ID: 432882
Sample Name:
Fax_Doc#01_5.html
Cookbook: default.jbs
Time: 21:41:02
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

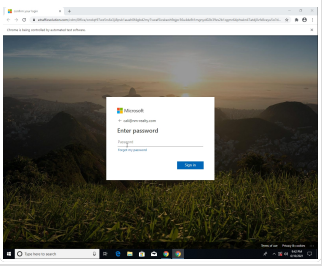
Analysis Report Fax_Doc#01_5.html

Overview

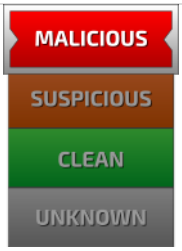
General Information

Sample Name:	Fax_Doc#01_5.html
Analysis ID:	432882
MD5:	0e73957b74aa54..
SHA1:	c1456fda553cd40..
SHA256:	ecc2656e7f58af1..
Infos:	

Most interesting Screenshot:



Detection



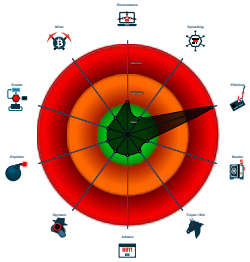
HTMLPhisher

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish3
- Yara detected Phisher
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5856 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Fax_Doc#01_5.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6264 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1600,13519744996372922803,2498414373330437516,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Fax_Doc#01_5.html	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected HtmlPhish3

Yara detected Phisher

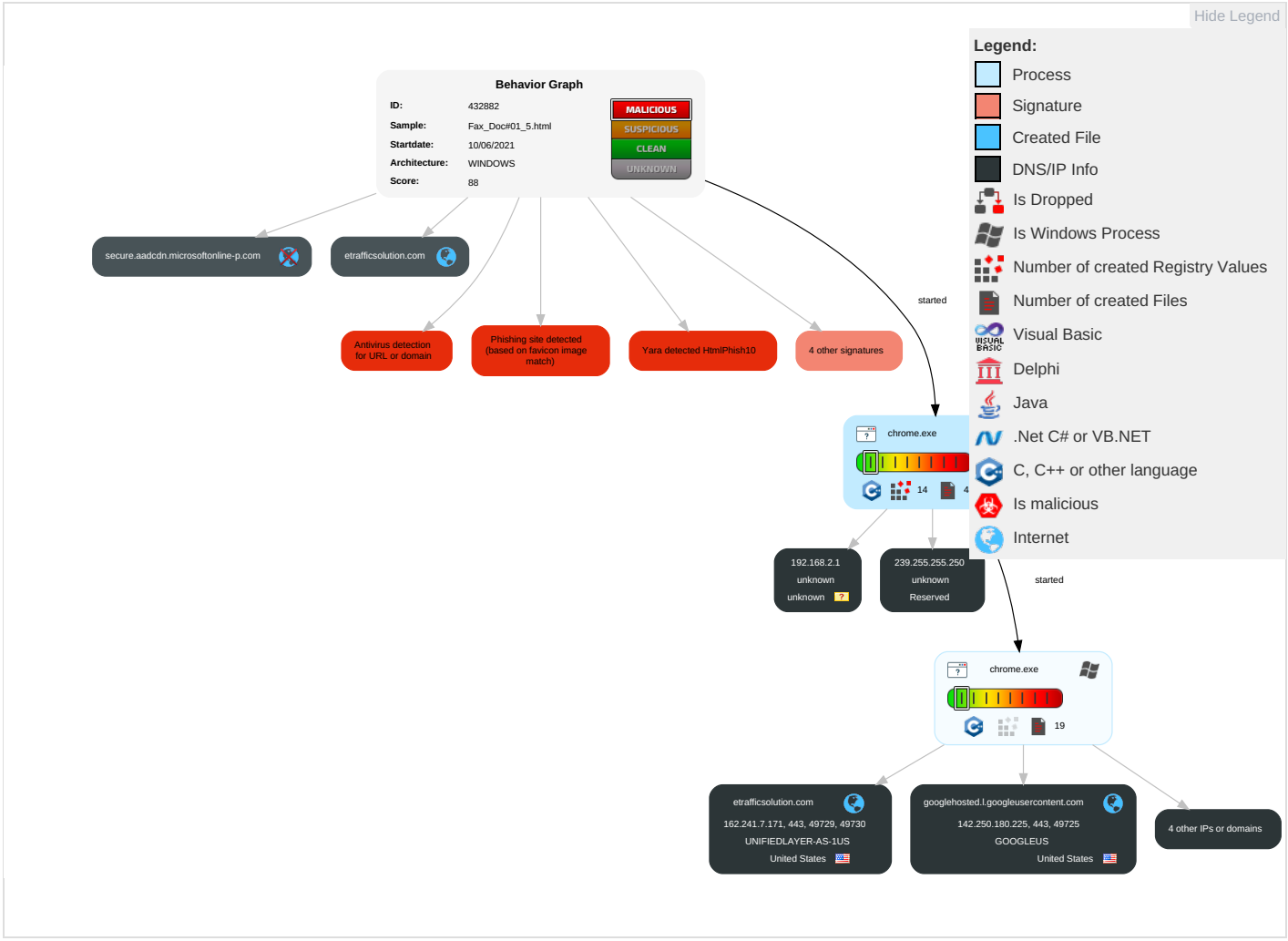
Phishing site detected (based on image similarity)

