ID: 466598
Cookbook: browseurl.jbs
Time: 10:10:48
Date: 17/08/2021
Version: 33.0.0 White Diamond

Table of Contents

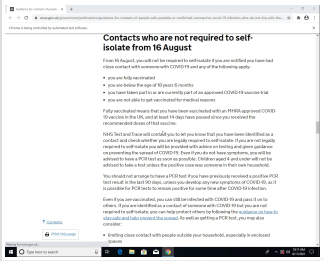
Windows Analysis Report https://www.gov.uk/governme…

Overview

General Information

Sample URL:	https://www.gov.uk/government/publications/guidance-for-contacts-of-people-...irmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt
Analysis ID:	466598
Infos:	

Most interesting Screenshot:



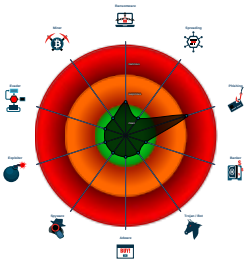
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Phishing site detected (based on log…
- Deletes files inside the Windows fold…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5844 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 384 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,13591179574770033270,10313266110045525433,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

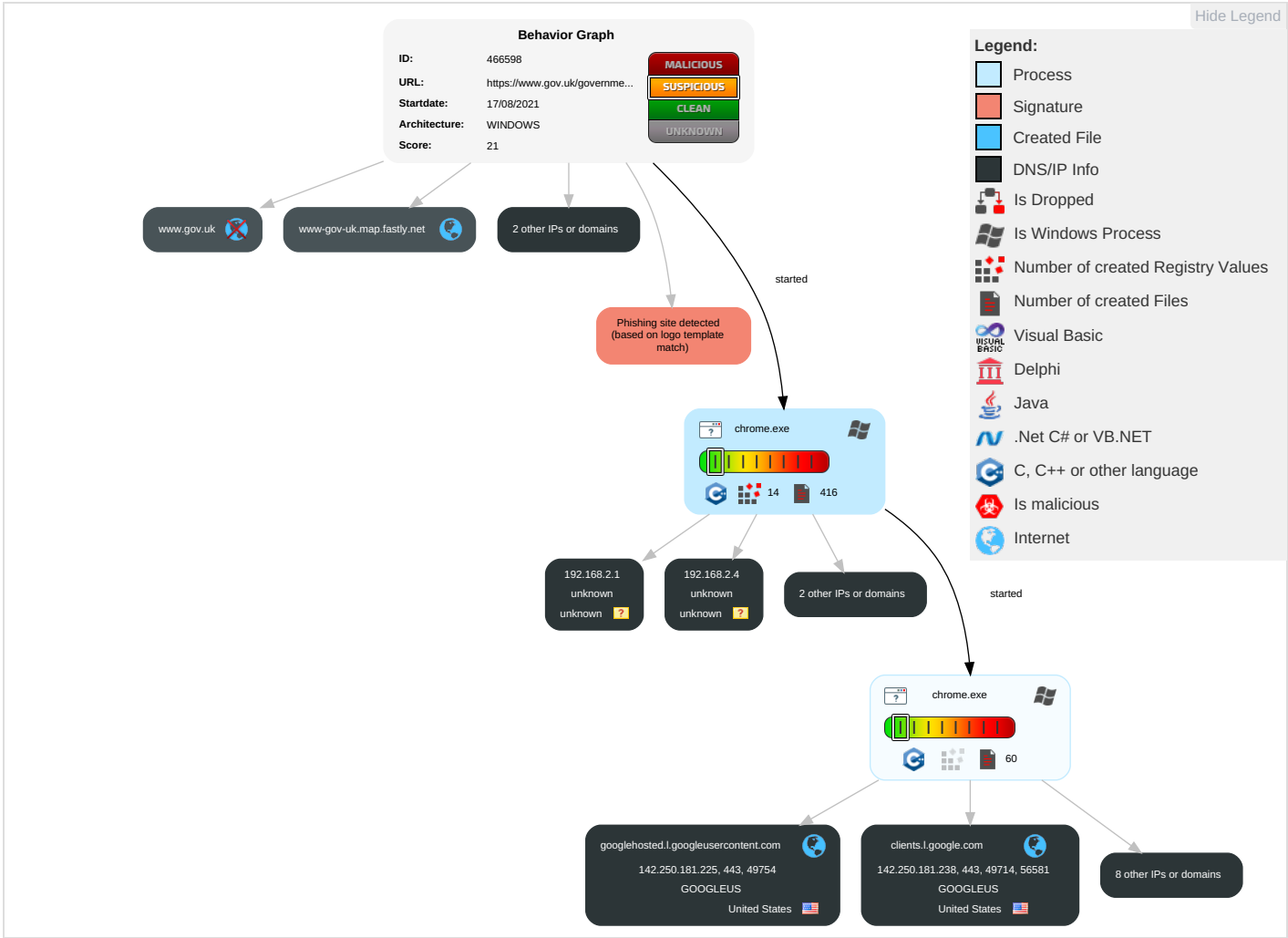
Phishing:

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)	File Deletion 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

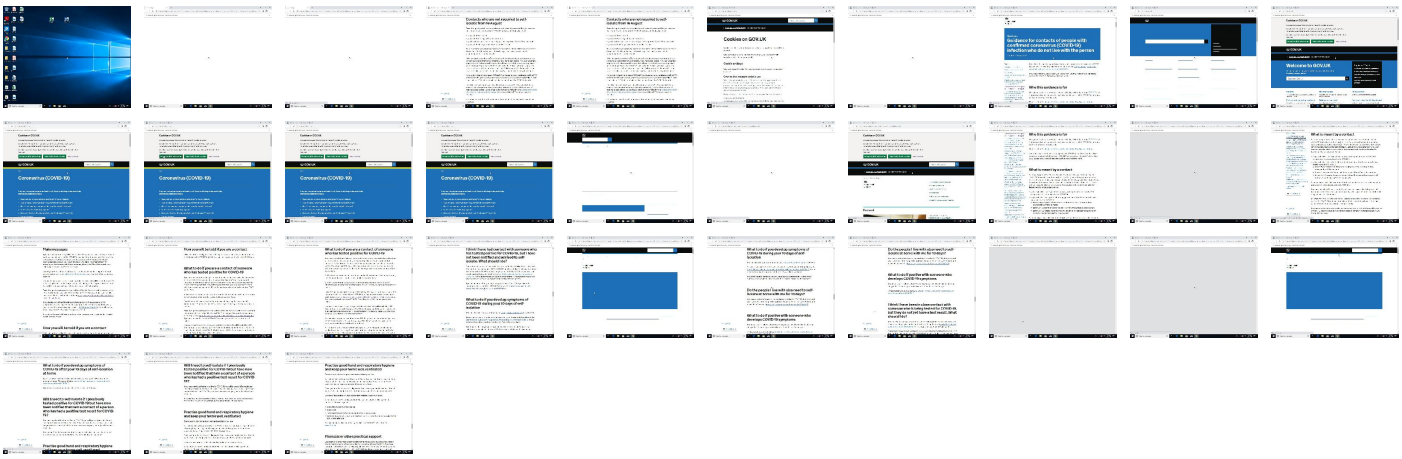
Behavior Graph

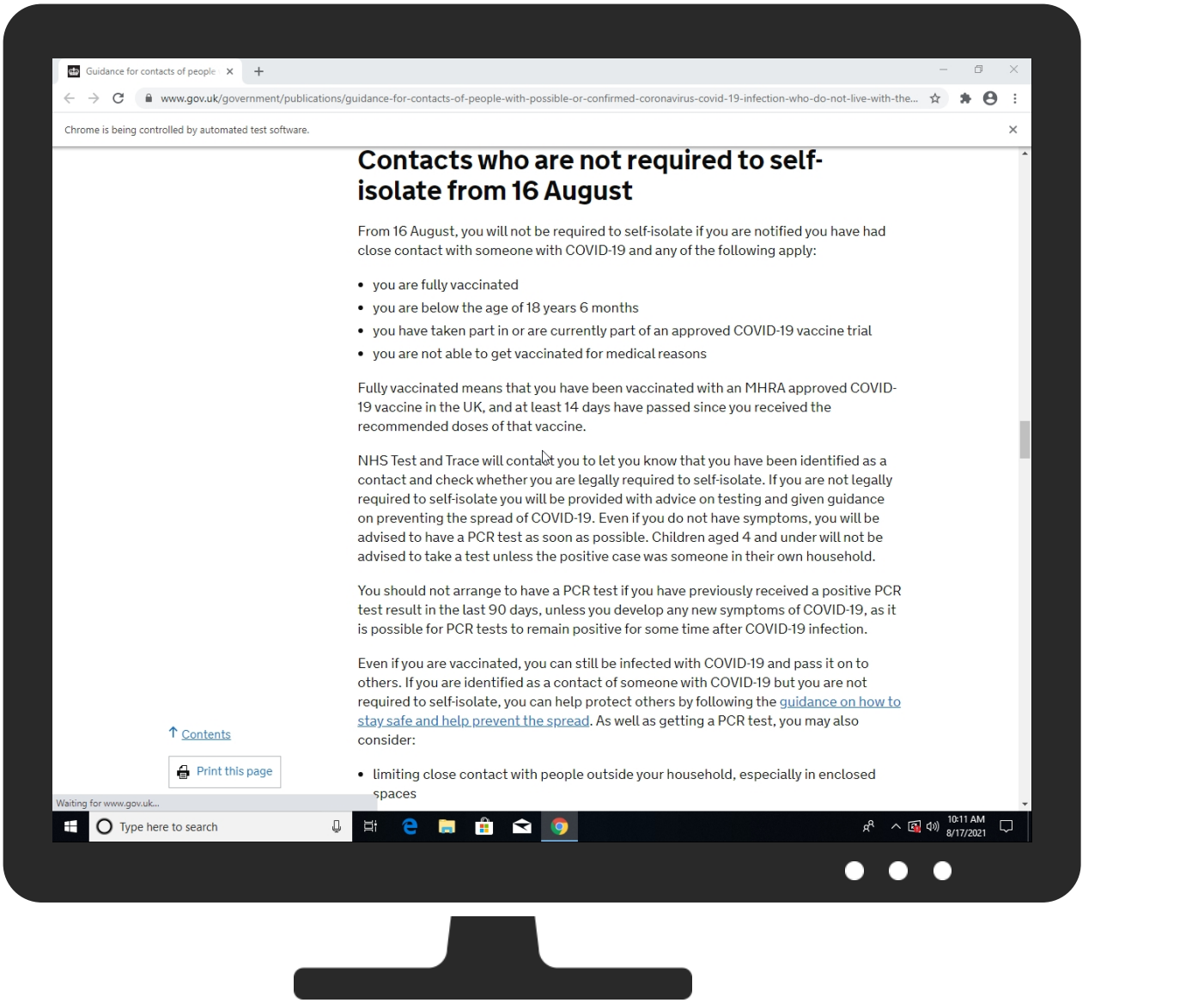


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt	0%	Virustotal		Browse
http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/assets/static/header-footer-only-d81fdcf7f18e7decb72d2de6302e85938f6b7198c4120d5e	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus-taxon/health-and-wellbeingc	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/help/cookies2	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/all?keywords=	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/help/cookiesCookies	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/opensearch.xml/(Z	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus-taxon	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/organisations/public-health-englandPublic	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/frontend/application-07c7cc25b2b557a01e70552a87e265dc4894c9f80199154f59b6e	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus-taxonCoronavirus	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/static/govuk_publishing_components/vendor/lux/lux-measurer-2953485ff03af7b	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/contact/govuk/problem_reports	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/0	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/2	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirme	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/(X	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/contact/govuk/email-survey-signup	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.gov.uk/coronavirus-taxon/health-and-wellbeing	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus-taxon/health-and-wellbeing(	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/help/cookiesk	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/opensearch.xml	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirusCoronavirus	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/t	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/Welcome	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/government-frontend/application-a9d421a8f8a509c0401cdb0d613dd33251d4f2cda6	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus5Coronavirus	0%	Avira URL Cloud	safe	
http://https://www.smartsurvey.co.uk/s/gov_uk?c=	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/static/application-e6ea5792082a9492390a9c635dc6189c0e50030123bc36b4440b38a	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/collections/application-98a9893e6c5d7cd0f3c525c7fde55b44d95837c3183df318e2	0%	Avira URL Cloud	safe	
http://https://www.gov.uk	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus-taxon~	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://www.gov.uk/assets/static/favicon-8d811b8c3badbc0b0e2f6e25d3660a96cc0cca7993e6f32e98785f205fc	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/coronavirus-taxon/health-and-wellbeingCoronavirus	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.237	true	false		high
www-gov-uk.map.fastly.net	151.101.0.144	true	false		unknown
clients.l.google.com	142.250.181.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.181.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.gov.uk	unknown	unknown	false		unknown
assets.publishing.service.gov.uk	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.gov.uk/government/organisations/public-health-england	true		unknown
http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt	true		unknown
http://https://www.gov.uk/help/cookies	true		unknown
http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person	true		unknown
http://https://www.gov.uk/coronavirus	true		unknown
http://https://www.gov.uk/	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.0.144	www-gov-uk.map.fastly.net	United States		54113	FASTLYUS	false
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.181.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	466598
Start date:	17.08.2021

Start time:	10:10:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt
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:	19
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:	SUS
Classification:	sus21.phis.win@52/240@8/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.gov.uk/help/cookies • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#content • Browse: https://www.gov.uk/ • Browse: https://www.gov.uk/coronavirus • Browse: https://www.gov.uk/coronavirus-taxon • Browse: https://www.gov.uk/coronavirus-taxon/health-and-wellbeing • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person • Browse: https://www.gov.uk/government/organisations/public-health-england • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#who-this-guidance-is-for • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#what-is-meant-by-a-contact • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#main-messages • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#how-you-will-be-told-if-you-are-a-contact • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#what-to-do-if-you-are-a-contact-of-someone-who-has-tested-positive-for-covid-19 • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#i-think-i-have-had-contact-with-someone-who-has-tested-positive-for-covid-19-but-i-have-not-been-notified-and-advised-to-self-isolate-what-should-i-do • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#what-to-do-if-you-develop-symptoms-of-covid-19-during-your-10-days-of-self-isolation • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#do-the-people-i-live-with-also-need-to-self-isolate-at-home-with-me-for-10-days • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#what-to-do-if-you-live-with-someone-who-develops-covid-19-symptoms • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#i-think-i-have-been-in-close-contact-with-someone-who-is-being-tested-for-covid-19-but-they-do-not-yet-have-a-test-result-what-should-i-do • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#what-to-do-if-you-develop-symptoms-of-covid-19-after-your-10-days-of-self-isolation-at-home • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#will-i-need-to-self-isolate-if-i-previously-tested-positive-for-covid-19-but-have-now-been-notified-that-i-am-a-contact-of-a-person-who-has-had-a-positive-test-result-for-covid-19 • Browse: https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#practise-good-hand-and-respiratory-hygiene-and-keep-your-home-well-ventilated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1a32918d-d645-4dcd-8d43-59e5917aa526.tmp	
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\1a32918d-d645-4dcd-8d43-59e5917aa526.tmp	
Category:	dropped
Size (bytes):	168154
Entropy (8bit):	6.0485722592841356
Encrypted:	false
SSDEEP:	3072:7LRKdezI6BuS9+zBWVEFtr1NkTFcbXafIB0u1GOJmA3iuR5:/RzI6Bz9+zBDFHNkBaqfIlUOoSiuR5
MD5:	21BA87DA5FE4C52B2D3FE95419D891CC
SHA1:	F24EF2F5B1044E2B1B6CFCB9846E44E33D904742
SHA-256:	665F35E1B293F13EFB645C0154D5D8FD4C79D9A98DC409506B043B679A76118A
SHA-512:	4AB5D158226B9FF476A3C1EE62D7D96F43AA3FFABA9D817ABC8F6DE87B210D168618B1191D11F52E9EBE83AA9D89EE1D43508587F6639464BAF9D1C190ACF5 D
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":1.629220304263824e+12,"network":1.629187905e+12,"ticks":3941110427.0,"uncertainty":4342566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016336051"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\326ec8e4-a848-455e-b9e8-d10452ffdcab.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7512455533328186
Encrypted:	false
SSDEEP:	384:1zhyWoPZM3AuVn52pNar/vOG3luk9H4hGRorzQOgxdUkQnrvymDgzgqaWJOUY6Nm:hCSVZq0Blsez0ewIfjWSKkG+Za
MD5:	8287397933DC98636066456DB61EC10F
SHA1:	46662E4BE18FB3CC67680B8165E10A3465F75750
SHA-256:	B833CF71C1A30EEF8D5A9F1961DB73961ACFB08D20FD0FC51F74A81FE96D1543
SHA-512:	B91AC7046D230A0B05846009011AE27CF652728C1E3D5F623124FAD9349A7D32678549ECF8D4DD9D442B4B4BF840F5C477903931FC8D4A76F9D9344BE584ECFA
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....B8.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\50a78e85-64ed-4aa3-8e2b-527755844699.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):	176637
Entropy (8bit):	6.078436028668586
Encrypted:	false
SSDEEP:	3072:C78LRKdezI6BuS9+zBWVEFtr1NkTFcbXafIB0u1GOJmA3iuR5:6URzI6Bz9+zBDFHNkBaqfIlUOoSiuR5
MD5:	7283775344361E9D0B9FA4B3230F765D
SHA1:	8CC12CFE8178500F4684F330CD64DAD7F810A139
SHA-256:	32367B88B0C795E69FEEBA0300F4421C8FAF75524918ACB8A59CA8C4104C2C0E
SHA-512:	CF95F8BFF237FE88D32F70E739AE6E1C84F715FEA6E8DC47FCC46BE6409234074407553A89B0AB5DE52A8E526B4B9983788E709786673ECEF356FB02D0F3016E
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":1.629220304263824e+12,"network":1.629187905e+12,"ticks":3941110427.0,"uncertainty":4342566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\52c24597-f43b-4b90-b2c1-fb56e269f41c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\52c24597-f43b-4b90-b2c1-fb56e269f41c.tmp	
Size (bytes):	176637
Entropy (8bit):	6.078435946904506
Encrypted:	false
SSDEEP:	3072:CX8LRKdezI6BuS9+zBWVEFtr1NkTFcbXafIB0u1GOJmA3iuR5:GURzI6Bz9+zBDFHNkBaqfIlUOoSiuR5
MD5:	22ED2D60B8628A846206399FF6EBE650
SHA1:	29CAD1F4BDFED7F77BB5D086022D4CBDEBEBFEE9
SHA-256:	20F698811FB110248E1A785590C3E6C0224D985FE6FE9D7642C72291550082E4
SHA-512:	023C087A3B885A7F8A0E373E7E24E7F029924C162AF3FD85D602CD4CE2B54DC8E760AA9A6A7BE1111171D7C1DA77FA2A28C2CD7B7FC0A11577150BF11D1946 6
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":1.629220304263824e+12,"network":1.629187905e+12,"ticks":3941110427.0,"uncertainty":4342566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5f79c021-51ef-4323-b070-78c39224e0fd.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):	176639
Entropy (8bit):	6.078433695492453
Encrypted:	false
SSDEEP:	3072:RxqLRKdezI6BuS9+zBWVEFtr1NkTFcbXafIB0u1GOJmA3iuR5:7KRzI6Bz9+zBDFHNkBaqfIlUOoSiuR5
MD5:	7EE2E515B00131DBCB45E7A0B8FB5BB6
SHA1:	48B9382BFDF1A5E09050553F71207ED883D39B65
SHA-256:	11777ED6CBB75F83D22E4360E13D1B99BA3179AE006BF78CCC815B7EFF9DD86C
SHA-512:	E0817433D733A0F3D55D9E53B11ADBA162890B241CD561348CB5FC5A91030511EE65E56FD7D5BE2C07FD858DF5AD035FC8DA02B576032F06FF9354DF250E80B
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":1.629220304263824e+12,"network":1.629187905e+12,"ticks":3941110427.0,"uncertainty":4342566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016336051"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\65e90f8a-c568-4770-9faf-4727ce968c80.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7512562398476805
Encrypted:	false
SSDEEP:	384:lzhyWoPZM3AuVn52pNar/vOG3luk9H4hGRorzQOgxdUkQnrvymD3hzgqaWJOUY6G:xCSVZq0Ylsez0ewIfjWSKkG+ZY
MD5:	F4683D42EAB78765A911CCD178D874C7
SHA1:	C58891E8B1E3870F9DD0C20D0625605390188ED4
SHA-256:	5AECBC1EFD0A26F3E0959F5CFE044B79C0DE14BCD7E5717142AD12562CF9DAC1
SHA-512:	D1DBBFE2C8FA6539B7F19F250026718A4733F491FD93BE5E8215413AD7AD2866842A039A776F3EC5435F98227EB1A550A8F06520630953C5C9BA00DC4D52F1BB
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....B8.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\76faf2b3-fcbc-4c10-84c6-c778a2a7083e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724

C:\Users\user\AppData\Local\Google\Chrome\User Data\76faf2b3-fcbc-4c10-84c6-c778a2a7083e.tmp	
Entropy (8bit):	3.750557541112515
Encrypted:	false
SSDEEP:	384:LzhyWoPZQAv2pNar/vOG3luk9H4hGRorzQOgxdUkQnrvymDgzgqaWJOUY6NX1KDn:bSVZq0Blsez0ewIfjWSKkG+ZI
MD5:	F7C3B53192003C5092C29B95DBB9D698
SHA1:	1EDD321930CC4ECA52B53EBC3CD93898B08766E1
SHA-256:	07B08C8246DB8DEB17F77E1FB5B5ABCCAD7747896C80AC6B4FC62236E016981C
SHA-512:	DB3D9D38F3B88098B3E6B916667E33D722E2C9D2B4D17FD09B914BE4BF3598F0921F98E7AABA6B63103B27512AC4E090BF3A387D7B116C0A2848B3670C8F0A0
Malicious:	false
Reputation:	low
Preview:	0j.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.......g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....B8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.......m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\01d3e7ed-9526-4936-af26-6e80c0475307.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5794
Entropy (8bit):	5.19722767006448
Encrypted:	false
SSDEEP:	96:n43zCD/IL9w7dicPcKI6ok0JCKL80NkkWS1e3bOTQVuwn:n4jCkL9w7IcPcz4KNNkkBcT
MD5:	970CB3690B2A977841C4E61DBD43D634
SHA1:	12932E774E2943C1442B726730768E30FFF3BCF7
SHA-256:	E7CEE546B138CBB8B2ABAB124737279A69FF629D8259B64D3277347561ABF2A9
SHA-512:	5313E7EC1C27018F9E8AC134867A0CD53F57B9A75D1A0FDB3BED654189EE1E0708E2995572B340930E5E0C2CE658D165F35C6AB861A9E94922FE2EA36D6359D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","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","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\09f9059d-572a-403b-ada1-45bc200902e4.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):	5793
Entropy (8bit):	5.197014166313657
Encrypted:	false
SSDEEP:	96:n43zCD/IL9w7dicPcKIQok0JCKL80NkkWS1e3bOTQVuwn:n4jCkL9w7IcPcF4KNNkkBcT
MD5:	DD8B48AEAF66CA6D114695960E46114C
SHA1:	7635C0406DDE0C0AEE7CB01F56F438A2E6E43C72
SHA-256:	9806032DAC59C56711C5E201B949F756374BC6B4343626CE73911065A162F85D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\09f9059d-572a-403b-ada1-45bc200902e4.tmp	
SHA-512:	F2F2640B6C52D1DD0C27AE31801E3BA8F1C4C0407470CEC25ED035E123EDBAB46785EE11649825EBE7DFFCA92385B7F869D5E607776992CE7AFA2432072E0C E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\0b80b546-c902-4c26-94c0-a932b864c90a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12d01cda-77f6-4066-adcc-9f47669f5db0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2fd98d03-4edf-407f-8bca-fa601e0961a4.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):	5820
Entropy (8bit):	5.199382548246241
Encrypted:	false
SSDEEP:	96:n43zCDbIL9w7dicPcKIzok0JCKL80NkkWS1eB0bOTQVuwn:n4jCYL9w7IcPcI4KNNkkBcBe
MD5:	B3C781FA20A480AF86681C797505C28F
SHA1:	A52D494811827B32431E5F67550D4939779DFF4F
SHA-256:	7D9AB75748A422A04D0CF41404A3BD490F0D13588C5A763C2148701DD73F66D2
SHA-512:	3CAD0E2D0F61CBAB668DFD9EFE71BBA4A37CB9C3CCD0668AEE5212EA1218D728554749CACC388F3CC9B07A2D7151F92363C324FAFE11CDB21522D348E956A 57
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2fd98d03-4edf-407f-8bca-fa601e0961a4.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\350dcdb8-ba95-4f2f-90fe-5c7f981fffe5.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):	4.871755235889535
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMZ:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhS
MD5:	AE133C52F86E27CD225F807F1DDB33A3
SHA1:	A0EB1D7B7D41F31993C975A8B5F27954F90B6DF8
SHA-256:	A795DA84B0B14FD651959C4E712B297CA76E50FAF03E18469336F5FB1BE5420A
SHA-512:	098D9CC2B0436B77AE03D9289C2DBF2316B0F0145C7AEE81F8F19A26964AB7F975F941CD2A9E14783E600602A195ED60A059B0EFEFFCEEC2BD0C5923E09663E 3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5d6ea73c-130a-4faa-a726-95a38a9b3ea5.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):	5793
Entropy (8bit):	5.1970691798259265
Encrypted:	false
SSDEEP:	96:n43zCD/IL9w7dicPcKIEok0JCKL80NkkWS1e3bOTQVuwn:n4jCkL9w7IcPcp4KNNkkBcT
MD5:	44F25108D5356F878C7A18E37750A4AC
SHA1:	7DB227DE144704339BC280C45F09CDEE07B48A67
SHA-256:	FB74ECB61139B29854C01D6095B74A73A03030AD76810493638F38C44BB2D6F0
SHA-512:	D0BA15F6F6B8A51086A4EC46C87F3A1E885FD87B594E5C1272FEDE53101E2F2D41631601B72CAB12D2407C15CBE37DC8D942A0D93A5D95E9707DDE7626CADE 6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\6bbc052a-bc2f-4949-ac6e-a5781e4d5fcb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1375
Entropy (8bit):	5.573915029250021
Encrypted:	false
SSDEEP:	24:YU5UA8/6H0UhVsTG1KUe5i8UA8zkq/HeUeXby2qUeXvlD7wUA86Z9RUenHQ:YU5UA86UUhVseKUe57UA7qPeUer2Uefv
MD5:	897B7FF8D3C68F79CD295A7F2E295404
SHA1:	D603DE74B583D70CE7C052FAD9A9BA8747EE9208
SHA-256:	B781EC956D5CF36A4354AA373E84A914C6EE770C1BD279ACE7198B53CCEDFEAC
SHA-512:	37945D1DF0F42A629EB4AD318B9D20025D91918CB0EC102F49A07FA3C45E2FC153C28B70EAE5C740DA4D4555CC848F50EFB73EEA560FC6131ABA23379397AB 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6bbc052a-bc2f-4949-ac6e-a5781e4d5fcb.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1660756334.070589,"host":"Dl4Fc0vl/YypYkpsDR3ijy3cXV29/8t3AjQ0T8PW0dA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629220334.070594},{"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":1660756334.053618,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629220334.053623},{"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_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a23dc42-e054-44e2-8ec7-b24461d39635.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):	16745
Entropy (8bit):	5.577393978151346
Encrypted:	false
SSDEEP:	384:uZvtbLleBXw1kXqKf/pUZNCgVLH2HfDErUrjqTp/4q:mLlOw1kXqKf/pUZNCgVLH2HfYrUGp/N
MD5:	ACA4D984F1DC1110CD58E79078840A2F
SHA1:	28AC49A9A71B8B8204D3C3CC57D7570144395E34
SHA-256:	0591A1E0EBB3E1A3A1ABA9F3A961403D06619A76A7B106CA55BFFAFB6748B20E
SHA-512:	9EBBDC24B27E6864C583E03C1BDA5189FFD1ABE3B25CE3A80EDDB93802B701959AC8612BA8748F5B929DB4247F28A059F88D496B0FC8F939FB7F5AD4AEF508A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273693900341891","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d87884f-567c-45e2-a832-ea5c4e84e9b5.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):	2350
Entropy (8bit):	4.902752451710999
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5sN5TsJRLsAdKRD9sJtyKsU3zsTMHdTssqzkqFYhbG:JTnOCXGDHz85QZKedyGdTqjChS
MD5:	9B1377FB64A08961153DA0A6F9D7A603
SHA1:	D086D76AE8B45F44B6455C1DF4E6C2DD94DD8D71
SHA-256:	403C1841EA52EB9734C174F523705BFF83ED30F215E67410BEB89ECC8F508931
SHA-512:	4981A18AAACAC9C45B3CC0EED8724A8DAEBCE3D8BCF64F6FAF558A315926C4B825CC368F7C2541D4E9EE367349248509C1C9D881026EA9D7D6D2BFAB83BEE187
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://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":"1327628590 5019600","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13276285905027610","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a2f711f-b38d-478c-a39b-95afa9e31a62.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):	5820
Entropy (8bit):	5.199073632734545
Encrypted:	false
SSDEEP:	96:n43zCDbIL9w7dicPcKIpok0JCKL80NkkWS1eB0bOTQVuwn:n4jCYL9w7IcPcu4KNNkkBcBe
MD5:	A8CC264E27E5F6BCB9F656D43B0293F4
SHA1:	EAE30EFE6B3629855F459669B5D05E5BC0607934
SHA-256:	06ACE104EEAC601E465FC4AFBD9945CD6F1F7472C5DECFC5EDBE58B84B851DDB
SHA-512:	3B5076524894562BDFDE7B08AEC5A250281BBFF5DF9BC7D47228E30A9F8A23CE85BAC58AF5D8AE7AAB499452BC36F95FE1398BFE48225D13AE9A48F8A98ED558
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a2f711f-b38d-478c-a39b-95afa9e31a62.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\8ead5b1b-23c2-4a67-b00c-22489637a07c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536123015573268
Encrypted:	false
SSDEEP:	384:uZvt6LleBXw1kXqKf/pUZNCgVLH2HfDErU+HGdnT7jqTw/4w:5LlOw1kXqKf/pUZNCgVLH2HfYrUuGdnJ
MD5:	CBC871E63EAE5DE579F89F7C13828597
SHA1:	D771A4871DBC97AE10896B16E629DB7058E61807
SHA-256:	8D4A181D114B6B30CF4DBCEA6359699FA6C5BE9DEFEBC0701E72B20401D846CF
SHA-512:	F5D18C1A91F689348CE4D70D9DC54E0515CA4FF52A75CBC8646159B35B2BDA95316494C06255E1C24BADD81F34DE09077F6975313F5704B8F6465ED8B5087A98
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273693900341891","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.174318744473518
Encrypted:	false
SSDEEP:	6:mpIgolL+q2PWXp+N23iKKdK9RXXTZIFUtp8IgrUzKWZmwP8Igrq+LVkwOWXp+N2v:sSlL+va5Kk7XT2FUtp8imW/P8LLV5f51
MD5:	D8C32DFBC208BCA9279A9E7010CA2730
SHA1:	7BE5116637EB303B5217F0F04166AEBFFCA7B86A
SHA-256:	88D796FCD1DE2FF593CAC22144504E74FE43AB4892EB7762C2C6259B68C76FA3
SHA-512:	4AC4E0DC8A1FF859FB6DBFCB851676F5B314D84E74F916839AD5D05C8AF103A9DAA4E0B85EBD2106FCB0E9DE8B404FC218FACFDE0EF3C53D185C62E55207E 1AC
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.025 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/17-10:11:58.061 10ec Recovering log #3.2021/08/17-10:11:58.062 10ec 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\AutofillStrikeDatabase\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.174318744473518
Encrypted:	false
SSDEEP:	6:mpIgolL+q2PWXp+N23iKKdK9RXXTZIFUtp8IgrUzKWZmwP8Igrq+LVkwOWXp+N2v:sSlL+va5Kk7XT2FUtp8imW/P8LLV5f51
MD5:	D8C32DFBC208BCA9279A9E7010CA2730
SHA1:	7BE5116637EB303B5217F0F04166AEBFFCA7B86A
SHA-256:	88D796FCD1DE2FF593CAC22144504E74FE43AB4892EB7762C2C6259B68C76FA3
SHA-512:	4AC4E0DC8A1FF859FB6DBFCB851676F5B314D84E74F916839AD5D05C8AF103A9DAA4E0B85EBD2106FCB0E9DE8B404FC218FACFDE0EF3C53D185C62E55207E 1AC
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.025 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/17-10:11:58.061 10ec Recovering log #3.2021/08/17-10:11:58.062 10ec 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):	5.1296692972616
Encrypted:	false
SSDEEP:	6:mpIgPQaL+q2PWXp+N23iKKdKyDZIFUtp8IgPSMKWZmwP8IgPQjLVkwOWXp+N23ir:sNL+va5Kk02FUtp8cLW/P8GLV5f5KkWJ
MD5:	3318FE8D4A1EA896DE4C119297D0DF0E
SHA1:	84A5E8C7A4A28C7E588A64AC6CF6C516D7D32834
SHA-256:	5490774027CD735DB2B19DF8BDF1E50FC94C82403701AFBCDC426527462AA560
SHA-512:	8CDF9F86743AC88B349883AA319EDB5BC8258B0960004E67D70A0A0196A308452451152DB1AB48D0B07EA74A2FCD5C99FCCFD4C477680829A9C24ED25C421BA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.015 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/17-10:11:58.017 10ec Recovering log #3.2021/08/17-10:11:58.018 10ec 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\BudgetDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.1296692972616
Encrypted:	false
SSDEEP:	6:mpIgPQaL+q2PWXp+N23iKKdKyDZIFUtp8IgPSMKWZmwP8IgPQjLVkwOWXp+N23ir:sNL+va5Kk02FUtp8cLW/P8GLV5f5KkWJ
MD5:	3318FE8D4A1EA896DE4C119297D0DF0E
SHA1:	84A5E8C7A4A28C7E588A64AC6CF6C516D7D32834
SHA-256:	5490774027CD735DB2B19DF8BDF1E50FC94C82403701AFBCDC426527462AA560
SHA-512:	8CDF9F86743AC88B349883AA319EDB5BC8258B0960004E67D70A0A0196A308452451152DB1AB48D0B07EA74A2FCD5C99FCCFD4C477680829A9C24ED25C421BA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.015 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/17-10:11:58.017 10ec Recovering log #3.2021/08/17-10:11:58.018 10ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e652be799556508_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	54982
Entropy (8bit):	5.707606235701624
Encrypted:	false
SSDEEP:	768:+toZa1CBSp9n7cxUcg8DxpptPfMTUxmSJq8Sbm5Gjt+hndHJuZwC4:HhBUn7cxlnJfgUnSbmfQ+/
MD5:	D381BC6F3E6CA6C66015447F3AD7EAE0
SHA1:	938DEA0AA6EFA6F3A9A858749EAE6C0D9C445F9B
SHA-256:	AD1DFFE3512AD1905FDF80F902E972B8706EF6DF8D3B8E3C3A5879443EDEB960
SHA-512:	910699AE7B317BBBA8DA095DD01F36652001AD8FD8498158CD1DBF3A0E61B08C042757EFCFF023E843DC44921420ECB95B1C0477A62716F42FD6E81F9C1C46C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>....._keyhttps://www.gov.uk/assets/collections/application-98a9893e6c5d7cd0f3c525c7fde55b44d95837c3183df318e2ca4bf64cae7d32.js .https://www.gov.uk/(X..Z(/.....d...D...#|{/.n..M...P.(.....A..Eo.....aT.....A..Eo.....'.1.....O.....p.....$.....(S.Q...`X....L`p.....L`.....(S.....Ia.....Qe.n.m....nodeListForEach.E.@.-.....P.....u...https://www.gov.uk/assets/collections/application-98a9893e6c5d7cd0f3c525c7fde55b44d95837c3183df318e2ca4bf64cae7d32.js...a.....D`....D`....D`.....`....&...&...!&.(S.\.`t....L`.....Q.@.....exports...Q.@..LL....module....Q.@.....define....Qb.GF.....amd...Q.`.}\.....GOVUKFrontend.....K`....Dq.....s.....s...\..'...s.....&.(.....&...&.^.....\.....(Rc.....I`....Da&...,.....d.....@...P.....#d..... .....&.(S...`..... L`.....(S...`.....0L`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\25dc75807f183917_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3057
Entropy (8bit):	5.903403122856595
Encrypted:	false
SSDEEP:	48:wOEbfZ6k6kA90AOE8axCU8UPsGpj1VfUKFczeNYHITZRlYV:6Ek6kA9yaMfU0a1VsKFcR2CV
MD5:	975E955BCC1B2C1A4FABBC552286DD2E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\25dc75807f183917_0	
SHA1:	1A0AFF65C229CA943F171AC112F0267B0EEFF559
SHA-256:	9AF4F8E9CC978F3B5C0BAAF1623784A5FB4BFCC739CCEA558037F2991FB72692
SHA-512:	C44BEF529F04641BC130701D9AED006A4A1726EC61AF8AC16022269523 76BE49FC797575880ED6E3E8EE2120A9CA85D6D932C1F700DE80077381B51274D21E60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://www.gov.uk/assets/static/govuk_publishing_components/vendor/lux/lux-measurer-2953485ff03af7b9ea4c6a6170eeae0e42d13011e7ab0d7f31552c6c68b1ea08.js .https://www.gov.uk/.r..Z(/.....*...?7~....I.....a..._"3..A..Eo.....A..Eo.....r..Z(/.x.....'.....O....8....D.....(S.)...`.....xL`8.....L`.....Qe&.Dz....LongTaskObserver.(S.9..`(....\L`*....pRc4.....Qbv^.G....f.....Qb.bo.....o.....Qb.@h....t.....Qb.+.....r.....M...Qbf.....s.....Qb..,[....m.....R..h.....I`....Da.....(S.....Ia....Y.....q.....@.-.....P.....https://www.gov.uk/assets/static/govuk_publishing_components/vendor/lux/lux-measurer-2953485ff03af7b9ea4c6a6170eeae0e42d13011e7ab0d7f31552c6c68b1ea08.jsa.....D`....D`....D`.....@..`....&...&....&....&.(S...Iac.....Qb&.....e.....d.....&.(S.....Ia.....Qb.....n.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58dcc872f6f82664_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46310
Entropy (8bit):	5.7013957369607615
Encrypted:	false
SSDEEP:	768:KcX6cdcRUnbir+1lv40804oFShUXpfCr+sXQ:RXaAbzlv4080bSi6qsXQ
MD5:	718C8A9C9DEEBB12DECF2CB3A360B012
SHA1:	7AAD0F8F7FD9C045264111004448979BFE2ECADD
SHA-256:	843A281AA4273B8AF0764374D823DFCD0CA613CB9DCF79A219B3E362F9C15D2B
SHA-512:	91E6F81EB0E94FC1D042F23074A501B357EDDDFFF81C8F6AA568CE1C32C8FBF15174EF3C6B2FF1661EE24EBFEEFAFFDBE4387C130551AF12BDFD4E7A7A194290
Malicious:	false
Reputation:	low
Preview:	0\r..m.....0....._keyhttps://www.gov.uk/assets/government-frontend/application-a9d421a8f8a509c0401cdb0d613dd33251d4f2cda659d76ef69a14aacdb14544.js .https://www.gov.uk/2{..Z(/.....R.....$-..K&i.R$`>++.%.r...{. .9A...A..Eo.....H.....A..Eo.....'.....O.....n.....(S....`.....L`f.....L`.....(S.....Ia.....Qe..kO....nodeListForEach.E.@.-.....P.!....}...https://www.gov.uk/assets/government-frontend/application-a9d421a8f8a509c0401cdb0d613dd33251d4f2cda659d76ef69a14aacdb14544.js...a.....D`....D`....D`.....`....&...&..1.&.(S...H.`J.....L`.....Qc:.....matches...Qeb.....matchesSelector..$Qg..m.....webkitMatchesSelector.... Qf&..$....msMatchesSelector....(S.....Pd.....t.matches...a....j...I\....d.....K`....Dl.....(...'....(.....(.....(.....(.....-.....(Rc.....I`....Da@.....c.....P.....d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bec73f7a155285b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	170696
Entropy (8bit):	5.945961621474943
Encrypted:	false
SSDEEP:	3072:N+vFqKsQ+TNg7eLG5WWouSOGBdrF6dlLbht:N+NogNWR1Oq67
MD5:	9CADFDAD431030EC57F04FDC7498C2C3
SHA1:	AB8E37FE0F27691925C4E1CE2B5FFD86ABC5B554
SHA-256:	2B168E655ABD9A4B0EB0CC895B999566F3AE1150156A11613B301867DDE50D2E
SHA-512:	31CBE5B5866AAECC186A507830008BAB13F94DA2AEE0B3E7748B2683FF1683D50DEFB66DC8B2157491CD3FD2C2498C34581AF017297679CC80287CCB527B0CF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...nXO.....3321A31447CF7F0AB2FCB978E8AA1C998D148C687C7D8CE8F577F0A40B5CEA1D.....'.....O7.....h.....-..D.....d.....h.....<.....(S....`.....1.L`.....$L`.....(S.....Ia....Z.....QdJ.....parseCookie.E.@.-.....P.....w...https://www.gov.uk/assets/static/header-footer-only-d81fdcf7f18e7decb72d2de6302e85938f6b7198c4120d5e34b039037167d411.js.a.....D`....D`....D`.....`....&...&....&.(S...p.`.....L`.....0Rc.....Qb.f.....t...`....I`....Da....Z.....Q.@.e _....module....Q.@f..m....exports...Qc..c.....document.(S.....5.a.....1...a.....a.....a.....a.....Pc.....exportsa....'...I..1.....d.....K`....Dv(.....%.....s..6...&.(...s..)...&.(.....&..&.^.....&.-...%.....&.].....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9072e92199569f35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	172592
Entropy (8bit):	5.943484677247601
Encrypted:	false
SSDEEP:	3072:9g7fiEsFutztS7eLG5WWNt7WItGcstzVDb2z1eCzXpyd:+bZz6NW29WI7QVe95yd
MD5:	FB362A0FDA285D4DF21ED8613BC2A22D
SHA1:	B727394C8A4FE2FAEC782C081C68449F680027D3
SHA-256:	99C1F88F2B2BD3C6EB785C9C8C9D43F43AF1638D8CCDA9F3FC7F6216D17EFE30

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9072e92199569f35_0	
SHA-512:	13CA9E27C996F6F1EF2D4E221CB1F8FA55E8ABC9DCA69F12C38A5D8DC1933F6C17B613B7C4967C9CC9464EEDA120CA9FEE968DFFE1F53E9E80C9B07682220C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...{.n.....CF3A32A53346C9C69A86A6C6CD7CC8EB02461DE9BC70FE12D8B16C951C82E58B.....'.....O8.....%.....(....-..D...p.....d.. .....h.....(S.E...`>....5.L`.....$L`.....(S.....Ia....Z.....Qd..... .parseCookie.E.@.-....|P.....p...https://www.gov.uk/assets/static/application-e6ea5792082a9492390a9c635dc6189c0e50030123bc36b4440b38a47e05d8ec.jsa.....D`.. ..D`....D`.....`....&...&....&...(S.p.`.....L`.....0Rc.....Qb&./.....t..`....I`....Da....Z.....Q.@.N.....module....Q.@6'.p....exports...Qc.....document.(S.....5.a.....a..... .....a.....!....a.....a.....Pc.....exportsa...'...I.....Q.d.....K`....Dv(.....%.....s..6...&.(...s..)...&.(.....&..&.^.....&.-...%.....&.].....d....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9bb1330eefc74d67_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.925045192663084
Encrypted:	false
SSDEEP:	6:mvlPYGLRfhD4CyLRyRigTDPQRLR6jr1Gv31NzK6tpPSWzmlXym3gq4nzCl2v31Nq:ElD49RyR3DXAv31HPSWKlXym3aO0v3
MD5:	63E94F0A0F445E4EEF0D9F6CEE758116
SHA1:	816569EB48B5CD00711EFA8B2F24F181D6C6C80C
SHA-256:	8F1ACF9A4E0D2DF325DC94E54722F871832226B01FD0DDBDC059827A53EE5827
SHA-512:	79C0B009363605C47B4CDAB00CE69E36B5DDE520F2386CB6232BBBFF79A9ED4A61F18D9B3020DDAE0003541C4A9A06CAC432BDB7363863BFCF6D7C56425BFB1B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a',....._keyhttps://www.gov.uk/assets/static/header-footer-only-d81fdcf7f18e7decb72d2de6302e85938f6b7198c4120d5e34b039037167d411.js .https://www .gov.uk/....Z(/.....J.....dM....\.?C..].M.x.2.Js5.....Lc.A..Eo.....A..Eo.....Z(/. ...3321A31447CF7F0AB2FCB978E8AA1C998D148C687C7D 8CE8F577F0A40B5CEA1DdM....\.?C..].M.x.2.Js5.....Lc.A..Eo.....lL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af71836a8101eb20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.883714142008262
Encrypted:	false
SSDEEP:	6:mKOYGLRfhD4zrrcpRXRkvIRLRk1h1P80rThK6tzYso/cmgEuYKE+P80rnll:C4HqRX2Vb/7NcYEuY0b
MD5:	42870A3E35EB9629367E6CC536916ADD
SHA1:	765C50D4BE5EB0BE94148812352506FF4E12B801
SHA-256:	33D377E55521F6AF8FA4119ECC7CF697AB4FB0EBCFF63F67A91BB6A2770EE971
SHA-512:	D292DA3C0B9B05514718104FA0C5B054A9A636A133FBB065FB3085D70018BBB2CA0E10276A93475A2446AEA6A75989D8BB2C4BDBEE52C633712FB8F47E7792C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.gov.uk/assets/static/application-e6ea5792082a9492390a9c635dc6189c0e50030123bc36b4440b38a47e05d8ec.js .https://www.gov.uk /0.}.Z(/.....ZA.....I.....Q.|...u..uC+$..A..Eo.....q0.....A..Eo.....0.}.Z(/.....CF3A32A53346C9C69A86A6C6CD7CC8EB02461DE9BC70FE12D8B16C 951C82E58B.ZA.....I.....Q.\|...u..uC+$..A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0b345af007be2d4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58931
Entropy (8bit):	5.735801252493477
Encrypted:	false
SSDEEP:	768:9nKmczxdcLfrBHDnI8vc6jayCo9+G0Oo11hS9mGz1dvHTfDD:9nHg29H/vcLy5+71cFxhzf/
MD5:	8D398EBC7B892D3BE32105A453DC1D21
SHA1:	10D8805709A99C630C19F2E4B4E2DA306CDA2A67
SHA-256:	C1E62824C5281C464098BC7C1B3A5A1440264C27B8D27B372EC9592B14FF5694
SHA-512:	FB8D4349C289142868B4A2069292830D8949E3611F201CE8593798ABC787F4E27D8AB2E3E7F84DBD9626CAAE25C4E015429381E27FBA7E6FAF53A0E9B4964CD2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0b345af007be2d4_0	
Preview:	0\r..m.....W....._keyhttps://www.gov.uk/assets/frontend/application-07c7cc25b2b557a01e70552a87e265dc4894c9f80199154f59b6e4565a8fc5c7.js .https://www.gov.uk/.~}.Z(/.....}...jN.....1.G...A..Eo.....Z.....A..Eo.....'."....O...@.....T.....(.....(S.Y...`h.....L`r.....L`.....(S.....Ia.....Qe&.....nodeListForEach.E.@.-.....P.....r...https://www.gov.uk/assets/frontend/application-07c7cc25b2b557a01e70552a87e265 dc4894c9f80199154f59b6e4565a8fc5c7.js..a.....D`....D`....D`.....`v...&...&...!&.(S.H.`J.....L`.....Qc>.....matches...Qe6.4f....matchesSelector..$Qgv'd.....webkitMatchesSelector.... Qf.r.....msMatchesSelector....(S.....Pd.....t.matches...a....j...l\..A#d.....K`....Dl.....(...'....(.....(.....(.....(.....-.....(Rc.....I`....Da@.....c..... ...P.....d.....

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):	0.8856666807299104
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwrQX1uy8bMaX:TekLLOpEO5J/Kn7UmxV
MD5:	7A2A70BAF680F351F3E90B4E86BF382D
SHA1:	61CBF22EECDED848CF6761B68143BFBE4DB78CC5
SHA-256:	A4D703853639FF41F1D645BC134BC0AD394CDE3AFFAC019DB7CDD34998CFD1E7
SHA-512:	640CD3ED4B04BA3413AF868566FF2A8D4EB0B57B03FE12C00B573F16876425D790BCEF746DE6BBB6204B8A25FE135FEDE2AC886CCDD6B240D06AE81FCE777F DC
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9674642995990733
Encrypted:	false
SSDEEP:	24:zcLgAZOZD/FqLbJLbXaFpEO5bNmISHn06UwR8:z8NOZFq5LLOpEO5J/Kn7Ue8
MD5:	5DABE034AF0A80F55FD6723F6A998AA7
SHA1:	38AD6DC01AD2A47B34F10928FBBCEAC00F9C91BC
SHA-256:	212C666A21FF15DF8B7E5573D49202DF67E2A982D10BDE07013CC2BD87661120
SHA-512:	9FCA12B6A742F247E04262881A150D646B4680C54B1DB71927E79629003867121BD42727E6C63450EDC0C709FE629627126DE48F1BD46938CD4202AC165C6EDC
Malicious:	false
Reputation:	low
Preview:	.....j,m..... ....

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):	92407
Entropy (8bit):	3.610431925813685
Encrypted:	false
SSDEEP:	768:qrrkE4Sa+n+Wepa83H8DBrSw8yRcAUJpx9Z4Yf:qrAE4Sa+n+Wepa83Hu5R8yG7pfZ4Yf
MD5:	ED2C8A50F73B61B87AE5EE9650DC855B
SHA1:	359479DF6525A413018AA598DE606D6053D753E4
SHA-256:	BE82FE419000A5D5A60501F3AD4E8431176766DD4C974C09C20F370CA7C60D21
SHA-512:	04364F9B5072B93134489FFB8DF0AD22BF89CDC4439C9610934836BFF3CEB4DF4DDBD2AB87C303EF69E810568310FBFBA93B9E5F33DA2B313EF9D61D5AC5CF 4
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...62037b48_84f0_4cc6_9db3_4e5d5b01fae3..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....%...https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt...x...G.u.i.d.a.n.c.e. .f.o.r. .c.o.n.t.a.c.t.s. .o.f. .p.e.o.p.l.e. .w.i.t.h. .c.o.n.f.i.r.m.e.d. .c.o.r.o.n.a.v.i.r.u.s. .(.C.O.V.I .D.-.1.9.). .i.n.f.e.c.t.i.o.n. .w.h.o. .d.o. .n.o.t. .l.i.v.e. .w.i.t.h. .t.h.e. .p.e.r.s.o.n. .-. .G.O.V...U.K.....h.....`.....0.....i

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2099415891603
Encrypted:	false
SSDEEP:	6:mpIg5FZ3+q2PWXp+N23iKKdK8aPrqIFUtp8Ig5FFLWXZmwP8Ig5F9VkwOWXp+N2A:sf73+va5KkL3FUtp8fLK/P8fTV5f5Kkc
MD5:	0566AD46B5B5CEF2C97EDA0A2F6E431E
SHA1:	A0585228427539956985F4DFCA00319A3CF5D620
SHA-256:	77961E06A07EFB981A4882C85B1B0F8DF93982307675092FC64DDA88C509A319
SHA-512:	A806525481F2576601F1D0712320111AA78C1FBC1B4A9CC2D51DFA1E4FFBB6EAC58C3561F8BFAC4A6201C6A0FCBB6490664B6CFB2111CAE5FA16CB5A1969CE8C
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.669 172c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/17-10:11:40.671 172c Recovering log #3.2021/08/17-10:11:40.672 172c 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 Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2099415891603
Encrypted:	false
SSDEEP:	6:mpIg5FZ3+q2PWXp+N23iKKdK8aPrqIFUtp8Ig5FFLWXZmwP8Ig5F9VkwOWXp+N2A:sf73+va5KkL3FUtp8fLK/P8fTV5f5Kkc
MD5:	0566AD46B5B5CEF2C97EDA0A2F6E431E
SHA1:	A0585228427539956985F4DFCA00319A3CF5D620
SHA-256:	77961E06A07EFB981A4882C85B1B0F8DF93982307675092FC64DDA88C509A319
SHA-512:	A806525481F2576601F1D0712320111AA78C1FBC1B4A9CC2D51DFA1E4FFBB6EAC58C3561F8BFAC4A6201C6A0FCBB6490664B6CFB2111CAE5FA16CB5A1969CE8C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.669 172c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/17-10:11:40.671 172c Recovering log #3.2021/08/17-10:11:40.672 172c 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:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	5.145860414195606
Encrypted:	false
SSDEEP:	6:mpIg5lOq2PWXp+N23iKKdK8NIFUtp8Ig5zZmwP8Ig5SzkwOWXp+N23iKKdK8+eLJ:sfwva5KkpFUtp8fz/P8fa5f5KkqJ
MD5:	7F274FD0A8063AD55314862BF3410E0A
SHA1:	88C00655BF360E3BBE73F926270723C776719EA3
SHA-256:	DC00835B376AEB7A877D81426DB3C407EA5AE66B3BA272F76AA34081E8930FFC
SHA-512:	D70625CC7CB9128C4062FFBAE85ABA0A2C4B76B8E1DD795175569F79450E99C04EC2A9128F6D4EE81D9AB860CD45D93E0B51E708CCC57D84BAC02446F10CF28
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:44.041 1714 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/17-10:11:44.043 1714 Recovering log #3.2021/08/17-10:11:44.044 1714 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\Extension State\LOG.oldx (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.145860414195606
Encrypted:	false
SSDEEP:	6:mpIg5lOq2PWXp+N23iKKdK8NIFUtp8Ig5zZmwP8Ig5SzkwOWXp+N23iKKdK8+eLJ:sfwva5KkpFUtp8fz/P8fa5f5KkqJ
MD5:	7F274FD0A8063AD55314862BF3410E0A
SHA1:	88C00655BF360E3BBE73F926270723C776719EA3
SHA-256:	DC00835B376AEB7A877D81426DB3C407EA5AE66B3BA272F76AA34081E8930FFC
SHA-512:	D70625CC7CB9128C4062FFBAE85ABA0A2C4B76B8E1DD795175569F79450E99C04EC2A9128F6D4EE81D9AB860CD45D93E0B51E708CCC57D84BAC02446F10CF28
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:44.041 1714 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/17-10:11:44.043 1714 Recovering log #3.2021/08/17-10:11:44.044 1714 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	75776
Entropy (8bit):	3.1213095551162207
Encrypted:	false
SSDEEP:	192:maLjrpEhcv/6mxfCSqvLBiI6q60qLB49m7RqLhvHSgo5I6qzmujB4LqLhqQsHSLc:hjVaEyKqz1RmqCFCCHZF9
MD5:	E457FC8EB082AAE46B748227A374B6C5
SHA1:	8FE029DDA3F99DC4E8E040BCFFF9B8A015677D53
SHA-256:	76065E0CA37973A10EF793A227C90D6126E30C0358CD15A1E9EE4C20741833FD
SHA-512:	BFFBFB2B78DB5CC419D08343BA1324B1401BB233D6C39F346DE5583EC42A25DD946F027ECB359788B02AACF8D0CD46D24291F8224D21AEDA7F21E30AB6B4D38
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75616
Entropy (8bit):	2.4784306592791756
Encrypted:	false
SSDEEP:	192:ALdO8ZLBrqf0qLBNI6q3tjHSvlFRqLhLujz4LqLh0QsHSF5xJeujFH4LqLhQCujC:AjZKcV8DN3ZF34hZFc
MD5:	AC33DAA1EDA1BBDEEFB2A905C537FB8C
SHA1:	A5F11C18DD106BB92834B62CDFF9C3280E287045
SHA-256:	A82B05B7344CAF1DB848ECC839D3EA956D1B7BEB450A472B5D7588BC9517A234
SHA-512:	3CF7EC95EA4F485F86BA2CA5ACE06EE373CD00D30076F126F7AF873ED2F3D7AAF5E1AB84DCB64D6A54CB6423E0922B90DA50EED0A1CF0384484E2BCEACF43625
Malicious:	false
Reputation:	low
Preview:	.....3;IY..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.259822397525336
Encrypted:	false
SSDEEP:	6:mpIgfrL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp8Igf3nzKWZmwP8IgfBqLVkwOx:shL+va5KkTXfchI3FUtp8JmW/P8/qLV6
MD5:	541961F069F55A6155F2C66407C7D991
SHA1:	F6C6AADB848A72E8970D2976059D8E83F16D7CA5
SHA-256:	449652774076200 07AFFE3098E688CFF2CCCF91DBB842F48508FCA054C856C11
SHA-512:	D7284C859038CDE9F750701FD9B389523CA1C3E88E9180A4323406C9F085E364059E1558B27B87E2EC657A57B757E9833060A89FE07EF227D3D976DC9EFE6A50
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.845 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/17-10:11:57.986 10ec Recovering log #3.2021/08/17-10:11:57.992 10ec 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\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.259822397525336
Encrypted:	false
SSDEEP:	6:mpIgfrL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp8Igf3nzKWZmwP8IgfBqLVkwOx:shL+va5KkTXfchI3FUtp8JmW/P8/qLV6
MD5:	541961F069F55A6155F2C66407C7D991
SHA1:	F6C6AADB848A72E8970D2976059D8E83F16D7CA5
SHA-256:	449652774076200 07AFFE3098E688CFF2CCCF91DBB842F48508FCA054C856C11

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
SHA-512:	D7284C859038CDE9F750701FD9B389523CA1C3E88E9180A4323406C9F085E364059E1558B27B87E2EC657A57B757E9833060A89FE07EF227D3D976DC9EFE6A50
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.845 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/17-10:11:57.986 10ec Recovering log #3.2021/08/17-10:11:57.992 10ec 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):	5.1808854455186095
Encrypted:	false
SSDEEP:	6:mpIgfvuVjjL+q2PWXp+N23iKKdK25+XuoIFUtp8IgfQoKWZmwP8IgfrWlLVkwOWZ:s1uVjjL+va5KkTXYFUtp82W/P8xWlLVL
MD5:	B4363B06D13C5C16073B0CCEED31E4E9
SHA1:	53E23580A180CA0FA3E614DB31DF0835C4D1AC87
SHA-256:	7039AE28B3A9DFD8DD63788AF075D9C4129F9E2D07EFF5E4FC685652EE7D7985
SHA-512:	CA2B920924F8AE189F5C87AEF60142B3A368ADAD459BD22BA5BB6EBC272AB2CB15A2631DCFBED1ABEFC383D94BCB9655B980973B3928F0F2610FA24602F10143
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.060 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/17-10:11:57.063 10ec Recovering log #3.2021/08/17-10:11:57.064 10ec 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.1808854455186095
Encrypted:	false
SSDEEP:	6:mpIgfvuVjjL+q2PWXp+N23iKKdK25+XuoIFUtp8IgfQoKWZmwP8IgfrWlLVkwOWZ:s1uVjjL+va5KkTXYFUtp82W/P8xWlLVL
MD5:	B4363B06D13C5C16073B0CCEED31E4E9
SHA1:	53E23580A180CA0FA3E614DB31DF0835C4D1AC87
SHA-256:	7039AE28B3A9DFD8DD63788AF075D9C4129F9E2D07EFF5E4FC685652EE7D7985
SHA-512:	CA2B920924F8AE189F5C87AEF60142B3A368ADAD459BD22BA5BB6EBC272AB2CB15A2631DCFBED1ABEFC383D94BCB9655B980973B3928F0F2610FA24602F10143
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.060 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/17-10:11:57.063 10ec Recovering log #3.2021/08/17-10:11:57.064 10ec 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):	5.213161439826708
Encrypted:	false
SSDEEP:	6:mpIgfzyFlL+q2PWXp+N23iKKdKWT5g1IdqIFUtp8Igf9uzKWZmwP8Igf9ulLVkwb:spWlL+va5Kkg5gSRFUtp8LW/P8aLV5fz
MD5:	96A4F5FACD3CD737C589690B0C6261E7
SHA1:	61DCAFD9A76045DF80A1A0B93A4773EEFEAB24BA
SHA-256:	ABF37896FC87B02F4D38B0E326F2ECD31F15ABFB29BB4282C3ECB553FAE07BBA
SHA-512:	130737FE7EB4315EBD6F81426D2F745D812F63E436289666A93833AA081B429A6F83BE48CF114BF4735956BCB3B4251A9BBD1CC99A138B0658499C64D13E60A1
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.046 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/17-10:11:57.048 10ec Recovering log #3.2021/08/17-10:11:57.048 10ec 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\GCM Store\Encryption\LOG.old (copy)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.213161439826708
Encrypted:	false
SSDEEP:	6:mpIgfzyFlL+q2PWXp+N23iKKdKWT5g1IdqIFUtp8Igf9uzKWZmwP8Igf9ulLVkwb:spWlL+va5Kkg5gSRFUtp8LW/P8aLV5fz
MD5:	96A4F5FACD3CD737C589690B0C6261E7
SHA1:	61DCAFD9A76045DF80A1A0B93A4773EEFEAB24BA
SHA-256:	ABF37896FC87B02F4D38B0E326F2ECD31F15ABFB29BB4282C3ECB553FAE07BBA
SHA-512:	130737FE7EB4315EBD6F81426D2F745D812F63E436289666A93833AA081B429A6F83BE48CF114BF4735956BCB3B4251A9BBD1CC99A138B0658499C64D13E60A1
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.046 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/17-10:11:57.048 10ec Recovering log #3.2021/08/17-10:11:57.048 10ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	217088
Entropy (8bit):	1.4810452813633321
Encrypted:	false
SSDEEP:	192:mdWn83BJdginVnLBEHMe1JSdfin3xc3B0qLB0FcuinzT/aGvc50qLBj0RNMe1JS0:sqP+pygbAfVl4nJFi1xFK3
MD5:	7FED28DE63BD2646F58D544514CCEAAA
SHA1:	712E371EBD7E726B44E14FF073CF4098ADB457BA
SHA-256:	D1A6986974913EBDE05C33C9C4FF65649F9DFEFE76FD9DAFE56B524C32A35F81
SHA-512:	9360FE4503F57F4E358BF3BEC702E65DF244E2510F2EAD673F72BF46A531BD2FE63D1849CC9340746096E73251D1DD8B2D7F5C6F1FF4B0A03194A3D2F15C9199
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2389
Entropy (8bit):	5.766030799049495
Encrypted:	false
SSDEEP:	48:Qq63PIb9zK5cYHL+aTRcKua9UzqMQ7MQqChqMQ7MQNn5:Q/PIb9zK5G0cKhuYddhYdNn5
MD5:	70ADFD6AFCD804DBC521D78C6FC27B62
SHA1:	4362E73173954D21EE8EFD460BF89CBAD4F34D44
SHA-256:	59849D52D7D6943B488A4065CAEBF9CA1F1D1A365B75997551C7862ED18A2145
SHA-512:	09CBF1AD345B31F1D108D60E07A57A0CA106CC06FA118BDF01D031DF83E4A13F613F9B1F2692AD0D26D162EC8CD446735731D48743A66B70C65E6FFFFEDE507
Malicious:	false
Reputation:	low
Preview:	....."....19..confirmed..contacts..content..coronavirus..covid..do..for..gov..government..guidance..https..infection..live..not..of..or..people..person..possible..publications..the..uk..who..with..www..2.....1.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....x...:

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):	229376
Entropy (8bit):	1.0885506714639055
Encrypted:	false
SSDEEP:	192:KZBOdhXuLB/dWpi93B0qLBpHMe1JSd3uziC+aGvc50qLBhNoDFcuihL3ujrGvc5j:KXJpjPv5KfRMoGO/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
MD5:	F4172C8283FCEA1CE290401F3A8345FF
SHA1:	4B1392DA2471F8FEFC0FFBBAA83B6047631F4668
SHA-256:	4714CFA1DFE06C67AC06D05799E4686743DEE230864669A78B5FBD23BCD7E7D1
SHA-512:	6F0ABE85092864A5489486B3F95780FC9C14A54DD3B0EE987148DABC856AFDD7BBE00935472AAB2BA2C5B6E8CE724EE2333541ACBCC93EB12DB0222CF028F4BD
Malicious:	false
Reputation:	low
Preview:	.....X/..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last SessionNH (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92407
Entropy (8bit):	3.610431925813685
Encrypted:	false
SSDEEP:	768:qrrkE4Sa+n+Wepa83H8DBrSw8yRcAUJpx9Z4Yf:qrAE4Sa+n+Wepa83Hu5R8yG7pfZ4Yf
MD5:	ED2C8A50F73B61B87AE5EE9650DC855B
SHA1:	359479DF6525A413018AA598DE606D6053D753E4
SHA-256:	BE82FE419000A5D5A60501F3AD4E8431176766DD4C974C09C20F370CA7C60D21
SHA-512:	04364F9B5072B93134489FFB8DF0AD22BF89CDC4439C9610934836BFF3CEB4DF4DDBD2AB87C303EF69E810568310FBFBA93B9E5F33DA2B313EF9D61D5AC5CF4
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...62037b48_84f0_4cc6_9db3_4e5d5b01fae3.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....%...https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt...x...G.u.i.d.a.n.c.e. .f.o.r. .c.o.n.t.a.c.t.s. .o.f. .p.e.o.p.l.e. .w.i.t.h. .c.o.n.f.i.r.m.e.d. .c.o.r.o.n.a.v.i.r.u.s. .(.C.O.V.I.D.-.1.9.). .i.n.f.e.c.t.i.o.n. .w.h.o. .d.o. .n.o.t. .l.i.v.e. .w.i.t.h. .t.h.e. .p.e.r.s.o.n. .-. .G.O.V...U.K.....h.....`.....0.....i

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.478828120583191
Encrypted:	false
SSDEEP:	48:Zl5GWma79Ml8dbHo4VbQSefgGw5NrS0U9RdiN9b:8a79MDdbHo4VbQ5fgGwTrS09
MD5:	DC2A3C657A3920482100F6EE15359CF6
SHA1:	F518F31E0B70E7D44F7E45B28EAA5B32CFAF7278
SHA-256:	C0B9BEAD31F9ACE5BFA9EAC56A7ACE890DB5D9E27EE549F8EFE21713ED275B94
SHA-512:	157419E54A5196A3B868706297CD7E65661CCF3D778BF19A53EE2B3B4DE5BF0FA4E8878E6E700C09598579D0FE2F6B993D43EE923122C72AB3D9E36FFB8D3ACA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	..$....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..496968000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-17 10:11:59.63][INFO][mr.Init] MR instance ID: c713922e-8ede-4262-864e-ecf3814bfb26\n","[2021-08-17 10:11:59.63][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-17 10:11:59.63][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-17 10:11:59.64][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-17 10:11:59.64][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-17 10:11:59.64][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-17 10:11:59.64][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.186525055787896
Encrypted:	false
SSDEEP:	6:mpIg50Si4q2PWXp+N23iKKdK8a2jMGIFUtp8Ig5kRNJZmwP8Ig5NLDkwOWXp+N2s:sfri4va5Kk8EFUtp8fqJ/P8fJD5f5Kkw
MD5:	EDD03712B3F03D3C3AB62C0DCF029A79
SHA1:	390E8A56A12996C38AD7B7DD2744FB5ACE186DBE
SHA-256:	5CD41CE4DD49FF0862899C9994C1C97F12C8327A3B76879587BFE19143F1D8A6
SHA-512:	545CFC93198615B268B0BA8EDB0BF176449A394590DCBD4EFF7E51D1665AA35CC5B080D05595225E3E419E25569D8BB073CB490415BF47DCBAB24455BFEE5FCE
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.347 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:40.350 1464 Recovering log #3.2021/08/17-10:11:40.351 1464 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.186525055787896
Encrypted:	false
SSDEEP:	6:mpIg50Si4q2PWXp+N23iKKdK8a2jMGIFUtp8Ig5kRNJZmwP8Ig5NLDkwOWXp+N2s:sfri4va5Kk8EFUtp8fqJ/P8fJD5f5Kkw
MD5:	EDD03712B3F03D3C3AB62C0DCF029A79
SHA1:	390E8A56A12996C38AD7B7DD2744FB5ACE186DBE
SHA-256:	5CD41CE4DD49FF0862899C9994C1C97F12C8327A3B76879587BFE19143F1D8A6
SHA-512:	545CFC93198615B268B0BA8EDB0BF176449A394590DCBD4EFF7E51D1665AA35CC5B080D05595225E3E419E25569D8BB073CB490415BF47DCBAB24455BFEE5FCE
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.347 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:40.350 1464 Recovering log #3.2021/08/17-10:11:40.351 1464 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\Network Action Predictor	
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):	49152
Entropy (8bit):	1.1075751489415895
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOuOqAuhjspnWOtOqAuhjspnWOsOqAuhjspnWOI:HBsfz
MD5:	7A89B069CA76818D80040CB3AB19D46D
SHA1:	D17F7D8F785F729FB5B2458AC56F3CB58D70369B
SHA-256:	4FE528EE79AD1C33B2CBEB610E2D9C69917C3993BF6026B838602968F0FBF4BE
SHA-512:	4CE4E94C3BDC7679786D8E1CC3AF663945946B250771FCBAD34474865B5AB865B612F99AB3A08EC6B18F6617B8527C3C913F82C5D6959D0D8762C0B91062612D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	51344
Entropy (8bit):	1.0601346907950957
Encrypted:	false
SSDEEP:	96:l0UOqAuhjspnWO7kOqAuhjspnWOja0OqAuhjspnWOEEOqAuhjspnWOo:6yainSxCr
MD5:	46553DE33E16C63F85DF62E9F74F6119
SHA1:	2DD249EC98049F4077ED48B67CFCE04139911C6A
SHA-256:	3437594329A7294E66DA1444502B2B5C4894D07793FECBEE56D46DB3977EEB44
SHA-512:	5E9F4E38DC1633D4CDEA06E2F31EA17A3BD0108318903BFB8DDA2DB4510AF126F0D8D144BED36E1AE35909220FBD5361E7132D097CA6529450E06A63785BFC 9
Malicious:	false
Reputation:	low
Preview:	.....RN..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
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):	2350
Entropy (8bit):	4.902752451710999
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5sN5TsJRLsAdKRD9sJtyKsU3zsTMHdTssqzkqFYhbG:JTnOCXGDHz85QZKedyGdTqjChS
MD5:	9B1377FB64A08961153DA0A6F9D7A603
SHA1:	D086D76AE8B45F44B6455C1DF4E6C2DD94DD8D71
SHA-256:	403C1841EA52EB9734C174F523705BFF83ED30F215E67410BEB89ECC8F508931
SHA-512:	4981A18AAACAC9C45B3CC0EED8724A8DAEBCE3D8BCF64F6FAF558A315926C4B825CC368F7C2541D4E9EE367349248509C1C9D881026EA9D7D6D2BFAB83BEE 187
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_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.c om","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1327628590 5019600","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13276285905027610","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateP (copy)	
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):	4.871755235889535
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMZ:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhS
MD5:	AE133C52F86E27CD225F807F1DDB33A3
SHA1:	A0EB1D7B7D41F31993C975A8B5F27954F90B6DF8
SHA-256:	A795DA84B0B14FD651959C4E712B297CA76E50FAF03E18469336F5FB1BE5420A
SHA-512:	098D9CC2B0436B77AE03D9289C2DBF2316B0F0145C7AEE81F8F19A26964AB7F975F941CD2A9E14783E600602A195ED60A059B0EFEFFCEEC2BD0C5923E09663E 3
Malicious:	false
Reputation:	low
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\Network Persistent State[(copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State[(copy)	
Size (bytes):	4219
Entropy (8bit):	4.871755235889535
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMZ:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhS
MD5:	AE133C52F86E27CD225F807F1DDB33A3
SHA1:	A0EB1D7B7D41F31993C975A8B5F27954F90B6DF8
SHA-256:	A795DA84B0B14FD651959C4E712B297CA76E50FAF03E18469336F5FB1BE5420A
SHA-512:	098D9CC2B0436B77AE03D9289C2DBF2316B0F0145C7AEE81F8F19A26964AB7F975F941CD2A9E14783E600602A195ED60A059B0EFEFFCEEC2BD0C5923E09663E3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.1562379563190115
Encrypted:	false
SSDEEP:	6:mpIg581Iq2PWXp+N23iKKdKgXz4rRIFUtp8Ig53WZmwP8Ig5fkwOWXp+N23iKKdA:sfsIva5KkgXiuFUtp8f3W/P8ff5f5Kkt
MD5:	DC52C2621F560122D256CC70D5B0D6E7
SHA1:	F23FE9E93F94163492520DAA90E12ABBA4CB6B22
SHA-256:	2862EBEA297BB5CA802ACC10CABA9E3B1C3B074C1F685C795D33CC8F6AF25988
SHA-512:	DFA3E0CD2A5539655357A5A1C93910DBF09A6778F3E9E0B27E9DD40A4EC94F77172C5D57F1146A680A2BADBADEFA0B4F35656641858D95CE662EC8C6560AE7A
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.709 1714 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/17-10:11:40.710 1714 Recovering log #3.2021/08/17-10:11:40.711 1714 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\Platform Notifications\LOG.old." (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.1562379563190115
Encrypted:	false
SSDEEP:	6:mpIg581Iq2PWXp+N23iKKdKgXz4rRIFUtp8Ig53WZmwP8Ig5fkwOWXp+N23iKKdA:sfsIva5KkgXiuFUtp8f3W/P8ff5f5Kkt
MD5:	DC52C2621F560122D256CC70D5B0D6E7
SHA1:	F23FE9E93F94163492520DAA90E12ABBA4CB6B22
SHA-256:	2862EBEA297BB5CA802ACC10CABA9E3B1C3B074C1F685C795D33CC8F6AF25988
SHA-512:	DFA3E0CD2A5539655357A5A1C93910DBF09A6778F3E9E0B27E9DD40A4EC94F77172C5D57F1146A680A2BADBADEFA0B4F35656641858D95CE662EC8C6560AE7A
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.709 1714 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/17-10:11:40.710 1714 Recovering log #3.2021/08/17-10:11:40.711 1714 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\Preferences (copy)	
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):	5820
Entropy (8bit):	5.199382548246241
Encrypted:	false
SSDEEP:	96:n43zCDbIL9w7dicPcKIzok0JCKL80NkkWS1eB0bOTQVuwn:n4jCYL9w7IcPcI4KNNkkBcBe
MD5:	B3C781FA20A480AF86681C797505C28F
SHA1:	A52D494811827B32431E5F67550D4939779DFF4F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
SHA-256:	7D9AB75748A422A04D0CF41404A3BD490F0D13588C5A763C2148701DD73F66D2
SHA-512:	3CAD0E2D0F61CBAB668DFD9EFE71BBA4A37CB9C3CCD0668AEE5212EA1218D728554749CACC388F3CC9B07A2D7151F92363C324FAFE11CDB21522D348E956A 57
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\PreferencesTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5794
Entropy (8bit):	5.19722767006448
Encrypted:	false
SSDEEP:	96:n43zCD/IL9w7dicPcKI6ok0JCKL80NkkWS1e3bOTQVuwn:n4jCkL9w7IcPcz4KNNkkBcT
MD5:	970CB3690B2A977841C4E61DBD43D634
SHA1:	12932E774E2943C1442B726730768E30FFF3BCF7
SHA-256:	E7CEE546B138CBB8B2ABAB124737279A69FF629D8259B64D3277347561ABF2A9
SHA-512:	5313E7EC1C27018F9E8AC134867A0CD53F57B9A75D1A0FDB3BED654189EE1E0708E2995572B340930E5E0C2CE658D165F35C6AB861A9E94922FE2EA36D6359D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273693900660636","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\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):	1.0115010927535908
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoj:wIElwQF8mpcSJ2Yj1
MD5:	DC15E2DF573FBE0EFBA13F99984D9FD0
SHA1:	2C9FFA5326CDE400771ABB4EFEE76C61DF5DEB21
SHA-256:	DC7A2A640AE5FF794B4ACBFBAA93F2EB710BAF2C8875EC766B1766C7DDAEAF34
SHA-512:	33748070371DC904DFE1777CBAA277518CC8377BBF5AC5BF5409DCDE2F027CD59F3827B50AC9BD4FC50906692945454CE268E0F0E1C9C27FAA43B42B4FF4312
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....C..........g...^.........j...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8247557263658405
Encrypted:	false
SSDEEP:	48:X8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU/6:X8hIElwQF8mpcSG
MD5:	6996B41177F9D536C23D6B68FB4D9A30
SHA1:	B8D93B0A3F87F1EE49269341649866083488 61B8
SHA-256:	D5AD879B2F5B8551A7E7094074ADECA75AD6E5B5F37D5AF4DE9A0A1F5F3FF8D9
SHA-512:	64C39595CAC3B6D4E37C0548892CA52F887FF4A5D6143D2F894CAF1A8765D479703794C89AD05A364C2CB3113A965C7C1952DC723D5489F39412551D3B92B107
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Preview:	.....m..*..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	16745
Entropy (8bit):	5.577393978151346
Encrypted:	false
SSDEEP:	384:uZvtbLleBXw1kXqKf/pUZNCgVLH2HfDErUrjqTp/4q:mLlOw1kXqKf/pUZNCgVLH2HfYrUGp/N
MD5:	ACA4D984F1DC1110CD58E79078840A2F
SHA1:	28AC49A9A71B8B8204D3C3CC57D7570144395E34
SHA-256:	0591A1E0EBB3E1A3A1ABA9F3A961403D06619A76A7B106CA55BFFAFB6748B20E
SHA-512:	9EBBDC24B27E6864C583E03C1BDA5189FFD1ABE3B25CE3A80EDDB93802B701959AC8612BA8748F5B929DB4247F28A059F88D496B0FC8F939FB7F5AD4AEF508A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273693900341891","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesTM (copy)	
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):	5.536120910430683
Encrypted:	false
SSDEEP:	384:uZvt6LleBXw1kXqKf/pUZNCgVLH2HfDErU+HGmnT7jqTF/40G:5LlOw1kXqKf/pUZNCgVLH2HfYrUuGmnh
MD5:	09EA42A9C788C7551710192A8E3446B2
SHA1:	14D4DBA1FBCEC99222939026FB3CFD64D7C0D0DE
SHA-256:	CE34C4657444F1910D9FD4F1B86B5E12F3CDD73AC986385D50F691D92199C180
SHA-512:	CF0F1352C90804E7F155C367E9F3BCB925E1D69AC2028638C2018FF9F7D6E2D083DA3772AA35D829915002CA5C60C2EFCAA68EF03A82A5F3350BCC41A81BA71A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273693900341891","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	557
Entropy (8bit):	5.051222361564813
Encrypted:	false
SSDEEP:	12:5ljljljle7cDdiSw93+4UUesusZ8+nAUS:7ZZZe7cDdVwl+ZbOC+n
MD5:	CA95D157A4043FABCD77E3C292F8EFCE
SHA1:	D55F0AD7C8FED2ADD26580ABF0E705833C5800FA
SHA-256:	BC08A3BDAC4F02F1691B25F6882C76B8BBB54EA967061F8A902690648A0583C6
SHA-512:	A0D3292564783260DD9B91356A462379CF3B8102F5DB16CF7C6CFEB3EB0418D332D291F970CF64734E6668EA5FD7C8ACA522EFD3BF8D2E0AFFC313190F1C618
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Preview:	..&f.....&f.....&f.....&f.....P[$.a.....next-map-id.1.Bnamespace-c47b3f2b_6012_4fb2_b6ca_77e018a99407-https://www.gov.uk/.0...a.....next-map-id.2.Bnamespace-9b1fa18c_67dd_4bf4_9c65_0a3c31101231-https://www.gov.uk/.1...+.....map-0-this is the test string.N..a.....next-map-id.3.Bnamespace-6431b6ea_7ab8_4217_9110_f2dbae914627-https://www.gov.uk/.2(.H.+.....map-1-this is the test string4.+i+.....map-2-this is the test string0y.....

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):	5.160914660288381
Encrypted:	false
SSDEEP:	6:mpIg51+9+q2PWXp+N23iKKdKrQMxIFUtp8Ig5tN2WZmwP8Ig5tN9VkwOWXp+N23z:sfs9+va5KkCFUtp8fHJ/P8fH9V5f5Kkf
MD5:	55BD86241F59A8C1C0766BC9AFF421C7
SHA1:	72EF43CA217A9CB2C49BEF9DA1A55F62FD191887
SHA-256:	084F896A2C6324793968D0ECEFE80B197B3C8704869791C9E55C1E93442E3C76
SHA-512:	E3F40256EFC8E1C9CCD6F1FD6F1A08B5EE11D0307947BCD4FA7C3D2B6CE7DB248F4222CD1657CECE7D6E434E4A3CB00040DA54043878DAD252384DA21254121
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.576 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/17-10:11:40.577 150c Recovering log #3.2021/08/17-10:11:40.577 150c 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.160914660288381
Encrypted:	false
SSDEEP:	6:mpIg51+9+q2PWXp+N23iKKdKrQMxIFUtp8Ig5tN2WZmwP8Ig5tN9VkwOWXp+N23z:sfs9+va5KkCFUtp8fHJ/P8fH9V5f5Kkf
MD5:	55BD86241F59A8C1C0766BC9AFF421C7
SHA1:	72EF43CA217A9CB2C49BEF9DA1A55F62FD191887
SHA-256:	084F896A2C6324793968D0ECEFE80B197B3C8704869791C9E55C1E93442E3C76
SHA-512:	E3F40256EFC8E1C9CCD6F1FD6F1A08B5EE11D0307947BCD4FA7C3D2B6CE7DB248F4222CD1657CECE7D6E434E4A3CB00040DA54043878DAD252384DA21254121
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.576 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/17-10:11:40.577 150c Recovering log #3.2021/08/17-10:11:40.577 150c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.137777767639469
Encrypted:	false
SSDEEP:	6:mpIg50Mq2PWXp+N23iKKdK7Uh2ghZIFUtp8Ig50BZmwP8Ig50SfkwOWXp+N23iKm:sfJva5KkIhHh2FUtp8fo/P8frf5f5Kks
MD5:	5DEF23A55925763F7306CB55B4BE920B
SHA1:	51A0376BD2A6C52FCAEB7EF3D44AD9D60412DF9A
SHA-256:	0DDE693F2D2CA8E2DC5005C04F1E325DEC9401B806A9F65C29E57616785E2038
SHA-512:	3148D3F1ED69A8A29888D4D5299DACF029C0DEB65579B2ABEA81EA5B24B85CF562ADF794D230BC6833A91327D7082AB565FBB1CF9CE77FEA4D38DA5161694EA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.342 f00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/17-10:11:40.346 f00 Recovering log #3.2021/08/17-10:11:40.347 f00 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\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.137777767639469
Encrypted:	false
SSDEEP:	6:mpIg50Mq2PWXp+N23iKKdK7Uh2ghZIFUtp8Ig50BZmwP8Ig50SfkwOWXp+N23iKm:sfJva5KkIhHh2FUtp8fo/P8frf5f5Kks
MD5:	5DEF23A55925763F7306CB55B4BE920B
SHA1:	51A0376BD2A6C52FCAEB7EF3D44AD9D60412DF9A
SHA-256:	0DDE693F2D2CA8E2DC5005C04F1E325DEC9401B806A9F65C29E57616785E2038
SHA-512:	3148D3F1ED69A8A29888D4D5299DACF029C0DEB65579B2ABEA81EA5B24B85CF562ADF794D230BC6833A91327D7082AB565FBB1CF9CE77FEA4D38DA51616940EA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.342 f00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/17-10:11:40.346 f00 Recovering log #3.2021/08/17-10:11:40.347 f00 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\33ae1c87-f4ea-48f8-addb-a4792888f475.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):	4.986775197192121
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Kn:YHO8sdBsB6MAsBdLJlyH7E4f3K3X
MD5:	0D1F7A36AD610D2F08709B1EF88F1B09
SHA1:	237E8E7BC7891D987DEA1D2EB1DA9DA511396D11
SHA-256:	5C36B7E531EE8DF00FE937FDE21AF4D1B6606EAD4B5F98D56396DDCEF1C4249A
SHA-512:	37DAD8F9F2008D7B287A03964F0AE41FA4EBED92987B3872E022758857131971BC486638D0339774E80DF01A669B68DB4729D48E49EC5DE714F27ADF20B247AC
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5b4eb01f-948e-4969-a9ff-16e9e3d3b179.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\6105b951-0a00-4a0c-a395-8f364a987908.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\6105b951-0a00-4a0c-a395-8f364a987908.tmp	
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.232765169896165
Encrypted:	false
SSDEEP:	6:mpIg5Fd+q2PWXp+N23iKKdKusNpV/2jMGIFUtp8Ig5FSZmwP8Ig5FuVkwOWXp+Nh:sfb+va5KkFFUtp8f4/P8fIV5f5KkOJ
MD5:	495EC8DB8D48CC1FCCB63775009F9BED
SHA1:	FCBBDAF340149433F1B63F657D65E6A7F2AB6A2F
SHA-256:	26198F9317649233D2F542A4D88FFB6D24A3E11B01CE36DCFE1C65571ACFD72C
SHA-512:	27B348FAA63EE50D7D1C68361BF87B653DECD20B8D08BAC91DD1C9D2B27C749100CA97068B14DDB3EFB0D55319DFCA7EFFE2B8F2C9F4FE4111B784DA38801DA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.618 172c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:40.620 172c Recovering log #3.2021/08/17-10:11:40.620 172c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.232765169896165
Encrypted:	false
SSDEEP:	6:mpIg5Fd+q2PWXp+N23iKKdKusNpV/2jMGIFUtp8Ig5FSZmwP8Ig5FuVkwOWXp+Nh:sfb+va5KkFFUtp8f4/P8fIV5f5KkOJ
MD5:	495EC8DB8D48CC1FCCB63775009F9BED
SHA1:	FCBBDAF340149433F1B63F657D65E6A7F2AB6A2F
SHA-256:	26198F9317649233D2F542A4D88FFB6D24A3E11B01CE36DCFE1C65571ACFD72C
SHA-512:	27B348FAA63EE50D7D1C68361BF87B653DECD20B8D08BAC91DD1C9D2B27C749100CA97068B14DDB3EFB0D55319DFCA7EFFE2B8F2C9F4FE4111B784DA38801DA
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.618 172c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:40.620 172c Recovering log #3.2021/08/17-10:11:40.620 172c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State79 (copy)	
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):	4.986775197192121
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Kn:YHO8sdBsB6MAsBdLJlyH7E4f3K3X
MD5:	0D1F7A36AD610D2F08709B1EF88F1B09
SHA1:	237E8E7BC7891D987DEA1D2EB1DA9DA511396D11
SHA-256:	5C36B7E531EE8DF00FE937FDE21AF4D1B6606EAD4B5F98D56396DDCEF1C4249A
SHA-512:	37DAD8F9F2008D7B287A03964F0AE41FA4EBED92987B3872E022758857131971BC486638D0339774E80DF01A669B68DB4729D48E49EC5DE714F27ADF20B247AC
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.2785229228347115
Encrypted:	false
SSDEEP:	12:sfy9+va5KkmiuFUtp8fm1/P8f1V5f5Kkm2J:sfyKa5KkSgufJftf5Kkr
MD5:	B1B783D37AF4A3194AFBD46D2EDC169F
SHA1:	D06527641C1BC8054883FD46F04A7EDD56F805DE
SHA-256:	320EB55A61F37F81E005455E779F9B9D461F0C6469598C5CEE145AEF8DA1EF4F
SHA-512:	EF4E4DFAAB876EB77215E87ABEE5C49A844B04CDD08772C567C0873916DBCEAAE5B963C09690D784703FF93D80627617048390398A355673E62123CE31113C1D
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.698 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/17-10:11:40.702 87c Recovering log #3.2021/08/17-10:11:40.703 87c 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.2785229228347115
Encrypted:	false
SSDEEP:	12:sfy9+va5KkmiuFUtp8fm1/P8f1V5f5Kkm2J:sfyKa5KkSgufJftf5Kkr
MD5:	B1B783D37AF4A3194AFBD46D2EDC169F
SHA1:	D06527641C1BC8054883FD46F04A7EDD56F805DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
SHA-256:	320EB55A61F37F81E005455E779F9B9D461F0C6469598C5CEE145AEF8DA1EF4F
SHA-512:	EF4E4DFAAB876EB77215E87ABEE5C49A844B04CDD08772C567C0873916DBCEAAE5B963C09690D784703FF93D80627617048390398A355673E62123CE31113C1D
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:40.698 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/17-10:11:40.702 87c Recovering log #3.2021/08/17-10:11:40.703 87c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.254328112343714
Encrypted:	false
SSDEEP:	6:mpIgNdKq2PWXp+N23iKKdKusNpZQMxIFUtp8IgNSvvZZmwP8IgNFkwOWXp+N23iA:sLdKva5KkMFUtp8LU/P8LF5f5KkTJ
MD5:	DE27FC9A52D24EAED8B767D57B9A241D
SHA1:	6F6D325E11EE49FC5F0865BDC48F435FD3593FC8
SHA-256:	7580535FA0252C8A82FD45AFB1A4B118DDD90E5D6D7DA28B59FE3AEE06497920
SHA-512:	55B75736E2DA0E16520695D6FB7A84014B349931BB9E1D95073A45153F9623E3B6E4BDC3D31D7553EA69E6FBDDCEB88311DE9FBD066DE50B3C0CF25CCD341AF
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.036 6d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/17-10:11:58.037 6d0 Recovering log #3.2021/08/17-10:11:58.038 6d0 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\Session Storage\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.254328112343714
Encrypted:	false
SSDEEP:	6:mpIgNdKq2PWXp+N23iKKdKusNpZQMxIFUtp8IgNSvvZZmwP8IgNFkwOWXp+N23iA:sLdKva5KkMFUtp8LU/P8LF5f5KkTJ
MD5:	DE27FC9A52D24EAED8B767D57B9A241D
SHA1:	6F6D325E11EE49FC5F0865BDC48F435FD3593FC8
SHA-256:	7580535FA0252C8A82FD45AFB1A4B118DDD90E5D6D7DA28B59FE3AEE06497920
SHA-512:	55B75736E2DA0E16520695D6FB7A84014B349931BB9E1D95073A45153F9623E3B6E4BDC3D31D7553EA69E6FBDDCEB88311DE9FBD066DE50B3C0CF25CCD341AF
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:58.036 6d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/17-10:11:58.037 6d0 Recovering log #3.2021/08/17-10:11:58.038 6d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\30c6e1a0-924c-4f5b-af17-2e797d03477c.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):	4.954409809181979
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K3X:YXsdvjX6gjXdL3yH7n/y
MD5:	F7EA7FF47D0FD3626EC4879195182336
SHA1:	B1FFD61A260C441A09C636B0F32937D08E45AE3D
SHA-256:	E52C4807EA6A80D9FE9394046D2A5CE282135C3A8C5B714F77083C907AED7C81
SHA-512:	C7D891EFDF23A367CDB27D21535D838EB44FCF98F475DAD15E9DCFB829E1F0FB0FE55B1A073548C3725A8ED5451A63405B1DE4E3726D1124AE08939B3823937
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\40ba44b9-d58e-403b-bd06-b65948ddc914.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):	4.954409809181979
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K3X:YXsdvjX6gjXdL3yH7n/y
MD5:	F7EA7FF47D0FD3626EC4879195182336
SHA1:	B1FFD61A260C441A09C636B0F32937D08E45AE3D
SHA-256:	E52C4807EA6A80D9FE9394046D2A5CE282135C3A8C5B714F77083C907AED7C81
SHA-512:	C7D891EFDF23A367CDB27D21535D838EB44FCF98F475DAD15E9DCFB829E1F0FB0FE55B1A073548C3725A8ED5451A63405B1DE4E3726D1124AE08939B3823937
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.1882657059222
Encrypted:	false
SSDEEP:	12:sWva5KkkGHArBFUtp8L/P8bz5f5KkkGHAryJ:s0a5KkkGgPguYZf5KkkGga
MD5:	25A90D4DC6F7EF0E3B5F337583D6E399
SHA1:	80D6F467C4AA07505CAB56BCB0D053848E6E42CC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA-256:	5EECDC9C5F7C2E4CC68872A846CC0F78C8ECF8F0E487A602F7603CE8B1BD60B2
SHA-512:	93DE31C405A53905FB95575EBB4DFEC74531E2AB8399F293D6B679502B9F57950E8C7EC9F0413732E9E92C19C3FE4F17BDACCE037C2C3C05A686661C2F81EF7
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.781 6d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:57.785 6d0 Recovering log #3.2021/08/17-10:11:57.787 6d0 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.1882657059222
Encrypted:	false
SSDEEP:	12:sWva5KkkGHArBFUtp8L/P8bz5f5KkkGHAryJ:s0a5KkkGgPguYZf5KkkGga
MD5:	25A90D4DC6F7EF0E3B5F337583D6E399
SHA1:	80D6F467C4AA07505CAB56BCB0D053848E6E42CC
SHA-256:	5EECDC9C5F7C2E4CC68872A846CC0F78C8ECF8F0E487A602F7603CE8B1BD60B2
SHA-512:	93DE31C405A53905FB95575EBB4DFEC74531E2AB8399F293D6B679502B9F57950E8C7EC9F0413732E9E92C19C3FE4F17BDACCE037C2C3C05A686661C2F81EF7
Malicious:	false
Reputation:	low
Preview:	2021/08/17-10:11:57.781 6d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/17-10:11:57.785 6d0 Recovering log #3.2021/08/17-10:11:57.787 6d0 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\Network Persistent State7c (copy)	
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):	4.954409809181979
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K3X:YXsdvjX6gjXdL3yH7n/y
MD5:	F7EA7FF47D0FD3626EC4879195182336
SHA1:	B1FFD61A260C441A09C636B0F32937D08E45AE3D
SHA-256:	E52C4807EA6A80D9FE9394046D2A5CE282135C3A8C5B714F77083C907AED7C81
SHA-512:	C7D891EFDF23A367CDB27D21535D838EB44FCF98F475DAD15E9DCFB829E1F0FB0FE55B1A073548C3725A8ED5451A63405B1DE4E3726D1124AE08939B3823937
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

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

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/17/21-10:11:44.899830	TCP	2515	WEB-MISC PCT Client_Hello overflow attempt	49715	443	192.168.2.3	142.250.184.237

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 17, 2021 10:11:44.831609964 CEST	192.168.2.3	8.8.8.8	0x8155	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.836349010 CEST	192.168.2.3	8.8.8.8	0x3d8a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.842320919 CEST	192.168.2.3	8.8.8.8	0xde04	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:47.633496046 CEST	192.168.2.3	8.8.8.8	0x2678	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:57.178653002 CEST	192.168.2.3	8.8.8.8	0x2eaa	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:11.150069952 CEST	192.168.2.3	8.8.8.8	0xaefc	Standard query (0)	assets.publishing.service.gov.uk	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:14.843712091 CEST	192.168.2.3	8.8.8.8	0x9e0f	Standard query (0)	assets.publishing.service.gov.uk	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:48.576738119 CEST	192.168.2.3	8.8.8.8	0x2b74	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 17, 2021 10:11:44.866134882 CEST	8.8.8.8	192.168.2.3	0x8155	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:11:44.866134882 CEST	8.8.8.8	192.168.2.3	0x8155	No error (0)	clients.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.871397018 CEST	8.8.8.8	192.168.2.3	0x3d8a	No error (0)	accounts.google.com		142.250.184.237	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www-gov-uk .map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www-gov-uk .map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www-gov-uk .map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:44.875967979 CEST	8.8.8.8	192.168.2.3	0xde04	No error (0)	www-gov-uk .map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www-gov-uk .map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www-gov-uk .map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www-gov-uk .map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:47.670437098 CEST	8.8.8.8	192.168.2.3	0x2678	No error (0)	www-gov-uk .map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:11:57.212033033 CEST	8.8.8.8	192.168.2.3	0x2eaa	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:11:57.212033033 CEST	8.8.8.8	192.168.2.3	0x2eaa	No error (0)	googlehosted.l.googleusercontent.com		142.250.181.225	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:11.185983896 CEST	8.8.8.8	192.168.2.3	0xaefc	No error (0)	assets.publishing.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:12:11.185983896 CEST	8.8.8.8	192.168.2.3	0xaefc	No error (0)	www-gov-uk .map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:11.185983896 CEST	8.8.8.8	192.168.2.3	0xaefc	No error (0)	www-gov-uk .map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:11.185983896 CEST	8.8.8.8	192.168.2.3	0xaefc	No error (0)	www-gov-uk .map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:11.185983896 CEST	8.8.8.8	192.168.2.3	0xaefc	No error (0)	www-gov-uk .map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:14.876641035 CEST	8.8.8.8	192.168.2.3	0x9e0f	No error (0)	assets.publishing.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:12:14.876641035 CEST	8.8.8.8	192.168.2.3	0x9e0f	No error (0)	www-gov-uk .map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:14.876641035 CEST	8.8.8.8	192.168.2.3	0x9e0f	No error (0)	www-gov-uk .map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:14.876641035 CEST	8.8.8.8	192.168.2.3	0x9e0f	No error (0)	www-gov-uk .map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:14.876641035 CEST	8.8.8.8	192.168.2.3	0x9e0f	No error (0)	www-gov-uk .map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www-gov-uk .map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www-gov-uk .map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www-gov-uk .map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
Aug 17, 2021 10:12:48.609584093 CEST	8.8.8.8	192.168.2.3	0x2b74	No error (0)	www-gov-uk .map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 17, 2021 10:11:47.721724033 CEST	151.101.0.144	443	192.168.2.3	49732	CN=www.gov.uk, O=Government Digital Service, OU=Government Digital Service, L=London, ST=Greater London, C=GB CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Oct 23 18:31:03 CEST 2020	Wed Nov 24 17:31:03 CET 2021	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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Aug 17, 2021 10:12:14.919996023 CEST	151.101.0.144	443	192.168.2.3	49809	CN=www.gov.uk, O=Government Digital Service, OU=Government Digital Service, L=London, ST=Greater London, C=GB CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Oct 23 18:31:03 CEST 2020	Wed Nov 24 17:31:03 CET 2021	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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Aug 17, 2021 10:12:14.920211077 CEST	151.101.0.144	443	192.168.2.3	49808	CN=www.gov.uk, O=Government Digital Service, OU=Government Digital Service, L=London, ST=Greater London, C=GB CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Oct 23 18:31:03 CEST 2020	Wed Nov 24 17:31:03 CET 2021	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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5844 Parent PID: 968

General

Start time:	10:11:39
Start date:	17/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.gov.uk/government/publications/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person/guidance-for-contacts-of-people-with-possible-or-confirmed-coronavirus-covid-19-infection-who-do-not-live-with-the-person#exempt'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 384 Parent PID: 5844

General

Start time:	10:11:41
Start date:	17/08/2021
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=1632,13591179574770033270,10313266110045525433,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly