLVkwOWXp+N23iKKdK8h:l9+va5KkL3FUtpzj1/Pz9V5f5KkQJ
MD5:	4AABB127F529F0AAE9C20A87E61A8E20
SHA1:	F8C8FC1EE98D2355A5EE9A83BE2DD4F9493B9625
SHA-256:	06F5F1FF52254F14F80D5D323C5594F1C66D269F9A6AB822DB21080316CE17D7
SHA-512:	E0BCC72F724004C955C3A61E4D05CB28667729A78436F8802F8E63677DF2E15B8B68D02E30B7F4DD96DB872282272022EAA2BBBE2507D3CFF5A39D9039E449A8
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.831 19c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-03:07:04.833 19c Recovering log #3.2021/07/22-03:07:04.833 19c 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SHA-512:	9AB34C225D94941297FF47B3BBB36713AFB06C38179366E6F87F2E51FC19598DE621921657FEBD15EC63CDC874629442CF071C91C069E6482D82F402FB126FB2
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:07.052 518 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-03:07:07.054 518 Recovering log #3.2021/07/22-03:07:07.055 518 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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.214888075943969
Encrypted:	false
SSDEEP:	6:mLDnMq2PWXp+N23iKKdK25+Xqx8chI+IFUtpq4ZZmwPqmzkwOWXp+N23iKKdK25N:QMva5KkTXfchI3FUtpTZ/Ptz5f5KkTXc
MD5:	1751E0FD4CC7DF2406AD3505F3458AC7
SHA1:	CD8629388FA9C86E1AFEA5869A96297F0389A6A2
SHA-256:	231C7E6509914001A3B4D8E2D235C9A011BEA890747328029C92E30B0A2ADF8D
SHA-512:	02AA8AA32C5D0CDB7FCEB13E2A800C1F9983615A9A62520026D4632DCD0CCEA3A6E4C85C4A1D5ABDF6793243C0D98627DEEF3E7278E9E392F1398D491758996
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.109 1a64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-03:07:20.111 1a64 Recovering log #3.2021/07/22-03:07:20.113 1a64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.156809149423264
Encrypted:	false
SSDEEP:	6:mLLjIq2PWXp+N23iKKdK25+XuoIFUtpqJnjZZmwPqq3FkwOWXp+N23iKKdK25+Xp:YjIva5KkTXYFUtpSZ/PF5f5KkTXHJ
MD5:	4275CC40C6FA0CEC71690322F60EE501
SHA1:	2B9139A6A9D7FC5F7884E9F59CA937A173CCB22D
SHA-256:	62833217763C5FFC14E2726881FBD81CBF57DD57DD3C6B4C0C6259C063636207
SHA-512:	A0B643016261DC202A789F8782B4C81C63A051911E765B61831D8CFA2BC03460EA7D890F9023282FB03A8C5A11824D23B3B615B78FAD947514CC10C6F76073AC
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.101 1a64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-03:07:20.103 1a64 Recovering log #3.2021/07/22-03:07:20.104 1a64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.223197473405902
Encrypted:	false
SSDEEP:	6:mLbtgjyq2PWXp+N23iKKdKWT5g1IdqIFUtpqbmTm1ZmwPqbmTwRkwOWXp+N23iKN:ugjyva5Kkg5gSRFUtppA/PpwR5f5Kkgk
MD5:	BFF633397E5B66F7464BDC2895906746
SHA1:	CE99647179ECE6E0AB2ECF493B243FF1409B2C6F
SHA-256:	64100DF2F348F6ADE63FF937CFB14F7CB01A85B69D5EBC48C70A759BB911D610
SHA-512:	1B1726FABAB5DC7D59AD49B42CF8F78AE2D1CE56878B75181C3470D2090C68A3C076EB10BD94D8D77612DFA29EE179ACB2C3C463AA91E608EA47044EF7DE6571
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.065 1654 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-03:07:20.066 1654 Recovering log #3.2021/07/22-03:07:20.066 1654 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Size (bytes):	296
Entropy (8bit):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8Eflypt:89
MD5:	DE7FFD13F99802E90E2064D8F82B21A0
SHA1:	BF32600B24DE1ADF4DC5C3BEF579C17A9CAAB7C1
SHA-256:	28BFEBF72ECEDF415653C2B16938521E053FCFA14CD574568D270206FAF23975
SHA-512:	A1C5D6AC919B2F01C2584F5389F2B8EFC5AE03F793C5B8A970511A549CFE0BC795DA3DC8848701D3420539899F5C8AD7EDFE6FE037E00FF21A3462C036FC3C9
Malicious:	false
Reputation:	low
Preview:	.'..(...../=.I& /.....

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):	0.13398107375171425
Encrypted:	false
SSDEEP:	12:TL+A/qE6f0IPr9WDcelNHNuQ9GI/jlTIPr9WDL:TLxqgKEnlNtu+KEL
MD5:	23C7CC0E9E9B8D724E6A320839C2EA30
SHA1:	36BE2AC780AE7A72635DDB0D710B9DAA69EA5C24
SHA-256:	9144C13347F17C632DD341391695F63873A880C7851B8463A87F70DA313848D5
SHA-512:	06E66A74F4EBA58C8FB4489AC2AD39EB5B5E0722518C79014DBD3A8703696C2E3E3A074668C1FA2B3820DCEC1382CAA2AC9906C220F6092175CC4A63CDD11B5
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):	823
Entropy (8bit):	5.300067011357527
Encrypted:	false
SSDEEP:	24:e2HnAGHSfOlj1kerm4/qhfLG4muY78BJgskfa9yBDOxoLFqLKEslym:e2HAGyf8bMfNrU7kLKEskm
MD5:	D38F837EA33BD769976FAD1DD43EF735
SHA1:	6F68F705D824BA4202D05C13C9295F1227274D44
SHA-256:	19828B25A6D4AC102465DA093C326DFD63FF32422AC126CDCAEF1645D688E84D
SHA-512:	80DF552BB3278560E885FE9F54520B8C3D7D884D1B85C04996D1DE8F51880E07B39E78F2ECA891D0070961C09072C7D67BB0F579E1262465BCFB954A2AF87F5C
Malicious:	false
Reputation:	low
Preview:	....."j....appdomain..cloud..east..html..https..microsoft..modfs..object..online..s3..sdsmdsds..storage..us..word*.....appdomain.....cloud.....east.....html.....https..microsoft.....modfs.....object.....online.....s3.....sdsmdsds.....storage.....us.....word..2.....3.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w..:.....B..... ....*Khttps://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html2.Microsoft Word Online:.....J.....")1;AG.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11649219887606886
Encrypted:	false
SSDEEP:	6:AB1lqg9bNFlWCj/lQEl3lB/04/fMt76Y4QZVRtRex99pG/4HaqR4EZY4QZv8fOp:ABGqqLBj/N3lp04nMWQA9LFBBQZ8fOp
MD5:	6A825E7785558123A1049A01786C5963
SHA1:	41410FC43E9CA9E40BDA09D814EAF7C2C987744A
SHA-256:	5DFCA47DAF937EA36B3490B2282F9333C7C8EF797528C3E6D8978D3301C3100F
SHA-512:	2EF4253215DAAD25E87EBCDEB2B35272861F3688807280A0CCE9BAC08846A7E9CBC4C8A9DEE84C4F652BDE55CBE3B3AD6B6ADD7D28B254BDCD5CB12B29E66367

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Malicious:	false
Reputation:	low
Preview:	.....Rh..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.448505079825895
Encrypted:	false
SSDEEP:	48:u60GV5La7mMF8dblN2HbQSefgGN/8NrS0U9RdiN9o:/na7mMedblN2HbQ5fgGNkrS0i
MD5:	502D5600274D4D76AF892969A8ED042F
SHA1:	38363C1D0E3C774330399B2DCDA94EA01A0C4DE9
SHA-256:	65AD8E6C042FF2C8C3E2A5CC4E3EF4DE243490EF5FFDEA4A136CC018F4C83980
SHA-512:	C2B5BF6F20C5E1592C813D9A872992582C1344295E2B1B2896C6815AA7F191D2AEA1DF7B733985FB7E98FC436CAD8F98C86D7F45A89FE69AF4AB5DE8E0B38A77
Malicious:	false
Reputation:	low
Preview:	.,.D...*.....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..297224000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 03:07:21.31][INFO][mr.Init] MR instance ID: 304c3cc8-731e-43dc-8d50-9f0cec119531\n","[2021-07-22 03:07:21.31][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 03:07:21.31][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 03:07:21.31][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 03:07:21.31][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-22 03:07:21.31][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-22 03:07:21.32][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.159173294985484
Encrypted:	false
SSDEEP:	6:mLai+q2PWXp+N23iKKdK8a2jMGIFUtpq8TXZmwPqiDVkwOWXp+N23iKKdK8a2jM4:C+va5Kk8EFUtpp/PjDV5f5Kk8bJ
MD5:	FBDA05F10D133E872DB20ACE19CAE1D1
SHA1:	58719DCF4CA65EEDA8BCC972DA9D7FB73D661730
SHA-256:	F28D91816D8A8404B8DDF282B671FBEA17E5B95DDF6A8ADA640AC557352ACB09
SHA-512:	2B2EDD8411BC13849AA9638CECED3FA2AA34244CAD8EF203E2DBFB99872796505E78FC793A85825DF063AE88F67313CEA365ABF3DE018DDCAB0B3D4099DC2E9
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.503 cbc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-03:07:04.504 cbc Recovering log #3.2021/07/22-03:07:04.506 cbc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.255392748088993
Encrypted:	false
SSDEEP:	6:mLjQL+q2PWXp+N23iKKdKgXz4rRIFUtpqiUiG1ZmwPqsiQLVkwOWXp+N23iKKdKt:T+va5KkgXiuFUtpPUl1/P3V5f5KkgX2J
MD5:	C7DE81010741720A05A206CDB6AF8377
SHA1:	149A83A19400E76646C64B945AF0CADA2FEC3019
SHA-256:	BC73EFAC463558C714AEE383C03F503EA01C6814B9068066ACB1BEE2BAB27E90
SHA-512:	3BE4AC9742BF2C8CBE01E74B67C39BDE25559BACA92639A4290AD8BF8554CED6D99F7989D5513AD8EA509C17ABB1FE144A206D03C00B4798766107953604961
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.862 19c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-03:07:04.865 19c Recovering log #3.2021/07/22-03:07:04.866 19c 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):	28672
Entropy (8bit):	1.359584886229828
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdt2vZO1SIoP11:wIElwQF8mpcSR1loC58oBicrL8J1
MD5:	7BBB3A8819C143402A96D4CAE3165954
SHA1:	75606874C77CBCA2C663A13A2EA6136266A7B647
SHA-256:	B8A087E00A74BD42FECB1F49AF25EAFB57A609E13389B87470BECF0B68ACD397
SHA-512:	5FFB2D48E27AA82228DA5481EDAD3DAFE51DC702A6C676440C15604168AF1CD695A9F70CD7871DDFADF912259A1E74F88D998858772C39F2A3817539CED84E
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:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6275524871555378
Encrypted:	false
SSDEEP:	48:ScqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUv+4:SchIElwQF8mpcSF
MD5:	46DE860DA75AAC19F77E2C1E980DD30D
SHA1:	B87222C907C4309FCC2854883BC96AAE79A6B74A
SHA-256:	FAC5C4463726ECE06632F7C79BC42BE161ECABE71672FF8D94ABA9EC8994B985
SHA-512:	1840FD74D3D6B4DDF13248D3A3BFF19C013135DFA798DE074E2CC324D72AAB64939B2F78E1A39DDA33C13981E374B3CAC2248E65482081D7B360EEEB7C2AE7D
Malicious:	false
Reputation:	low
Preview:	.....-a..... ....

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):	317
Entropy (8bit):	5.163957568642727
Encrypted:	false
SSDEEP:	6:mLTAQL+q2PWXp+N23iKKdKrQMxIFUtpqLFFpG1ZmwPqhwQLVkwOWXp+N23iKKdKf:Q9+va5KkCFUtp71/P0V5f5KktJ
MD5:	E5CE34D259F0BB0457EBDDAE34ACDA10

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
SHA1:	0594E2945C8B7245099A1FAA2829D4F2E5FEE193
SHA-256:	992D30B9CB354B0C7FB35A86DC9BD1B6E767FA2D9306C55DF24ACE9EAA3472EB
SHA-512:	52C5FC6F26BCA0F8660265FAF26C5CECF3685E1AC8A2DDD2F031BC33994845650454161BE6831386B2DDAB2022719CB2C82CD6E4C6C47EDC1CB1AD872B786(A
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.733 19c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-03 :07:04.734 19c Recovering log #3.2021/07/22-03:07:04.735 19c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.1772426454132
Encrypted:	false
SSDEEP:	6:mLcT3+q2PWXp+N23iKKdK7Uh2ghZIFUtpqhZmwPqYukVkwOWXp+N23iKKdK7Uh2w:nTOva5KklhHh2FUtpA/Pzuk5f5KklhHd
MD5:	3B84B02C34A8A8EAA89D8A9DAC2787E3
SHA1:	5787E3D928642B343D76C194D49DA1CF02CFF4EE
SHA-256:	988699594AD306B91B5E8F1EAC841559F27C59F49CA441FB707D8BE7DE019449
SHA-512:	08412DADB5EBD93686C634DA57F85FC77FEF6E5EE5A930DE9F1DBFAACD7194D9CAC24B6C166F753265D1CF6E020D2C16C1955824F6881535FED2A2C48897D5 0
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.463 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/07/22-03:07:04.466 1438 Recovering log #3.2021/07/22-03:07:04.467 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\416766e9-efa1-46c2-aa4a-fbc33de cb317.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.258024097318011
Encrypted:	false
SSDEEP:	6:mLzQL+q2PWXp+N23iKKdKusNpV/2jMGIFUtpqqiG1ZmwPqqiQLVkwOWXp+N23iK4:3+va5KkFFUtp1l1/P1nV5f5KkOJ
MD5:	3A30A85C661BCCBDD83616893E876DB3
SHA1:	CA99F1D14293C19268CE5B74EDC08C844C0672E3
SHA-256:	38B4227AE0055F949FA669B15F4E7A258D4CFB41D52F1256836F59734B674635
SHA-512:	3D97CD95A3E97255EB41BD496E734F88FEC955D8210BA920A54FA66AC1AB4102CF654C1C4B175E4E951E7F97CE02156BD8F140754EF41246914E49915728F3A0
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.804 19c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-03:07:04.806 19c Recovering log #3.2021/07/22-03:07:04.806 19c 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):	429
Entropy (8bit):	5.2901488555774785
Encrypted:	false
SSDEEP:	6:mLW9q2PWXp+N23iKKdKusNpqz4rRIFUtpqeZmwPqiQZkwOWXp+N23iKKdKusNpqS:T9va5KkmiuFUtpR/PPQZ5f5Kkm2J
MD5:	F99143F4C7C0AC327FF11744CBB27F54
SHA1:	2ED7063216DF0F093E7BFFE8898FA3911FBDA5FD
SHA-256:	0A60054ECFEFF15189BB174021EF2F130037228B57FA1EF52A3C0AF580017E19
SHA-512:	EC73E5EDC77A2DC19F29D9655FA6AAC93C11F3FC3DDF4BCB95C781E2DD0E9632F5F87D585D12A790E1C2616C84645C5F09E9DDA678D93E4A242A1052212608A
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.861 5d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/22-03:07:04.864 5d0 Recovering log #3.2021/07/22-03:07:04.865 5d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.2560686206720195
Encrypted:	false
SSDEEP:	6:mLqeq2PWXp+N23iKKdKusNpZQMxIFUtpq0XZmwPqLBkwOWXp+N23iKKdKusNpZQq:Jeva5KkMFUtpPX/PQ5f5KkTJ
MD5:	B536F215F1394A076686764CB62AC853
SHA1:	29403559342A739BE8321D5885EA902675B974BE
SHA-256:	BD75FB7167601D27B317962728E09F30EDD53EB89087FE0B9441F91EBD624A61
SHA-512:	8A4EFB6CF350F8215EBAE5B316E8A4A49E7816FD6582810915F0CA80000358769CD48202BED8430D42634A096D5AE6178836FEC4190172B9BE88F5F9BE589245

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:21.053 480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-03:07:21.055 480 Recovering log #3.2021/07/22-03:07:21.056 480 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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):	430
Entropy (8bit):	5.175246416091765
Encrypted:	false
SSDEEP:	12:2ova5KkkGHArBFUtpYC/PwF5f5KkkGHAryJ:2aa5KkkGgPg0f5KkkGga
MD5:	E890D8F1A8B10D1AEEDE70CE4DFD1056
SHA1:	A18E4C6032AB71D6B6734F700E34211CD3A9DB19
SHA-256:	74419C33665D3EBBBCDEA5C7F9F2CE9AA05681C00EDA8F22530A945FAE530ADB
SHA-512:	9FA9E1BCB1FA5BC5D8A2CEC6C6BA91D85DFA25F687DFC8950730F6CF285A642FA87BE5B4BF1576A73919D6487B134B1204F7CA6134B28CAF8FB94A8C8913238
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:19.727 1018 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-03:07:19.728 1018 Recovering log #3.2021/07/22-03:07:19.729 1018 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):	429
Entropy (8bit):	5.21764261296401
Encrypted:	false
SSDEEP:	12:Kva5KkkGHArqiuFUtprh/Ps5f5KkkGHArq2J:wa5KkkGgCgRMf5KkkGg7
MD5:	C16C02D2BBAAFD6CB18561EC21D3E5E4
SHA1:	3E0ECC0FA137C36F2E967567942C1BFEB0B2C853
SHA-256:	2DAC657A44544A8F9AB8A28F2C442C2456A331EE14143E9B75448DE4338D711D
SHA-512:	EE9A7D2F0A441517F1C4EEECE87EF6030011DAF7C35D37C96CC73E3A4E814FA88C59759C8B574E014985166784CCFE3AC0FD45DA0BB8523CDFB03BBA80A5A73
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:19.740 480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/22-03:07:19.742 480 Recovering log #3.2021/07/22-03:07:19.743 480 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
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):	415
Entropy (8bit):	5.199286200953574
Encrypted:	false
SSDEEP:	12:5eva5KkkGHArAFUtpB9/Pq5f5KkkGHArfJ:58a5KkkGgkg3+f5KkkGgV
MD5:	91C0F227B265E556CAE7A5DDECEDE7FC
SHA1:	594BFE906C74E31085140226E8C3CF569AC8FB8E
SHA-256:	B0DCDD8713880C0C8C91B56E1DEDB79DBA3D5BD88D8A7C00562281F066DB7457
SHA-512:	3B3547AD018A0708D781C0DEA4DAA6003E629019F0D923B24E613906E649272CCCFB137F321DEE649FB00F5C4EA067FC69F2C8348C992FCDEDB15C532B081C B
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:35.076 480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/07/22-03:07:35.078 480 Recovering log #3.2021/07/22-03:07:35.079 480 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\a21f8c24-9f31-455f-a2b0-216a16b75ef5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.249841660241894
Encrypted:	false
SSDEEP:	6:mLxq2PWXp+N23iKKdKpIFUtpqKZmwPqZFkwOWXp+N23iKKdKa/WLJ:ova5KkmFUtpL/Pw5f5KkaUJ
MD5:	B39BE78D72EA3A1FBA2C3799F522F8EB
SHA1:	E7118CA592B46FF779497B7A75697F0D69C7E63C
SHA-256:	7CAA158C08D79431704CDFD100C35037F0503A7E4262A113A455854A1006C64B
SHA-512:	CBFC4C94B4F852F1860C19D5C2394F04221C34F463C409157A527C50D221309C24C820EF51128AD57D64CFDA9666AF581B7A9476451B811CC077666791F59508
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:04.476 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-03:07:04.478 1650 Recovering log #3.2021/07/22-03:07:04.479 1650 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.28162733570995
Encrypted:	false
SSDEEP:	6:mLQAq2PWXp+N23iKKdKks8Y5JKKhdIFUtpqxZmwPqVqZkwOWXp+N23iKKdKks8Yx:eva5KkkOrsFUtp2/PbZ5f5KkkOrzJ
MD5:	419B935B1959DD6EB34F493AF8667C7A
SHA1:	96DD3DAF62D84725308C7D3120B5338E4B76E313
SHA-256:	5987986258C2980F30A3F757D0F0E40C382F19624C09A3571996F4AB9055563A
SHA-512:	58FE9D47028D46BDC4A85048CFA5BE0D18EA73017ADAD86D372D489E2C4BC826261092B82AA439ADFCA7BB5E11A383F6ED5649BB9822B75C5BF8CE0DF314CF0
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:21.278 5d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-03:07:21.280 5d0 Recovering log #3.2021/07/22-03:07:21.281 5d0 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:sq/FU:pU
MD5:	634471FC2C5AFA8C81487CA35B74FD39
SHA1:	9B43E911D0D876222AFF373EBF7A6844F4DF1EE0
SHA-256:	CFDCAEF68F43DC9E3793ABDB9480C3ADFEBBF46894908DB1AD801D28D3E00C3E
SHA-512:	936F05A3F7C4D34A7EC97539590252AE8C1AF475D893E3B9CBE087DBE8D38116B80D93B2C63DB1AA061318C237A67A49FCF2D667E9EF229D62F5EBB4C36D860
Malicious:	false
Reputation:	low
Preview:	....HOb. ...

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.452206820967872
Encrypted:	false
SSDEEP:	3:tUKIO4FFFRQyZmwv32O4ESCddFWSV8s2O4ESjkSWGv:mLT9ZmwPqESC1jVvqESjhtv
MD5:	47D8D28DB6BEFBF4A58EE09736632ED9
SHA1:	B60C1B18D9C5C2C03CE15121EC5885D4D3D8DC22
SHA-256:	476881143034C2898898B4515FDC124D5DFD0FD066F73FD4695B10AF0F882CB7
SHA-512:	2472E8E070BF2A7EBC2BA976CCADF79E5719694D0E46D2F4F874251C0344AAAE37A86E06297E1A37015732F1931B7CD051315C5F7AE5C1A48D099552C1658487
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:17.019 1a64 Recovering log #3.2021/07/22-03:07:17.173 1a64 Delete type=0 #3.2021/07/22-03:07:17.174 1a64 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\de5a43af-04ac-4778-a551-52c286e3cdf3.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):	5.536052208243878
Encrypted:	false
SSDEEP:	384:tr6tJLlHxfXv1kXqKf/pUZNCgVLH2HfDdrUFHGnnTkCGKI4Lx:cLlRPv1kXqKf/pUZNCgVLH2HfxrUZGnZ
MD5:	19E89A5CE8581283DCD0EEFA130C8CD8
SHA1:	893EC3824AD04164B45A9F56170A3C2F0BEADA37
SHA-256:	F08E47CB36D8D784D7BCCC8A903B51B99C82F133A783BCD95181C915489C5E5D
SHA-512:	DA949F1BD02A188691A2706DF89C9C81591470A9D4DDF2D1C33BF0282A084B8D7C3F0BF3F517D875A852A499CC6C58513DD703E4A1133E7D4B6ABFAE1618E2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de5a43af-04ac-4778-a551-52c286e3cdf3.tmp	
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":"13271422024475459","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\ded6f638-ae4c-42b7-9b14-152384447ea8.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):	1375
Entropy (8bit):	5.585328068230778
Encrypted:	false
SSDEEP:	24:YI6H0UhsVIUYZTG1KUokq/HeUeXby2qUeXvPb7wUkWBYxYUtdWRUenHQ:YI6UUhseUrKU5qPeUer2UefvwUkqsYUl
MD5:	683A90EF71A3BBD2ACB1C0AFEFDEBAED
SHA1:	F2845EF86DFA57F2F017F4AD2558ED4F378BAA9C
SHA-256:	7845D3F8473C9BBEF1E0549D08B6AB449FCB2CAA413557F33653246EB7F0F841
SHA-512:	DACE857717BAD820E01BFEB5B13A1DDD0A85B3A927DFEAF855356E43C44C511444319F79867B448B1287FAAA3F89E73C8B872310D699428E4F9EEE409E35BD85
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658484430.396977,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXlu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948430.396982},{"expiry":1658484430.392552,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948430.392559},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1658484429.514028,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e457b25e-85fe-4f2c-bf98-bc0b08df1041.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):	3199
Entropy (8bit):	4.878326408920693
Encrypted:	false
SSDEEP:	48:Y2TntwXGDHz5sARLsqTsI2d+4sg8qepsx6qC5gJQ6Nh8VsTkzsWyKsg3zsHMHlYV:JTnOXGDHzPti+grXxC5GQ6NCoEVeGihH
MD5:	D1D897B751F6864EEB982E1E8510207A
SHA1:	F95212D6F2441A5947F7F7FAB34B9AAD63667135
SHA-256:	B7F27FA42E15E75EFD9E41675CA7177A94032C1BF550F4064A36E56F7F6880E4
SHA-512:	A6D37F6CF4B5DEB49BF876237C99F25D5C7D7871D966FE6E0951862F6B139C7C92B47B8E260BECCFED96B304C79D8AE95C774149A8C33F451A15B5810E9F562
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.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":"13274014029513915","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274014029540607","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expira

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb9d68f7-1081-455a-b701-3f8bb1eed39a.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):	1879
Entropy (8bit):	5.598581384649867
Encrypted:	false
SSDEEP:	48:YQ+VwUfrUe6UUhseUrKU5qPeUer2UefvwUkLsYUblwUNUenw:9UDUDUU/UrKU0PeU9UEYU9YUxUNUD
MD5:	C07F96845D69F7884BF29AC31067622A
SHA1:	3B2EAE452FA3520173F4899A7224BBA9C4F81E89
SHA-256:	23EC08AD4831765F918F09705CA910F6FCC1630C47A55C99D27C4DA3DE17CCA4
SHA-512:	73FFDB9239E34AFD132D97725774E52129B5FB643A045C5B44C85542B6137BFD5B35C38A33FC3BC59127CBBE3BA7177BB513DE645738E22B24855AD47150A273
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb9d68f7-1081-455a-b701-3f8bb1eed39a.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1642728461.191247,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948461.191253},{"expiry":1626948761.134859,"host":"GGApl7UvK2CYbnERSYSoCoHcYUdXwzjjAzjTFCIkpg0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948461.134863},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658484430.396977,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948430.396982},{"expiry":1658484430.392552,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626948430.392559},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.178980322842148
Encrypted:	false
SSDEEP:	6:mLZsq2PWXp+N23iKKdKfrzAdIFUtpqZcJhZmwPqZ5kwOWXp+N23iKKdKfrzILJ:ysva5Kk9FUtpCcJh/PC55f5Kk2J
MD5:	1E12EE57B5C5A880C379969724EC46AD
SHA1:	31D79B94D8FDB1282BE2070C9A871E689A56C92A
SHA-256:	A6700B6B4061BB1B225BA3E64EAFC17D5105045C4F40A4462675A2AC9249544F
SHA-512:	22F2A0D9BD0EA9F743338D9B308E0D03A238E799733CA8483F223A937E2C0FCA756A90D018AC17FDAFF7459B839A3489D64ACBD5CB064B832B6695C18ACF8B6C
Malicious:	false
Reputation:	low
Preview:	2021/07/22-03:07:20.264 480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-03:07:20.265 480 Recovering log #3.2021/07/22-03:07:20.266 480 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Eflt4Wl/:8lWl
MD5:	98040FEAE18D99ADA38CE2364C042524
SHA1:	923BB988E6F59F926C5260AFF141FE92CE1F3B58
SHA-256:	CCCC8C97BAE28401B50510C101067A7117CD267CCF9482DF18F45BDC0733B81F
SHA-512:	A6B2FCF940D022A48E3ED5CAA499368114A687F6E8338C1C458A3A215D7EB47888007E18DA6A41899391ABA84A71604EDD13E8F2F8132F26F9844A994910B2DF
Malicious:	false
Reputation:	low
Preview:	.'..(.....q7.I& /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\a7c32f2e-5b24-4f23-b0f2-6df4c3f9767b.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):	174418
Entropy (8bit):	6.07917618863958
Encrypted:	false
SSDEEP:	3072:7pKkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:VRExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	B1ECE61A4A200D21BF409AECC18B45B7
SHA1:	BEBC75A1B5918D2449028219579E59742161E6F2
SHA-256:	F64D5A8E29F7E2FE11581A5B22984DA808E2BDEE1522DA1B80E1F90FF586B84A
SHA-512:	E9BA2137546AB0B589401E94974B7DFD0DFB94FA5A47691E3B7E60C5F7530D0F21A5C76F49D0A85DE5606461C89A41C1CA47D53C8A05EF33CCB3C362A2844C4
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\e643cb09-4351-45d5-b8a5-5da34b2f124d.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):	174418
Entropy (8bit):	6.079175843378621
Encrypted:	false
SSDEEP:	3072:7UbkZExZKKJEuwA4x37SiHnDcWYKWFHFcbXafIB0u1GOJmA3iuRz:waExzgRx37iWYFzaqfIlUOoSiuRz
MD5:	B83C5F36CE419D34F4EBF1426FD5810C
SHA1:	CB62C906217D63B6000389B5885BE6A362067270
SHA-256:	D05E67FA5C17374F188E1BB02114273F32C97241BEA4CACFE90139D3CC2FB7EC
SHA-512:	EED5514EE4A9D4FBA88C09F4A36FBB9ADF5D0167F6FDDFC94D6794B3F40CD84ED235FAEB636F5BD5838DAFFBBC71D36B9D7D33C00BE6D6BC3C6AD8F22380 8318
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":1.62694842776141e+12,"network":1.62691603e+12,"ticks":6045435072.0,"uncertainty":4813034.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8f79434-7e5d-4349-8052-697d335fa3b0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7512609257792824
Encrypted:	false
SSDEEP:	384:JDqNVrw+3IXXV8ix8NhrKvFf3uBreHP2GyVrgDFFx+/L7qrI5mA7A/h15aOr7NNZ:J+KNFOPa2we7ZbXEHrCjKZf1lF

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8f79434-7e5d-4349-8052-697d335fa3b0.tmp	
MD5:	742CA9DD73C61A29B9AE85FE5DAB52F8
SHA1:	FCC317C0A87DFE261E1CCCEA8139B9A5EBA74D1F
SHA-256:	CDFEFEB7B7EBCA56334D1EBB9FE22C28411B91BF6E2F408D8AB5E63B35153654
SHA-512:	8DB8AB15B128B184443901F776A4CEB7C44D116B901206FE28373AEF933361F449C7B2E4D56D88B7FD8865A3E1A8524845F3BF7E8F29B0DB3BAC27A71DA5D7D
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\3384_1989888281\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C 2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5b74393f-7076-48f5-9317-5a8adf23afb1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\8a37d301-8775-42d5-a559-f0cd26099b95.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

C:\Users\user\AppData\Local\Temp\8a37d301-8775-42d5-a559-f0cd26099b95.tmp	
Preview:	.

C:\Users\user\AppData\Local\Temp\8d850e53-6506-4244-92de-aab2d23bf488.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16458
Entropy (8bit):	4.649026265975929
Encrypted:	false
SSDEEP:	384:t5Jz13iXxKtTeTF/MoF0OPumxJbiJteC+J1JBJhJSrLUxF:t5Jz13ioTeTF/MoF0OPumDbuteCAfzTL
MD5:	A39820E59381F9C950CF0684684A28A0
SHA1:	059182441E793D7DF92C80BFCA5795A5608FD454
SHA-256:	8D3E56B4F04DA99698DE4084D07763C2CE9B3A64C73FC2A07F89EBAA2832FE13
SHA-512:	7342A7367F80C4F4DEAAA6EC93C8EC8D52BFA27EBDC4A6039ECEA9D29619E99159B5CCF71276A63386C5D0CEF0A2E12B6A679F5DA0D2D25CC2A056BD2F614AEA
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 15629795f863d6c1fa9a2078b1709f62900b7e9c5a5ec01d0a2f6485b89b2ef8 18bb9eaa5f42d5026e0747423ad92c413bef4f2988bb548264a1eedad6079643.SERVER_HANDSHAKE_TRAFFIC_SECRET 15629795f863d6c1fa9a2078b1709f62900b7e9c5a5ec01d0a2f6485b89b2ef8 3ad31d689c4bdeea2a5b54b1e8bb0367e76569c61c834f87e000eda5daa88ac6.CLIENT_HANDSHAKE_TRAFFIC_SECRET b68a34bb783bdd7ce8664d734d7eea4b7379510fdcc0acbf6df1932d1f1ed3ad 3e2390e3a3505edbb5965039f47564cbb11a4affa954a12962113e18bacc3f85.SERVER_HANDSHAKE_TRAFFIC_SECRET b68a34bb783bdd7ce8664d734d7eea4b7379510fdcc0acbf6df1932d1f1ed3ad fc521e25d906af8236a438c81bc1da3c55a59a34242ce623177116195a62960c.CLIENT_HANDSHAKE_TRAFFIC_SECRET 714b966fb3a30b55d0f2ce64f138931331aa4816c7a581d4298335ae278cf03c 06c7cf209daa029e0592467de6967801453 7b5c33fe6a2c4b0b56057fac91fc4.SERVER_HANDSHAKE_TRAFFIC_SECRET 714b966fb3a30b55d0f2ce64f138931331aa4816c7a581d4298335ae278cf03c 7f592250275d60dc61fbd9fd7b6ebb02e626b2e33b98aa9a7fe8cb2246ccf343.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\f15b416b-f54d-4a31-b14e-d47f92170d39.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_dir3384_1226577643\5b74393f-7076-48f5-9317-5a8adf23afb1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\5b74393f-7076-48f5-9317-5a8adf23afb1.tmp	
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\cs\messages.json	
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\el\messages.json	
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3384_1226577643\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

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 22, 2021 03:07:09.824434996 CEST	192.168.2.3	8.8.8.8	0x2b5f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:09.833070040 CEST	192.168.2.3	8.8.8.8	0x482	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:09.839157104 CEST	192.168.2.3	8.8.8.8	0xc111	Standard query (0)	sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.732525110 CEST	192.168.2.3	8.8.8.8	0x80fe	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.735167980 CEST	192.168.2.3	8.8.8.8	0xc1f9	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.735321045 CEST	192.168.2.3	8.8.8.8	0xc478	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.582585096 CEST	192.168.2.3	8.8.8.8	0x1640	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.583286047 CEST	192.168.2.3	8.8.8.8	0xb28e	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.584168911 CEST	192.168.2.3	8.8.8.8	0x6de2	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.585082054 CEST	192.168.2.3	8.8.8.8	0x742e	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.696691990 CEST	192.168.2.3	8.8.8.8	0x72b5	Standard query (0)	i.gyazo.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:13.455822945 CEST	192.168.2.3	8.8.8.8	0xb0d	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:13.455887079 CEST	192.168.2.3	8.8.8.8	0x9747	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:18.299388885 CEST	192.168.2.3	8.8.8.8	0xced3	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 03:07:09.890366077 CEST	8.8.8.8	192.168.2.3	0x2b5f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:09.890366077 CEST	8.8.8.8	192.168.2.3	0x2b5f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:09.897722006 CEST	8.8.8.8	192.168.2.3	0x482	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 03:07:09.908602953 CEST	8.8.8.8	192.168.2.3	0xc111	No error (0)	sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud	s3.us-east.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:09.908602953 CEST	8.8.8.8	192.168.2.3	0xc111	No error (0)	s3.us-east.cloud-object-storage.appdomain.cloud		169.63.118.98	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.801059961 CEST	8.8.8.8	192.168.2.3	0x80fe	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.801059961 CEST	8.8.8.8	192.168.2.3	0x80fe	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:10.804533958 CEST	8.8.8.8	192.168.2.3	0xc478	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:10.824430943 CEST	8.8.8.8	192.168.2.3	0xc1f9	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:11.240302086 CEST	8.8.8.8	192.168.2.3	0xac18	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.641102076 CEST	8.8.8.8	192.168.2.3	0x1640	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.641102076 CEST	8.8.8.8	192.168.2.3	0x1640	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.644455910 CEST	8.8.8.8	192.168.2.3	0x6de2	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:11.645788908 CEST	8.8.8.8	192.168.2.3	0x742e	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:11.645788908 CEST	8.8.8.8	192.168.2.3	0x742e	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.652086973 CEST	8.8.8.8	192.168.2.3	0xb28e	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:11.785686970 CEST	8.8.8.8	192.168.2.3	0x72b5	No error (0)	i.gyazo.com		104.19.143.111	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:11.785686970 CEST	8.8.8.8	192.168.2.3	0x72b5	No error (0)	i.gyazo.com		104.19.142.111	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:13.507947922 CEST	8.8.8.8	192.168.2.3	0x9747	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:13.513040066 CEST	8.8.8.8	192.168.2.3	0xb0d	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:13.513040066 CEST	8.8.8.8	192.168.2.3	0xb0d	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Jul 22, 2021 03:07:18.365578890 CEST	8.8.8.8	192.168.2.3	0xced3	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 03:07:18.365578890 CEST	8.8.8.8	192.168.2.3	0xced3	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	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 22, 2021 03:07:11.780383110 CEST	151.101.112.193	443	192.168.2.3	49741	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 22, 2021 03:07:13.609967947 CEST	151.101.112.193	443	192.168.2.3	49758	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3384 Parent PID: 992

General

Start time:	03:07:02
Start date:	22/07/2021
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://sdsmdsds.s3.us-east.cloud-object-storage.appdomain.cloud/modfs.html'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4752 Parent PID: 3384

General

Start time:	03:07:05
Start date:	22/07/2021
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=1640,15935976310440818806,8945249272788690503,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021