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

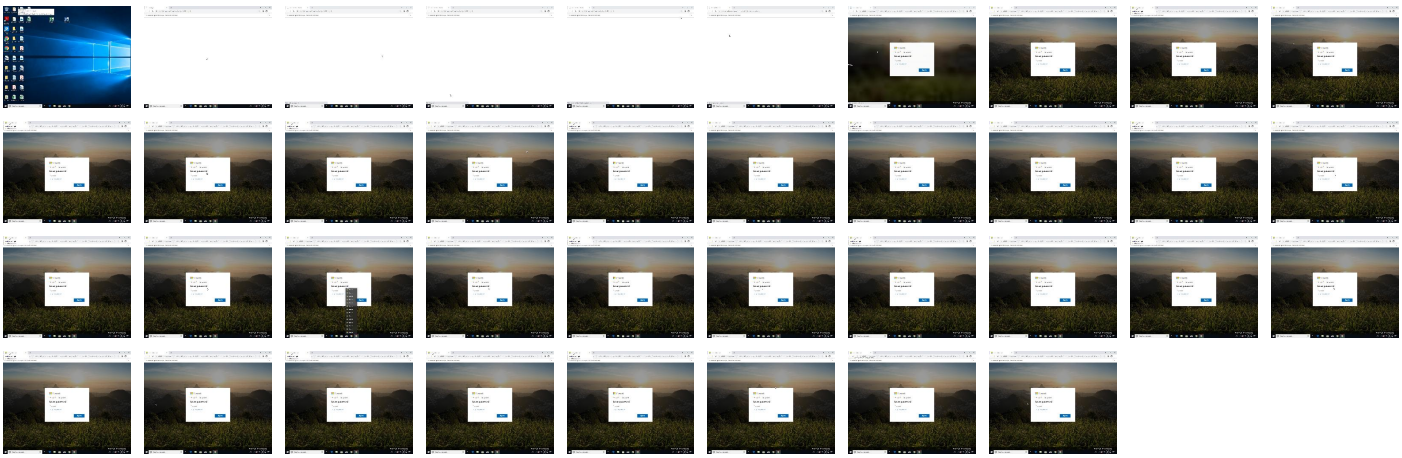
Behavior Graph

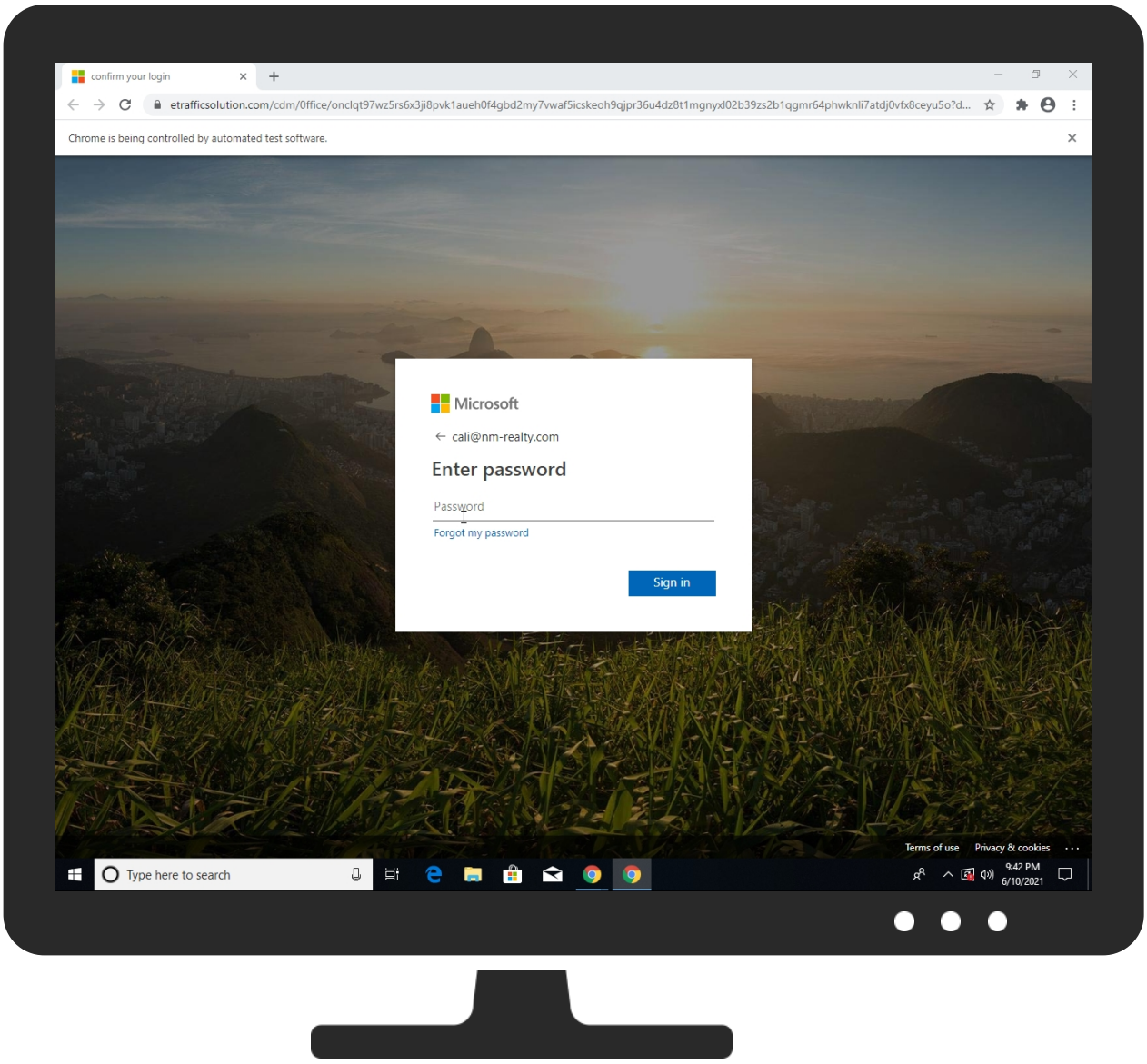


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://etrafficsolution.com/cdm/0ffice/onclqt97wz5rs6x3ji8pvk1aueh0f4gbd2my7vwaf5icskeoh9qjpr36u4dz8t1mgnyxl02b39zs2b1qgmr64phwknli7atdj0vfx8ceyu5o?data=Y2FsaUBubS1yZWFsdHkuY29t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	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://etrafficsolution.com/cdm/0ffice/Y2FsaUBubS1yZWFsdHkuY29tconfirm	0%	Avira URL Cloud	safe	
http://https://etrafficsolution.com/cdm/0ffice/onclqt97wz5rs6x3ji8pvk1aueh0f4gbd2my7vwaf5icskeoh9qjpr36u4dz	0%	Avira URL Cloud	safe	
http://https://etrafficsolution.com/cdm/0ffice/Y2FsaUBubS1yZWFsdHkuY29t6	0%	Avira URL Cloud	safe	
http://https://quantlab.sutherlandresearch.com/cgdin/v4/cali	0%	Avira URL Cloud	safe	
http://https://quantlab.sutherlandresearch.com	0%	Avira URL Cloud	safe	
http://https://etrafficsolution.com/cdm/0ffice/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://etrafficsolution.com/cdm/0ffice/Y2FsaUBubS1yZWFsdHkuY29t	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
etrafficsolution.com	162.241.7.171	true	false		unknown
quantlab.sutherlandresearch.com	197.242.146.206	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://etrafficsolution.com/cdm/0ffice/onclqt97wz5rs6x3ji8pvk1aueh0f4gbd2my7vwaf5icskeoh9qjpr36u4dz8t1mgnyxl02b39zs2b1qgmr64phwknli7atdj0vfx8ceyu5o?data=Y2FsaUBubS1yZWFsdHkuY29t	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
162.241.7.171	etrafficsolution.com	United States		46606	UNIFIEDLAYER-AS-1US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
197.242.146.206	quantlab.sutherlandresearch.com	South Africa		37611	AfrihostZA	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432882
Start date:	10.06.2021
Start time:	21:41:02

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fax_Doc#01_5.html
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
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:	mal88.phis.winHTML@36/183@6/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:41:54	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	ATT00005.htm	Get hash	malicious	Browse	
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	
	Kancelaria Marszalka's-Protected-Fax.htm	Get hash	malicious	Browse	
	Docc.html	Get hash	malicious	Browse	
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	WheelerIndustries_Doc#92543.htm	Get hash	malicious	Browse	
	Remittance-Advice.htm	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	
	INVOICE-PAID_02PDF.html	Get hash	malicious	Browse	
	Payroll Adjustment for employee.html	Get hash	malicious	Browse	
	0F4F0709D120ABA22D4687BFABFA5004DD54B0FC C6EF1.exe	Get hash	malicious	Browse	
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	
	212161C3EFE82736FA483FC9E168CE71#U007eC2 #U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	
	212161C3EFE82736FA483FC9E168CE71#U007eC2 #U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.23206.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Bulz.383129.29566.exe	Get hash	malicious	Browse	
	New_Messagejacob@steinborn.comMessage.html	Get hash	malicious	Browse	
	treetop-payroll-075491-pdf.HtmL	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	WcCEh3daIE.xls	Get hash	malicious	Browse	• 162.241.77.193
	KCTC International Ltd.exe	Get hash	malicious	Browse	• 192.254.185.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 74.220.199.8
	supply us this product.exe	Get hash	malicious	Browse	• 50.87.146.199
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 192.185.74.169
	3arZKnr21W.exe	Get hash	malicious	Browse	• 192.254.235.195
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	HM-20210428 HBL.exe	Get hash	malicious	Browse	• 192.254.180.165
	INQUIRY. ZIP.exe	Get hash	malicious	Browse	• 50.87.190.227
	audit-78958169.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	research-1315978726.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	ExHNIXd73f.exe	Get hash	malicious	Browse	• 108.167.142.232
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	viVrtGR9Wg.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	DEMLwnv0Nt.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	audit-367497006.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	analysis-31947858.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	research-531942606.xlsb	Get hash	malicious	Browse	• 192.185.33.8
AfrihostZA	New Order.exe	Get hash	malicious	Browse	• 154.0.165.45
	sample1.doc	Get hash	malicious	Browse	• 41.76.213.144
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 169.1.24.161
	HU4TEm4Vr7.exe	Get hash	malicious	Browse	• 169.0.142.82
	product specification.xlsx	Get hash	malicious	Browse	• 169.1.24.244
	ppc_unpacked	Get hash	malicious	Browse	• 169.214.149.159
	MGuvcs6Ocz	Get hash	malicious	Browse	• 169.208.248.210
	z3hir.bin	Get hash	malicious	Browse	• 169.128.215.34
	IMG001.exe	Get hash	malicious	Browse	• 169.106.68.226
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 169.1.24.244
	YPJ9DZYIpO	Get hash	malicious	Browse	• 169.107.27.65
	PO#41000055885.exe	Get hash	malicious	Browse	• 154.0.167.80
	2ojdmC51As.exe	Get hash	malicious	Browse	• 102.182.93.220
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 154.0.173.248
	payslip.exe	Get hash	malicious	Browse	• 169.1.24.244
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 41.76.213.144
	document-1915351743.xls	Get hash	malicious	Browse	• 197.242.147.47
	tems order.exe	Get hash	malicious	Browse	• 154.0.167.156
	INV3249732836.xlsm	Get hash	malicious	Browse	• 154.0.168.63
	New order.exe	Get hash	malicious	Browse	• 154.0.167.156

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	wa71myDkbQ.exe	Get hash	malicious	Browse	• 162.241.7.171

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Current-Status-062021-81197.xlsb	Get hash	malicious	Browse	• 162.241.7.171
	logo.png.exe	Get hash	malicious	Browse	• 162.241.7.171
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 162.241.7.171
	WcCEh3dalE.xls	Get hash	malicious	Browse	• 162.241.7.171
	ATT00005.htm	Get hash	malicious	Browse	• 162.241.7.171
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 162.241.7.171
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 162.241.7.171
	iX22xMeXIc.exe	Get hash	malicious	Browse	• 162.241.7.171
	QWkt5w3cO2.exe	Get hash	malicious	Browse	• 162.241.7.171
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 162.241.7.171
	vTtOheCXBQ.exe	Get hash	malicious	Browse	• 162.241.7.171
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 162.241.7.171
	Check 57549.Html	Get hash	malicious	Browse	• 162.241.7.171
	audit-78958169.xlsb	Get hash	malicious	Browse	• 162.241.7.171
	Docc.html	Get hash	malicious	Browse	• 162.241.7.171
	askinstall39.exe	Get hash	malicious	Browse	• 162.241.7.171
	Lista e porosive.exe	Get hash	malicious	Browse	• 162.241.7.171
	askinstall39.exe	Get hash	malicious	Browse	• 162.241.7.171
	SecuriteInfo.com.Trojan.GenericKD.46459351.411.exe	Get hash	malicious	Browse	• 162.241.7.171

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:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wlEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8SI...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1181739797487062
Encrypted:	false
SSDEEP:	6:kKFUe8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:9U8kPlE99SNxAhUe3OMx
MD5:	4574F296BE68F321BA06621F4BC41E50
SHA1:	18B9BE77A2E4AAB06DE1844C76B7BC3CBB61C445
SHA-256:	58DA110B0699F4D708EA5403C8B7A703F825DC381C68096DB145AFE33A30BB08
SHA-512:	C86536F8FF35B7F1EB7EB41F854286D048F969A45ACBA7A1F82703A92F8A8C6B04D5594E72D531F6425AC2372CEA9B726B1079346C6DA6A5BCA9985765CED42
Malicious:	false
Reputation:	low
Preview:	p..... .....q/Q.|^..(..... .....L.....&.....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...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.::.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\436feff7-db2e-4fef-97dc-2d6a2736e72a.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):	164141
Entropy (8bit):	6.050668144292564
Encrypted:	false
SSDEEP:	3072:6R4ryDswL0T4qxb8lHqzEYFcbXafIB0u1GOJmA3iuRY:oIAsZ8qxKaqfIlUOoSiuRY
MD5:	155C1A28C5657294606B980DCBB5A22D
SHA1:	F4ED04FD56489A741F93A09BD3B4C153FF544CC3
SHA-256:	06BDEFE6A23CE8A10D59300C5B3E18C6CF1C58583640750F35D40517B83EEFEB
SHA-512:	FD998362BCDC918273CDC9329A2514738521741B9C789A60842750ED1F15C049D145343588B7AC48D6E6046B0A1A8F0357D1C4E392D06EEE7037E3F287653479
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":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\4ff2b261-4f3a-4497-a9f6-64cf8bc28c9f.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):	172374
Entropy (8bit):	6.080121355546503
Encrypted:	false
SSDEEP:	3072:OxJR4ryDswL0T4qxb8lHqzEYFcbXafIB0u1GOJmA3iuRY:4TIAsZ8qxKaqfIlUOoSiuRY
MD5:	6718199E082E08BF7E9C87D72CB37743
SHA1:	9B9DBD888685D5BB94F4B0A8DBC808E80C528332
SHA-256:	78BD63C2A5F0A1AB7167FB27489E453FD736F8701C243C4D6D886F9B1FA49D61
SHA-512:	A6A115BFD2484C182D8F725591FE549F9837498CA8D4607ABB597DAE0B6AFD449CF07257A755AC3691F32FE8A458C5DD6FB8A111CA4EFFD4CC880E4EFBB141E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\4ff2b261-4f3a-4497-a9f6-64cf8bc28c9f.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\5a0c0938-afec-45c3-aa09-b22d1892f4b6.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):	172374
Entropy (8bit):	6.080122415727292
Encrypted:	false
SSDEEP:	3072:VxJR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:jTIAsZ8qxKaqfIlUOoSiuRY
MD5:	7E0222C654651DE85E8E37526D67363A
SHA1:	352505E8F1885626C8AB81F1A594CE4134B85781
SHA-256:	1846E3F86734AD84060A9B86045131485A91D411ED60437D27AD2CF1E83F2CE2
SHA-512:	1376838EC6AB77F17F341123D6226C584C8A7C81F1540FD2670A4AF213AB4B9E3E42E6AC11FA8075C4E2B733C17C40C62B9B7732045DBF889B2178B53DD1D46E
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":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016854670"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\66f07040-887d-405d-bbb8-7f73d982fafa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7525577255708487
Encrypted:	false
SSDEEP:	384:9jIHP1K49W5FVW8LaNjr4v/V3QvJIHRkGUTre5P3xIp1Nkr+zm+p6l7vboOJZnNa:J66V1aVQQke7TtxknLOlKrFfhS
MD5:	9BBF1E9E1E3267F6C1A323A2BDD87A2D
SHA1:	92FCB818A4D3DDE64698F9304F7FACE519B30FAA
SHA-256:	E1F8E5D6646F328F86932AA46D1BF21000B3906AD67BC89F22AB367667EAE2AB
SHA-512:	C4BB43D642BC417742BAA2DC150F6B1D4D0E59FC6FFCFA45E48889A77576FA7EFAED9CE4671E5D1C5CF83836653E43FAB9DFE835D63D4BE2083BE16B75FABEFF
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.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b5726be-a262-4498-a68e-108c69f09d44.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7524558380845936
Encrypted:	false
SSDEEP:	384:tjIHP1K49W5FVW8LaNjr4v/V3QvJIHRkGUTre5P3xIp1Nkr+zm+qU6l7vboOJZnd:Z66V1aV0Qke7TtxknLOlKrFfhX
MD5:	B1647158C5413B0338CE43E778CB1F4B
SHA1:	86505B2A3BE77108604430A8FEF5EA3865B81725
SHA-256:	3A1546B58BCF036C95C51714F84086C2030051C3C1FC99B8071940B31E39E479
SHA-512:	03273D6334B810226883BA0068592CB0EC7978DB4B7B1C444F98969D19858D98D0EFC45E9617B7B06058A7A0B32F3B9C4C1A20DDCC2EC72692D98317DFD6AA9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b5726be-a262-4498-a68e-108c69f09d44.tmp	
Preview:	.t.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\...... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8ec1852d-6402-4d93-b34c-34ae60bc93f4.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):	172374
Entropy (8bit):	6.080121355546503
Encrypted:	false
SSDEEP:	3072:OxJR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:4TIAsZ8qxKaqfIlUOoSiuRY
MD5:	6718199E082E08BF7E9C87D72CB37743
SHA1:	9B9DBD888685D5BB94F4B0A8DBC808E80C528332
SHA-256:	78BD63C2A5F0A1AB7167FB27489E453FD736F8701C243C4D6D886F9B1FA49D61
SHA-512:	A6A115BFD2484C182D8F725591FE549F9837498CA8D4607ABB597DAE0B6AFD449CF07257A755AC3691F32FE8A458C5DD6FB8A111CA4EFFD4CC880E4EFBB141 E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"os_crypt":{"encrypted_key":"RFBB UEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2 ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfl jw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_p assword_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

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:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Preview:	sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0241c1b1-06a9-4f48-b461-ab2d9c99dfc9.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):	5641
Entropy (8bit):	5.16736986478828
Encrypted:	false
SSDEEP:	96:ndCBK12RlN2RdmNcVUXok0JCVRWL8VbOTQVuwn:ndCs2RukcmS4VY6
MD5:	5850A18ABF18E5AC0FA20C6567A190C4
SHA1:	294C9A9A96348929A749F6658CF3938DA8077D87
SHA-256:	F7AD6C9B8E541A50FC6AE170343CAD62A4DE3A8A387011BEA44DC758CB3B7B1C
SHA-512:	9355894229F26464CD82B26AC9225BF15E058C237B6DBE7280A48E1D806D92A7A0BB8596B9DB28DF508D8D68B3E13857479A96B8DA692116FD649DDDC5129DB
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267860109001298","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4138ae71-24c5-4c7c-b0f4-5700c7db0bdb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61b7d524-bdb1-4be1-ab69-b8034bf4b953.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535677285381711
Encrypted:	false
SSDEEP:	384:WQx1t3LlnSX71kXqKf/pUZNCgVLH2HfDhrUGHGpnTZ+aq4BSj:vHLlA71kXqKf/pUZNCgVLH2HftrUmGpS
MD5:	D13D5A624093849C27EAE6BF13212F12
SHA1:	2AD492B9E596F5647D4C138516EF5B7D458A0018
SHA-256:	B697C51CC8900E6CF3E6F53CA873838CD35845D27DACCD065F7A785804E1E474
SHA-512:	CED260FDA7726BD708A675ACFE32F0FC0A640B4A9155E48ECF3B216A79C78BA7BF951F76B94D7879949D965372B41729B9F071E0E05F1C5C96B116CB87DE4C0
Malicious:	false
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":"13267860108735169","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\729f9522-9f32-48c4-a3da-98fa5f8a891a.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):	2051
Entropy (8bit):	4.906569014048792
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5sODsQTsxRLsSH9sryKsAA3gYhbD:JTnOCXGDHz99wBEuxhH
MD5:	86BAD5871D274EB831D1B3AC0F6BC830
SHA1:	593383EE55EC7AAF08313D826F0382FC83A9DF21
SHA-256:	050492F7F63EB9FC4D06C387F1E87BF4696A803AF28AD9EA2ACBCEE4607D6DC0
SHA-512:	D074EA6C69F1C54A3B96F0910FCF59E9F7760D8DCAC3657ECC4E3760F1C60A7AD2EC55C430F8249D9F703EBAC36A1F5619E41A561DA7C22E67968A5FB5C1F0A
Malicious:	false
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://fonts.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":"13270452113635765","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270452113637084","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

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):	5.252272255935648
Encrypted:	false
SSDEEP:	6:mwOoiq2PWXp+N23iKKdK9RXXTZIFUtpDOTZmwPDOJkwOWXp+N23iKKdK9RXX5LJ:1iva5Kk7XT2FUtp4/Pg5f5Kk7XVJ
MD5:	275288EDF62ECF44D5E657C9067D615E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
SHA1:	AD9F3F2FE48545F4387004C6A266B07C38DDDD50
SHA-256:	F88BCB3A98DE81F6D51464E48C420FED3E6163E2A3AD39D1DB61C8031C472224
SHA-512:	E64039953B4690F24F8C88B6D7673389D906BC95CEA1522F6709012652E472D16E2241775E2C197C4C7732DFD0E146BD0BB58C6AD789250B53779FE2F3C82AEC
Malicious:	false
Preview:	2021/06/10-21:41:52.386 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/10-21:41:52.389 1824 Recovering log #3.2021/06/10-21:41:52.389 1824 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):	5.202737433995103
Encrypted:	false
SSDEEP:	6:mwO+iq2PWXp+N23iKKdKyDZIFUtpDOmXZmwPDOmFkwOWXp+N23iKKdKyJLJ:Diva5Kk02FUtpJ/PD5f5KkWJ
MD5:	27411A039436CF68D66606641448E665
SHA1:	0DDE15E4F97999CB929262A6E53F57D8F776E5F5
SHA-256:	7EE4F58DCCC5C4A21A1D3425D2073018444B30CEBBCE6C7A6A17902D4383F355
SHA-512:	733A7F8EF61F8F971C4AF2CAF73ED20541ABEC7FFE57AD9939468960CAB53429E61B0BB3D8DE2D5E84590BD80ECB6A653DE445CE16E07F1F9703EF050F059E B
Malicious:	false
Preview:	2021/06/10-21:41:52.380 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/10-21:41:52.382 1824 Recovering log #3.2021/06/10-21:41:52.382 1824 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.8464827583649175
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwkETo/cLQn:TekLLOpEO5J/Kn7UUlLA
MD5:	E811F5DB926776574EAD1C04B48A94DA
SHA1:	4E99F3B77E022F7D49F0C3C38603A93539961182
SHA-256:	8663F31AAC104B67EE46DB34853843940E264FC48DF092CCC7DA94F302D3BACB
SHA-512:	A5F49C886C32ADED5475A4A84BB1FA4DD781E4539186F168B599E7EB4E4B5DA1D5326593EF84C918ED350075C17273EA256BA7BCBC19AD091141DE1CA249D0 0
Malicious:	false
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):	0.9672971041711909
Encrypted:	false
SSDEEP:	24:7cLgAZOZD/vqLbJLbXaFpEO5bNmISHn06Uwg68:78NOZvq5LLOpEO5J/Kn7Us8
MD5:	DAA923E2ECA70A6662419EAA9A1C56A6
SHA1:	58DDB855E3F4A94ECEF1E7A0D5EF91247E060A3C
SHA-256:	65EE422DCAD299D576B13F9B4EAEDF24E18CA01670C0FC2BA16A1FE8C4457FE1
SHA-512:	D426040C8B2FCBD924B899415FF81CAD2D92259C4D02ABEB13DCF11E397E4256EE6AB402B37B876AAF602EFF873522ECD8394ADAB7669DAFE2169DC8C87F7 38
Malicious:	false
Preview:	.....U..... ....

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):	2047
Entropy (8bit):	3.7192877090267222
Encrypted:	false
SSDEEP:	24:34SRRQ3lrlAKWjyHBlfj4lDHXpjI+6c+V73uAkU8rj7wl/WxHZ1/1:34W8xP8yHBl7o7XpcrLuA18ro/mb9
MD5:	E3F1DD247F60E90AB9E10E354E385397
SHA1:	14EB712CA402E0F45659845FAA4C2FB3062E7E93
SHA-256:	4A449D55A5901236553A91548108226FE10CF16586FAB54F288F68399965F759
SHA-512:	B918A5CB5E905D6043F15A91A48D68F95D66394021B012973B5D75919A360E3C6B8B441EF8822C77EABF5E8FD38987BBBB6107914DFB9618D6C0E07731614A4A
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...dd3be39e_9bc7_42e2_bce2_d252408f152b.....i.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....|.....2...file:///C:/Users/user/Desktop/Fax_Doc%2301_5.html.....h.....`.....B v.....B v.....(.....l...2...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.F.a.x._.D.o.c.%.2.3.0.1._.5...h.t.m.l.....8.....0.....8..... .....2...file:///C:/Users/user/Desktop/Fax_Doc%2301_5.html.....h.#/.....

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
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
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):	320
Entropy (8bit):	5.243925796012806
Encrypted:	false
SSDEEP:	6:mwrWwQ+q2PWXp+N23iKKdK8aPrqIFUtpDrSngZmwPDrSnQVkwOWXp+N23iKKdK8h:xva5KkL3FUtpj/P55f5KkQJ
MD5:	3B8EB4AA664CBD3267A5694C248721B6
SHA1:	E9F9717D9E30C73523590FC613EC2C04009375E9
SHA-256:	791694DCECE9755441970B93FFA5590E9F41AECF5A9EC02B41E7B6CE886BB924
SHA-512:	BFB2F7DC22F2215D0C21107EB0DE6041D80BFBAB27DE6C17BA4CC6D6A5FEB3294EF8EB9574AC2F42C94E5714BB78A594F63315D8BA83D2F71149EA3022D19E54
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Preview:	2021/06/10-21:41:49.006 18b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/10-21:41:49.007 18b8 Recovering log #3.2021/06/10-21:41:49.007 18b8 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.246500104636915
Encrypted:	false
SSDEEP:	6:mwYHL+q2PWXp+N23iKKdK8NIFUtpDYW11ZmwPDYWjLVkwOWXp+N23iKKdK8+eLJ:mL+va5KkpFUtpjX/PjjLV5f5KkqJ
MD5:	CE46F7F693376FB039E7C707C6753039
SHA1:	9B52301D595EBAF5878A5CD10BA91AAA5EB5F560
SHA-256:	282F6F533244F37EE848ECCA37832FD5FDBA511863A8999BB3D5D42B56775F57
SHA-512:	98D9FABBC330F4F40F16D83DFA31D0510402E53A3E9B102813682C6155E77BDFF3B36F91BA06F986188BBF192036F66BCC7D711CF216089D97FB9678FACE869E
Malicious:	false
Preview:	2021/06/10-21:41:51.247 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/10-21:41:51.248 189c Recovering log #3.2021/06/10-21:41:51.248 189c 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
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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.8829307511552027
Encrypted:	false
SSDEEP:	48:yBmw6fUd5XpcE0rlnw1Ok02TXUBdsxxpXpcCrN:yBC5/wsn2TkvuE2
MD5:	C99E67800E8D73A70D51BB35044A0C8F
SHA1:	6CD2C820D101950A75177E045D20F6EFF9A90C8A
SHA-256:	ACA6A289C4AB4DCFF3769A663AD03F0E1F3F1AADB1CC236625549D3855D0F1F3
SHA-512:	0ED1E482761A07B069E161B4754166C95D90B3879E7F504C069ECF3161390B20473EAB5196E55015BBE5B7B6186EED0AA145A52C696F361F412D5420D33CF99C
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7747425587319341
Encrypted:	false
SSDEEP:	24:U6yLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwc3n:U6dBmw6fU73n
MD5:	A9B5088B10E4DB93653037A1E80C63FC
SHA1:	A3241671C8BDB9EFF7F1149B16748530E5E09A22
SHA-256:	4F2D5412698D0070D08E9DF0F862E32606E8CD0EC3F0B5DD7B67CCFEE6365531
SHA-512:	919F5AAAA1AA7B7D1453BC78DC72C850B5CBD67D040259DFDE91147D59E2F5721EEF9EE1367A31DD041DB5339900994245855592 5F7EAB7542C4C02004436A2
Malicious:	false
Preview:	.....N.g[..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
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):	5.287377360771771
Encrypted:	false
SSDEEP:	6:mwO4q2PWXp+N23iKKdK25+Xqx8chI+IFUtpDOUZmwPDOPkwOWXp+N23iKKdK25+M:/va5KkTXfchI3FUtpv/PW5f5KkTXfchn
MD5:	AEB7BC83EA092AD514EEDFE2E187A75D
SHA1:	ABF1DC5FC334BB0F521639F5AC23354668254A67
SHA-256:	30F143C4A4BF070602B19A47D8F09799332B9453652424FB7245FAD63E97F278
SHA-512:	784640C7F0BC5F3B8E17CA9785517A6B124326B5687E1491A2F9C0592E778C72E824754D73D5B9FFEB0C43AD53B5E87801D5FE39AD034EB26F9D9BA287D5A900
Malicious:	false
Preview:	2021/06/10-21:41:52.369 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/10-21:41:52.371 1824 Recovering log #3.2021/06/10-21:41:52.372 1824 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):	5.22996958394787
Encrypted:	false
SSDEEP:	6:mwOHbq2PWXp+N23iKKdK25+XuoIFUtpDOvNZmwPDOv/kwOWXp+N23iKKdK25+Xu6:kbva5KkTXYFUtp+/Py5f5KkTXHJ
MD5:	B197C36E368DCC5D4776086DB7756BA7
SHA1:	79CA4B017AD2EF46A62DCC1BF77114C60B90B12C
SHA-256:	D9AD020EB73ECEDD6F568E9179D6E7D7CF9B5A0BF6F3CF48F681C58DEC839881
SHA-512:	C09AAA3C2C4D1781FF061FCCFB3CB0A21FD9AEE5C50072B70CD2B33B716DFACD0F3EB365453573FA65B1C758B66475EA756A4BD29EA1C02FE83DB9CBA46E2240
Malicious:	false
Preview:	2021/06/10-21:41:52.364 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/10-21:41:52.365 1824 Recovering log #3.2021/06/10-21:41:52.365 1824 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):	5.277855123443057
Encrypted:	false
SSDEEP:	6:mwOEMq2PWXp+N23iKKdKWT5g1IdqIFUtpDO4+ZmwPDOY/kwOWXp+N23iKKdKWT5i:Cva5Kkg5gSRFUtp6/P75f5Kkg5gS3SJ
MD5:	E8E859CD16556EBAA1DE7AFFD1AE7181
SHA1:	FFF3132E32BC0A930FCF1BAAC7731DBD858FD71C
SHA-256:	FDD93D87668C8D4E2F74A89A11FF3A7237C2CA999E6388B040EA1C9E68F1B412
SHA-512:	CF5318FE1887319604A5CAAAD9C73516A17295F0AB86039079BCFC4C5C77FCDC3193C6CFBF59B0FBD413775C5CA0A44713BB2CC8C01A2F535F6530CBEA26741
Malicious:	false
Preview:	2021/06/10-21:41:52.357 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/10-21:41:52.358 1824 Recovering log #3.2021/06/10-21:41:52.359 1824 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:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Encrypted:	false
SSDEEP:	3:8EflHal:8ll
MD5:	34AA59E6A098E40AC4781109DF1BCFB9
SHA1:	0E89336A4B97CDFC45DBAE6F9BEAEC6F889A7B0A
SHA-256:	4836E355CD49094B1AB07ABB4390CC2346ADADE4C3108FC75E410F5D61C972C2
SHA-512:	8DDB288018E2E1FB25CE029E5B6B81799F80FADCE07F74FCFABC8BF6C4B7FEDD1A395B5A94248E8E7F01E18019E0D90C650D676D2BA486B35129B8761E0FC46
Malicious:	false
Preview:	.'..(.....j.#/.....

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):	0.44395832270093155
Encrypted:	false
SSDEEP:	24:TLxC7p35XpjILL+HmHSJ0UArv7mW1RlN5SayqAXpjIJBuDz:TO7Xpcu9hAj7t1RYnXpcJBy
MD5:	1BF39E01443CCF954A9A4763E59BC7BE
SHA1:	6FB3004721B6C57B4C44E0F08D126D23D9B7EA1E
SHA-256:	0AFB84E2FBE31B21EC4CC237A0CC94BDA02A94400C615112DEC79BCA34CBDB06
SHA-512:	F3FA96E2EE6ECFA892DDF58BC86BE7FC2961ACE0DA4DB4CE3D2A4F49801DE08282DF3B55230F959794C90A888F3964D61888241858ACC9B19BD4908B3293B17
Malicious:	false
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):	584
Entropy (8bit):	5.116932773318731
Encrypted:	false
SSDEEP:	12:h3mI9nBKh/nUthW6p9rA8on/BO6Kd33Bk778B/xgskZBa9sdnuYkJB4dk5PI:hRt/1pOJO6Kd3xY78BJgskfa9inuYkJk
MD5:	F99ED075AA48A23368AEE5E544D51858
SHA1:	9354A71D69DED16EDD0880CB6D81B88D51026499
SHA-256:	F859AC9ACE3EFCD0D395C28908AFAFECF6521E24F0E6E99D5F783ADF32C9279E
SHA-512:	FD6B652B1B62040F4A1C142CFAB53D147A0A49C2E605806751B615989EFF50893145E8B01ED55EE2FDF76FB785F1CDEBE5B7083563001ACFE5A3186BF384A067
Malicious:	false
Preview:	....."9....01..5..c..desktop..doc..fax..file..user..html..users*a.....01.....5.....c.....desktop.....doc.....fax.....file.....user.....html.....users..2.....0.....1.....5.....a.....c.....d.....e.....f.....h.....i.....k.....l.....m.....o.....p.....r.....s.....t.....u.....x.....z...\..... .....BZ...V..... .....*2file:///C:/Users/user/Desktop/Fax_Doc%2301_5.html2.:.....J.....#*,

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):	0.11619645219658946
Encrypted:	false
SSDEEP:	12:ED0X2BqLBj/d3laf4nMWQA9LTBQZ8fO9H:GqLBd39bNTTfmH
MD5:	27CB553643468D27AC812408BB8B58F9
SHA1:	BA537669AB1E5EDC5378576A8FB7527029181ED3
SHA-256:	3334B3AE2F1083E80532E27473C95199D774F6C15744E63FB76DBFA619694487
SHA-512:	D1FF36D1BAA6FCFAF21C6556F00D814756E41853CE25AB278CA97ACE1D359F9ABC5D5010027E0FBD7E8A3AF815BD9D12707C5DFAF7893DEF323AFF28AA69B2D2
Malicious:	false
Preview:	.....Vr..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2954
Entropy (8bit):	5.4712693500255964
Encrypted:	false
SSDEEP:	48:q7GWFa75Mc8dbTl1ubQSefgGvNrS0U9RdiN9hu:Ca75MvdbTl1ubQ5fgGVrS0Pu
MD5:	82DE61079F4A99331F30C7E3B392B50F
SHA1:	610B1C32EFFB521AE8E3022841FAB0E3BCE6DC44
SHA-256:	D7A3337558643E1C5D6222B7A1DD31A4EB81D4FFC5E9F4EE7D463F3F6FD0DA18
SHA-512:	0B8F76C324B2C515CF0DBB7BF592AAD80B0803E23B807B611AA5A7F0750DA210E1DC0A44CE57F407BE59239E4CBC2EDE26E3D33906C589DF2090E50AB39F74C3
Malicious:	false
Preview:	FjU...*.....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..84020000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-10 21:41:58.32][INFO][mr.Init] MR instance ID: cfa3bb4b-147a-4938-ad21-f4d854522732\n","[2021-06-10 21:41:58.32][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-10 21:41:58.32][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-10 21:41:58.32][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-10 21:41:58.32][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-10 21:41:58.32][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-10 21:41:58.32][INFO][mr.CloudProvider] I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.231254512393577
Encrypted:	false
SSDEEP:	6:mwJq2PWXp+N23iKKdK8a2jMGIFUtpD2ZmwPDxFkwOWXp+N23iKKdK8a2jMmLJ:Vva5Kk8EFUtpi/PdF5f5Kk8bJ
MD5:	DFDCDD44977788F2FA30CDDF5A2CBCF8
SHA1:	2DEA1BFFE079596224DE9C6FBAA2B4DE2069985D
SHA-256:	8DFCB6BF35A3B7CB84809263F075CA79D84BA51E17FFB622CEB9E1EC132FFDF0
SHA-512:	10D5BB73DCFD0226F3F5E59D3D0D1DF3320B008FCC61BA4A29285586C9B6BAB74FDB7911694471A8765A872BE12AD5D4D0A68E36907811D4B642A444452BA97
Malicious:	false
Preview:	2021/06/10-21:41:48.794 1894 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:41:48.796 1894 Recovering log #3.2021/06/10-21:41:48.797 1894 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2685785902261335
Encrypted:	false
SSDEEP:	6:mwPQ+q2PWXp+N23iKKdKgXz4rRIFUtpD79SgZmwPDhQVkwOWXp+N23iKKdKgXz4n:Jva5KkgXiuFUtp/Z/Pu5f5KkgX2J
MD5:	F1F398F05F732D4B5A9E46BF0B516B9E
SHA1:	3532E1643FAC1BFAFC85A7805EE1D2A2F27370CE
SHA-256:	E3A616FEA43FFE0CB0354271FB7166337E73648DBD265D121C2D5C86A4AE43F5
SHA-512:	97EFDC73E7B63A2A2C752DA9E72B6FE5B5C171282B67530C0854D22BC4F2081ED71FFF6D30736D2E46B8941ED0109A69B0227A058DCA28EF90DF80E708F9E88
Malicious:	false
Preview:	2021/06/10-21:41:49.037 18b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/10-21:41:49.038 18b8 Recovering log #3.2021/06/10-21:41:49.039 18b8 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):	20480
Entropy (8bit):	1.0105841952787697
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAon:wIElwQF8mpcSJ2Yf1
MD5:	0124155AA8DF263D664BDFFA0B5BC9EF
SHA1:	04374E4C1067C9FDC367B77A268AD32D7BF15C7C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA-256:	85F973F0EF195884CE31EC141A3D9EF35FE98DEBED99C89FC67A4E62F4FB6DCA
SHA-512:	CB9A7F5D303A0BA20A6AE994C892FDE26C9350E4A81887BF2D93783B921A50ADB54C4E1B7EA267C5FB107FD2BE39C9B60B5F2D78DC1CA9213DDA52BF7FE1C251
Malicious:	false
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):	21044
Entropy (8bit):	0.8259510821036131
Encrypted:	false
SSDEEP:	48:bwqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUm6:bwhIElwQF8mpcSX
MD5:	8F9D4860A6452092B4C3EF3FA5E10240
SHA1:	E115A68C7F9705C0A3998EB288C4AF909C425C06
SHA-256:	4196884DA12476E10FBFAD057E8EDDC257EE98201DB8AA55219C4EF0ECE1B3C9
SHA-512:	4DD576BFC16019979671B429E5DCB62885C7553FDE59D4B82E02D412791DB5A167260D11FCD4B22897D9CE0C6E44E877622A503243440FF3F15B12CE1F5503F4
Malicious:	false
Preview:	.....6.....

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:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.207202761004707
Encrypted:	false
SSDEEP:	6:mwQQ+q2PWXp+N23iKKdKrQMxIFUtpD4SgZmwPD4SQVkwOWXp+N23iKKdKrQMFLJ:8va5KkCFUtp0X/P0F5f5KktJ
MD5:	7E486CF7A133E18F49AA37FBBB9F82BD
SHA1:	445DFEC377BE18BE962EB9CDC61E0179C09E544D
SHA-256:	E40FFF1D745E4B1671CD2754CB66E477946AF7BC31F67EA38FBAF209AD1DA51D
SHA-512:	528DF119C279C49177B27CD404D8C2C63A29E2F79826964855A183FB2C4F63612DD29339D40275AF41A423309873B4792921428D04ABFA3D59DA0DFFFFBC0F37
Malicious:	false
Preview:	2021/06/10-21:41:48.923 18b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/10-21:41:48.924 18b8 Recovering log #3.2021/06/10-21:41:48.924 18b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Size (bytes):	348
Entropy (8bit):	5.1631180567321975
Encrypted:	false
SSDEEP:	6:mwQo9+q2PWXp+N23iKKdK7Uh2ghZIFUtpDWJZmwPDj9VkwOWXp+N23iKKdK7Uh2w:B9+va5KkIhHh2FUtpaJ/PX9V5f5KkIh9
MD5:	39FC85387B3C23B004B66D2A1D2238C8
SHA1:	714317B4E8DE7D36F365251523BD7CAC77C77C0B
SHA-256:	13FFE363258603FC3C65759ED5D79DFB0B85032869AF3DDB617DF5777EE091F4
SHA-512:	F6264E7D898D8D4D580D6C72824DE847EF580D567209B96B9EE5F4AC33C03180724A637402A5442A838787613DAA000744095A9609F11D6478B06EE243E2DC71
Malicious:	false
Preview:	2021/06/10-21:41:48.720 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/06/10-21:41:48.721 184c Recovering log #3.2021/06/10-21:41:48.722 184c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.265615628080055
Encrypted:	false
SSDEEP:	6:mwEnSQ+q2PWXp+N23iKKdKusNpV/2jMGIFUtpDogZmwPDSFudSQVkwOWXp+N23i3:AnOva5KkFFUtpF/PeFe5f5KkOJ
MD5:	8A27D7897EB3EF9F57DA431B50355106
SHA1:	02FE4C1EADBD14C1E347409DCE86A9DB81D12C9A
SHA-256:	16C5E949E0A5CD497A6720E5744D42639FA484D8C87C2DCA90842993D72E64B3
SHA-512:	20E11A9FE997574450A75A2C14E47F63AA1827AA7D98C73685012546611B94482FB07D2D3E9AECC99BBC75B50F6C44DFC60948895C1EF1FB7A96590A3ECBEAB A
Malicious:	false
Preview:	2021/06/10-21:41:48.988 18b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:41:48.989 18b8 Recovering log #3.2021/06/10-21:41:48.990 18b8 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2897197024883305
Encrypted:	false
SSDEEP:	6:mw7cyq2PWXp+N23iKKdKusNpqz4rRIFUtpDvMI1ZmwPDvUpjRkwOWXp+N23iKKdA:Pcyva5KkmiuFUtp//PQpjR5f5Kkm2J
MD5:	0CFFCF9424F0FE76E8A1EC759B7C873B
SHA1:	3242AC69FD16F15551DFD4D6A2F73C0ED70D0278
SHA-256:	531DEFB359DE858E41CF735E45FB0DFE88EF09BA1C279E3261798DB9BEE922A9
SHA-512:	B1CA27110B4BC7F7A243B85BABBB779B6A61F87306A646F8686A2240006184BE56BC975C35C151FB5F79C11D8363F093971597DE69F9E3F8BB9196AFC617FA81
Malicious:	false
Preview:	2021/06/10-21:41:49.038 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/06/10-21:41:49.040 1850 Recovering log #3.2021/06/10-21:41:49.041 1850 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
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.276314739120851
Encrypted:	false
SSDEEP:	6:mwGidv+q2PWXp+N23iKKdKusNpZQMxIFUtpDGiWFEQZmwPDGiWFEAVkwOWXp+N2R:KO2va5KkMFUtp6F/P6X5f5KkTJ
MD5:	5223AD2F76928F647008B75D79954A00
SHA1:	764AE64C1DB88ECBA3093A867F6B8B5DD401201B
SHA-256:	3CE933CB9E67ECEF2A29F6BAB49FE403306E2864AA891E8FF28612BEFEF4FCA9
SHA-512:	AFB0A6E1EA149390C17323C9E140599AE9EAF34DC05C6DDCFC19BE4D4619562D3D9FF376E1D609F31C8E3419B3EB1468B6AFAD683387AE8C8080D26D32E1055
Malicious:	false
Preview:	2021/06/10-21:42:05.379 18a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/06/10-21:42:05.381 18a8 Recovering log #3.2021/06/10-21:42:05.381 18a8 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\b9227181-1a84-46fd-9bd9-5855d3519a29.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
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\nmmhkkegccagdldgiimedpiccmgmieda\def\650fd7f0-0481-4e99-bacf-87408dcaf3e0.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\650fd7f0-0481-4e99-bacf-87408dcaf3e0.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
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):	5.225526409350957
Encrypted:	false
SSDEEP:	6:mwcCwQ+q2PWXp+N23iKKdKkGckArV/2jMGIFUtpDcjgZmwPDcdQVkwOWXp+N23ik:Qva5KkkGHArBFUtpd/PF5f5KkkGHAryJ
MD5:	B4976B1846C648974983EECB889E5B45
SHA1:	2885238D4A15C7323FE63A0D74C61586AD12A34B
SHA-256:	4DBA992A2F1B0C96215CFD8768760434DB513F3CF39754B26E17ACEFDC004AD7
SHA-512:	19CE946F872FBAB24729CC7F22D57B81475A96E1D7EE4469E685CDB70F140F726428C3A79CA7E591B551867E992D828583E14CC5D3E17A76D48B6BC10F25362
Malicious:	false
Preview:	2021/06/10-21:41:55.305 18b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:41:55.309 18b8 Recovering log #3.2021/06/10-21:41:55.310 18b8 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):	432
Entropy (8bit):	5.219139037903551
Encrypted:	false
SSDEEP:	12:nva5KkkGHArqiuFUtp/vX/PS5f5KkkGHArq2J:va5KkkGgCgR8f5KkkGg7
MD5:	FC4CD790ECE55A64B489D948461102D8
SHA1:	4499558F5A8A1765210A4B97E97F2A5F6F2AE577
SHA-256:	2218B4C0F61095C928AE94E414A7C7BCE7CBAFBFA1757ACA1D128D3A7A1A6A40
SHA-512:	0E93116AB6B74766F7FAD0346A34ADD703892191ACF477E9069FEEF0BCE9EF59C76CC888CDB7860CA77BDACE7938ACAF2142794EE9926726CA44D37001E0588
Malicious:	false
Preview:	2021/06/10-21:41:55.310 18a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/06/10-21:41:55.313 18a8 Recovering log #3.2021/06/10-21:41:55.314 18a8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
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):	418
Entropy (8bit):	5.1929375605061185
Encrypted:	false
SSDEEP:	6:mwlE+q2PWXp+N23iKKdKkGckArZQMxIFUtpDlzG5ZmwPDlzGtVkwOWXp+N23iKKB:vva5KkkGHArAFUtpY/PA5f5KkkGHArfJ
MD5:	36B6A651B36BDC5BD5A98B63C1D7E4A5
SHA1:	0D977AC88E629ABE5F8799BD59D75B198CB9DC04
SHA-256:	204D678D70DD332135670191C03B36AFE3FAAA41F5F6CA73327F644EDA4CB2AC
SHA-512:	525074D0E8FDC5DBE561CD767AF7E15294276E5A4DBB81EA11CC39208F8A2CDB7B000A47283251A3E9BC9D6CDC9BD5C1819C386D0873139C2EA4482EFB485E
Malicious:	false
Preview:	2021/06/10-21:42:10.585 18a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/06/10-21:42:10.587 18a8 Recovering log #3.2021/06/10-21:42:10.587 18a8 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
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):	5.238899476884293
Encrypted:	false
SSDEEP:	6:mwlUl4q2PWXp+N23iKKdKpIFUtpDDlJZmwPD0UQ+vDkwOWXp+N23iKKdKa/WLJ:C4va5KkmFUtp3lJ/PVvD5f5KkaUJ
MD5:	67768CB88A0E983BD12254707825C3D6
SHA1:	E598E146F03F879CAF62BE8D336E1375B5CBC734
SHA-256:	F758FC66AD99E7781847DC59250DA760FC1B1EC761C99509FACBB84D927867A2
SHA-512:	97E05F61C9674E68D1FA395F5702581252C2DF6F37684A51AE6027732DB05EDBCF76C5D74FC4B30347906D1FD7255A076536F1855DB988005C874F527CD2A180
Malicious:	false
Preview:	2021/06/10-21:41:48.762 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/10-21:41:48.767 1820 Recovering log #3.2021/06/10-21:41:48.815 1820 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Entropy (8bit):	5.336649967656384
Encrypted:	false
SSDEEP:	6:mwkEeyq2PWXp+N23iKKdKks8Y5JKKhdIFUtpDk+1ZmwPDkfjRkwOWXp+N23iKKde:myva5KkkOrsFUtp5/PKjR5f5KkkOrzJ
MD5:	5A9FD686D0F48ED3E2127F4075024AEB
SHA1:	C520C51280A8AE02EC154FC20885EF472E600AB7
SHA-256:	1342953B4C84238080DDC3F8BFFE67C7106699942BD6DC06484AD4BDCA2DBCE1
SHA-512:	ED0E3727164DF475D08B44E099A1DD057A38D7CAFB08D91284AA0A5BC6FC2DFDAB102AEC4F902CA9D90CCC02630ECBA051E013CE20ECB90BB836E2099AFB 099
Malicious:	false
Preview:	2021/06/10-21:41:58.328 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/06/10-21:41:58.332 1850 Recovering log #3.2021/06/10-21:41:58.333 1850 Reusing old log C:\Users\user\AppData\Local\G oogle\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.541093410391278
Encrypted:	false
SSDEEP:	3:qpOCVlGl9jl5i8V/ZK5:SOCPGlplfVxK5
MD5:	122031A250136A8B181ED4D112D78816
SHA1:	5713E5E4D61B59D76AC97A943DDC874588D2F77E
SHA-256:	CDC15DE426F300724BB34D26CC018285C33BD255ECD480C6BAAC4B7E9BDA1F18
SHA-512:	F1C8DEA4BC6E79378EB2B90A26927B76424CA8D949A554BF7154A0EA2C23FC557EA7EE6432D4643B00C17B3509BCA8D521D47693830DF092D5CC5CB1E426F3 6
Malicious:	false
Preview:	.....0'9.....n#S.Ci.....TG..J.^.....f..M...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b3316109-df59-433c-b3d0-81ed1dc0d086.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf6e68f9-9726-4c14-84fc-916f297f48ed.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1207
Entropy (8bit):	5.584543086669919
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvKn7wUtRZ4wUgRUenHQ:YI6UUhVseKUewqPeUer2UefK7wUtRSw2
MD5:	66450F6D8566E90B68F18DF32ED95BAC
SHA1:	34DBDD70F1ECCDCA6EDE988190B8B3F420B0173C
SHA-256:	1A57DDE4655BEF61276FE464BAC587230B2A5BB14DF710AADBADF87E8DA645A8
SHA-512:	89AD6B85C9D4169E18E680E7ABFFA6EFAEBADEBBDDC77B1064BF7DF59F598B16064834A9073BBD2A9BA555122AC1F0DF91018165BBEEF1E8016CFEF3E9A10 ADC
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf6e68f9-9726-4c14-84fc-916f297f48ed.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1654922513.640411,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623386513.640415},{"expiry":1654922518.585708,"host":"+LCYPikJxOjeTMeNwsPDpkFmxWXugWYr8RjEVTinl5c=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd23bce1-2ecc-424b-912b-88ae58e0b5ca.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535743622213004
Encrypted:	false
SSDEEP:	384:WQx1tKLlnSX71kXqKf/pUZNCgVLH2HfDhrUGHGenTH+kq4E:v6LlA71kXqKf/pUZNCgVLH2HftrUmGec
MD5:	AFEB67C0BC4E0E112F2F179D909BC15A
SHA1:	AECDF4E12462A302DEB7AB00D4EDBDD253E06323
SHA-256:	2C2EFF0D8D01ABCEA6D37F92FC29152A2E657DF9627FA8BA09322432FF73ABDB
SHA-512:	4BD4B56524F8D52231A6E0B2752DF37A4BEC84F9191A9462274E2AB6C13F63FC1DE8D67A49BB7CA0CC831B75029C715012EEB9465CEBFD986D5A8E3DA59576 7
Malicious:	false
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":"13267860108735169","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
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):	4.371640041863937
Encrypted:	false
SSDEEP:	3:tUKUUiGgVFuFzKTyZmwv3GUiGjXdY7V8sGUiGjXcYl7WGv:mwMVFuXZmwPDFY7VvD77tv
MD5:	ADC641C0EE5C9015E8338A8648B1044F
SHA1:	89DAB8716293BAC4369FC86C60514E374A0509B1
SHA-256:	912E59CB8507E9E6F52DC49F90A61D5304555AC670447511EF6BAD4E51AF90F0
SHA-512:	13A761B32EAEB3B4DAA0571B80DCFC8BDB58F48745990C3EC7EF0829DFE03FDAAF8FA8259D24580BE9EDA2E8AC97FA2B44C6EA5A7ED734489E4C5E94A7061 CDC
Malicious:	false
Preview:	2021/06/10-21:41:52.182 1824 Recovering log #3.2021/06/10-21:41:52.228 1824 Delete type=0 #3.2021/06/10-21:41:52.229 1824 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
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
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dbbe9b01-fd8d-4fc4-b430-a1ab5a5e0eda.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):	5681
Entropy (8bit):	5.171685996769014
Encrypted:	false
SSDEEP:	96:ndChd12RlN2RdmNcVUXok0JCVRWL8tbOTQVuwn:ndC12RukcmS4VYi
MD5:	DB89079E363121187CC0A8F8EFBC4AD4
SHA1:	7F3DB974E3B2D9B60439A267D83C871BDBFCD749
SHA-256:	2AA8EB96EF70C8C46ED137A0FDCF3EE71A6D9A3C30971348A8FB2CF9F658D2A8
SHA-512:	1657B6EBAE46FFF2F86A52B12C4E2592648E3E672FA928F697804B3CFACD7A06D5026CB202D5347204FD1A6E337106E79B6D9B2B08C2FB4E5917FE15D866E932
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267860109001298","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.243350656058027
Encrypted:	false
SSDEEP:	6:mwOqyq2PWXp+N23iKKdKfrzAdIFUtpDOGA11ZmwPDOURkwOWXp+N23iKKdKfrzId:Nyva5Kk9FUtpBAX/P3R5f5Kk2J
MD5:	A63DFD168A92D3F11855E85CEBC7F70C
SHA1:	2A47A189A3B965E76EFA992FB3EADEDE898ACEE0
SHA-256:	583DB47DC423A8486340E3F3D25EB1EC2C0FD86A4B7A5B627009379CCE1E048C
SHA-512:	CEE1E0641583F95D552F6065639EE9D838A46AFCD9BBD31D1BCDFA4F44554ECD9FE9C9BE2EDEAF49668070867D2FCB94A02A9A6905510AA619DB44EF95ED57 1D
Malicious:	false
Preview:	2021/06/10-21:41:52.396 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/06/10-21:41:52.397 1850 Recovering log #3.2021/06/10-21:41:52.398 1850 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EfljP1/:869
MD5:	91110ADEF3DC1FAB5217295A8A5CF267
SHA1:	C94DBDEB1FE27F877C3C4747C67B7BBDE47F5040
SHA-256:	1FCBA94ED6DC351B3BC9E9AE7C3AE1AB417A5FA1C5B7F2E7FE274D115C5BE064
SHA-512:	5C73C09EDAAFA54F82C4EB22DEC356CBE086AEE3CA1476BAC41076925C36987A1B9719A8F9CDB269725045256545596D552A1336C34638DDFD73D4DA29B30D D
Malicious:	false
Preview:	.'..(.....j.#/ .....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5856_223913239\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197616
Entropy (8bit):	4.955722655128328
Encrypted:	false
SSDEEP:	3072:98Lqy5tdVRpn0eYzR089VDeWLQva3jUmykfftq/3fHn13M+Ya9tKd57s7J4zpd:aLqy5jV70eYzVDYvU0Hnq9
MD5:	715067CF2947DFA3FDABA45D010912D3
SHA1:	71D4506F6DD1BD109F7DA1ECEF70D05BF95CB544
SHA-256:	0F58B5D6F89BFFE34A44803F70AEFD5A435ABD692FDD00D3B1C88575933BA752
SHA-512:	A9216F2839E9F86B4A83770E5E6D9706E788D9ED8EC831CBF51C5F73EC38E03FD96C513601B8A29848B3610D55320DCB44C97F03840657D5E2A50C9EF1CC8C4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5856_223913239\Ruleset Data	
Preview:	.....(.....Q.....p.....P.....,..... .....geips.....K..8.....lgoog.....(D..P.....ozama.....4...h.....onwod.....{..... ..g.bat.....p.....uotpo.....ennab.....q.....nozam.....@T.....<R.....h...L...0.....|.....t...p.....h...d...`...\...\...|...`...P...@...$.....<...8.. .4...0.....(..... .....`...D.....p...T.....(.....\|...x...t...p...l...h...d...`..\...X...T.....L...H...D...@.....8..... 0...,...l...$... .....@..... .....X.....4.....x...t...p.....h.....l...P...X...T...P...L...H...D...@...<...8... 4...0...,...(...$... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\abe62296-f567-4a49-9c16-21e416115c65.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.752110270349871
Encrypted:	false
SSDEEP:	384:TjIHP1K455eLaNjr4v/V3QvJIHRkGUTre5P3xIp1Nkr+zm+p6l7vboOJZnNG1zK0:Y6V1aVQQke7TtxknLOlKrFfhi
MD5:	B15DB14BF4A6518415E54243033E6AF8
SHA1:	B3D02B847E0CE2C5FE400A1A273318400D7393D9
SHA-256:	181EA8988EF607BFE87B25A2F9185CDA2F6FB1E2C10EB241E99BD6F8DA3FBE58
SHA-512:	DCBB33BE8873F64A0BDBC2F88A0D2DC7C16A59A41C824CC0E2518CE1D85A7ED7933AB711D9CA77B65981CCB2B11E811D0F70D4130B6DB98CB75E9322BE6F9 02B
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\c853de00-ac69-4b33-a411-36417f1019a7.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):	164225
Entropy (8bit):	6.050826343253924
Encrypted:	false
SSDEEP:	3072:SR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:gIAsZ8qxKaqfIlUOoSiuRY
MD5:	95D30C81F5FB4E95C96177B280917E5F
SHA1:	41B1021C2D092C05D23D4BEF2A52564557D0DDBF
SHA-256:	1CEBFFAB82AB715346A61D81BBA06AEBD8A907444F48072B38CBC40F68538270
SHA-512:	51F626AB91E2E5DB7D686CFE38704CE5B7DCF32D926E45123DC170ECA6BFB52A8E59DDF78BA6F52D1711CAC27651A3C210C2E6A00E2DE7F60CE2BDE2C99A3 D87
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\cad277d8-3786-415c-8d45-611d350a228d.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):	164225
Entropy (8bit):	6.050826343253924
Encrypted:	false
SSDEEP:	3072:SR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:gIAsZ8qxKaqfIlUOoSiuRY
MD5:	95D30C81F5FB4E95C96177B280917E5F
SHA1:	41B1021C2D092C05D23D4BEF2A52564557D0DDBF
SHA-256:	1CEBFFAB82AB715346A61D81BBA06AEBD8A907444F48072B38CBC40F68538270
SHA-512:	51F626AB91E2E5DB7D686CFE38704CE5B7DCF32D926E45123DC170ECA6BFB52A8E59DDF78BA6F52D1711CAC27651A3C210C2E6A00E2DE7F60CE2BDE2C99A3 D87
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\cad277d8-3786-415c-8d45-611d350a228d.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\cf1198c0-767c-4e53-b004-1af435a61afa.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):	164329
Entropy (8bit):	6.051129524500773
Encrypted:	false
SSDEEP:	3072:SR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:gIAsZ8qxKaqfIlUOoSiuRY
MD5:	658F63E25BF562D7DD6F4E580F6A1B8E
SHA1:	AEE52F38E514746E21938CC7B1F565D5F2622437
SHA-256:	24BBB739F669F2E06F9711892CFE883959AEBC0A5AA5F6ACD9DD15583C31BAE3
SHA-512:	9A029ED738AB17F700FACDF55C7BF0A331F034A0A8A29EC5957F7BF10E1B4624EF7FD52BFEF559BF66F2829DD8CABF32DBD98E66EC280C56A297ACAD44D5AB8
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\cf4b256a-6c42-4b0a-8d18-fa6f23d2fce2.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):	164141
Entropy (8bit):	6.050668144292564
Encrypted:	false
SSDEEP:	3072:6R4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:oIAsZ8qxKaqfIlUOoSiuRY
MD5:	155C1A28C5657294606B980DCBB5A22D
SHA1:	F4ED04FD56489A741F93A09BD3B4C153FF544CC3
SHA-256:	06BDEFE6A23CE8A10D59300C5B3E18C6CF1C58583640750F35D40517B83EEFEB
SHA-512:	FD998362BCDC918273CDC9329A2514738521741B9C789A60842750ED1F15C049D145343588B7AC48D6E6046B0A1A8F0357D1C4E392D06EEE7037E3F287653479
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\dff1d77f-f6c8-4999-874e-5eb498ef3320.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):	163898
Entropy (8bit):	6.049953376520487
Encrypted:	false
SSDEEP:	3072:rR4ryDswL0T4qxb8IHqzEYFcbXafIB0u1GOJmA3iuRY:tIAsZ8qxKaqfIlUOoSiuRY
MD5:	3B0AAED25D4208AADF8BF92B4EBC1683
SHA1:	9A549DB885FDADA0238154742F065B4B4187FAAA
SHA-256:	358076879DF9D876FD00BABA1335351D133339B5C6A7F8FB32F9AD9BD62C9BEC
SHA-512:	51465FB8B69723D7B0A9D3F0E280D402ACDB07DE2A8DA57C3FD064A9886B3E455F1412E170D9B2E0E4983B34F3D30CCF15C87F59003471702E9C3FE54EC44F6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\dff1d77f-f6c8-4999-874e-5eb498ef3320.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016854670"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\e320b62b-0ac2-476a-baa6-3baf62f3d97b.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):	163984
Entropy (8bit):	6.050121611089966
Encrypted:	false
SSDEEP:	3072:JR4ryDswL0T4qxb8lHqzEYFcbXafIB0u1GOJmA3iuRY:TIAsZ8qxKaqfIlUOoSiuRY
MD5:	9BA2225D9CE919392D78F68CADF46BA1
SHA1:	FCCCB9AB7BB6E1458D6B7E92F5FDFD34D75569C7
SHA-256:	40D2BA8973D25A2E84D4A2FC74A189996F415B0F1965D4E287193806589843D7
SHA-512:	C4521A5D213E1E83A0345E2B78C516DAF389809F7EA65C9C7E5465C8F759187FF55ADD2A72F024AE51EB8E9BB5BAFE1A73AD36182798EC636F7A09CB2EB244EB
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62338651194934e+12,"network":1.623354114e+12,"ticks":95932953.0,"uncertainty":4808910.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016854670"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Temp\20b9c054-fed5-4faa-9b7a-33a2bfda6250.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
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\5856_1129837605\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):	3.9301659996057974
Encrypted:	false
SSDEEP:	3:SXlpS0VHAgzlURX/PVdAwtL:Si0G5X
MD5:	FF0CBA325E01ED1EAE9021FBC02D3362
SHA1:	ADD06DA6B8FF5D8234EE155166C7498A5CFF8977
SHA-256:	CBD1231298B252479D8A63155A8FC0CFBC94AC5E8F74D93C683BC182CA3EA245
SHA-512:	7420B818C45FE804ABA451687DADCFD18A80FCF43F5D783D0BCEFC77191C716374B5F4F7989469FF0BEAC422DA75FC534E71ECD8BFC38EF51ABAD42913C3A956
Malicious:	false
Preview:	1.2731bdeddb1470bf2f7ae9c585e7315be52a8ce98b8af698ece8e500426e378a

C:\Users\user\AppData\Local\Temp\5856_1796723235\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\5856_1796723235\manifest.fingerprint	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\5856_219756736\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):	3.897958469013786
Encrypted:	false
SSDEEP:	3:SVI4cFEHcXaEctMEVU7mdWTiRURn:SW48faMEVNKiRUR
MD5:	CD4B8C74A26F0A5D79AE1DF69F5197CE
SHA1:	9ECDA08487EB08B86E34D01956C8AFD51CD8EFDE
SHA-256:	8993F0A08C4038DFCB67362FB2BD32C259C46B33E9C3C46EADEEA9A6D7F023D6
SHA-512:	78BB3933DBBEA00A9DCCC3AC7FA893385045BC2F29E430ED24B9A36D0F33F59A3D2D67347733330FD485ECA713207E6E11A98267BC31C324A580DBC3942D24 A
Malicious:	false
Preview:	1.0db3813e964bb90b71997b663a9ffdf104128283a14ceb25e98364a5a16143db

C:\Users\user\AppData\Local\Temp\5856_493172788\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8417538334903507
Encrypted:	false
SSDEEP:	3:SRkGDEzGKb2dGMAz5Bi6QPEA1:SSUVKb2EMcXA
MD5:	C5EB6E81FF20793640FF1368767FE2E4
SHA1:	3838AB9769B8EA3F6F3241504099F6FB2591173C
SHA-256:	DB81C2532D8152C4606833C06B818B1C94FBDB0FBF98F0E89365AD4E7A093529
SHA-512:	3AE2FF526D5908E1B3F4AA5FDBBDF0D0859520CAFFCBF84BFA7D6DC31293CD08243B418533A526015BCF3F1A85E08CEBAB55ADE500D66F962EC8A19D3DA84 CD2
Malicious:	false
Preview:	1.4302cf764844fc6ca4cd4de8cf5e13481c4dd15b4bd8d667869f9ae2fb54f9bd

C:\Users\user\AppData\Local\Temp\65cc7ed4-2c1c-4378-8b92-7aa1e5834ec1.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
Preview:	.

C:\Users\user\AppData\Local\Temp\9061cc46-8dce-450a-ba9b-273cbb497b05.tmp

C:\Users\user\AppData\Local\Temp\9061cc46-8dce-450a-ba9b-273cbb497b05.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\c36e5fdc-b716-4885-8177-214453b337fc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\20b9c054-fed5-4faa-9b7a-33a2bfda6250.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
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.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_dir5856_1441600412\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\am\messages.json	
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "pl aceholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA 2
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4 C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": ".... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\de\messages.json	
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "1428448869078126731": {.. "message": "......... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE

C:\Users\user\AppData\Local\Temp\scoped_dir5856_1441600412\CRX_INSTALL_locales\es\messages.json	
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "121395798272387592O": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	4.984352448489721
TrID:	
File name:	Fax_Doc#01_5.html
File size:	147
MD5:	0e73957b74aa54a969a21c7ab6710515
SHA1:	c1456fda553cd4023654729634a60816ed52212a
SHA256:	ecc2656e7f58af1c48ebc553c0f648d4981c7757454657113f4c812958de0588
SHA512:	8a28a4cd1be5f6635db60bbb2b903bf3e15aafa97a8051af94b562a7e89bbd3cfc63e27c3c1b4e3dc84792d57aab19a2839db12ede3e7bb3be87c967571420a8
SSDEEP:	3:gnkAqRAdrygovHcIIRVJbkADFoCDRzIa0NIBRTsCQUcLd/epm3vIIb:7AqJH5IRjYmm6Ia0m1sxWIb
File Content Preview:	<script type="text/JavaScript">..setTimeout("location.href = 'https://quantlab.sutherlandresearch.com/cgdin/v4/cali@nm-realty.com';",0);..</script>

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:41:53.673746109 CEST	192.168.2.3	8.8.8.8	0xcf68	Standard query (0)	quantlab.sutherlandresearch.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:55.208950043 CEST	192.168.2.3	8.8.8.8	0x2318	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:57.187309980 CEST	192.168.2.3	8.8.8.8	0x5cf2	Standard query (0)	etrafficsolution.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:58.884813070 CEST	192.168.2.3	8.8.8.8	0x96ed	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:42:01.434111118 CEST	192.168.2.3	8.8.8.8	0xb22d	Standard query (0)	etrafficsolution.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:42:01.536361933 CEST	192.168.2.3	8.8.8.8	0x476c	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:41:53.855609894 CEST	8.8.8.8	192.168.2.3	0xcf68	No error (0)	quantlab.sutherlandresearch.com		197.242.146.206	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:55.280437946 CEST	8.8.8.8	192.168.2.3	0x2318	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:41:55.280437946 CEST	8.8.8.8	192.168.2.3	0x2318	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:57.370431900 CEST	8.8.8.8	192.168.2.3	0x5cf2	No error (0)	etrafficsolution.com		162.241.7.171	A (IP address)	IN (0x0001)
Jun 10, 2021 21:41:58.945364952 CEST	8.8.8.8	192.168.2.3	0x96ed	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:42:01.493155003 CEST	8.8.8.8	192.168.2.3	0xb22d	No error (0)	etrafficsolution.com		162.241.7.171	A (IP address)	IN (0x0001)
Jun 10, 2021 21:42:01.599734068 CEST	8.8.8.8	192.168.2.3	0x476c	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:42:01.819860935 CEST	162.241.7.171	443	192.168.2.3	49748	CN=etrafficsolution.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed May 19 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Aug 18 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:42:01.873261929 CEST	162.241.7.171	443	192.168.2.3	49749	CN=etrafficsolution.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed May 19 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Aug 18 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5856 Parent PID: 4884

General

Start time:	21:41:47
Start date:	10/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Fax_Doc#01_5.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:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 6264 Parent PID: 5856

General

Start time:	21:41:49
Start date:	10/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1600,13519744996372922803,2498414373330437516,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /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:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly