ID: 406920
Cookbook: browseurl.jbs
Time: 11:44:55
Date: 07/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

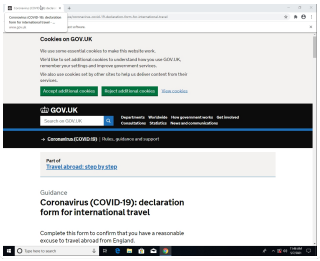
Analysis Report https://www.gov.uk/guidance/coronavir…

Overview

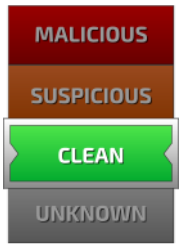
General Information

Sample URL:	http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel
Analysis ID:	406920
Infos:	

Most interesting Screenshot:



Detection

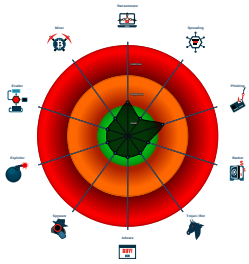


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 1880 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3080 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,6179841392289751219,8571533054898512681,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

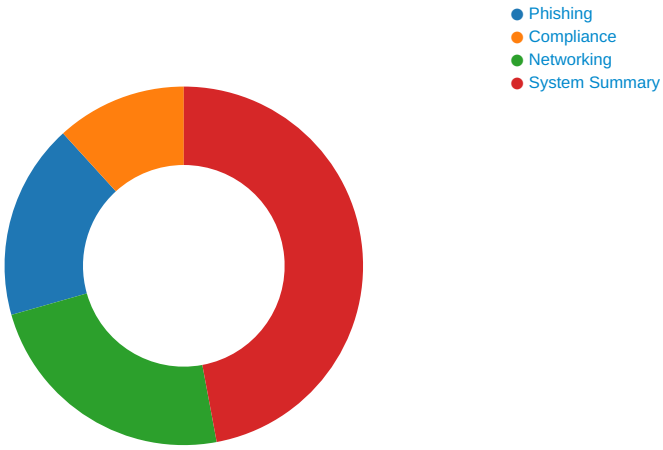
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



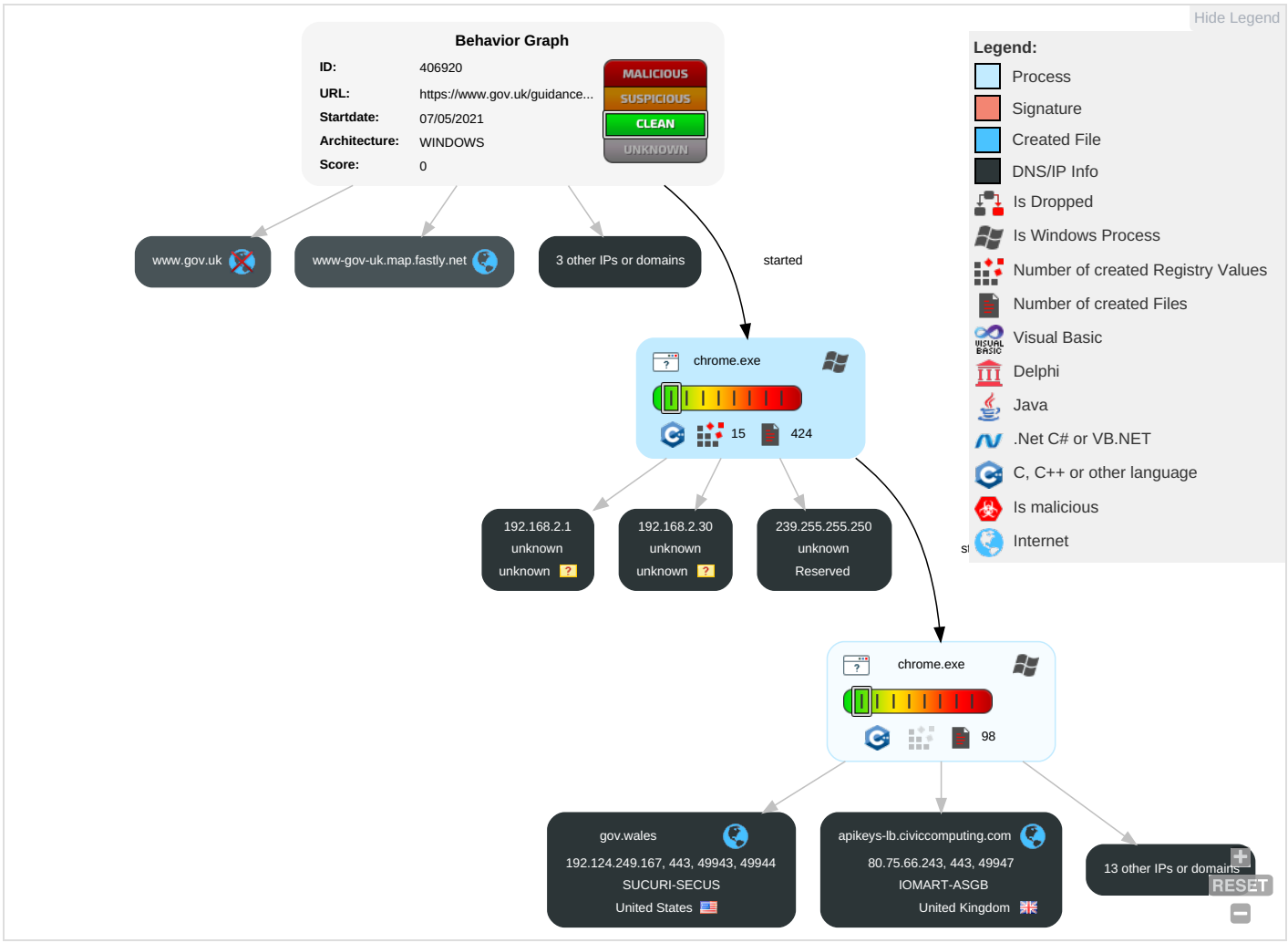
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

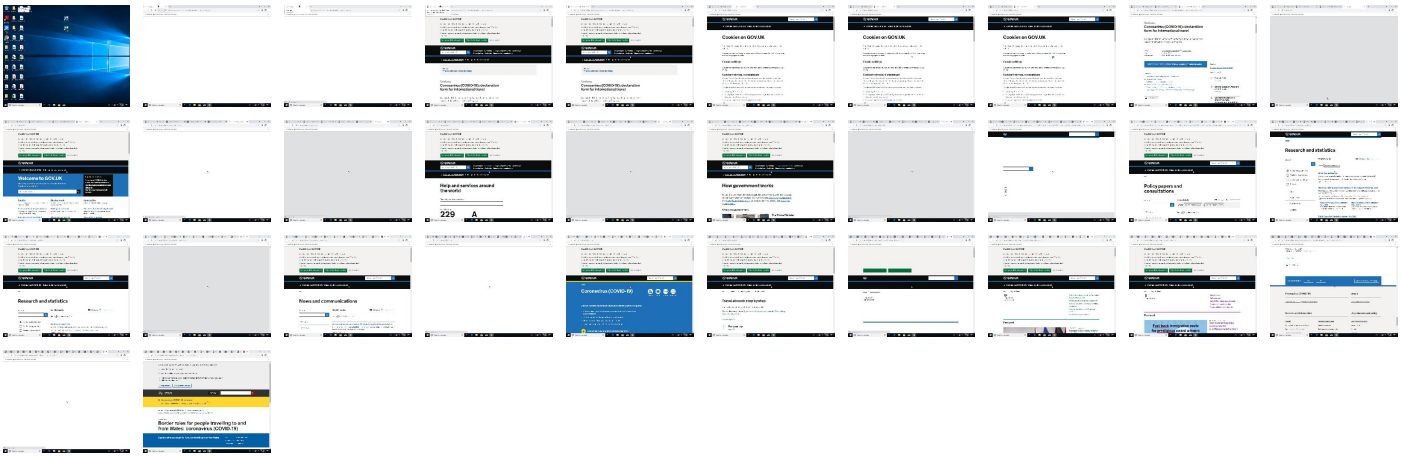
Behavior Graph

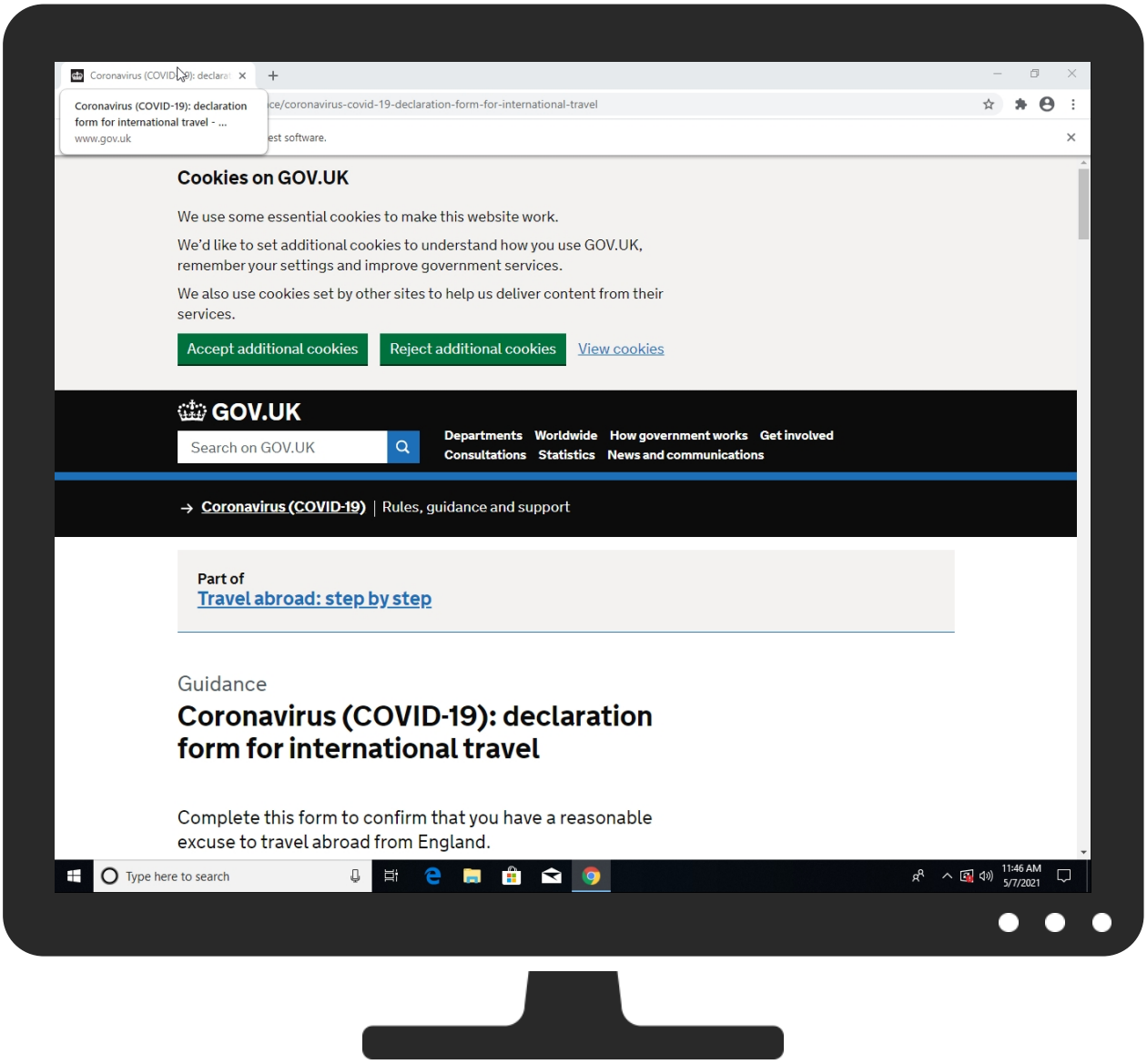


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel	0%	Virustotal		Browse
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel	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/P	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/research-and-statistics	0%	Virustotal		Browse
http://https://www.gov.uk/search/all?keywords=	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#historyJC	0%	Virustotal		Browse
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#historyJC	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/organisations/home-officeHome	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/travel-abroad#	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/contact/govuk/problem_reports	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/world	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/travel-abroad$	0%	Avira URL Cloud	safe	
http://https://cc.cdn.civiccomputing.com/8/cookieControl-8.2.1.min.js	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelCoronaviru	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/frontend/application-21540043d3d55868b19d5158a614c3398a0e48f2a86bf94460d0d	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/how-government-worksHow	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelDq	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/organisations/department-for-transportDepartment	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/contact/govuk/email-survey-signup	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/world/	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.gov.uk/travel-abroadTravel	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/news-and-communications.	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/help/cookies_	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelJCoronavir	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#contentJC	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirusCoronavirus	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/news-and-communicationsNews	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#historyCo	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/whitehall/application-25d2783e4154a9e14ef817c2183931744ea4f178fb0d4d2260f2	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/news-and-communicationsNews	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/g	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/worldUK	0%	Avira URL Cloud	safe	
http://https://www.gov.uk	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel-	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/news-and-communications	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/opensearch.xml/	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/static/favicon-8d811b8c3badbc0b0e2f6e25d3660a96cc0cca7993e6f32e98785f205fc	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/worldv	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/V	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirus5	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/finder-frontend/application-8661d997c1e894f90eb69be1fa453a61c919d00d637a11	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/coronavirusi	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelV	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/government-frontend/application-ad747abfe1bc91b2a7c9f5e232b5723efeb42522f2	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/help/cookiesCookies	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/news-and-communications5	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/static/header-footer-only-21591776c6c870857b1b0569af6e383cf216bcfbd4af446f	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/organisations/department-for-transport$	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel2JCoronavi	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#history;	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/assets/collections/application-410ff39f81f7c65f77da249d7fbcd1cdb0532f6c6562f4894a	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/research-and-statisticsw	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/government/get-involvedci	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#content#	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.gov.uk/government/worldUK	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/opensearch.xml	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/search/policy-papers-and-consultations?content_store_document_type%5B%5D=open_con	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gov.wales	192.124.249.167	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
d3bipqqt7o7bp0.cloudfront.net	143.204.209.98	true	false		high
www-gov-uk.map.fastly.net	151.101.0.144	true	false		unknown
apikeys-lb.civiccomputing.com	80.75.66.243	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.20.1	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
cc.cdn.civiccomputing.com	unknown	unknown	false		unknown
js-agent.newrelic.com	unknown	unknown	false		high
apikeys.civiccomputing.com	unknown	unknown	false		unknown
www.gov.uk	unknown	unknown	false		unknown
assets.publishing.service.gov.uk	unknown	unknown	false		unknown
bam-cell.nr-data.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.gov.uk/search/research-and-statistics	false	• 0%, Virustotal, Browse	unknown
http://https://www.gov.uk/coronavirus	false		unknown
http://https://www.gov.uk/world	false		unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#history	false		unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel	false		unknown
http://https://www.gov.uk/search/news-and-communications	false		unknown
http://https://www.gov.uk/government/how-government-works	false		unknown
http://https://www.gov.uk/government/organisations/department-for-transport	false		unknown
http://https://www.gov.uk/search/policy-papers-and-consultations?content_store_document_type%5B%5D=open_consultations&content_store_document_type%5B%5D=closed_consultations	false		unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#content	false		unknown
http://https://www.gov.uk/help/cookies	false		unknown
http://https://www.gov.uk/government/organisations/home-office	false		unknown
http://https://www.gov.uk/	false		unknown
http://https://www.gov.uk/government/get-involved	false		unknown

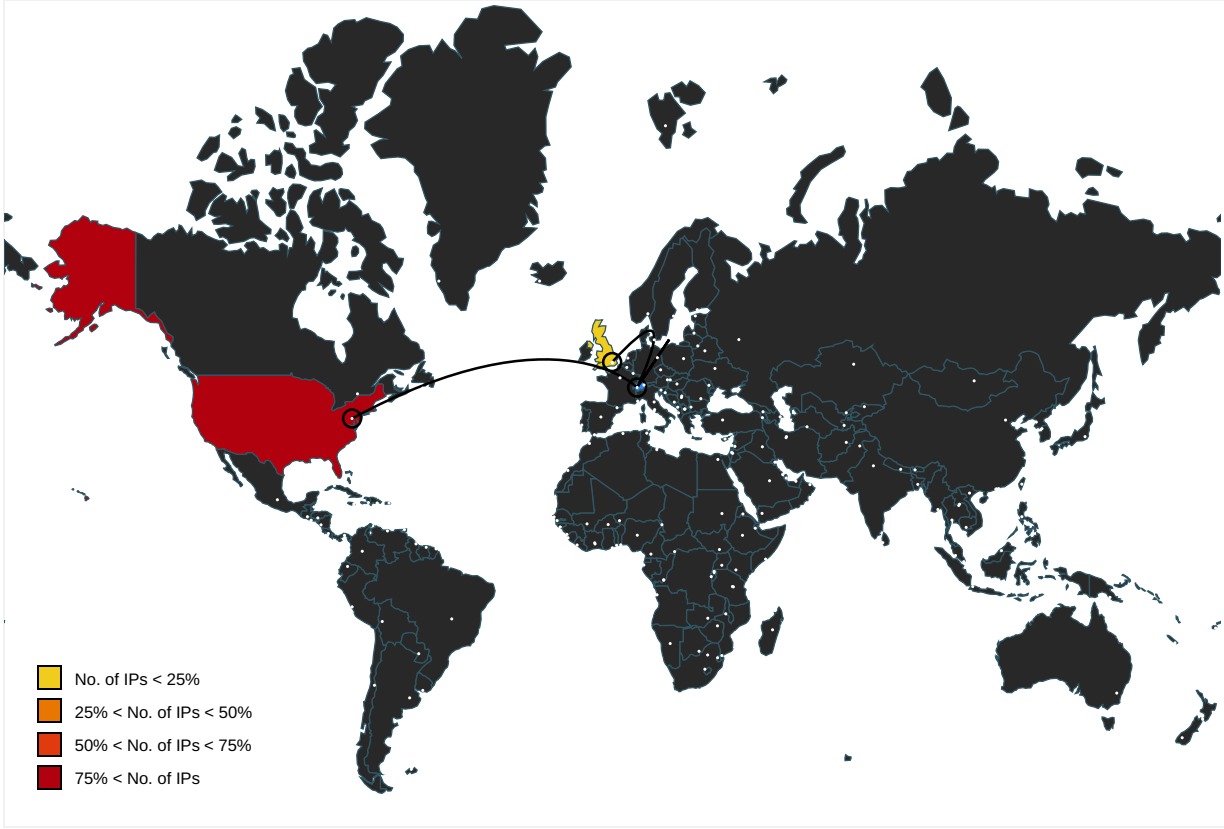
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	Web Data-journal.0.dr	false		high
http://https://www.gov.uk/P	e33fbbccd4fb1406_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	Web Data-journal.0.dr	false		high
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#content	Current Session.0.dr	false		unknown
http://https://www.gov.uk/search/all?keywords=	Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/sites/default/files/js/js_3KOrO4Ww6IO1xutFjJXt_EmChmgAZ2EhqrlxszFNDA0.js	4153868f0a0ac3d3_0.0.dr	false		high
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#historyJC	Current Session.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/organisations/home-officeHome	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/how-government-works	Current Session.0.dr, Favicons-journal.0.dr	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.gov.uk/travel-abroad#	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/contact/govuk/problem_reports	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/world	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/travel-abroad$	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cc.cdn.civiccomputing.com/8/cookieControl-8.2.1.min.js	9026c1cc08d6ff8f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelCoronaviru	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/assets/frontend/application-21540043d3d55868b19d5158a614c3398a0e48f2a86bf94460d0d	e33fbbccd4fb1406_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/how-government-worksHow	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/organisations/department-for-transport	Current Session.0.dr	false		unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelDq	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/organisations/department-for-transportDepartment	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/contact/govuk/email-survey-signup	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/world/	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/travellers-exempt-self-isolation-coronavirus-covid-19XBorder	Current Session.0.dr	false		high
http://https://www.gov.uk/government/organisations/home-office	Current Session.0.dr	false		unknown
http://https://gov.wales/travellers-exempt-self-isolation-coronavirus-covid-19	Current Session.0.dr	false		high
http://https://dns.google	4a15d653-c039-4f63-b5c9-c7d7be415ffb.tmp.1.dr, 26f4f584-665c-42b6-b953-80afd387994b.tmp.1.dr, f2293b67-125d-4be0-8230-bf54e91820dd.tmp.1.dr, c62a307f-e0e4-48d4-9d9c-151db6cd5188.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gov.wales/themes/custom/govwales/favicon/favicon-32.png	Favicons.0.dr	false		high
http://https://www.gov.uk/travel-abroadTravel	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/news-and-communications.	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/:	f936eb2c3f9dbfd5_0.0.dr	false		high
http://https://www.gov.uk/help/cookies_	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Web Data-journal.0.dr	false		high
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelJCoronavir	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#contentJC	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/coronavirusCoronavirus	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/news-and-communicationsNews	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#historyCo	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales	Current Session.0.dr	false		high
http://https://www.gov.uk/search/news-and-communications	Current Session.0.dr	false		unknown
http://https://www.gov.uk/assets/whitehall/application-25d2783e4154a9e14ef817c2183931744ea4f178fb0d4d2260f2	530ab17a5f4e2c6c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/news-and-communicationsNews	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/g	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/worldUK	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/travel-abroad	Current Session.0.dr, Favicons-journal.0.dr	false		unknown
http://https://www.gov.uk	26f4f584-665c-42b6-b953-80afd387994b.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel-	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/news-and-communications	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/opensearch.xml/	Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/assets/static/favicon-8d811b8c3badbc0b0e2f6e25d3660a96cc0cca7993e6f32e98785f205fc	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.gov.uk/government/worldv	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/themes/custom/govwales/favicon/favicon-32.pngr	Favicons.0.dr	false		high
http://https://www.gov.uk/V	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/coronavirus5	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/assets/finder-frontend/application-8661d997c1e894f90eb69be1fa453a61c919d00d637a11	3497f9ad7dc29f82_0.0.dr, bafcb963c6242693_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/	000003.log0.0.dr	false		unknown
http://https://www.gov.uk/coronavirusi	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travelV	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel	History-journal.0.dr, Favicons-journal.0.dr	false		unknown
http://https://www.gov.uk/search	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/travellers-exempt-self-isolation-coronavirus-covid-19Border	History.0.dr	false		high
http://https://www.gov.uk/assets/government-frontend/application-ad747abfe1bc91b2a7c9f5e232b5723efeb42522f2	5d3fa02a24aa480a_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/help/cookiesCookies	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/news-and-communications5	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/organisations	Current Session.0.dr, Favicons-journal.0.dr	false		unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#history	Current Session.0.dr	false		unknown
http://https://www.gov.uk/assets/static/header-footer-only-21591776c6c870857b1b0569af6e383cf216bcfbd4af446f	fad1842d86d53f14_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/government/organisations/department-for-transport$	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel2JCoronavi	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#history;	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/research-and-statistics	Current Session.0.dr, Favicons-journal.0.dr	false	• 0%, Virustotal, Browse	unknown
http://https://www.gov.uk/assets/collections/application-410ff39f81f7c65f77da249d7fbcd1cdb0532f6c6562f4894a	4cc2c4ec3f6fd94f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/research-and-statisticsw	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js	f9b6b42bceab5fdf_0.0.dr	false		high
http://https://www.gov.uk/government/get-involvedci	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/search	Current Session.0.dr	false		high
http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#content#	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/	fca4f098b45fdfca_0.0.dr	false		high
http://https://www.gov.uk/government/get-involved	Current Session.0.dr, History-journal.0.dr	false		unknown
http://https://gov.wales/travellers-exempt-self-isolation-coronavirus-covid-19W	Current Session.0.dr	false		high
http://https://www.gov.uk/government/worldUK	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://gov.wales/sites/default/files/js/js_aRVJ3MdDVYsxtzIyliTzcm576TFmee9hAxhtWFHgGbw.js	f936eb2c3f9dbfd5_0.0.dr	false		high
http://https://www.gov.uk/world	Current Session.0.dr, Favicons-journal.0.dr	false		unknown
http://https://js-agent.newrelic.com/nr-1208.min.js	ace99e70b2c6e69e_0.0.dr	false		high
http://https://www.gov.uk/search/opensearch.xml	Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/search/policy-papers-and-consultations?content_store_document_type%5B%5D=open_con	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown

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
80.75.66.243	apikeys-lb.civiccomputing.com	United Kingdom		20860	IOMART-ASGB	false
143.204.209.98	d3bipqqt7o7bp0.cloudfront.net	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.20.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
192.124.249.167	gov.wales	United States		30148	SUCURI-SECUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.30
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	406920
Start date:	07.05.2021
Start time:	11:44:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel

Copyright Joe Security LLC 2021

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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@46/199@13/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.gov.uk/help/cookies • Browse: https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#content • Browse: https://www.gov.uk/ • Browse: https://www.gov.uk/government/organisations • Browse: https://www.gov.uk/government/world • Browse: https://www.gov.uk/government/how-government-works • Browse: https://www.gov.uk/government/get-involved • Browse: https://www.gov.uk/search/policy-papers-and-consultations?content_store_document_type%5B%5D=open_consultations&content_store_document_type%5B%5D=closed_consultations • Browse: https://www.gov.uk/search/research-and-statistics • Browse: https://www.gov.uk/news-and-communications • Browse: https://www.gov.uk/coronavirus • Browse: https://www.gov.uk/travel-abroad • Browse: https://www.gov.uk/government/organisations/department-for-transport • Browse: https://www.gov.uk/government/organisations/home-office • Browse: https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel#history • Browse: https://gov.wales/travellers-exempt-self-isolation-coronavirus-covid-19

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 172.217.18.77, 172.217.20.14, 172.217.16.110, 95.168.222.144, 34.104.35.123, 172.217.23.10, 172.217.19.99, 184.30.24.56, 216.58.214.202, 216.58.214.234, 172.217.16.106, 172.217.18.74, 172.217.19.106, 172.217.20.10, 104.43.193.48, 40.88.32.150, 2.20.142.209, 2.20.142.210, 20.82.209.183, 172.217.20.3, 95.168.222.83, 142.250.186.136, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.147, 162.247.243.146, 92.122.213.247, 92.122.213.194 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, tls12.newrelic.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, r8.sn-n02xgoxufvg3-2gbl.gvt1.com, clients2.google.com, redirector.gvt1.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, edgedl.me.gvt1.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, r8---sn-n02xgoxufvg3-2gbl.gvt1.com, clients.l.google.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

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\09c759a1-eb54-40d2-bbb0-710e2d4da64f.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):	168028
Entropy (8bit):	6.08039048222972
Encrypted:	false
SSDEEP:	3072:fk5yUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:8OXPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	0AADEB91F18BFA25EF571788139D69BB
SHA1:	FCAADC428A1F247E52C2EB42D50711EEDBD007C7
SHA-256:	EEE9C25626F72219A0B030AD270CDD65419FA10D692E3E85497198236092AB4F
SHA-512:	1EB4E6C694A4C5897A88530515722E0333B39BC6C6F5AF9CDE6995A513A711905B8393250E654EFAFDB7ADFD153E4829D7779FA61DD4106284C7C36ED1997DB
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909287143"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a27a898-bc38-4bd6-8ec6-144bd4aeed11.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.746008130979292
Encrypted:	false
SSDEEP:	384:h7/8MeR7KluIVJ7Y7NkrVvAs3v8K7HGbGburpucOx/i6yNrJ0m9xT9e84A7OeCYE:NeKVpKSg/0e/aQKUH/eoKuQIBa
MD5:	824FBBA5326F1078CDBAB7184DE305DB
SHA1:	167613232B8619276DA5AD0BE9D6A3846E706541
SHA-256:	C8DE5F673627B2750DEF78EF76DAE41E48E89E9D2CD5C56DCE2881BF5F962E68
SHA-512:	4BAA61B56732A321DA817690131B296727622065018CE6F2ECE69E1339140E221ECEC89895A9F060608D1285EA7F8DCFDF394D220098DF69186C32CF7F58EAC2
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...R98.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\4698976b-48e6-49fa-9a53-b0a9aba92126.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):	168026
Entropy (8bit):	6.080390804946721
Encrypted:	false
SSDEEP:	3072:8kgyUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:zbXPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	937F1A66009EE0189E32731FC289EF46
SHA1:	8EEA86D64200E855E79D47FA108C3DE7E8A29E0F
SHA-256:	A6D85109DC98973A62A79FFB8F30C6C95B6F199B0BFA33B8173FE0E01D26368E
SHA-512:	76D3DC764560D477E1263AD6775A4C7FC61E3B40EC836097F6383084A5CBC8B873E73CAAF21941145157A8C206386A806F0BEF84ACEAD70D084F0AC6632F399
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\61ce7da3-3edd-4d61-9953-7adf82f57ff8.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):	159555
Entropy (8bit):	6.050357697624829
Encrypted:	false
SSDEEP:	3072:CyUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:pXPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	00E5EB5FAA1D6B1803F97BE89D01D4E8
SHA1:	43CFE4D3E1CA0880FA9CDC2BD99A7C4EA14B5777
SHA-256:	A126C529E4F0EF7ECE5FB36BC6DE95ADE7CF3BAC852891B76C4FBDD876C4F67A
SHA-512:	F34CF9E17978605785DA7A52CB82ED204E1CC61FF43C714A13DAB4A7D3046D80AB948EE56861895CB4AD42596C8B3899C43AC2B71824ED2283CF4D09FB4DDC5
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909287143"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\9e5114de-79de-4364-b923-351bbaf9df84.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\9e5114de-79de-4364-b923-351bbaf9df84.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	168028
Entropy (8bit):	6.080388686319545
Encrypted:	false
SSDEEP:	3072:fkxyUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:8GXPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	23A8131483BA752E17BA4EB30B35CCC8
SHA1:	5922F455867BF88E242C2E634A923C0CA9618E74
SHA-256:	F747D5C7CB9E7E7B34001498C5B247B2618B10D8ECAE8CA3CA50AA9F857A3FF2
SHA-512:	EF49F85A975EE65E078DA7B2320CDC9604AB3A111F0B34F37A5FAD16F8411AC0AA39296B76E7881055C1A6882D19895335DB578D49A75C3B0B27BD6C497CE4C
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909287143"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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:FkXJFlsz6VVJFlsz6VVJFlsz6I:+rJsrJsrJJ
MD5:	E4C3A0CCEDB71D53052C719DE30FD750
SHA1:	C89D101217D4AA05AD9C6FB24DB2037B3BCC630E
SHA-256:	B9ABED457F567199890198C9CE3B20954C73C458014CEB77C5E4514B1A8D8BF9
SHA-512:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C405803
Malicious:	false
Reputation:	low
Preview:	sdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a29e4d3-f8f6-4048-8ee1-139e17bfa212.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10d78e90-279c-47e8-a58c-08adc2c55b13.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):	1043
Entropy (8bit):	5.575667935804478
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevBoU1ohUeT7Z7wUNAgRUevxQ:YU6UUhveKUevGU16UepwUNHUev2
MD5:	864D31DED08565BFAB0C2F7DE7192AF4
SHA1:	0609A71641D8915075ABD3FEFC67E288817099EA
SHA-256:	51EE9C7FE992667E28445DE66BD4E6279160197FC77D9BB6A833AC806D5FCF3A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10d78e90-279c-47e8-a58c-08adc2c55b13.tmp	
SHA-512:	1163614BF7AFF4F4357659C123B22E326509EFE973FB0E8027C1B2B51E213FAC6CF406F1D1CE375D947753F5EC2D55280EDEE78AB7CF93AA05A53D10049B4F33
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1651949187.752821,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413187.752827},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1651949159.470215,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413159.470221},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\26f4f584-665c-42b6-b953-80afd387994b.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):	2363
Entropy (8bit):	4.906136613283507
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtwz5saTshRLsTCTRLsujyKs53zs/MHoYsYAkgYhbyD8:JnCDHXTxOzhkdx4OGobwhj
MD5:	D003F79C9AFEB44D72152285E0508581
SHA1:	45E146828D14761C013F131228B4D08CBF7664D8
SHA-256:	9A0876D853076AB86FDE3358128F93A6919732B5DA315B58BC1737D3FC29C724
SHA-512:	D8810C49CFCD725B9472502C286CA09756B0DDBB969E4E7CC1117D6FA9920B605761929DB04D022373B72DF690CF37D5B9F98070F29D56C86894DD503D01E88
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267478759457451","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267478759466418","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f079620-0104-4b55-8fa8-ea7ff21911e6.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):	5798
Entropy (8bit):	5.190578831164721
Encrypted:	false
SSDEEP:	96:ny3h54sf2Pz4YVlik0JCKL8kTk21NQAbOTQVuwn:n2hH20Y3k4KvTk2fd
MD5:	0E01A1D8D2CE5D4A0F706D9B8CB61B6E
SHA1:	DC90DA54AF467167154700FEDFC23A689A20E4E3
SHA-256:	BC051D75BFAD58ADDA3CFA0835D50DC5A8005BDFB2E05244ABC2EA62BB7C9B45
SHA-512:	A88C54178FE6E624572857728BA1FB96E72AF9C537D09F570177D386743F75DD520D356640156382B452ECBF67ACCE272197EAE0E1D6D8584334BBA365311439
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f854ad1-8843-4694-8853-8247bcdeb10c.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):	5772
Entropy (8bit):	5.189038484479347
Encrypted:	false
SSDEEP:	96:ny3h54/f2Pz4YVhik0JCKL8kTk21pbOTQVuwn:n2hy20Yrk4KvTk2b
MD5:	10DD6E4F0BED58030FA26B52DC4E54A3
SHA1:	C408CD235741E250BBDAA24011CFC20F95EA3DAA
SHA-256:	B837E43F3CA7D2B3A7E4AE16A77536C8C0E90DDD4C349AEE8ED04B032579C100
SHA-512:	B5C6039F6FE30D20EA38ADB51CA7C3DDEE18E6DE5C86A7D8ABD0F81414591F4095CF2A7CB85FC2AB908DD7A6E1ACC453D114CDC08B1A6EEFB56728E23DC7 E675
Malicious:	false

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f854ad1-8843-4694-8853-8247bcdeb10c.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3b3d3ba6-7c0e-4180-89fb-1c5a2cb9465f.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):	1211
Entropy (8bit):	5.572674491511608
Encrypted:	false
SSDEEP:	24:Ys2Ul6H0UhvrRlG1KUev2UBzshUeT7Z7wUNAgRUevxQ:YhUl6UUhveKUev2UB6UepwUNHUev2
MD5:	B3CCF99431DBAC3EEF3698A82F31E190
SHA1:	489DE91B5F36F6912E0D1B66845FAEDDF8F14061
SHA-256:	20E514EBBBC15765D91CF354B13F9B0180E0E9BAECE66FF4F68111FFE10A5D90
SHA-512:	16F7B289DE17AA9D01FC0366B408866AFCA903FA151781B7E7A1E1F8F1ABE2E20D7E8D81EFD47613EEFD46EE630DA3B0C54002456AD052DF0ADF90308ED1CB 5D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651949218.970577,"host":"Dl4Fc0vl/YypYkpsDR3ijy3cXV29/8t3AjQ0T8PW0dA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413218.970584},{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbl1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1651949218.516369,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413218.516374},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1651949159.470215,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40875ca4-1026-40f7-b1cd-090169ca4d3d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535761589900646
Encrypted:	false
SSDEEP:	384:71ZtnLlGFXA1kXqKf/pUZNCgVLH2HfDurUnHGKnTp/gy+4J:pLlyA1kXqKf/pUZNCgVLH2HfyrUHGKnr
MD5:	B72AC2DE4BB6A071206CE02F129D4F5B
SHA1:	5254890C30E47B0C584010AC2DCC0E8CE2AA6F59
SHA-256:	68495EAF29C5F619334E27A1E43939B7B1BEF18A2FE88A65F3624DA215BDD915
SHA-512:	CD2D3E5DE94C70F51F087FA119E8627B246AF2BB315BAF6CF8F0EF998D41378FC6B466F4347A826547ACD4FD78F8D5F87DD8ADB3DB987D7B03C6DCB40C7E7 32
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":"13264886756004585","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\48542e03-e7db-4041-89ee-b62cdc1a7bd2.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):	5161
Entropy (8bit):	4.992620286442267
Encrypted:	false
SSDEEP:	96:ny3h5Alf2pYVZik0JCKL8kTk21pbOTQVuwn:n2hu2pYjk4KvTk2b
MD5:	31BF1F1ACA0CC0F64F1C687F743C3B95
SHA1:	F37F16C07E7517BC18570473AF978FEE802A1EB2
SHA-256:	D87ED493AB268E99C6771F412B1FC627B202AD0FFDA4CA5605ABC74E225FBA88
SHA-512:	9A369D04AF4FF85B6503F0B36E634A8961F564B4F3007794F984A1E2F93ECD81C735883297D86C53FFCC83747BD17E6D230A0D218C31FD314459782668E284BA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48542e03-e7db-4041-89ee-b62cdc1a7bd2.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85af428f-7fa6-4dfc-89f5-651dc6e2d91a.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):	5771
Entropy (8bit):	5.18885454185774
Encrypted:	false
SSDEEP:	96:ny3h54/f2Pz4YV+ik0JCKL8kTk21pbOTQVuwn:n2hy20Yok4KvTk2b
MD5:	73A0180DCE5298F160E978B6C784B20D
SHA1:	4B5C864CB72CA7011A282D25D2ACA1497131756D
SHA-256:	EC83B2B8B53A60C0E516A25C6E3C496830F507836E4A4E4F0519D7545708CCFC
SHA-512:	D0E6E4FA238B01BBAC635209B546083C1230BBFE2153C416B55706C1CA75C88336379CFE367AFA2DACC27B29CE1721FA71A9E133B3625B5B3E460AC42E5AD8 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

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):	342
Entropy (8bit):	5.242130484784552
Encrypted:	false
SSDEEP:	6:mVwMS0+q2PcNwi23iKKdK9RXXTZIFUtpwwMScGmWZmwPwwMLiVkwOcNwi23iKKdi:pv0+vLZ5Kk7XT2FUtpZvcGmW/PZAiV5e
MD5:	A13122B44C90690FA9699D9412499FB4
SHA1:	BFCE09E8EC35AF6295C1856D2EAD701E07B80FB2
SHA-256:	BAAB7DD7152F83F80F17EBABDE0EAE368E904120269245422172E8C969BE8361
SHA-512:	3ECED92B034125EBDF5981F8FFFD8A9AA3B0D43F730CA4E16B434DAB49780BB36DA9D304A2537F3FC3C535F3EB228F1F467C4DDE58A17B231ACCEBF0F6237F 50
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:10.678 1bcc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/07-11:46:10.679 1bcc Recovering log #3.2021/05/07-11:46:10.680 1bcc 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):	326
Entropy (8bit):	5.223168780956459
Encrypted:	false
SSDEEP:	6:mVwMSU++q2PcNwi23iKKdKyDZIFUtpwwMSWbWZmwPwwMSW+VkwOcNwi23iKKdKyX:pvU++vLZ5Kk02FUtpZvyW/PZvRV54Z5A
MD5:	FF90FFA5DF0847559C3FF1530AAA1F4C
SHA1:	2219534B04EDC47E1F821F142FC4F94728F6E461
SHA-256:	162AC9BF0EE85CD306CB5207D1867F5CAA22CD153BA7F67BD908989040A7260E
SHA-512:	5F4ACDA4F4FC992516A45F44247088F788660459889079B0076791AFF75F695D44502C633A3F6302C03667F3B6C62A153702AA33EBF064AB483095E87ACECAC2
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:10.671 1bcc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/07-11:46:10.673 1bcc Recovering log #3.2021/05/07-11:46:10.673 1bcc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b7a5bbe87dc6be1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.8662297507363945
Encrypted:	false
SSDEEP:	6:mHYGLRfhDEqEJJZyQi/MwWBHiTmLRPyRD/WI2FXk2nST7/bK6twQq/SGlgZ2FXkZ:mLExyQ+MwlCT+C7W1XvST71aCEXX
MD5:	EA87F97327CF9435BB879FE2ACA96120
SHA1:	6FDB198D23375FC4A7ECBF7567D8EC2A34440C86
SHA-256:	F483B4BA8342B916BBC7B5CA47FF135125D08E78F6AACF0F3D31640DEF55831B
SHA-512:	A3E69BC07A4C3C94D783DD765D8C74EB6464BFE09E23C1B3037248894B3A0D928D07A0ADA8BAC2FAC5F38EA224CD083B0F8B0C2BA3A53E2CB8060A529AB12BE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5....._keyhttps://www.gov.uk/assets/whitehall/application-25d2783e4154a9e14ef817c2183931744ea4f178fb0d4d2260f2b4d400751336.js .https://www.gov.uk/... X /.....4>.....J.e.}>y6.A.>..Rh...;/.f..&.Y>.A..Eo.....8.....A..Eo..... X /.....F9F2CD90CC08BDDBF4D90574C745E49C2CB6EA6420F1C526E6A2F04160FF3AE2...J.e.}>y6.A.>..Rh...;/.f..&.Y>.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13b9e889e4e777c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.9936621028342545
Encrypted:	false
SSDEEP:	12:2/gQ4WP3lUFo1Yjs1kxNAYjCv841YjWn:2lQ4yEFAtOE05
MD5:	4C822121C50CB6DE044175E2A583F0C0
SHA1:	E69DFBD95A35791956D2197FC76F8459340F5BC3
SHA-256:	59136B423552A23D45FA0569D8CD2FF7017851B998F59A78FA2355D4B66A06FA
SHA-512:	33059CF5FC042FDAC96CC09DCA06348C46CB50DA83A09DEC4129D4C63F2B5AC98420CC53CD3DA9592F7F9AE8546D0DAC5B96765C4C23E37D02F66883BBED996
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.gov.uk/assets/static/header-footer-only-21591776c6c870857b1b0569af6e383cf216bcfbd4af446fbc145a969efadd0c.js .https://www.gov.uk/..J.X /.....',..j)..X.-.K..>.sw..4....A..Eo.....5j.....A..Eo.....J.X /.x...7998173EEB06017D11CA901044BA525EA3B4E1F6C7F60807E42DB83F86146DBD...',..j)..X.-.K..>.sw..4....A..Eo.....h...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3497f9ad7dc29f82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	163416
Entropy (8bit):	5.830348914030191
Encrypted:	false
SSDEEP:	1536:ZrAZuTHnBoqfohNBWO4LVQ3K565PZIrSaVWzr7eLG5WWohIwSQKYHE4RY/8xHZ:CsGl2mmWaUH7eLG5WWouwvtE4D
MD5:	4E3CA0EE4F31A2A9D794ACF7E2FBBB47
SHA1:	776851B0B29E37302493C723A40D37C71F256214
SHA-256:	72C37207B55A58E55B1D87617E304D79393D508F783A0834875790DCDB165A48
SHA-512:	0A217526C9875E9285A48F948DCA6887902E45D679BB1A45D16B8B237308D520FB301C9A6846F13A35208E835A4BF9EA78A129DEC5E23E823132E1EE83F95784
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....a.....655108C8F0FE4CB1D3BE6486E4AF6A86877F10D12FE8D970B755DC73E1B51D0C.....'..b....O5....|...{.....L.....(....-..D.....d.....h.....(.....(S.....`b....%.L`.....L`.....(S.....Ia.....Qe~.....nodeListForEach.E.@.-.....P.....y...https://www.gov.uk/assets/finder-frontend/application-8661d997c1e894f90eb69be1fa453a61c919d00d637a11048666ecf77c01d6ba.js...a.....D`....D`....D`.....``...&...&...(&...(S.p.`.....L`.....0Rc.....Qb.....t..`....I`....Da&.....Q.@.wa.....module....Q.@..hH....exports...Qcv.....document.(S.....5.a.....a.....a.....!....a.....a.....Pc.....exportsa....W...l.....*d.....K`....Dv(.....%.....s..6...&.(...s..)...&.(.....&..&.^.....&.-...%.....&.].....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4153868f0a0ac3d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.7567066227485615
Encrypted:	false
SSDEEP:	3:m+lidi/C8RzYDfMRmB8fYM5KcMsJpqUijXuwOJdWFvDAv+ltlHC0Mtljyi3Csn7F:maYQRmBYDPqUij+QDYJlOUCosHMZK6t

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4153868f0a0ac3d3_0	
MD5:	71A072091302B8DE26276F925B303055
SHA1:	42EA23B1274A7E2FAEE361DB76920D0C193D8D81
SHA-256:	188967181B8B544CBDE3C489D2849596389DBCB5CE7D32A87B6F1FB59BBEDCCD
SHA-512:	D77EF43F99BE4B1F8EA74B9CCADE7DA5112C36C50E802983E20F28CCDA6B30B95AC03CBF9F6518D210C7652B9E0410489BA7A4B5AC88C8205EB3B8393F56B5 11
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r.....$...._keyhttps://gov.wales/sites/default/files/js/js_3KOrO4Ww6IO1xutFjJXt_EmChmgAZ2EhqrlxszFNDA0.js .https://gov.wales/.r@#X /..... }..*~pJ.W.....n...56~.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4cc2c4ec3f6fd94f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50622
Entropy (8bit):	5.655016467701316
Encrypted:	false
SSDEEP:	768:OXng8EYjTYekHqou+h6aBn9R1SRUYtIBoqPC+s+uj:wE+ka+h3h927GoGs+a
MD5:	00C82C1E3E5B4C710A4394AA27713681
SHA1:	EC63C3B5A40534EE2B0912EA344220FF80EE597E
SHA-256:	D9F761690BBF00A7C50CBC624F90055558199553339C571A5AA2F1368B0C0862
SHA-512:	692D97D3DC6A01926A06FDE07FC4E9ABFBF596CA375F3FB12FD796FAFFEF6D4A80D7875852E22E88746A23D863802B7E037FE2F5DD9826B19D01FD581C7AB5E 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....SP.6...._keyhttps://www.gov.uk/assets/collections/application-410ff39f81f7c65f77da249d7fbcd1cdb0532f6c6562f4894aefd8ce7ae99b62.js .https://www.g ov.uk/.. X /.....(5.....n$..s.....k..[.4ro.....y.A..Eo.....A..Eo.....'.b.....O.....m..... .....\|.....(S... ..`\.....L`\|.....L`.....(S.....Ia.....Qe".....nodeListForEach.E.@.-.....P.....u...https://www.gov.uk/assets/collections/application-410ff39f81f7c65f77da249d7fbcd1cdb0532f 6c6562f4894aefd8ce7ae99b62.js...a.....D`....D`....D`.....a....`....&...&..!$&.(S.\.`t....L`.....Q.@:.....exports...Q.@r".y....module....Q.@.CB.....define....Qb.S.....amd. ..Q.`2.bU....GOVUKFrontend.....K`....Dq.....s.....s...\...'...s.....&.(.....&...&.^.....\.....(Rc.....I`....Da&...,.....d.....@...P.....q%d..... .....&.(S...`..... L`..... (S...`.....0L`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\530ab17a5f4e2c6c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197536
Entropy (8bit):	5.681645254265214
Encrypted:	false
SSDEEP:	3072:PoT++R8Hj5g1CJ6Fcs7LSUkRRGA4aLBDQSNXU/vm9ojfkNpSsbyA:i+S8Hj2Dd7vkl42NXWCDX
MD5:	0BF931D6AD22385A89DA1673990F141D
SHA1:	D166A4678C242C969B8FD5616046EFB28476A3B1
SHA-256:	A80232E79AEEA829B444140D1315776902D7ACE3E7FCC8A17C3B4BDCF5CE273A
SHA-512:	1D6662FC7A2B9A049678F8A0CDEAA4B8563C79C83705CEA7F2B1DF811594C76AE7075BBBCDBEF4737B28481C1DF0100767B6A48E43EDEC1B5173A756FF9C1F 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...L.On....F9F2CD90CC08BDDBF4D90574C745E49C2CB6EA6420F1C526E6A2F04160FF3AE2.....'.^....OA.....R.].....(..... .....(S.....`.).....L`D....LL`".....(S.....Ia..... .....Qe2.....nodeListForEach.E.@.-.....P.....s...https://www.gov.uk/assets/whitehall/application-25d2783e4154a9e14ef817c2183931744ea4f178fb0d4d2260f2b4d4007 51336.js.a.....D`....D`....D`.....`....&...&..q.&...(S...Ia.....QerA.....dean_addEvent...E....d.....&.(S...Ia.....Qd".k%....removeEvent.E.d.....&.(S. ..Ia!.....Qd.....handleEvent.E.d.....&.(S...Ia....c.....Qc^E.....fixEventE.d.....&.(S.....Ia}.....d..... Qf..D....govspeakBarcharts...E.d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d3fa02a24aa480a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	44974
Entropy (8bit):	5.693693985771101
Encrypted:	false
SSDEEP:	768:wBI6dckOBQ1cH2DzlnJudPrfM9pRxTzQMz3uiQqqAn:wBrOB1H2DzlnJkTOrxT80QqqI
MD5:	BD116BF7CB3543A6865D36F7BC624735
SHA1:	97B0D71B70A738E5F9C4A9A4D21F3534CFCC6494
SHA-256:	7141870D96ECE3E2CD038DBE561BD757B4EDCCE485BF736407EE41AFFB06D41D
SHA-512:	23A5BD0E0E702FE188B871E72CE7095FEA8901D6E6A36CE95E26A687AC9F525D69C75F52F02FDDEF9D708993489669434A5A78835748B0E8A8A32567BC368900
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d3fa02a24aa480a_0	
Reputation:	low
Preview:	0\r..m.....F.}....._keyhttps://www.gov.uk/assets/government-frontend/application-ad747abfe1bc91b2a7c9f5e232b5723efeb42522f22e6ff46a3b747b473145bf.js .https://www.gov.uk/..J.X /.....Eh|...:..!..9.G.,.x.....A..Eo.....A..Eo.....'.`z....O.....$.....(S.....`.....L`f.....L`.....(S.....Ia.....Qe.?.....nodeListForEach.E.@.-.....P.!.....}...https://www.gov.uk/assets/government-frontend/application-ad747abfe1bc91b2a7c9f5e232b5723efeb42522f22e6ff46a3b747b473145bf.js...a.....D`....D`....D`.....A....`....&...&... &.(S.H.`J.....L`.....QcZ.....matches...QeV.....matchesSelector..$QgFB.$.. ..webkitMatchesSelector.... QfB^.....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\Code Cache\js\8d2b15ad693bd09a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.783029716291904
Encrypted:	false
SSDEEP:	6:msVYQRmBYnEeodcWFE4+n+vYT05BNLkonrK6t:/r+eodRE4+n+X5Y2
MD5:	1379A18E32762E0DF6A02F5A29A361EC
SHA1:	8816503ECF80C1BFE10DBCE2490C3DED90FE9ADC
SHA-256:	B3B16B9492EF7D32B49185DE7639E5D8B1831D005D981E67E3462B0602DCEA27
SHA-512:	DF02DB6C305178EDAA6CCF63702641C81C80C9E8CF3E0EFDF9A015EA5CCC97EBE1C5F73B648CBC54E0BC0BBA16893DD5F9B0C9C2676240B9305C8CA5A104C6B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://gov.wales/sites/default/files/js/js_DYB8iVPl5Jn_VWFdK5m9dNqsDyCRuOV3LDVMShLn5zE.js .https://gov.wales/..F#X /.....0... ..7^.v2.....v....A..Eo.....bZ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9026c1cc08d6ff8f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.500495650421642
Encrypted:	false
SSDEEP:	3:m+lSAllLA8RzYDLWOkQ2LA9LznKSFvDA9+KlltlHCp/26Y1PWBtY4F6P5mKvl1pD:mU/VYGOoo7K9tlYs6btYQ6P4WDK6t
MD5:	36B5703BD497ED2AB7D3310C5DC413BF
SHA1:	20F941DC4163BCC4BDFAA4B483F08373A2D988DB
SHA-256:	43C2CB8CFA9314EB0D563C4DB083291426432AEEFC4A9CC662CB14FBFAE32AE1
SHA-512:	D10B1466963AF4587F58D9C895030FEFF1D17792D754E5280C71C3D2ADB75590710C109D308A88FAB114B6770F2807220FF773384535457AEA1D20AD230ED07E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.... qO...._keyhttps://cc.cdn.civiccomputing.com/8/cookieControl-8.2.1.min.js .https://gov.wales/..H#X /.....".u0 {....V..x.5..n]..hA...%j.A..Eo.....$..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ace99e70b2c6e69e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.5479172077976315
Encrypted:	false
SSDEEP:	3:m+lMZxlA8RzYFEDL5ASQATS3cFvDAeK9ltlHCDVz0RS/3LhMo/oyg4mn//pK5kt:mpYFEDL5VTqI+YDR0uLhMogn/hK6t
MD5:	2E1A031696E61189C37C7A71015DA890
SHA1:	AD073C276639438899055E6569D53B32FD507460
SHA-256:	2C0ECFA48EDCD2490724ABF37241BB5067A5EF047100270E8999C1644C377BCF
SHA-512:	8B97E3A8C9305AAC7D3E6403D4A658F91541A9CD78905B1C539164835E5E9217BADCD1DBFE896CC3C37168B4914D2EB72FDB737EC2EE86EA00EB86D68794150
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D.....N....._keyhttps://js-agent.newrelic.com/nr-1208.min.js .https://gov.wales/.JQ#X /.....@...p..A}?XT=.M?..._..v...(...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bafcb963c6242693_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bafcb963c6242693_0	
Size (bytes):	410
Entropy (8bit):	5.940934607823485
Encrypted:	false
SSDEEP:	6:m2YGLRfhwOFZGVp+/TWdhjzkINRLRNK62AdfKPAm8oyA3K6toqWcYeBjKQJjdOfp:lZjWdR5K25m8oyS1WkDJ05m8oy9
MD5:	6FB60D0772B30DBF7C4549AECB4ABF71
SHA1:	7026316A67D3F661E1A35DC29346A279EEF54F04
SHA-256:	C954AAE2EAAE607E6D96A8A95A7F9AA8D7CF80F587B91940B6143B70DBDA1F83
SHA-512:	4262A579A7A4E6F99E8717D1457FF24BE312B26E3BC097FEBDA97FA79F3FBA5924A5406ECA0DA176EF5AE2437E72A88503AFE7BC9D50C034FD5BB1C71DE31EA9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://www.gov.uk/assets/finder-frontend/application-8661d997c1e894f90eb69be1fa453a61c919d00d637a11048666ecf77c01d6ba.js .https://www.gov.uk/..]!X /.....Ue.....f....:.0..Z.....z?.w..r.<.z;.W...A..Eo.....A.b.....A..Eo.....]!X /..}..655108C8F0FE4CB1D3BE6486E4AF6A86877F10D12FE8D970B755DC73E1B51D0Cf....:.0..Z.....z?.w..r.<.z;.W...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e33fbbccd4fb1406_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	56795
Entropy (8bit):	5.717695724238655
Encrypted:	false
SSDEEP:	768:jW5ldcLjjuhvYll6R35u7kDd5qARTZuno5H0JnU79d:aoOvYlkZ5v5qBoeJnU79d
MD5:	1FE255F56C7E87D37DF9C66E38B5BC26
SHA1:	08925E946E9C86317712F891D3457ED0702D9A30
SHA-256:	E336790814D303FC1DB3E13EDE36C90845CFEBB386234912A0A2BD84E1075B0C
SHA-512:	03C5EB2E10B746FD2B2D7A16E884983107C6400E0A02F16D11C4FBC4AD694C5BBBCA50012C3489A25378FEF44D3B8B0F2064E10170B7E1D6A64F701393D0297
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8....._keyhttps://www.gov.uk/assets/frontend/application-21540043d3d55868b19d5158a614c3398a0e48f2a86bf94460d0d16619bce7d5.js .https://www.gov.uk/P...X /.....l.....*1.....hX...x...9..z.....N....A..Eo.....Z.3M.....A..Eo.....'.....O.....+.e.....(S.....`.....L`p.....L`.....(S.....la.....Qe.#.5....nodeListForEach.E.@.-.....P.....r...https://www.gov.uk/assets/frontend/application-21540043d3d55868b19d5158a614c3398a0e48f2a86bf94460d0d16619bce7d5.js..a.....D`....D`....D`.....`z...&...&..."&.(S.H.`J.....L`.....Qc..:.....matches...Qe..0....matchesSelector..$Qg."z.....webkitMatchesSelector.... Qf.r{.....msMatchesSelector....(S.....Pd.....t.matches...a....j...I\...#d.....K`....Dl.....(...'....(.....(.....(.....-.....(Rc.....l`....Da@.....c.....P.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f936eb2c3f9dbfd5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.702694604546111
Encrypted:	false
SSDEEP:	6:m97YQRmBYDvS/o9rFKlYu/l4RO1hxMESK6t:GtNvcoZC/IgVr
MD5:	1E88AA07CFDA44DD609C695DB4E0B128
SHA1:	24B1107B15152A878E50A1FB282161729828A5A0
SHA-256:	CC9E34E96F682EE9608AB1DA99E09F2DCDCFCEFC339D31DD4E314F3211CCB891
SHA-512:	7CC7D5A97CF8ABB4CAF24183C7C51C4A146597F9BD571209EBE3C62BF11C710A1496C497DD055E591C9344205918F667F7B33D024D89925685D8752CCF4CA3D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...YJw....._keyhttps://gov.wales/sites/default/files/js/js_aRVJ3MdDVYsxtzIyliTzcm576TFmee9hAxhtWFHgGbw.js .https://gov.wales/:.C#X /.....6.3.....XVz.....25oqqEA.A..Eo.....ll.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9b6b42bceab5fdf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.57580890789501
Encrypted:	false
SSDEEP:	6:mKQhyEYET08NWQASxYOno/PyYlLrxS5mDrQXhK6t:2y0g8NWQXnoHr0mDcX7
MD5:	9A065FCCF445196E7805C562BF5DADB8
SHA1:	DE314FE2B4106C54D23C9E0C2416286809E5A1BA
SHA-256:	BACD4725176E290EF70EF6CA440741E2CB7C614F1F371566DDD222F40116A508
SHA-512:	95398B58867985F38AC18F4BE95CF145B5B69794611F707D89765687F9D1278A796A8BCA084039FC8D0D2E926C3DFD0E742ADB2E60DF81F0DC7BCA75289F4456

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9b6b42bceab5fdf_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....Y$....._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js .https://gov.wales/.`N#X /.....`.#..5.GS..].... ,..y.a.g....%.*&.A..Eo.....'.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fad1842d86d53f14_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	175648
Entropy (8bit):	5.955080063876609
Encrypted:	false
SSDEEP:	3072:P6bOPr7OWjobCF7eLG5WWDH8PQFOx8LwWdZ/2qZI:P6bGx8GNWCcfGC
MD5:	B50F33EDD50ECDA163D03A2BDC182DD8
SHA1:	95179502C5612183106906C1AD7F03D198677A6F
SHA-256:	0BE771407DE7F51EA92636E886A770C17483C62E752002B553283BDBB439A80D
SHA-512:	3C7E24981A138CC179EB0E09662B529943E6A8AFD938A05B1BBA54EA716299DD234EA6D5D7610EB93820BEE1EEC6449B639A0E1F6AA7449F17C5CAECE67687 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...r..Z....7998173EEB06017D11CA901044BA525EA3B4E1F6C7F60807E42DB83F86146DBD.....'.....O9...h.....]..... -..D.....d..... .....h.....d.....`.....(S.=...`0....!.L`.....$L`.....(S.....Ia....Z.....Qdf.....p arseCookie.E.@.-.....P.....w...https://www.gov.uk/assets/static/header-footer-only-21591776c6c870857b1b0569af6e383cf216bcfbd4af446fbc145a969efadd0c.js.a..... ..D`....D`....D`.....`^...&...&....&.(S.p.`.....L`.....0Rc.....Qb.....t...`....I`....Da....Z.....Q.@..o.....module....Q.@...H....exports...Qc.hw.....document...(S.....5.a..... ....>...a.....a.....1?...a.....a.....Pc.....exportsa...'...I...=....d.....K`....Dv(.....%.....s..6...&.(...s..)...&.(.....&..&.^.....&.-...%.....&.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fca4f098b45fdfca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.6029196844243865
Encrypted:	false
SSDEEP:	3:m+leZ1A8RzYrSLSELDXZCLRCcWvNRAdGnKvlltlHCMn/l/qcPgJlwaVMmR4ltpK+:mbYGLSmXZCLRC21vlYMVPGXR4ZK6t
MD5:	88C7304A3670E24A8B696ACE498CB0EB
SHA1:	87CEC7F76617FE34C971718AB700BAFE2B364753
SHA-256:	A842EF227417F4762BB8D756A6B5DAA9E797B293ADCD4CB40D732AEFD3747087
SHA-512:	AB87F7050ED3E508F15A66A3556B598217248EFE9EFF8817BDFC1C7BD4B0BA520F444995997B93DF2AF8E40915EDCC5617933276CBC7B947243E4FB084285D9F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....N_s...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-MBLNKRW .https://gov.wales/..J#X /.....Z.....P.F..Z...IT.{....B.....2.6..A..Eo..... ....A..Eo.....

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):	0.8850047831749283
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwrQXeHA8ePZ2:TekLLOpEO5J/Kn7U0Jeo
MD5:	9A23528FDBDA2446A8659EE3B798CA24
SHA1:	F34C3F63FB7D79EF4B00FB98FA2B856474465F60
SHA-256:	CCC5D5A7347EA1948EA74BDDC92BDE96D3171EA92445F4CB195726CAF83B7B99
SHA-512:	2205735152441C98A45B3FA41AEE64118D1A961D30B5238B2C667083B3E4649958F057DA5DA9E2AB710AFE98AB5278B7E801CE6ADE04D9373A9201AAA3554298
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9677210026836875
Encrypted:	false
SSDEEP:	24:d2+tYeFzqLbJLbXaFpEO5bNmISHn06UwX8:d2UYehq5LLOpEO5J/Kn7Uc8
MD5:	1884D5749D4EEB83F22FF3D43D8AC5A6
SHA1:	0D50CC40140D09B45E8584756396560BE6984070
SHA-256:	FAD0C07A4FB7EFC09DA2B283CDBBDDEB934CFFA7E84EB891728B8DAD8FF405D9
SHA-512:	FC4E407CD319847A09F08729658A580A44A780515932975AD964915FD32567CEE0980369D22109D6EB89A1378E9CDB40E0C91FB2793AC4FE3E59C2DEF666CF6F
Malicious:	false
Reputation:	low
Preview:	.....2.2m..... ....

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):	39925
Entropy (8bit):	3.2135860425882763
Encrypted:	false
SSDEEP:	384:OCb3XBnCmN33e3BkXugGHr3d5bwabxi5363Xc+3wl63sFa3lF90X8v:OCbnNCQne2X1GHbQF5qRk68FaVFrv
MD5:	646E7926B964C4AFF2A90A6DF4984011
SHA1:	197E8DAF01867C806E27C622134BCF916237FA2F
SHA-256:	F74A9FB4E16E1A1720D5D0A9856F822E6711A4C48687194E2FA13C782C4F777B
SHA-512:	4E05317724B3DD3DC569070ECD46241F61D051992EBA4093464E348D8ADA62D2BB847ACD4C9CFD599E41DD4171639ADE7AA763CA7FC676C408210234CF82EC9
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...31cde1e6_56f0_4bfe_bff0_efe9172f094d.....0..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....-..(.....Z...https://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel..J...C.o.r.o.n.a.v.i.r.u.s. .(.C.O.V.I.D.-.1.9.).:. .d.e.c.l.a.r.a.t.i.o.n. .f.o.r.m. .f.o.r. .i.n.t.e.r.n.a.t.i.o.n.a.l. .t.r.a.v.e.l. .-. .G.O.V...U.K.|...x .....p.....h.....`..... .....(.....jY.....kY.....Z...h.t.t.p.s.:.//.w.w.w...g.o.v...u.k./.g.u.i.d.a.n.c.e./.c.o.r.o.n.a.v .i.r.u.s.-.c.o.v.i.d.-.1.9.-.d.e.c.l.a.r.a.t.i.o.n.-.f.o.r.m.-.f.o.r.-.i.n.t.e.r.n.a.t.i.o.n.a.l.-.t.r.a.v.e.l.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd..............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.................F...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	325
Entropy (8bit):	5.254850854325061
Encrypted:	false
SSDEEP:	6:mVJjoF3AQ+q2PcNwi23iKKdK8aPrqIFUtpwJtLgZmwPwbAQVkwOcNwi23iKKdK8h:XFN+vLZ5KkL3FUtpiE/PS9V54Z5KkQJ
MD5:	4CF50F96AE986D7D706366F4EB273BD2
SHA1:	E5D81A1AEF31E221114AC3CB2C4BAB896F27B824
SHA-256:	29C5CFDA75244DBEBF9FF5E5987E005940C8C29697A93B2A6457EEAFBF31A0D4
SHA-512:	3450219B6887337002F218C3E16C758DE7422A8BEC1651A012D6E649BC23CA2F6A71EFD7F769E975181501271B594F4CA4F8DAB262BCF4CB71061111BECE5E39
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.397 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/07-11 :45:56.399 57c Recovering log #3.2021/05/07-11:45:56.400 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

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):	325
Entropy (8bit):	5.240298410545787
Encrypted:	false
SSDEEP:	6:mVzpQ+q2PcNwi23iKKdK8NIFUtpwFPwgZmwPwFPwQVkwOcNwi23iKKdK8+eLJ:j+vLZ5KkpFUtp2Z/P2NV54Z5KkqJ
MD5:	58CE6DEE3C8674EE7362617A6F08B0DE
SHA1:	810866D96756065B2BCD1881BECB4838F937AE2F
SHA-256:	B691CAD42E70853AEB999C5C4291DF3E485EA04C8BB7A7EEEB5528D82C9AE90E
SHA-512:	B257D878A8F4CBFCA44F6E055A0394C2CCA5549992FC13D89FF76C275A941ED4C4A570E17B3BD95519297D7AB9A814C95A19D49774113543B26275FD59451191
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:58.588 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/07-11 :45:58.589 57c Recovering log #3.2021/05/07-11:45:58.589 57c 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=","VtBwXoadI3EP336rAiL33Gz19KGqtN+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):	65536
Entropy (8bit):	2.510603200068491
Encrypted:	false
SSDEEP:	768:TWVzMsT1FIsfe1FDsme1FPsue1FcUsgxe1Fq8o:T2zMsxFIsfGFDsmGFPsuGFcUsgxGF+
MD5:	536A4B4C3C7B96D4EA404909C43A6E3A
SHA1:	C1D017A7ED854D9157BC8CC8540D8E239346C41E
SHA-256:	2C86CC8921807F80C24C19CAB4E5108FAC962189CE8E08F5CE40D623133A5D92
SHA-512:	6A7664E76BFD4F74B4694214DE2E983EBA9F13AFB0FF74A66F84CA139B495DC798B7688CEAFB097EB21AD0B6C36F864E0C6FB957F4E569A53823283914666D2F
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):	60712
Entropy (8bit):	1.4264660183946936
Encrypted:	false
SSDEEP:	384:gh2nB1FBsce1F/s37e1FMCsm7e1F1CsXdHCj:VnB1FBsce1F/sLe1F7s4e1FksFo
MD5:	B173123B4ACECF10A0F3A72120E8B246
SHA1:	0779A12F01F11DD153AAD47686345683074E0A36
SHA-256:	B2212B5CF230F588F6E3D1466B8B4BEF13625B0DB7E235B04DF3282910CB5A35
SHA-512:	46542C7161614C1EC1E773F8E2DC71FED5FD909CDFDE010DBC50FD82210B8F41E003DBC6C0D7E49604801D53B8E458D4E240B8A17D3D3D0875B80E7813B3281
Malicious:	false
Reputation:	low
Preview:	.....c,..... ....

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):	380
Entropy (8bit):	5.280109267350162
Encrypted:	false
SSDEEP:	6:mVwV5g+q2PcNwi23iKKdK25+Xqx8chI+IFUtpwwMomWZmwPwwMGcNVkwOcNwi23U:pV6+vLZ5KkTXfchI3FUtpZaW/PZHgV5b
MD5:	FCCA6FC0E2333A50FD02FFCCED5DE40E
SHA1:	9D5096913551689377B5D4C0BF3A587A56AFA0DB
SHA-256:	E768FCE7E9430D8FE3DF006E289A1F33A4A1F00F81308181E3B8D99FFB1737AC
SHA-512:	24B8AD38D6E41B02AA5C21EF90DD1619C5174681BFA43ACC8E116C8058A61F58F321BECC589867B2D76487C8B9AE18DCBAA72D519CAF64E33ACD5D51974B40 9B
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:09.733 1bcc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/07-11:46:10.466 1bcc Recovering log #3.2021/05/07-11:46:10.494 1bcc 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):	366
Entropy (8bit):	5.241555159833339
Encrypted:	false
SSDEEP:	6:mVwV9WB+q2PcNwi23iKKdK25+XuoIFUtpwwVTWZmwPwwV2VkwOcNwi23iKKdK25y:pVUB+vLZ5KkTXYFUtpZVTW/PZV2V54ZR
MD5:	0400A7E54827E079B3C2C078B86B1BEB
SHA1:	EBBE67E25758758790292A8CBF87FDF2CB53051A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
SHA-256:	253601793570E13AE1231235EB6B7D41AD3B3CB17C016CDEFB05CC0FD928E31A
SHA-512:	2F19574D82C853D2B77CF7EB8BC44470A745F71D8DDFA4D0D8BC4AE6F179B918DE1410E96BC0738836FF0F3DB79010C855E703966D94883F5173130A64AA7BA
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:09.391 1bcc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/07-11:46:09.405 1bcc Recovering log #3.2021/05/07-11:46:09.412 1bcc 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):	338
Entropy (8bit):	5.280075794781651
Encrypted:	false
SSDEEP:	6:mVwVH+q2PcNwi23iKKdKWT5g1IdqIFUtpwwVTCWZmwPwwVDVkwOcNwi23iKKdKW4:pVH+vLZ5Kkg5gSRFUtpZVGW/PZVDV54h
MD5:	66DDF2233D242CF674B4C140DAAA619E
SHA1:	23A8AC30723CBF0673EA8A810E61917CF72A3D51
SHA-256:	146BCBD22811239AD5409BD89E3FFE1BD42FFF250E3182035889637EE0FB3A32
SHA-512:	03432F19A76B3D330FF1832AB2C3AC6D0C66950F128E11958F9DF3198A2FBE5E51AAFB13E136850CD9936B138B741077CDF6847D8BD17FB8D0D09F20EB2BE9E
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:06.913 1bcc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/07-11:46:06.915 1bcc Recovering log #3.2021/05/07-11:46:06.922 1bcc 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):	184320
Entropy (8bit):	0.9126146710806708
Encrypted:	false
SSDEEP:	3072:ePP7IFI73oGFW7q6GFi7pJGFRI7Y6xGFm:ePP7IFI7tFW7QFi7OFRI7jUFm
MD5:	98EEB26C88765C70A7683798BF524F13
SHA1:	84063D5333AEC183F1153CF0AF26CF50C8BF9FF3
SHA-256:	093726B6675E47C33E1E55F176258EEBB61700B54602846EC99AB9EF0B343275
SHA-512:	4B56A12241D066020559408B4BAD52AB6AFF04D089C2C56B3024361B6CEE1013A4604C621B476071FE0048A27576BA8DB1B89D85BE74C1F58255D34F302665FE
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):	888
Entropy (8bit):	5.452623175975301
Encrypted:	false
SSDEEP:	24:/6amxeY13aukKB5CZLPZMQbXoDY78BJgskfa9yBDOma1m0TW8tbasH5Wn:/54aukoCh5EHUja1ltbDA
MD5:	68AE43AC3F471822C75A208D81230DBC
SHA1:	BB9842379DD983D9DA9107588CAEA8C0B9A47D21
SHA-256:	C5AB743B0054C9F2C0CCEDB1E5E843DF2B0B9230F6CF71E1ED73313E81177BAA
SHA-512:	6E7CBA7249B2515E2D2FE94B33EEFE4EABB477FBED5ED583B318811B297E76C427FAC9D201991967905A4A075DFBA0753766E7BFF98B643BB4DBE24E8BFB3388
Malicious:	false
Reputation:	low
Preview:	....."h....19..coronavirus..covid..declaration..for..form..gov..guidance..https..international..travel..uk..www*.....19.....coronavirus.....covid.....declaration.....for.....form.....gov.....guidance.....https.....international.....travel.....uk.....www..2.....1.....9.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w...:w.....B..... .....*Zhttps://www.gov.uk/guidance/coronavirus-covid-19-declaration-form-for-international-travel2JCoronavirus (COVID-19): declaration form for international travel - GOV.UK:.....J!.....(.1=BFT.....$)-;DH

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):	187824
Entropy (8bit):	0.69150560457724
Encrypted:	false
SSDEEP:	384:2WgT1F47uYe1FzYX7Exe7e1FladYX7y3Xi7e1FhdYX7WN/LC:hgT1F47je1FW7Sge1Flf72Ee1F67QG
MD5:	B2D170BF6A2E6CBBC1459D904B55571F
SHA1:	C6920035EA7AEAA806356052262D1E67F80B39A4
SHA-256:	48250AD0E60C59D00C940E864B6622910D4CC97667330CF023A8471319FF4021
SHA-512:	79F476AA98EB514A8E22F792BCAA3D12777A5D97F67737C8D100C59F8ED6E7F0B09A304AC0922B84526BB1AA3A5613F15CF25D720B6CA383AF277137A7252536
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.480534096957366
Encrypted:	false
SSDEEP:	48:BHnGg/claa71aMxd8dbpYBmRgprbQSefgGeNrS0U9RdiN9t:p90laa71aMx2dbpYBmRgprbQ5fgGSrSS
MD5:	7F0951CEF3DAB0296508023EA7A98A15
SHA1:	72C36BD6E9A062D56574E3FD63DD3059E9A1DF26
SHA-256:	85C1EE178FC008743542069DB621901430B5BF3D668C754B95A57C87ABDF50D5
SHA-512:	CC3F5B7989BC04B2FB59997D1FC0179F860393120159508AA39AB5CBC9F31ADAD6A92726721D4894110DC0B3B25784D00951D3D19E36E57560B32099D8CD83D
Malicious:	false
Reputation:	low
Preview:	...%...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..572390000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-07 11:46:14.49][INFO][mr.Init] MR instance ID: 88f30593-ae8c-4007-bed4-6a65b9a5de86\n","[2021-05-07 11:46:14.49][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-07 11:46:14.49][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-07 11:46:14.49][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-07 11:46:14.49][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-07 11:46:14.49][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-07 11:46:14.49][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):	337
Entropy (8bit):	5.253532266641821
Encrypted:	false
SSDEEP:	6:mVHC4+q2PcNwi23iKKdK8a2jMGIFUtpwHQFmZmwPwHWNVkwOcNwi23iKKdK8a2jz:QC4+vLZ5Kk8EFUtpg6m/PgOV54Z5Kk8N
MD5:	393447B095283C3A93C47508F5BE5CE1
SHA1:	75C6E596D44CB1CC4612A53674683479B462A855
SHA-256:	00C2369D83EFA4B43E4EDAD76AB69426BB4973F08A440B956E84448724B31D32
SHA-512:	A0F359D1DDA26E55FC8427D9D16A90A0DCC2AD5760160E25680660AED17D2F84B8A4CF87944361742D5D3D1F3B11E21329CF7AF7CCA7EC38FFB87B393F9D8F6
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.093 8bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/07-11:45:56.095 8bc Recovering log #3.2021/05/07-11:45:56.096 8bc 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):	73728
Entropy (8bit):	1.1531356703209745
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
SSDEEP:	96:vOqAuhjspnWOfOqAuhjspnWO/OqAuhjspnWObOqAuhjspnWOy3YOqAuhjspnWOI7:HiiK1mRm
MD5:	935093C2243504D602283E4F994E3439
SHA1:	3DBB75823D4B88F857371FA5F809F6A6075AA460
SHA-256:	E99691A292E902C561A4F015F79064F29661F6931F9CCF5BD17AC9E563807184
SHA-512:	B757199CCDC549AC0C056BD08A2641FC41F6C78FC2DB79ACA9AF19429D8198DC0F0F7D129475257454E66B16EFBCDDC932B9265EBD3039E9A2DD61B7127194D
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:	dropped
Size (bytes):	77016
Entropy (8bit):	1.0944668102993582
Encrypted:	false
SSDEEP:	96:FlWUOqAuhjspnWO9kOqAuhjspnWOGP0OqAuhjspnWOpMEOqAuhjspnWOrUOqAuhP:qyQi/SbCiyIiP
MD5:	97659192064DA6A7DB8AD7665B57733D
SHA1:	284B857DC3AFD07FE268AB81990547B386440D30
SHA-256:	D31036B6187A8C7521B3BBE63BE11EB13068C05228F342474237741 49A456617
SHA-512:	D486647B6BA7DFC22CAD2372F198D64F82C495A44730735C2C4E3434CADCF20A7277AFD3341194104E00F81F4832BBE2866B7D86B0AE44681371EC52D97E4C0
Malicious:	false
Reputation:	low
Preview:	.....y..... ....

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):	339
Entropy (8bit):	5.231104435765628
Encrypted:	false
SSDEEP:	6:mVPQ+q2PcNwi23iKKdKgXz4rRIFUtpwwP3AgZmwPwwP3AQVkwOcNwi23iKKdKgXS:5+vLZ5KkgXiuFUtpVPZ/PVPNV54Z5Kkt
MD5:	8D422FE3CE934DA7CCC9D6D8AFA180AA
SHA1:	737A2ECBCABF6750986FC36C3BAD34B62EB25B8A
SHA-256:	096E43F51506FA212B1F6D273574502E5182C0C350DFFFC308D1AC57E8E9F194
SHA-512:	450115A8447C03E79E1293B6165D2D8141C72F990001DFA9AD8234B06FF0A6A8515C385929E0F904938AC2805A4F1ED01A6C043159301DB19BA7246884EEDFCF
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.423 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/07-11:45:56.425 57c Recovering log #3.2021/05/07-11:45:56.425 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.0114014506959284
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoU:wIElwQF8mpcSJ2Yi1
MD5:	7C1A2011D2BBCE4FFE977FEACB7FDD39
SHA1:	AE3216712A5C66DE35DFD8A740CBC2B2A1A3623F
SHA-256:	A28629CDAC2F463EBBB8E0BD042671275F5E202C8A20ABF5BCBF5B41807EAB0B
SHA-512:	70545A084B1E236A36C5E18867F7FCFAECBCC5E16B4E92F4E013F62586F7070045AE696E0D18657FD59E0A717CBD5B7A2F0DA8927F67D75A5F4BF2A4BB85998
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
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):	0.82537563615284
Encrypted:	false
SSDEEP:	48:d0qklopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUR6:d0hIElwQF8mpcSY
MD5:	327CF28937BD051ED78C6A18D54638B3
SHA1:	DF594427B41EE9368FDC5D9A6C3EADE4F138A5C4
SHA-256:	23F8C20AE7429586E6F7733A77DA91F2458FC00171491C7F38D6B0E4181F0C1D
SHA-512:	EB70EC9F1E789FE2CEA44D9287666E24A423B83C68251292B74B578E3ECEE1F23D4E8473D932CBFC31EEF90976E739B09C1EBE09234321EC7793D0CD382C537
Malicious:	false
Reputation:	low
Preview:	.....8.A..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.1827002401718625
Encrypted:	false
SSDEEP:	12:5lKIX7NGTKtfXw93FuXlmQshLe9XlEdK2JIayOluy7:7KIX7Nz9wl0XonJe91EYNayOlH
MD5:	50C601CDA0CBDB296D0EA756DD80FEE4
SHA1:	10ECBED064661B3D2330DAFC9E7A105CF5E1B3D5
SHA-256:	BBA4008629B13E77C745800D1023BFE96230450678F6B8FA8A1D6B262AA93EEE
SHA-512:	1980FC984213C3CB924E00EF1C6C43FCFEF7AD6362FE9C22A9BE134F45C5AE71E3F77BF6BBCBD31B95B9465678EAB9960AEA7B53D7BECA860DCB6BF125036 75
Malicious:	false
Reputation:	low
Preview:	..&f.....c..a.....next-map-id.1.Bnamespace-31cde1e6_56f0_4bfe_bff0_efe9172f094d-https://www.gov.uk/.0V.e.....V.e.....V.e.....a..... .....next-map-id.2.Bnamespace-5a642eef_4e50_4664_b7d0_c1993b629fd3-https://www.gov.uk/.1. .....\].!a.....next-map-id.3.Bnamespace-29b8a147_dd 75_4a0a_b7ac_17e743cd566f-https://www.gov.uk/.2....a.....next-map-id.4.Bnamespace-f53a6056_ebdb_405a_92f1_6c579338098d-https://www.gov.uk/.34.+i+.... .....map-2-this is the test string...:a.....next-map-id.5.Bnamespace-b8041dfc_b988_4e73_ab08_fa2294b41e4a-https://www.gov.uk/.4

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):	328
Entropy (8bit):	5.1966333907608835
Encrypted:	false
SSDEEP:	6:mVJbVL+q2PcNwi23iKKdKrQMxIFUtpwJ311ZmwPwJOlLVkwOcNwi23iKKdKrQMFd:RvLZ5KkCFUtpq11/Pl54Z5KktJ
MD5:	F0C9705C25F8826096B4E55F92196A4A
SHA1:	ACF071A22F9086C6312B61E51D822047F8807C02
SHA-256:	F39C1228980EC1A84C71CF0EE251BB4759DFBA874F5D327EC5F7DE84360B0CA6
SHA-512:	1A1899948287D25D16A00C8BBC79F344C9140F679E0A94C27FB1A4A5C2D4913FF7F4F64FC44F2F75D5622B3294388BECD62844720B04C2371ADC7030A0AE79B9
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.305 17a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/07-1 1:45:56.307 17a8 Recovering log #3.2021/05/07-11:45:56.308 17a8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.207850406784615
Encrypted:	false
SSDEEP:	6:mVN2opQ+q2PcNwi23iKKdK7Uh2ghZIFUtpwN0LigZmwPwOuRQVkwOcNwi23iKKdb:7b+vLZ5KkIhHh2FUtpdH/PuKV54Z5Kks
MD5:	90893206296FC960912F0720075052CC
SHA1:	266347E77D77CBB3C98110078F56776C4B6508ED
SHA-256:	CA8954BDBDDFCE51FA744F3B82819A14C0E617EF891F8F432B768C83ACE621B7
SHA-512:	5881DD8BB5011BA225B65BE06E825C7E1E8704F82D81A6B971484ED0CC508CDAC36A68C4D38E88FC857A96438FF9BF166CA265F737F1B484FEAD1FA44F4336F
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.037 179c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/05/07-11:45:56.039 179c Recovering log #3.2021/05/07-11:45:56.040 179c 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\4a15d653-c039-4f63-b5c9-c7d7be415ffb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","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):	435
Entropy (8bit):	5.280254598733388
Encrypted:	false
SSDEEP:	6:mVJVoNAQ+q2PcNwi23iKKdKusNpV/2jMGIFUtpwJbYwgZmwPwJpkAQVkwOcNwi2u:Ok+vLZ5KkFFUtpL/PEk9V54Z5KkOJ
MD5:	FD60618FD3089DCB53EBD64499AAD256
SHA1:	342B1D670285B939BB3B5FCBBB848A1C9132E0B7
SHA-256:	36B31CFEC1F5AFA3BC653207251DC203F7DC83CE9770B1C678685C71F9D2D303
SHA-512:	1C149EA88748D75A7C43B588BD5965942FEEB9C471A9D7786BD3AABDD65354A5A5553A0A25F0C5D6B734FA8D9CA63A9F9051AEB04244D767262C7F7055654E3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Preview:	2021/05/07-11:45:56.337 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/07-11:45:56.339 57c Recovering log #3.2021/05/07-11:45:56.340 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.3251337789519715
Encrypted:	false
SSDEEP:	6:mV5Us9+q2PcNwi23iKKdKusNpqz4rRIFUtpw5WK3JZmwPw5AVkwOcNwi23iKKdKr:Ds4vLZ5KkmiuFUtpmJ/Pd54Z5Kkm2J
MD5:	C23278250A73F6AF5DF45CC7B271D95E
SHA1:	9BBF9706C7625DDFBDA2188D67F8D52360848257
SHA-256:	87DF800EB6FED393CB0F38B21825CAE5EE009594850158A46495370979A98C2B
SHA-512:	F99E61E75D293CA82AC48C6CD0A4362FBADFF3680F7AF0982E51440AD69C75975E30D17CD393B1998B18699FC50A076AA85DCD230005A9CC4C3FC615897665E
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.431 878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/07-11:45:56.433 878 Recovering log #3.2021/05/07-11:45:56.434 878 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):	423
Entropy (8bit):	5.293141271110033
Encrypted:	false
SSDEEP:	12:pzTFN+vLZ5KkMFUtpZz5/PZzT4V54Z5KkTJ:pXMl5KkUgjj36o5Kkl
MD5:	CC894448A2CCC687F571E92E42F5151E
SHA1:	D6ADA49754E5853ECD828D9C92E7BE548E9CD149
SHA-256:	1F56F490C02A7AD1903D2F53E12764A06081299C72BDA81FCDAFA66064D7CC30
SHA-512:	3E4E607C3317B0C4651ABB928F12BF202148F9D177847E014E52B24618D4DB9904957B377BD675D03708DDC99FB52269734BC7C7A08211E538CB64ACB71FD0A0
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:13.146 8bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/07-11:46:13.148 8bc Recovering log #3.2021/05/07-11:46:13.149 8bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	438
Entropy (8bit):	5.23254225578706
Encrypted:	false
SSDEEP:	12:pVEvLZ5KkkGHArBFUtpZVRz1/PZVRz54Z5KkkGHAryJ:pkl5KkkGgPgj/9o5KkkGga
MD5:	5137D8C355B2099898BCEC029676CEBB
SHA1:	8A2C064DE618368EFC04672B0CBF2FF7CA3E1070
SHA-256:	61E6624D5D0C83F05707387D67DBCC1738F071B4B5FDAABC0CCFDFA933B305AF
SHA-512:	1642E5E1C519F2FE45ED17FCCE6A4036807483889BBB61CCF0E4D3D913D82D31897600C7B5E84A9939A6B5E9DE70BA110DB470ABF06112667987D0375D25746
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:07.363 1794 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/05/07-11:46:07.365 1794 Recovering log #3.2021/05/07-11:46:07.365 1794 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.25174144312673
Encrypted:	false
SSDEEP:	12:pV13+vLZ5KkkGHArqiuFUtpZVu/PZVjV54Z5KkkGHArq2J:pcl5KkkGgCgjWRo5KkkGg7
MD5:	1FA7B964CF4CE797C20D11EF912DC1CC
SHA1:	2C37D7288001B1FB4CF7242EA08F808E29B3DD66
SHA-256:	D0D1180DB8E2460815B38A6CA08B43924D458EF97BCFDE649B035A5A444595FA
SHA-512:	0E5E8EC0145B8CF1B2AF0D20661898E79F80705B73076B14364461461546CEA567F62A7039B5982DB65DDFE0A955BFEED39FBBEC698C87C011EFC7CC4FF9609
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:07.383 8bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/05/07-11:46:07.384 8bc Recovering log #3.2021/05/07-11:46:07.385 8bc Reusing old log C:\Users\user\AppData\Local \Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	423
Entropy (8bit):	5.195395859620627
Encrypted:	false
SSDEEP:	12:pyN+vLZ5KkkGHArAFUtpZs/PZTV54Z5KkkGHArfJ:py6l5KkkGgkgjSro5KkkGgV
MD5:	CC36063AF26039720B8565CDB41FD66D
SHA1:	E120E42D9A6D3B130E2C9C0291D97E583FD323E1
SHA-256:	CF4E04B22DE51EB310640046C6979D5CE33B02A02C095108485605A3BDBA030B
SHA-512:	1C90A536603B33E08CBCF4EACA30C7B9F4DF55AAAC42A1B4E275D8A251EDF8400EC31F5BF02C8CDAB9960F2707446866BA8AF9CE886AADE4A082687D35EBE26B
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:22.761 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/07-11:46:22.763 57c Recovering log #3.2021/05/07-11:46:22.764 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\f2293b67-125d-4be0-8230-bf54e91820dd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.23682698060725
Encrypted:	false
SSDEEP:	6:mVrGlyq2PcNwi23iKKdKpIFUtpwNw1ZmwPwNc+RkwOcNwi23iKKdKa/WLJ:8GlyvLZ5KkmFUtpH/PgR54Z5KkaUJ
MD5:	8FB074F89023D01C9BB3F001BD5FD5F6
SHA1:	A7EF1D813FC41522C599933CD3EAE8FFBB5DFC2E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SHA-256:	936C7D177CA0135144A2525BE3B2D7DF2A891CE6D0ABEF4FF055911E290F870E
SHA-512:	6632B2B27E2F5D6DC7DCC4C6ADB81411E4897AA0474DE86C1060B581E653E9E55AF5E046379A49777F1903A488C531E705B52FDE9A59D650F593D1AC49B2337
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:45:56.029 17c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/07-11:45:56.030 17c0 Recovering log #3.2021/05/07-11:45:56.031 17c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	407
Entropy (8bit):	5.332058612943443
Encrypted:	false
SSDEEP:	12:pd+vLZ5KkkOrsFUtpZtB/PZtVV54Z5KkkOrzJ:pql5Kk+gjlro5Kkn
MD5:	687AD266CFBB409200D3BA6A6B255398
SHA1:	47576D0A7CB39D652B5DC7F8C46474535A64B3D2
SHA-256:	42CD6692F2F9BF951F72E35479E2431599EAE3307A48A5F6182EA95E5C114ACC
SHA-512:	179F3712EAA62A8C9528B79A463A216CB2A745CACF9838EB0114A0DAC53176A611DC38F51F3C9B611C8E98C26114D7BE94667DB2841016E292BE9C1145104439
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:14.484 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/07-11:46:14.486 57c Recovering log #3.2021/05/07-11:46:14.486 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.984904915836519
Encrypted:	false
SSDEEP:	6:Ccyu+jq7+OOK4DI5eMru+bWMtL4tOtRp4zdjTEt4v:CoOK4D0e7GWsQ//
MD5:	2FD2004FA3888F03ADBEC6701708BD21
SHA1:	7CA0893FF02EF682856C72EB5FC241A9473F38F2
SHA-256:	A2413FE86CF591B5DD2F0843393E711C16DCA8755D2CC9796746922A0441ED2D
SHA-512:	4CFC267CB5798F8A394A04B9DC15D34BA68644FB7F0216351DA3E946CC9D8EF83D7F5F75FAD10573DFF8DAB099AAC29EFF211754C7C7C13860E270D27ADEA57
Malicious:	false
Reputation:	low
Preview:	......{T!X.....|....{.....b.-~.-!.....bL..+.....[.....c0.....f.6....."Q..~.....3)N.....4..O.@>D.....O..1i....IQ...`.....PC=..=.....w.....}.....U.....SP.=.....3'$.....v....I..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	
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):	4096
Entropy (8bit):	1.7435321363487153
Encrypted:	false
SSDEEP:	24:LLTqGePNH4OJ33YZt2rjBY+AD9+oJVWdbyBADkq:mH1BYZtmY/VCbybq
MD5:	1A313D2025B58FFC27B58BFFD7EE576C
SHA1:	E57F5F1ECD756E83657D87528A62F96F93596C1F
SHA-256:	7379F1C250EC8EE4C9C2E895268011B06B118D4CF31BA8658C6083340FFE1023
SHA-512:	6AFCCB978595F41DFA762BFA624FDC87F95E421DB77ADF34F969E7787DE23A6AFBA6DE81A3BA37CF13DB5767B6B79192BAC3111B72B21DCD61871AA75A9AD18
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4636
Entropy (8bit):	1.2915040233700366
Encrypted:	false
SSDEEP:	12:sTlhZt28ojEElYDI7tIPcV2Z2kY/oJVWdYQtwBtIPDkGsyBtEXnJ9:sTfZt2rjBY+AD9+oJVWdbyBADk9yLk9
MD5:	C015C1C7B9B22C5730994FC4E9D137A7
SHA1:	1AEA7D16CAC05A92843C42762D1FCB2ADCA940A2
SHA-256:	08561E3C0DCEF08FECF984DC1090B35D2ED75DFFFAB44C0286002C70CD4EC250
SHA-512:	A564C45118D9894F6C75EDD29B61D5CB95B1EFA7BC5768D65766490BA9A3A7B237A745FCA3587A1BCB95300963D6EE651D6ECD0561961B46E297B01672C1C2F
Malicious:	false
Reputation:	low
Preview:	.....$..... .....$..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac2822df-3aef-4ae6-b0ff-30ce08c53cfc.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):	5.535877346142152
Encrypted:	false
SSDEEP:	384:71ZtnLlGFXA1kXqKf/pUZNCgVLH2HfDurUnHG9nTp/g1+4O:pLlyA1kXqKf/pUZNCgVLH2HfyrUHG9nx
MD5:	5ADDA8F5030ABF21F04DC42B5A313CEF
SHA1:	F64190CFE5D6FBC740602E30AD6C91FD39B70676
SHA-256:	69191BC836D2F737340C5F5322E3FA3D93A713A36B6B0905EDE3C438D1F9B632
SHA-512:	BC439420F5A8C5A9D17D6E29AC99A7A7C70866DA360B9C11E9B40193BF39FD9F7BAD54D16E5DBA31FF33A4BE950C130FB96EF0A8B9D6BC10F5E9D95C5B2BCFA7
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":"13264886756004585","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c62a307f-e0e4-48d4-9d9c-151db6cd5188.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):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c9a00579-09e4-44ca-a2de-5d8f853f7bd3.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\Default\c9a00579-09e4-44ca-a2de-5d8f853f7bd3.tmp	
Size (bytes):	1043
Entropy (8bit):	5.575031766655093
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevuUthUeT7Z7wUNAgRUevxQ:YU6UUhveKUevuUDUepwUNHUev2
MD5:	477BF5310BAA068689AB5DEC41FC3EC4
SHA1:	68FC32753732F77709A664A69C0294DE2BADDD41
SHA-256:	F13C23DE42DC941A3212DFB058CCAB3FF15130AD594C8AC330BD42EC8EB7408E
SHA-512:	6C7768EA98BC595536E29937721F62AC2B6D57CE500153E05153E26EF051FD57EF726C65313B54707FFC683D7B86A91D84504FD6C13F2C3709E3CF78D00955E9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1651949168.967734,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413168.967739},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1651949159.470215,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413159.470221},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce2876dd-1d57-496f-820a-68fec2f06d20.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):	5771
Entropy (8bit):	5.188947335088039
Encrypted:	false
SSDEEP:	96:ny3h54/f2Pz4YVDik0JCKL8kTk21pbOTQVuwn:n2hy20Y5k4KvTk2b
MD5:	79F520CF00037115AAC2CD333890BE3D
SHA1:	E984BCA642E72AF470332E067C2D303EC01B8B1C
SHA-256:	053B8BFDE5E2E3A657F8B0A6B9979DC131DAAA79A54891275B3A1D2A5AF8E503
SHA-512:	1F56B781EFBD99EA57C50DD08C61EDA60BB53D5E34DED44C753C4FE6EF8A51CAC15F7B16FC2C90868C13C853ECCF0A65C6C2D554644021DD711CAC56548FF F5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d96011a7-d68a-477a-8244-5603dc1db8fe.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):	16918
Entropy (8bit):	5.580021274661027
Encrypted:	false
SSDEEP:	384:71Zt2LlGFXA1kXqKf/pUZNCgVLH2HfDurUE/gO+4b:ALlyA1kXqKf/pUZNCgVLH2HfyrUE/B+w
MD5:	12D040D7B4C2F8CA97F81AFEB47BDB78
SHA1:	50096110FB693499F55171570A955AC7B0587D23
SHA-256:	DD2A1560C2721C772FAA274CBDF0D827E6838738DB67707F2E8B7B302DD2DFF6
SHA-512:	4FB9213977B71CE9496D2034E1333A1FED4BA8705327E2AD7206D3217CFBC5E01D5AC7E3D011E1964B02FDF83984C0147575F0DCE52101F8E4F628D5BE05B5F
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":"13264886756004585","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.539484143880081
Encrypted:	false
SSDEEP:	3:tUKDS0VV8O0dWZmwv39S0VVTSFOb7V8s9S0VVTSFOb7WGv:mVwV8OCWZmwPwwVeFOHVvwwVeFOHtv
MD5:	9E57306C51157C090081B7BA22D69AEA
SHA1:	D6785F9F045EF39169BAFA6A4883274D7191177C
SHA-256:	71AF14AB09A1ABC1BECF8B3E0C69954DBEE57A550EAB1FDA9880E952829B17A4
SHA-512:	8F77006A23D71A867ECF324FAA73676BEE0AA3DA8EA2B29D4B0E183E1001821B6D79CB2F65C3A43E68EEF6758E319EDAC4438DCCB6DB8C0CDA63706504B83AB0
Malicious:	false
Reputation:	low
Preview:	2021/05/07-11:46:05.240 12cc Recovering log #3.2021/05/07-11:46:05.387 12cc Delete type=0 #3.2021/05/07-11:46:05.387 12cc Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de36b082-cf43-44a9-92fd-825e4b06b8ef.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):	5772
Entropy (8bit):	5.188772150493617
Encrypted:	false
SSDEEP:	96:ny3h54/f2Pz4YV3ik0JCKL8kTk21pbOTQVuwn:n2hy20Ylk4KvTk2b
MD5:	A4BB10E13EF2C264C6CC55E5EFB1E40C
SHA1:	1D2DAF0323EB63DE44D97BCD115894400F73944B
SHA-256:	692991039B7B49716DCEC1C3DAF695D74C6C36FE4B1B99C5B8E46E566B42D33F
SHA-512:	B4C20DEA37404739950F7CA3F3FD46FDBA95D3ED775BDBAE7975D1C15A5390D030B0D51646101E6CAA9C48A457BD66D223AFE47D2FDD53A5E16B14317C745FD5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de36b082-cf43-44a9-92fd-825e4b06b8ef.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264886756394818","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\df4f7e83-fc8a-447c-b311-c03b7692d827.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):	1211
Entropy (8bit):	5.565826250497193
Encrypted:	false
SSDEEP:	24:YPfUgq6H0UhvrRlG1KUev+gbURshUeT7Z7wUNAgRUevxQ:YPfUgq6UUhveKUevtbURuUepwUNHUev2
MD5:	94B08BAB20BDECE19018354066B0A126
SHA1:	BE65A52B54F34C09EEF5F305BEF5797EE9E98E39
SHA-256:	D769B9BEDA0219472ACE224B43F328D2DAD36A42C3DFD3B4243E316BBCCABA2D
SHA-512:	5067BA3DF0F49950EA2FC06D73ED17C0B9B4978FC286AA5790E76C4E5B00613E61CD193079A18DED080718095A8AD8178EE06E99B9A38FC3B6BE5588696B5B8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651949193.206445,"host":"Dl4Fc0vl/YypYkpsDR3ijy3cXV29/8t3AjQ0T8PW0dA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413193.206452},{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1651949198.192181,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413198.192186},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1651949159.470215,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f3a5cb4e-f830-4f6a-b58c-e83c606b6a46.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):	1211
Entropy (8bit):	5.572606517344263
Encrypted:	false
SSDEEP:	24:YPfUgq6H0UhvrRlG1KUevGDUXHhUeT7Z7wUNAgRUevxQ:YPfUgq6UUhveKUevqURUepwUNHUev2
MD5:	146A7E6CCFD81147811CD7FC96625D92
SHA1:	8D886109879FDBBABE52685E0FB70E74AA402990
SHA-256:	6DA095F524F6FD50A8ED908BA84C47198D6045CD9C9E4CC5F9CC9FC76601D25D
SHA-512:	E2ED8E5C3E0D92A6C13CDD98A71CB0426FCE306E7324933E4563C87D563185EBDCD09D80F2695C4FE6022DEB79ED69F7A51FAA807179514FE34513055FD3088
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651949193.206445,"host":"Dl4Fc0vl/YypYkpsDR3ijy3cXV29/8t3AjQ0T8PW0dA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413193.206452},{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1651949208.529476,"host":"nC2obLkia+mErTGSP8RG64GGxhXlrvxI73GMyQBEhAk=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620413208.529479},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1651949159.470215,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	343
Entropy (8bit):	5.257848453122663
Encrypted:	false
SSDEEP:	6:mVwIYw4Q+q2PcNwi23iKKdKfrzAdIFUtpwwIMNAgZmwPwwIdFwQVkwOcNwi23iKA:pGV+vLZ5Kk9FUtpZrNJ/PZ63V54Z5KkS
MD5:	42581088B9A7FE22CB56C2F6C749CFFE
SHA1:	FAF4302247A284FE05FB9EE61781FB39A8FCF2D6
SHA-256:	4F2DF97F17C2B276C8CC33A6D4EC21A9557AD1103FF50D6DA3F3BEEF29C9E78D
SHA-512:	D3AF52409237B2322B414C9B59C7D7917B3348C297E32025D8F4DF98A763B81060B7382854970B74700B0754864ECA26E18BD45325C8AE749F568403456B58C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/05/07-11:46:14.188 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/07-11:46:14.190 57c Recovering log #3.2021/05/07-11:46:14.191 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\a3121961-e5f8-4e7b-b330-2442d20319f3.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):	168025
Entropy (8bit):	6.080390208599209
Encrypted:	false
SSDEEP:	3072:8kJyUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:z+XPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	9C830261F327E0D9649F1709FBCEE1E3
SHA1:	50DD4F5A384A0778C43827CE50D6E312B4CAD091
SHA-256:	3A18D26A2122769F9328739205250ABCC0AB7B0850FB37AC1FC3DDD7C7344E87
SHA-512:	B4879BF346CF7B403D9E244DDE5300AE0A8C25332D838C0B9CB220B8C39B36F760EFED1142D8B42669FF4C69F05AFF65D898E1ABAF3CE06DC65C5333BC81481
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5586f39-5dcc-4750-a22f-cc2569165338.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5586f39-5dcc-4750-a22f-cc2569165338.tmp	
Size (bytes):	92724
Entropy (8bit):	3.7458234069129244
Encrypted:	false
SSDEEP:	384:n7/8MeR72uZY7NkrVvAs3v8K7HGbGburpucOx/i6yNrJ0m9q9e84A7OeCYNh1sVP:1KVpKS//0e/aQKUH/eoKuQIB6
MD5:	AAACE2AEDB2C97AFC9A3866387AAE1FC
SHA1:	BAD92D5D175847DB93A990E52FA75F2937D93D80
SHA-256:	39FABE96C1563228625C1514032BC6E1F6664605FAF65BBEF1A4B1B7A1F773DB
SHA-512:	155ADE81694FFA27A19E346C97D5A7438295BE228261EF6E87AAFDF92DFBCBD114D8C84C1DB8A503312AC1DF801690778FD6F7CDB9C1DEB3E77EB836D4E693C3
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...R98.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\b5a30127-cde3-4d96-b1d6-b2f05f63c369.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7463353144187774
Encrypted:	false
SSDEEP:	384:x7/8MeR7KlulVJ7Y7NkrVvAs3v8K7HGbGburpucOx/i6yNrJ0m9q9e84A7OeCYNx:9eKVpKS//0e/aQKUH/eoKuQIBt
MD5:	9DDA50F0883C8389D51C90E326BF74AB
SHA1:	7F5A2D5BAB696496677FEA1A9573A4B578D800D1
SHA-256:	5C967A8726DC94B370D67799AF6E593C37596CDDC506B3A4791B3A1822836359
SHA-512:	FD0EAF6E949AB8BA4DF990683417AE99A859CCD9BEABB60BAFE50EF8B6D6B1A2F76CD0C68E5A4463E16B9DB10FAAC0FEC5A0470C79CF4498E4261F6BC400F148
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...R98.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\f2eae259-a1ae-41b7-9a47-9bed91064303.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):	168025
Entropy (8bit):	6.080389323799754
Encrypted:	false
SSDEEP:	3072:8kOyUOzhVSf8Smc2qcBB2nb6yqwwxYFqWvLA7bV/nYorVcI8XIssElYTRK:zVXPSlcBknNRFhvgbV/njhcI8II6RK
MD5:	CEF3D98E08D6F214309C110C5F672BB7
SHA1:	C9D23FEAD23CC4507D3774FA1D17A3422B71DEF8
SHA-256:	DA9E5339D5CE9FA65F1D940C7F311400F4CA9195E2272AA70C89FB07B8497420
SHA-512:	4B7DADF269B7FA43CDC64C8C1D86C4FF94C9E5F973C479A09713C641946373223C3253F8F98214B0D29C91ED48E7F53F45AB4927ED89F564C80AFB50EF7CE0A
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":1.620413159187576e+12,"network":1.620380761e+12,"ticks":121189708.0,"uncertainty":4556716.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\3c12779d-782d-44c9-9a03-5a440d0a72b5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531

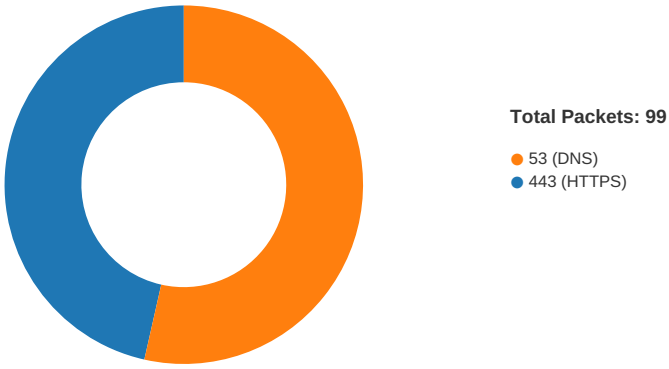
C:\Users\user\AppData\Local\Temp\3c12779d-782d-44c9-9a03-5a440d0a72b5.tmp	
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:45:59.734551907 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.735599995 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.780201912 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.780363083 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.781091928 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.781243086 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.789897919 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.790311098 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.833468914 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.833751917 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.834681034 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.834707022 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.834719896 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.834738016 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.834845066 CEST	49700	443	192.168.2.7	151.101.0.144

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:45:59.836148977 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.836175919 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.836188078 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.836199999 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:45:59.836277962 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:45:59.836302996 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.217001915 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.220201969 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.220513105 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.223702908 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.224543095 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.264624119 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.264650106 CEST	443	49702	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.264885902 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.266731024 CEST	49702	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.267446041 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.267473936 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268469095 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268505096 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268529892 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268532991 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.268552065 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268573046 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.268575907 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268599987 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268620968 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268620968 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.268641949 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.268668890 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.270140886 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.270596981 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.270627975 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.270692110 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.270721912 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.272619963 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.272656918 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.272713900 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.272761106 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.274518013 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.274543047 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.274576902 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.274604082 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.361718893 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.361778975 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.361835003 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.361983061 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.362065077 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.362118959 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.362169027 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.362216949 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.362272024 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.363404036 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411803961 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411833048 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411848068 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411861897 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411876917 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411890030 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411959887 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.411990881 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.412070990 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.412075996 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.412095070 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.412111998 CEST	443	49700	151.101.0.144	192.168.2.7

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:46:00.412116051 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.412169933 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.412983894 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.413014889 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.413085938 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.414669037 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.414693117 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.414779902 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.416378975 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.416403055 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.416474104 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.418186903 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.418212891 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.418287039 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.419862032 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.419887066 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.419966936 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.421536922 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.421561956 CEST	443	49700	151.101.0.144	192.168.2.7
May 7, 2021 11:46:00.421628952 CEST	49700	443	192.168.2.7	151.101.0.144
May 7, 2021 11:46:00.423120022 CEST	443	49700	151.101.0.144	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:45:50.592552900 CEST	58562	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:50.641401052 CEST	53	58562	8.8.8.8	192.168.2.7
May 7, 2021 11:45:51.754530907 CEST	56590	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:51.811716080 CEST	53	56590	8.8.8.8	192.168.2.7
May 7, 2021 11:45:53.577861071 CEST	60501	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:53.631576061 CEST	53	60501	8.8.8.8	192.168.2.7
May 7, 2021 11:45:54.939285040 CEST	53775	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:55.000463963 CEST	53	53775	8.8.8.8	192.168.2.7
May 7, 2021 11:45:55.182149887 CEST	51837	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:55.243810892 CEST	53	51837	8.8.8.8	192.168.2.7
May 7, 2021 11:45:57.682735920 CEST	55411	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:57.731602907 CEST	53	55411	8.8.8.8	192.168.2.7
May 7, 2021 11:45:59.515937090 CEST	58739	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:59.522605896 CEST	60338	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:59.544887066 CEST	58717	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:59.548655033 CEST	59762	53	192.168.2.7	8.8.8.8
May 7, 2021 11:45:59.588094950 CEST	53	60338	8.8.8.8	192.168.2.7
May 7, 2021 11:45:59.597337961 CEST	53	58739	8.8.8.8	192.168.2.7
May 7, 2021 11:45:59.604810953 CEST	53	58717	8.8.8.8	192.168.2.7
May 7, 2021 11:45:59.616204977 CEST	53	59762	8.8.8.8	192.168.2.7
May 7, 2021 11:46:00.372466087 CEST	58052	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:00.434989929 CEST	53	58052	8.8.8.8	192.168.2.7
May 7, 2021 11:46:00.505059958 CEST	54008	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:00.575901985 CEST	53	54008	8.8.8.8	192.168.2.7
May 7, 2021 11:46:00.996901035 CEST	59451	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:01.054122925 CEST	53	59451	8.8.8.8	192.168.2.7
May 7, 2021 11:46:01.355479956 CEST	52914	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:01.421355009 CEST	64569	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:01.422188997 CEST	53	52914	8.8.8.8	192.168.2.7
May 7, 2021 11:46:01.470232010 CEST	53	64569	8.8.8.8	192.168.2.7
May 7, 2021 11:46:02.471096039 CEST	52816	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:02.528346062 CEST	53	52816	8.8.8.8	192.168.2.7
May 7, 2021 11:46:02.762099981 CEST	50781	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:02.821485043 CEST	53	50781	8.8.8.8	192.168.2.7
May 7, 2021 11:46:02.856076956 CEST	54230	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:02.904772043 CEST	53	54230	8.8.8.8	192.168.2.7
May 7, 2021 11:46:04.237345934 CEST	50452	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:04.289199114 CEST	53	50452	8.8.8.8	192.168.2.7
May 7, 2021 11:46:06.247670889 CEST	59730	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:46:06.298124075 CEST	53	59730	8.8.8.8	192.168.2.7
May 7, 2021 11:46:06.316752911 CEST	59310	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:06.427615881 CEST	53	59310	8.8.8.8	192.168.2.7
May 7, 2021 11:46:14.947990894 CEST	58820	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:15.007982969 CEST	53	58820	8.8.8.8	192.168.2.7
May 7, 2021 11:46:15.749330044 CEST	60983	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:15.798877954 CEST	53	60983	8.8.8.8	192.168.2.7
May 7, 2021 11:46:22.106750011 CEST	49247	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:22.169092894 CEST	53	49247	8.8.8.8	192.168.2.7
May 7, 2021 11:46:27.492013931 CEST	52286	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:27.543490887 CEST	53	52286	8.8.8.8	192.168.2.7
May 7, 2021 11:46:29.040411949 CEST	56064	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:29.097656012 CEST	53	56064	8.8.8.8	192.168.2.7
May 7, 2021 11:46:31.771579027 CEST	63744	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:31.833014011 CEST	53	63744	8.8.8.8	192.168.2.7
May 7, 2021 11:46:32.181181908 CEST	61457	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:32.231868029 CEST	53	61457	8.8.8.8	192.168.2.7
May 7, 2021 11:46:33.680314064 CEST	58367	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:33.731823921 CEST	53	58367	8.8.8.8	192.168.2.7
May 7, 2021 11:46:34.097312927 CEST	60599	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:34.164076090 CEST	53	60599	8.8.8.8	192.168.2.7
May 7, 2021 11:46:34.268038988 CEST	59571	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:34.328932047 CEST	53	59571	8.8.8.8	192.168.2.7
May 7, 2021 11:46:34.552155018 CEST	52689	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:34.601136923 CEST	53	52689	8.8.8.8	192.168.2.7
May 7, 2021 11:46:37.612215042 CEST	50290	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:37.666701078 CEST	53	50290	8.8.8.8	192.168.2.7
May 7, 2021 11:46:40.695812941 CEST	56209	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:40.746267080 CEST	53	56209	8.8.8.8	192.168.2.7
May 7, 2021 11:46:41.619515896 CEST	59582	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:41.669651985 CEST	53	59582	8.8.8.8	192.168.2.7
May 7, 2021 11:46:43.143147945 CEST	60949	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:43.191848993 CEST	53	60949	8.8.8.8	192.168.2.7
May 7, 2021 11:46:44.869834900 CEST	58542	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:44.918700933 CEST	53	58542	8.8.8.8	192.168.2.7
May 7, 2021 11:46:52.738435984 CEST	59179	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:52.814815044 CEST	53	59179	8.8.8.8	192.168.2.7
May 7, 2021 11:46:57.333453894 CEST	60927	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:57.403369904 CEST	53	60927	8.8.8.8	192.168.2.7
May 7, 2021 11:46:57.973808050 CEST	62026	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:58.042140961 CEST	53	62026	8.8.8.8	192.168.2.7
May 7, 2021 11:46:58.208879948 CEST	59453	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:58.267822981 CEST	53	59453	8.8.8.8	192.168.2.7
May 7, 2021 11:46:58.337243080 CEST	62468	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:58.399210930 CEST	52563	53	192.168.2.7	8.8.8.8
May 7, 2021 11:46:58.405471087 CEST	53	62468	8.8.8.8	192.168.2.7
May 7, 2021 11:46:58.456572056 CEST	53	52563	8.8.8.8	192.168.2.7
May 7, 2021 11:47:01.392724991 CEST	54721	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:01.461915016 CEST	53	54721	8.8.8.8	192.168.2.7
May 7, 2021 11:47:06.367243052 CEST	62826	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:06.450968027 CEST	53	62826	8.8.8.8	192.168.2.7
May 7, 2021 11:47:07.092861891 CEST	62046	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:07.153359890 CEST	53	62046	8.8.8.8	192.168.2.7
May 7, 2021 11:47:07.219310045 CEST	51223	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:07.268048048 CEST	53	51223	8.8.8.8	192.168.2.7
May 7, 2021 11:47:07.482465982 CEST	63908	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:07.534142017 CEST	53	63908	8.8.8.8	192.168.2.7
May 7, 2021 11:47:07.544190884 CEST	49226	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:07.603673935 CEST	53	49226	8.8.8.8	192.168.2.7
May 7, 2021 11:47:07.801577091 CEST	60212	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:07.850296974 CEST	53	60212	8.8.8.8	192.168.2.7
May 7, 2021 11:47:08.029865980 CEST	58867	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:08.080688000 CEST	53	58867	8.8.8.8	192.168.2.7
May 7, 2021 11:47:08.394486904 CEST	50864	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 7, 2021 11:47:08.468652964 CEST	53	50864	8.8.8.8	192.168.2.7
May 7, 2021 11:47:14.777492046 CEST	61504	53	192.168.2.7	8.8.8.8
May 7, 2021 11:47:14.830348015 CEST	53	61504	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 7, 2021 11:45:59.544887066 CEST	192.168.2.7	8.8.8.8	0xcbd8	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)
May 7, 2021 11:46:02.471096039 CEST	192.168.2.7	8.8.8.8	0xb0ef	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)
May 7, 2021 11:46:06.316752911 CEST	192.168.2.7	8.8.8.8	0xb500	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)
May 7, 2021 11:46:29.040411949 CEST	192.168.2.7	8.8.8.8	0xa1e2	Standard query (0)	assets.publishing.service.gov.uk	A (IP address)	IN (0x0001)
May 7, 2021 11:46:31.771579027 CEST	192.168.2.7	8.8.8.8	0xd2de	Standard query (0)	assets.publishing.service.gov.uk	A (IP address)	IN (0x0001)
May 7, 2021 11:47:01.392724991 CEST	192.168.2.7	8.8.8.8	0x8546	Standard query (0)	www.gov.uk	A (IP address)	IN (0x0001)
May 7, 2021 11:47:06.367243052 CEST	192.168.2.7	8.8.8.8	0xa4f7	Standard query (0)	gov.wales	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.092861891 CEST	192.168.2.7	8.8.8.8	0xc07f	Standard query (0)	cc.cdn.civiccomputing.com	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.482465982 CEST	192.168.2.7	8.8.8.8	0xc209	Standard query (0)	apikeys.civiccomputing.com	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.544190884 CEST	192.168.2.7	8.8.8.8	0x66d	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.801577091 CEST	192.168.2.7	8.8.8.8	0x6899	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
May 7, 2021 11:47:08.029865980 CEST	192.168.2.7	8.8.8.8	0x74b	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
May 7, 2021 11:47:08.394486904 CEST	192.168.2.7	8.8.8.8	0xfaaf	Standard query (0)	gov.wales	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www-gov-uk.map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www-gov-uk.map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www-gov-uk.map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
May 7, 2021 11:45:59.604810953 CEST	8.8.8.8	192.168.2.7	0xcbd8	No error (0)	www-gov-uk.map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www-gov-uk.map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www-gov-uk.map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www-gov-uk.map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 7, 2021 11:46:02.528346062 CEST	8.8.8.8	192.168.2.7	0xb0ef	No error (0)	www-gov-uk.map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:06.427615881 CEST	8.8.8.8	192.168.2.7	0xb500	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:46:06.427615881 CEST	8.8.8.8	192.168.2.7	0xb500	No error (0)	googlehosted.l.googleusercontent.com		172.217.20.1	A (IP address)	IN (0x0001)
May 7, 2021 11:46:29.097656012 CEST	8.8.8.8	192.168.2.7	0xa1e2	No error (0)	assets.publishing.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:46:29.097656012 CEST	8.8.8.8	192.168.2.7	0xa1e2	No error (0)	www-gov-uk.map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:29.097656012 CEST	8.8.8.8	192.168.2.7	0xa1e2	No error (0)	www-gov-uk.map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:29.097656012 CEST	8.8.8.8	192.168.2.7	0xa1e2	No error (0)	www-gov-uk.map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:29.097656012 CEST	8.8.8.8	192.168.2.7	0xa1e2	No error (0)	www-gov-uk.map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:31.833014011 CEST	8.8.8.8	192.168.2.7	0xd2de	No error (0)	assets.publishing.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:46:31.833014011 CEST	8.8.8.8	192.168.2.7	0xd2de	No error (0)	www-gov-uk.map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:31.833014011 CEST	8.8.8.8	192.168.2.7	0xd2de	No error (0)	www-gov-uk.map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:31.833014011 CEST	8.8.8.8	192.168.2.7	0xd2de	No error (0)	www-gov-uk.map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
May 7, 2021 11:46:31.833014011 CEST	8.8.8.8	192.168.2.7	0xd2de	No error (0)	www-gov-uk.map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www.gov.uk	www-cdn.production.govuk.service.gov.uk		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www-cdn.production.govuk.service.gov.uk	www-gov-uk.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www-gov-uk.map.fastly.net		151.101.0.144	A (IP address)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www-gov-uk.map.fastly.net		151.101.64.144	A (IP address)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www-gov-uk.map.fastly.net		151.101.128.144	A (IP address)	IN (0x0001)
May 7, 2021 11:47:01.461915016 CEST	8.8.8.8	192.168.2.7	0x8546	No error (0)	www-gov-uk.map.fastly.net		151.101.192.144	A (IP address)	IN (0x0001)
May 7, 2021 11:47:06.450968027 CEST	8.8.8.8	192.168.2.7	0xa4f7	No error (0)	gov.wales		192.124.249.167	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.153359890 CEST	8.8.8.8	192.168.2.7	0xc07f	No error (0)	cc.cdn.civiccomputing.com	d3bipqqt7o7bp0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:07.153359890 CEST	8.8.8.8	192.168.2.7	0xc07f	No error (0)	d3bipqqt7o7bp0.cloudfront.net		143.204.209.98	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.153359890 CEST	8.8.8.8	192.168.2.7	0xc07f	No error (0)	d3bipqqt7o7bp0.cloudfront.net		143.204.209.67	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.153359890 CEST	8.8.8.8	192.168.2.7	0xc07f	No error (0)	d3bipqqt7o7bp0.cloudfront.net		143.204.209.51	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.153359890 CEST	8.8.8.8	192.168.2.7	0xc07f	No error (0)	d3bipqqt7o7bp0.cloudfront.net		143.204.209.101	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 7, 2021 11:47:07.534142017 CEST	8.8.8.8	192.168.2.7	0xc209	No error (0)	apikeys.civiccomputing.com	apikeys-lb.civiccomputing.com		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:07.534142017 CEST	8.8.8.8	192.168.2.7	0xc209	No error (0)	apikeys-lb.civiccomputing.com		80.75.66.243	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.603673935 CEST	8.8.8.8	192.168.2.7	0x66d	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.603673935 CEST	8.8.8.8	192.168.2.7	0x66d	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 7, 2021 11:47:07.850296974 CEST	8.8.8.8	192.168.2.7	0x6899	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:08.080688000 CEST	8.8.8.8	192.168.2.7	0x74b	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 7, 2021 11:47:08.468652964 CEST	8.8.8.8	192.168.2.7	0xfaaf	No error (0)	gov.wales		192.124.249.167	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
May 7, 2021 11:46:02.655308962 CEST	151.101.0.144	443	192.168.2.7	49719	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		
May 7, 2021 11:46:31.925214052 CEST	151.101.0.144	443	192.168.2.7	49796	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

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1880 Parent PID: 608

General

Start time:	11:45:54
Start date:	07/05/2021
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/guidance/coronavirus-covid-19-declaration-form-for-international-travel'
Imagebase:	0x7ff76d1c0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 3080 Parent PID: 1880

General

Start time:	11:45:56
Start date:	07/05/2021
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=1572,6179841392289751219,8571533054898512681,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8
Imagebase:	0x7ff76d1c0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly