ID: 412529
Cookbook: browseurl.jbs
Time: 18:52:23
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

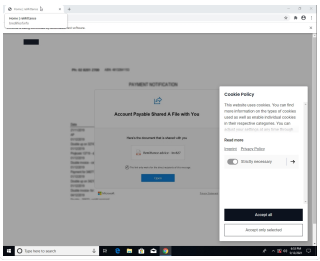
Analysis Report https://www.bredlifeof.info/

Overview

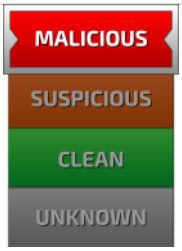
General Information

Sample URL:	http://https://www.bredlifeof.info/
Analysis ID:	412529
Infos:	

Most interesting Screenshot:



Detection



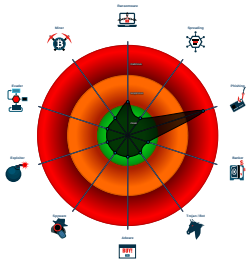
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6128 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.bredlifeof.info/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5172 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,19381948695824494,2468386753968997499,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1772 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

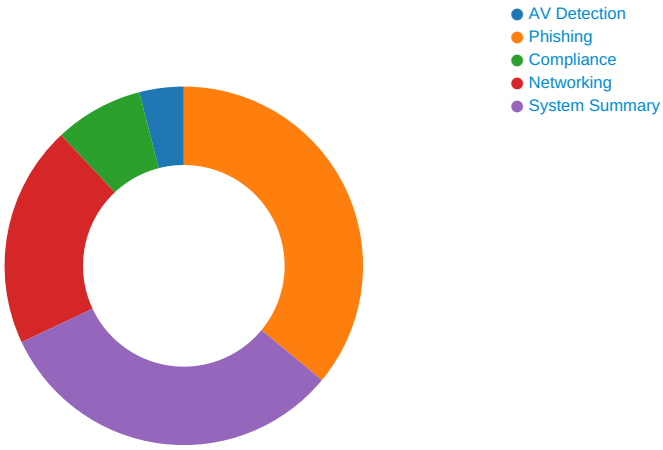
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

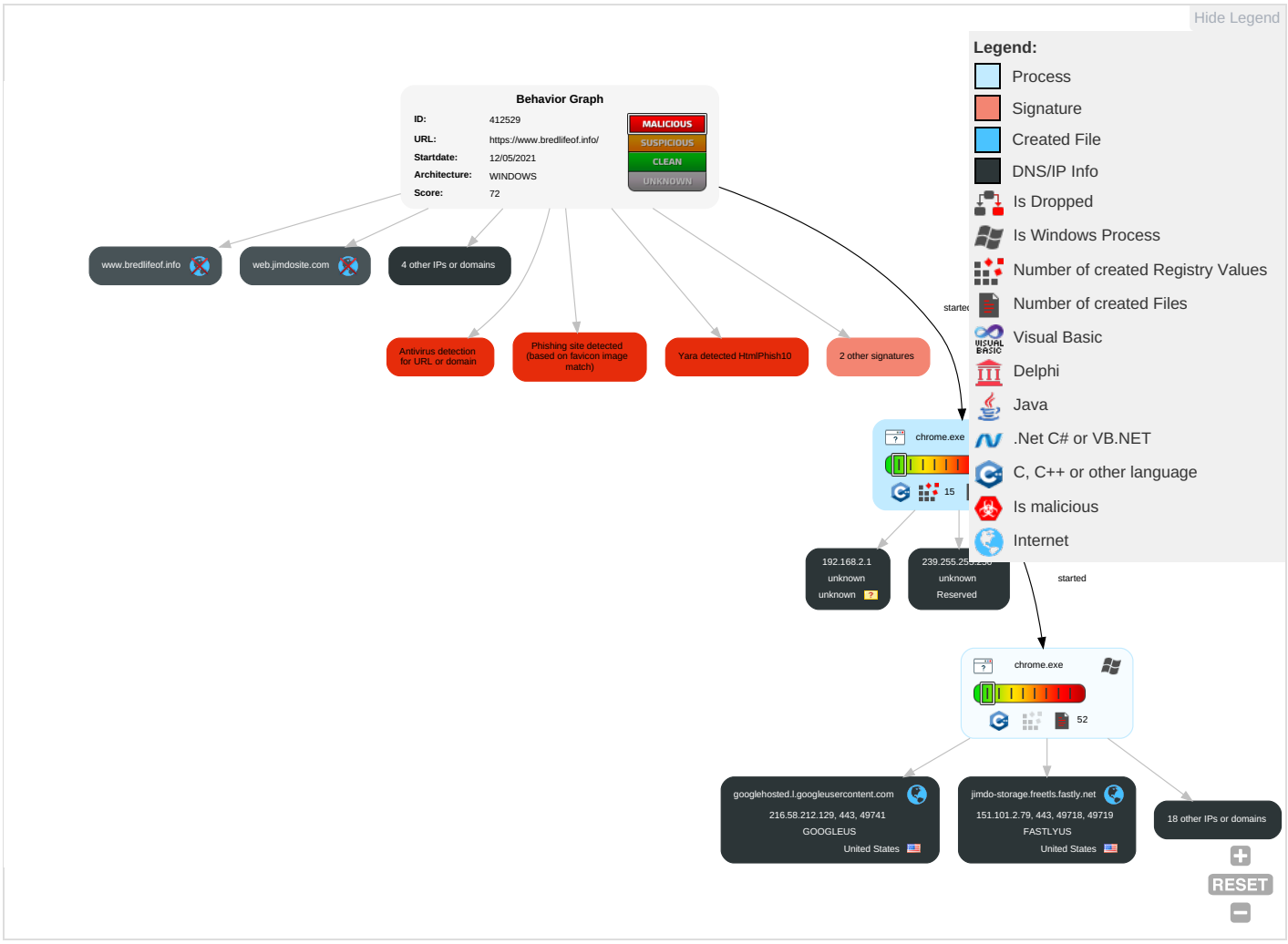
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

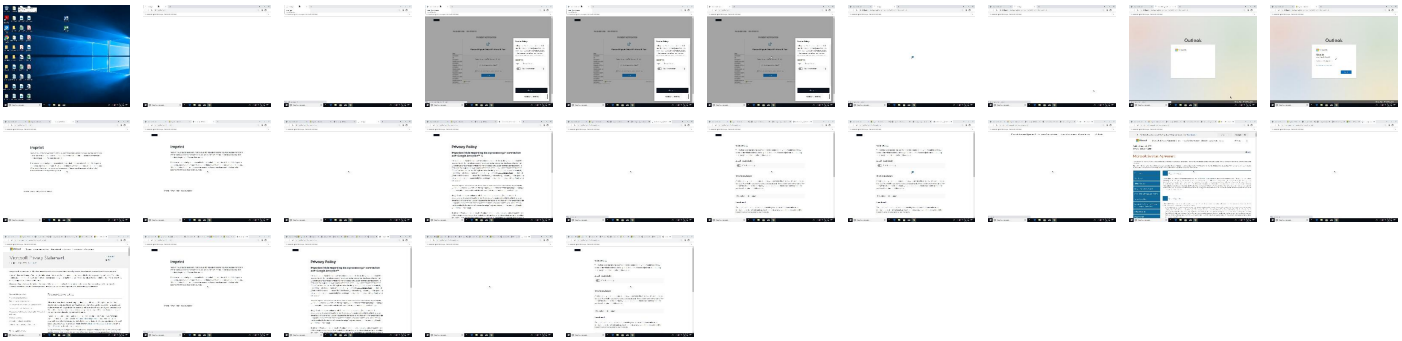
Behavior Graph

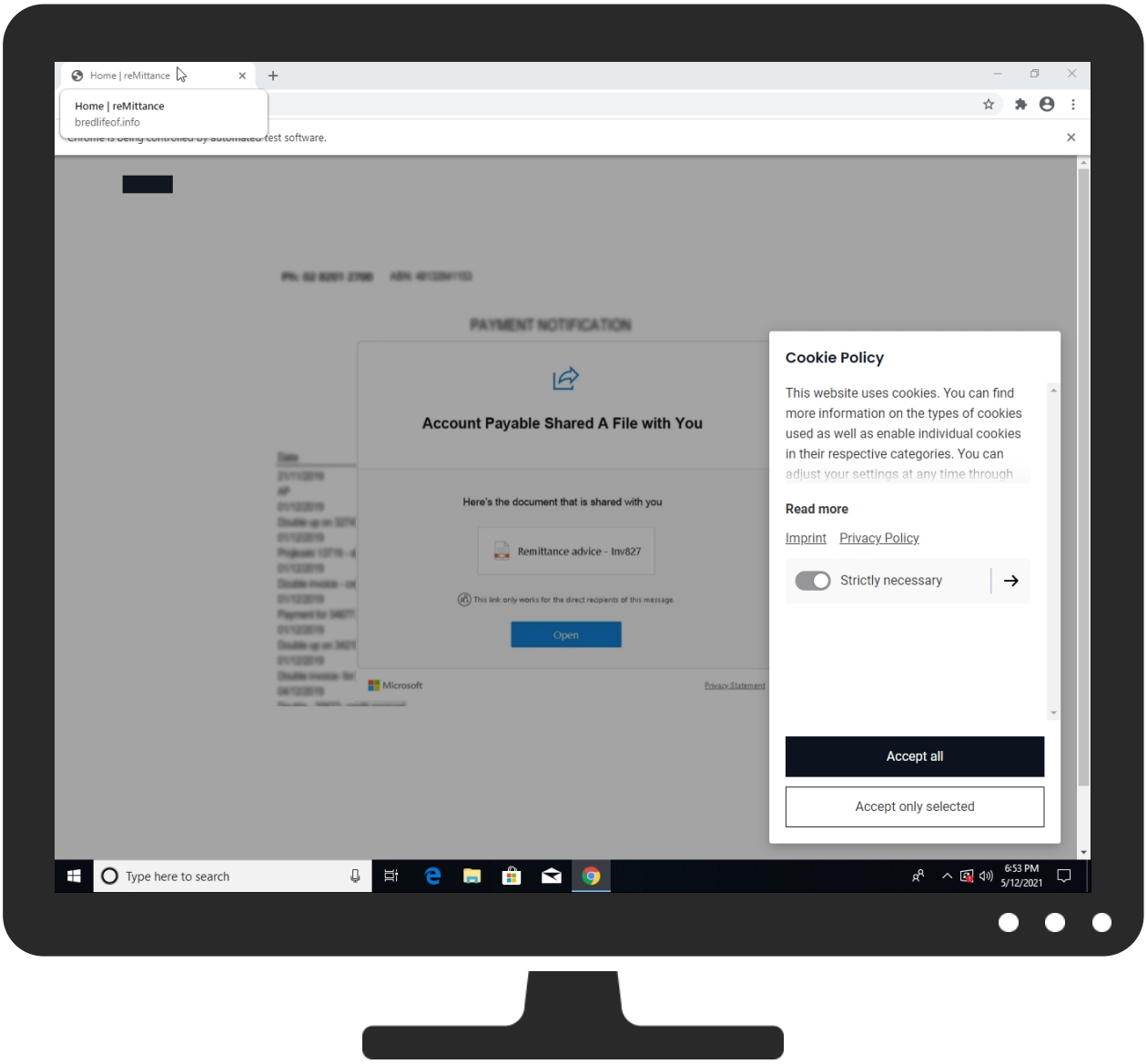


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.bredlifeof.info/	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://4dfffgghmhkh.s3.eu-west-3.amazonaws.com/gdfhfgkhkhjkhf/saue8.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://nemo-bp-prod.jimdo-platform.net/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://help.jimdo-dolphin.com/hc/fr/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Fredoka	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/de/articles/115005745466-Wie-richte-ich-eine-E-Mail-Weiterleitung-	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Martel:400	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/es/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://jimdo.com)	0%	Avira URL Cloud	safe	
http://https://nemo-cs-kt-stage.jimdo-platform.net/v1/	0%	Avira URL Cloud	safe	
http://https://checkout.jimdo-stable-staging.com/	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/en-us/articles/115005745466-How-do-I-setup-Email-Forwarding	0%	Avira URL Cloud	safe	
http://https://nemo-category-prediction-stage.jimdo-platform.net	0%	Avira URL Cloud	safe	
http://https://cms.jimdo-stable-staging.com/s/storage/	0%	Avira URL Cloud	safe	
http://https://op-image-super-resolution.jimdo-platform.net/	0%	Avira URL Cloud	safe	
http://https://cms.jimdo-stable-staging.com/s/account/	0%	Avira URL Cloud	safe	
http://https://www.kddi-webcommunications.co.jp/security/	0%	Avira URL Cloud	safe	
http://https://www.jimdo.help/hc/it/articles/212083686-Come-disdire-l-abbonamento	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Varela	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/de	0%	Avira URL Cloud	safe	
http://https://nemo-tts-stage.jimdo-platform.net/	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/nl/articles/360022894071-Wanneer-is-mijn-Dolphin-webshop-klaar-voo	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005738383	0%	Avira URL Cloud	safe	
http://https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/cms/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Raleway:300	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/nl/articles/115005738383-Hoe-verbind-ik-mijn-G-Suite-	0%	Avira URL Cloud	safe	
http://https://www.bredlifeof.info/privacy-policy/Yj#	0%	Avira URL Cloud	safe	
http://https://www.bredlifeof.info/imprint/?E	0%	Avira URL Cloud	safe	
http://https://t.jimdo-platform.net/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=PT	0%	Avira URL Cloud	safe	
http://https://www.jimdo-status.com/).	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005745466	0%	Avira URL Cloud	safe	
http://https://www.bredlifeof.info/privacy-policy/Q	0%	Avira URL Cloud	safe	
http://https://catamphetamine.gitlab.io/country-flag-icons/3x2/	0%	Avira URL Cloud	safe	
http://https://cms-backend.jimdosite-stage.com/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Playfair	0%	Avira URL Cloud	safe	
http://https://cms.jimdo-stable-staging.com/s/business-profile-service/	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/css?display=swap&family=Rubik:400	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/es/articles/115005738383--C%C3%B3mo-configuro-Google-G-Suite-	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/nl	0%	Avira URL Cloud	safe	
http://https://www.bredlifeof.info	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/es/articles/115005745466--C%C3%B3mo-redirecciono-mis-emails-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jimdo-dolphin-static-assets-prod.freetls.fastly.net	151.101.2.79	true	false		unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
s3-r-w.eu-west-3.amazonaws.com	52.95.155.72	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
jimdo-storage.freetls.fastly.net	151.101.2.79	true	false		unknown
dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com	52.49.20.157	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
fonts.jimstatic.com	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
www.bredlifeof.info	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
assets.onestore.ms	unknown	unknown	false		unknown
4dfffgghmhkh.s3.eu-west-3.amazonaws.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.bredlifeof.info/cookie-settings/	true		unknown
http://https://www.bredlifeof.info/privacy-policy/	true		unknown

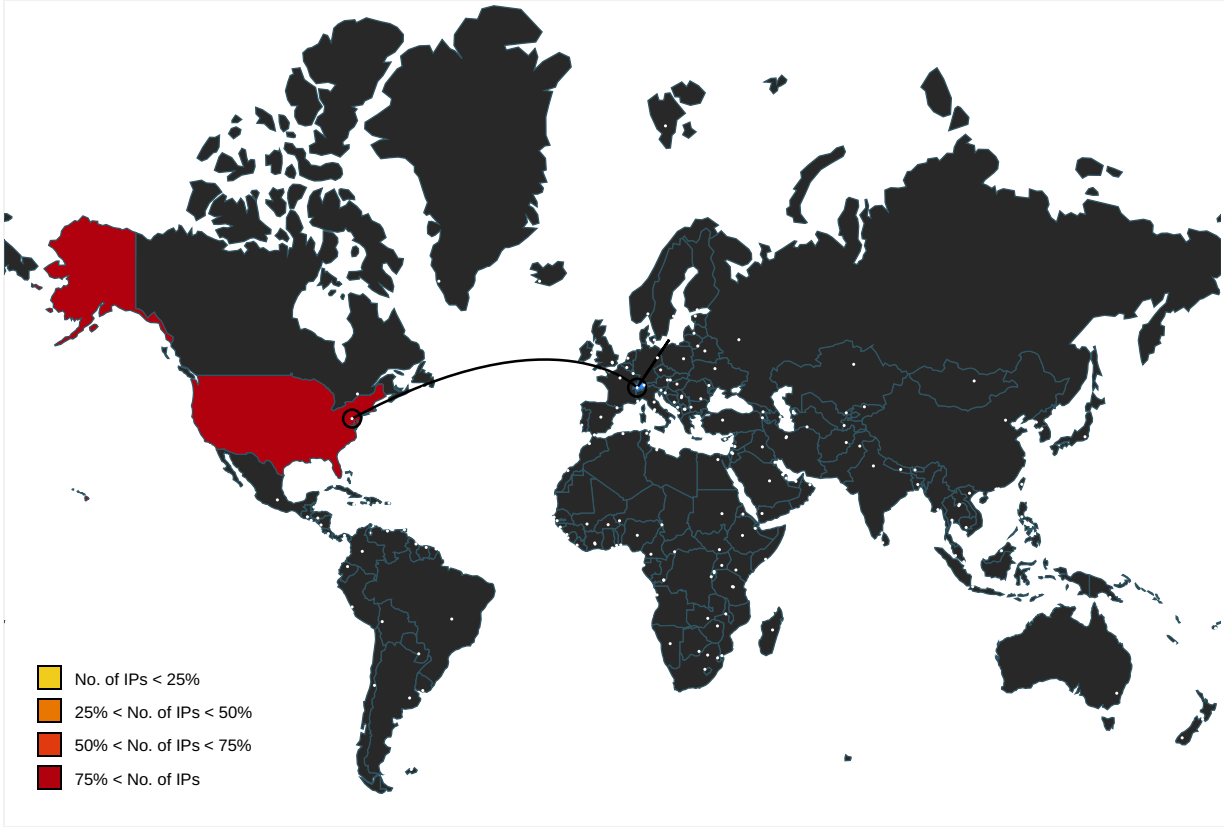
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.bredlifeof.info/cookie-settings/	Current Session.0.dr	false		unknown
http://https://nemo-bp-prod.jimdo-platform.net/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/info/jimdo-video-consultation-terms-of-service/)	5014fd48897e10fa_0.0.dr	false		high
http://https://cms.jimdo.com/s/nemo-wsvar/	5014fd48897e10fa_0.0.dr	false		high
http://www.trustedshops.com/tsdocument/WIZARD_TERMS_en.pdf	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/it/supporto-shop-online-pmi)	5014fd48897e10fa_0.0.dr	false		high
http://www.trustedshops.com/tsdocument/WIZARD_TERMS_de.pdf	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/fr/articles/360058420551/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.spotify.com/de/legal/privacy-policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://fonts.jimstatic.com/css?display=swap&family=Fredoka	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.jimdo-dolphin.com/hc/de/articles/115005745466-Wie-richte-ich-eine-E-Mail-Weiterleitung-	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://stripe.com/cookies-policy/legal	5014fd48897e10fa_0.0.dr	false		high
http://https://fonts.jimstatic.com/css?display=swap&family=Martel:400	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://storage.jimdosite.com/	5014fd48897e10fa_0.0.dr	false		high
http://https://it.jimdo.com/info/condizioni-generali/)	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/es/articles/360058420551/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://logo.e.jimdo.com/	5014fd48897e10fa_0.0.dr	false		high
http://https://jimdo.com)	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	low
http://https://nemo-cs-kt-stage.jimdo-platform.net/v1/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/de/info/jimdo-online-videoberatung-nutzungsbedingungen/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.privacyshield.gov/welcome)	5014fd48897e10fa_0.0.dr	false		high
http://https://es.jimdo.com/info/condiciones-generales-2017/	5014fd48897e10fa_0.0.dr	false		high
http://https://nl.jimdo.com/info/business-listings-terms/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/info/cancellation/	5014fd48897e10fa_0.0.dr	false		high
http://https://jp.jimdo.com/info/cookies/policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://checkout.jimdo-stable-staging.com/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.jimdo.com/info/cookies/policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://cms.jimdo.com/s/billing/	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/en-us/articles/115005745466-How-do-I-setup-Email-Forwarding	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://nl.jimdo.com/info/impressum/	5014fd48897e10fa_0.0.dr	false		high
http://https://nemo-category-prediction-stage.jimdo-platform.net	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cms.jimdo-stable-staging.com/s/storage/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://op-image-super-resolution.jimdo-platform.net/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://de.jimdo.com/info/business-listings-terms/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.youtube.com/watch?v=pB-003Fu6AI&feature=youtu.be	5014fd48897e10fa_0.0.dr	false		high
http://https://cms.jimdo-stable-staging.com/s/account/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/fr/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.google.fr/analytics/terms/fr.html)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.kddi-webcommunications.co.jp/security/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/it/2020/03/23/coronavirus-consigli-per-imprese-e-professionisti/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/fr/	5014fd48897e10fa_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.jimdo.help/hc/it/articles/212083686-Come-disdire-l-abbonamento	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://fonts.jimstatic.com/css?display=swap&family=Varela	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.jimdo-dolphin.com/hc/de	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://nemo-tts-stage.jimdo-platform.net/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cms.jimdo.com/s/upgrade-frontend-api/	5014fd48897e10fa_0.0.dr	false		high
http://https://nl.jimdo.com/info/herroepingsrecht-en-formulier/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/nl/noodhulp-webshop-ondernemers)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/info/privacy/	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/nl/articles/360022894071-Wanneer-is-mijn-Dolphin-webshop-klaar-voo	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.bredlifeof.info/privacy-policy/	Current Session.0.dr	false		unknown
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://www.spotify.com/legal/privacy-policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005738383	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/cms/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.spotify.com/nl/legal/privacy-policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://fonts.jimstatic.com/css?display=swap&family=Raleway:300	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/info/privacy/)	5014fd48897e10fa_0.0.dr	false		high
http://https://4dfffgghmhkh.s3.eu-west-3.amazonaws.com/	0d4dbbbfb0e94616_0.0.dr, Network Action Predictor.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/nl/articles/115005738383-Hoe-verbind-ik-mijn-G-Suite-	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.bredlifeof.info/privacy-policy/Yj#	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.jimdo.com/info/condiciones-generales/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.bredlifeof.info/imprint/?E	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.jimdo-platform.net/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://fonts.jimstatic.com/css?display=swap&family=PT	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dash.e.jimdo.com/websites/	5014fd48897e10fa_0.0.dr	false		high
http://https://fr.jimdo.com/info/politique-de-confidentialite/).	5014fd48897e10fa_0.0.dr	false		high
http://https://de.jimdo.com/info/agb/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo-status.com/).	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://de.jimdo.com/info/cookies/policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.bredlifeof.info/imprint/	Current Session.0.dr	false		unknown
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005745466	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.bredlifeof.info/privacy-policy/Q	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.jimdo.com/info/cookies/policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://catamphetamine.gitlab.io/country-flag-icons/3x2/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cms-backend.jimdosite-stage.com/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://fonts.jimstatic.com/css?display=swap&family=Playfair	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://it.jimdo.com/info/cookies/policy/	5014fd48897e10fa_0.0.dr	false		high
http://https://cms.jimdo.com/s/cms-frontend-api/	5014fd48897e10fa_0.0.dr	false		high
http://https://es.jimdo.com/info/about/	5014fd48897e10fa_0.0.dr	false		high
http://https://cms.jimdo-stable-staging.com/s/business-profile-service/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://json-schema.org/schema	5014fd48897e10fa_0.0.dr	false		high
http://https://help.jimdo-dolphin.com/hc/ja/articles/360058420551/	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.jimdo.com/about/	5014fd48897e10fa_0.0.dr	false		high
http://https://fonts.jimstatic.com/css?display=swap&family=Rubik:400	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.jimdo-dolphin.com/hc/es/articles/115005738383--C%C3%B3mo-configuro-Google-G-Suite-	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.jimdo-dolphin.com/hc/nl	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cms.jimdo.com/s/cms-backend/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/fr/aide-eboutique-PME)	5014fd48897e10fa_0.0.dr	false		high
http://https://nl.jimdo.com/info/privacy/	5014fd48897e10fa_0.0.dr	false		high
http://https://es.jimdo.com/info/politica-de-privacidad/)	5014fd48897e10fa_0.0.dr	false		high
http://https://www.spotify.com/us/legal/privacy-policy/	5014fd48897e10fa_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://de.jimdo.com/info/impressum/	5014fd48897e10fa_0.0.dr	false		high
http://https://www.bredlifeof.info	000003.log3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.jimdo-dolphin.com/hc/es/articles/115005745466--C%C3%B3mo-redirecciono-mis-emails-	5014fd48897e10fa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://fr.jimdo.com/info/conditions-d-utilisation/)	5014fd48897e10fa_0.0.dr	false		high
http://www.trustedshops.com/tsdocument/WIZARD_TERMS_it.pdf	5014fd48897e10fa_0.0.dr	false		high
http://https://www.jimdo.com/fr/info/politique-de-confidentialite/	5014fd48897e10fa_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.49.20.157	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
52.95.155.72	s3-r-w.eu-west-3.amazonaws.com	United States		16509	AMAZON-02US	false
52.16.206.246	unknown	United States		16509	AMAZON-02US	false
151.101.2.79	jimdo-dolphin-static-assets-prod.freetls.fastly.net	United States		54113	FASTLYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412529
Start date:	12.05.2021
Start time:	18:52:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.bredlifeof.info/
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@37/193@17/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://4dfffgghmhkh.s3.eu-west-3.amazonaws.com/gdfhfgkhkhjkhf/saue8.html • Browse: https://www.bredlifeof.info/imprint/ • Browse: https://www.bredlifeof.info/privacy-policy/ • Browse: https://www.bredlifeof.info/cookie-settings/ • Browse: https://www.microsoft.com/en-US/servicesagreement/ • Browse: https://privacy.microsoft.com/en-US/privacystatement • Browse: https://www.bredlifeof.info/imprint/ • Browse: https://www.bredlifeof.info/privacy-policy/ • Browse: https://www.bredlifeof.info/cookie-settings/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 92.122.145.220, 13.88.21.125, 216.58.212.173, 142.250.185.206, 142.250.185.78, 142.250.184.195, 95.168.222.144, 151.101.2.2, 151.101.66.2, 151.101.130.2, 151.101.194.2, 95.168.222.76, 52.147.198.201, 69.16.175.10, 69.16.175.42, 2.20.143.16, 2.20.142.209, 142.250.186.74, 142.250.185.74, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 184.30.24.56, 20.82.210.154, 92.122.145.53, 152.199.19.160, 92.122.213.219, 92.122.213.200, 184.30.25.170, 13.107.246.60, 13.107.213.60, 92.122.213.247, 92.122.213.194, 92.122.213.240, 84.53.167.109, 172.217.23.99, 34.104.35.123, 172.217.16.131 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, assets.onestore.ms.edgekey.net, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, a1945.g2.akamai.net, www.microsoft.com-c-3.edgekey.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, statics-marketingsites-eus-

	ms-com.akamaized.net, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, a1778.g2.akamai.net, e10583.dspg.akamaiedge.net, fs.microsoft.com, content-autofill.googleapis.com, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, aadcdnoriginneu.azureedge.net, part-0032.t-0009.t-msedge.net, skypedataprdcolcus16.cloudapp.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, statics-marketingsites-wcus-ms-com.akamaized.net, www.googleapis.com, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, edgedl.me.gvt1.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, privacy.microsoft.com.edgekey.net, dual.part-0032.t-0009.t-msedge.net, au.download.windowsupdate.com.edgesuite.net, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, i.s-microsoft.com, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, e12564.dspb.akamaiedge.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, f2.shared.global.fastly.net, accounts.google.com, cs22.wpc.v0cdn.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, firstparty-azurefd-prod.trafficmanager.net, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus16.cloudapp.net, c.s-microsoft.com, privacy.microsoft.com, e13678.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com • 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. • VT rate limit hit for: https://www.bredlifeof.info/

Simulations

Behavior and APIs

Time	Type	Description
18:53:32	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	119726
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	3072:GNOqOrdDdJPAX1LHAeNOqOrdDdJPAX1LHA/:aOrdRyX1LH7OrdRyX1LHC
MD5:	BD3E93AD23BB0CA00C44D8774C63E84F
SHA1:	03FB85A6B46615FAEB2D3E29FBC399593D7B5D15
SHA-256:	3526E251E631B67BC547442F85BFE5DD97A109CBC0189F04E1BD40D988EE18B5
SHA-512:	49571828C169BDC5D526D1A48A84002F075F846091DCB26032951EDB1D0A01FCCB0A66646E153B976F048F540009B6A368AFD830531A3F8E2F9CC7E5AFCE6AC
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X...,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g. lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,.]*....5.....\../ d.F>.V....._.J....."....wI..'..z...j..Ds....Z...[.....N<.d.?<....b..,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.I...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c..o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1573376927823986
Encrypted:	false
SSDEEP:	12:5q9KphZkPlE99SNxAhUeSKuMphZkPlE99SNxAhUeSKO:5jhZkPcUQUjKukhZkPcUQUjKO
MD5:	B1A85393F4AE84616C0C64EE3D42D071

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA1:	5A1AD580DC46C88F0231190C188C0A70D35F6565
SHA-256:	2470A6F11094B1DAF508E86C71B6199E240A05128A884F7D639960C0921017B4
SHA-512:	C640BC902331291074990525230 3ED1D82D5C19164474F8D61AEF131293778A1C129959162CC8A85EB89E4CD1BCBE5CE25CFF99BFE537A554AB23B915B0DE79
Malicious:	false
Reputation:	low
Preview:	p..... .....Q.G..(..... .....Y5.....$.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...p..... .....B.G..(..... .....Y5.....$.....h.t.t.p.:. /./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\2f46a0a8-13c9-40f4-ac08-d0a19d91fb38.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7493020341940424
Encrypted:	false
SSDEEP:	384:Nn+ltzoibgz7VU6poNJrCvNX3mpnCHTeGatrYLxtxm3fj+r8dms4+oHDtJD9mOzM:ta2R1K7SDnawerRXUOIn72TKVbBpY
MD5:	093AA7E9A53EE9B34F9D0470D89F34F7
SHA1:	8235D7EC1F9D0B7D4E9E3FB958165FAB2FBCCB35
SHA-256:	6A04060306A840FE6AD9C4081282F6778F30E8561AA91B8FF2326228191E5FE7
SHA-512:	8A20AED086760D1ADD7A7F30A2264385142C7E5F5B170F4EE8DE20B0CC570920961692E40FDE59CF83FE3708BD451BC7E0789A3A981382FC05E2FB0ED4C1E54
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....98.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\3bdc1bd8-7801-4ffe-b8c2-a8d534673511.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):	160435
Entropy (8bit):	6.050144757049686
Encrypted:	false
SSDEEP:	3072:DbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:DiyDhXHwbtgbV/njhcI8II6Ri
MD5:	B76266412D2ED4AE140269F4226D0BB3
SHA1:	34610AE5E59682CE4AE5569EF27D9FC821BC2C32
SHA-256:	858210624D1E9BE690F20CD4FB8FA25840E8A02EFFBADEAC925DCC7B164EF2F3
SHA-512:	116FC041AF07634A09516CA2B2971D0AE36435E7C0AFE03ED7ABD0DA249BBB0FB6F85D2267C376168B57EFC354A09A07792CB1ECA10327DFB4BDB4FFF19316 3
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"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":"13245951909260519"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d7ea40d-b2be-47e9-bcb1-4699a8aa695b.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):	168898
Entropy (8bit):	6.079941245865379
Encrypted:	false
SSDEEP:	3072:3kxbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:0xiyDhXHwbtgbV/njhcI8II6Ri
MD5:	38144475B9D98C97D182D09603A8DD5A
SHA1:	97D80F7D399C267BEAC58EEFC412BA01C930B375
SHA-256:	9BABB896D2EE24D86315F4A3CD79C4525324EF5D0FD661B93AA46B5545B2BE2F
SHA-512:	8EA0744BF069D73A932D6746F9BD9274598BFF75255288A95CAAA0D1218537F474A87AD59552F7BACEBFD185EC8E4676F1587760F8550AF647ED73EF5F1507A4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d7ea40d-b2be-47e9-bcb1-4699a8aa695b.tmp	
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/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\8009cf7f-7af9-4b01-94ca-a16c4c171f76.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):	168897
Entropy (8bit):	6.079940755764839
Encrypted:	false
SSDEEP:	3072:3kNbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:0NiyDhXHwbtgbV/njhcI8II6Ri
MD5:	E81B6219A80E966516442406493D6161
SHA1:	C67E2418F8091260FABBF45FE875AEAB5BAC6C57
SHA-256:	0C98021FDD5930349F29D925C898F13363A7ECB544F8DCE40E9296DC03DB407C
SHA-512:	AA05A27C044275E0267E9A90303B486839C851A4C9D35C18F6239CD15E0D11EE27CC12961FC516CAFB80B1C335B6FF0929D4370B930358FCEC670B8F367BFDE
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/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\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:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C4058034
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\24f229c6-4e51-46d0-9fba-b39ff9c4f997.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):	5.565687439786089
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevEhUeT7VYRU62LCh7wUCTRUevxQ:YU6UUhveKUevGUeiU64CpwUWUev2
MD5:	0FB5FB7806322424C89831B2D5BA9F09
SHA1:	F652BC29F352D23852FD83E21680C71CA5554C96
SHA-256:	123F49338D55EC80C39744B7B5A281D627C8E6B6BAA68FD69FAC8A5B7BC7B4ED
SHA-512:	CEF7D3C9923E69D8F004128719A62F6A54BEA2769995F01236665BC2B2369DC77F14DC2FAFA7F56F84EF3FAC7588B1DADCEA6CFE0CA7F2DC465212015023BE2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24f229c6-4e51-46d0-9fba-b39ff9c4f997.tmp	
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":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1652406798.820941,"host":"59uCM2DZ4BMR0SsedMye7m5slYNZQDNszNz+YKp3RhI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870798.820945},{"expiry":1652406798.307069,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870798.307074},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3235b847-119b-4a8d-9a57-865166d176c7.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):	5.535997465444448
Encrypted:	false
SSDEEP:	384:suntpLl1zXf1kXqKf/pUZNCgVLH2HfD+rUAVHGVnTpXKI/o4Q:FLlpf1kXqKf/pUZNCgVLH2HfirUApGVA
MD5:	9D79DEE4F04099F56A011A9DE01718D7
SHA1:	6402BE272BA8F649831E187DA8D18E30797757A1
SHA-256:	ECE88B4994BF25DB49AD4E951A8EE596131033D90C15132A45DCD8F67DE129A6
SHA-512:	B0BA495A3DFD74F82A16831E6A208002548B4BA5968736286BC18CEA77F19F3F3918C7FD43CDEA5916AE3414B06675BC7E0A4D8A8ED59674EF910442DAFC038
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":"13265344393250038","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3a80123a-bfb8-4150-b848-e0c6c263503e.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\3bd1e7c2-c21a-4898-a18a-00bbd6808fd7.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):	5768
Entropy (8bit):	5.1988168665219545
Encrypted:	false
SSDEEP:	96:nG3hh/12tsYVvik0JCKL8kKkx1EbOTQVuwn:nyhL2tsYhk4KvKkxs
MD5:	A738ECD4BBE7C432EB062E1EF721BCE3
SHA1:	1C95A57A444375A9A341C9C11D9EF5BF2EA4D34C
SHA-256:	404561430710614D1511607C17AA2DA03C27FCFE86A56664434A8500C361ED86
SHA-512:	9C9E00D9E4D00C74BB87559A2C3EF2394ED06E19EC1E633671D787225154B2BABACB13F7DE52281AADE4020F79C18A20FFF53E27CDBD4AD73245E4241019378B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3bd1e7c2-c21a-4898-a18a-00bbd6808fd7.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c03f67d-e221-412f-911b-4e33fb95eade.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):	1209
Entropy (8bit):	5.568819068769705
Encrypted:	false
SSDEEP:	24:YinWswUz6H0UhvrRlG1KUevEhUeT7VYRU62LCh7wUCTRUevxQ:YqVwUz6UUhveKUevGUeiU64CpwUWUev2
MD5:	2705B82373CA09A628BE823E7D5BEEA4
SHA1:	AD855A6C5F454399AF48114493ABE7ED397D8371
SHA-256:	FAE6301728E47112E2973DF9155D76385F0B0E4F8E568B1D062BC9980DDEDCC6
SHA-512:	EDF7EE3E820ACF35A5685B3D2C71892BC260EEACE84FB4E7512EE9742E707C9B7F063954AC5CE38550CD85F713C3DA3DDC1494DDED13C0607C04549D647099
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1636650811.7257,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870811.725704},{"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":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1652406798.820941,"host":"59uCM2DZ4BMR0SsedMye7m5slYNZQDNszNz+YKp3RhI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870798.820945},{"expiry":1652406798.307069,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c4d20c7-7910-4ef9-a9d6-6c1bd2132032.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\5ed51093-3e3c-45b4-ae88-2ea3cc0dd293.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):	5159
Entropy (8bit):	4.987604510372071
Encrypted:	false
SSDEEP:	96:nG3h9o/2pYV+ik0JCKL8kKkx1EbOTQVuwn:nyhk2pYEk4KvKkxs
MD5:	1785C85A706E353C7E291D6DD24DDA78
SHA1:	702C5CEE9B58AC1A22F66C14743FC15CF98775F4
SHA-256:	38E7D9E561DA23FE6929AB98167DFC9BBE6105AAD405519E79E26DD7603C2228
SHA-512:	D2D8261FE1588F17672898BB31A710513244B510A8CE62A57D091FE95C595D3439151397ED998F2FFA1FDFAB5BD77D4840506BE3687E80C3531077CF66CB5262
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ed51093-3e3c-45b4-ae88-2ea3cc0dd293.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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\77d23cd9-e180-43b5-bc28-ab53c37e485e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5172
Entropy (8bit):	4.989620863673815
Encrypted:	false
SSDEEP:	96:nG3h9l12pYV+ik0JCKL8kKkx1EbOTQVuwn:nyhl2pYEk4KvKkxs
MD5:	4169D136C424151B09580AA3F3052508
SHA1:	A60FA4332D884C36FBAE89A8452097B828CBA482
SHA-256:	43B77E66EE7CC9894D21C91E7EF15FA07BDEC4B924B253905814C7A5A3F57EC0
SHA-512:	F810B9743B287E882879086AC115683B804CD90FE0FA85D33F047D50085245900464CB8B3FBBA61D924DD05D63DD243B12F5455C320892C5B3EDE24F1DFD1B04
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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\7d212659-315d-4afe-84f8-2f479041344f.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):	5.535689272968269
Encrypted:	false
SSDEEP:	384:suntpLl1zXf1kXqKf/pUZNCgVLH2HfD+rUAVHGSnTpXKIyo4j:FLlpf1kXqKf/pUZNCgVLH2HfirUApGSQ
MD5:	B0804F1E0AB6E0B70291177CA84FB146
SHA1:	86AD94E09CFB1A9542040EBEEF38747AC14EE0AF
SHA-256:	66898C80618B8C44E1E2D7DA87CBE2906BCF277477E7C53557E68E577F78532F
SHA-512:	DF9B456DD6FBAC3EC0C359BB6DE4FF9284059F0B683EDA7C555729D34467569F2A0D0D6D90AD37A4E2C63497D94E4D35DB64AA653D3FFDB8960C4E7B605A8 2
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":"13265344393250038","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\872a72db-ddfe-467b-bda7-514307da2b94.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3268
Entropy (8bit):	4.871547013068202
Encrypted:	false
SSDEEP:	96:JnCDHXTxOzfFFE2+6NZjOJqGeFVFi+UVmLmVeVAYhj:JnCDHXTxOzfFFE2+6NZjYqJ3FTaa4QAQ
MD5:	40B9F62D03E1309F1FC835C7F64BCB5C
SHA1:	7A5640C84DA7356D4E7A76C3F4E75003B3A1888C
SHA-256:	57736C8AFF1D74D474069B15A33303C4D28F1E0F292EE4F8A164BA2484FDD8F3
SHA-512:	8CC98F038DD6388A85D24FEC0F1E99A69C7771D0A6ACAA2F2F191E00F25D5CC45129BDE769CC5A262EEF423EE3F454B8468796D3F5415D40467DCFBC51180C 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\872a72db-ddfe-467b-bda7-514307da2b94.tmp	
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":"13267936398306928","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267936398318075","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com",""

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):	5.236357770384187
Encrypted:	false
SSDEEP:	6:mXsdGNcM+q2PcNwi23iKKdK9RXXTZlFUtp8DJZmwP8DcMVkwOcNwi23iKKdK9RX3:sdcM+vLZ5Kk7XT2FUtp8DJ/P8DcMV545
MD5:	0878979224DCC77A63FF73537EF7EE67
SHA1:	B76B327E30B12DF96BF17F68A10F412357D995AE
SHA-256:	B9ECE0603E3591FC1BD759273DFEE537F0A95C618A95389A85FC532C3B7FA221
SHA-512:	AB411014211248DEBA360622D0483E8F7D243B6FA228575DC7BE0627B8E83E5F14EDA9E84A02D58523A27D83D89BBBCF632BAD1247BDAE489B4CF9F50CBDE4C
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:34.151 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-18:53:34.153 168c Recovering log #3.2021/05/12-18:53:34.153 168c 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):	5.241277978982018
Encrypted:	false
SSDEEP:	6:mXDVuA3cM+q2PcNwi23iKKdKyDZlFUtp8DJWJZmwP8DJWcMVkwOcNwi23iKKdKyX:sDMA3cM+vLZ5Kk02FUtp8DoJ/P8DocML
MD5:	76A663C12CDA5E6DD50DA7DFD265CC1E
SHA1:	79216C09B5B997D76A6A258C1B4781330D7ADF90
SHA-256:	E9C0F0968B51D216E27D06F98AF1EDC7F46CFA45A73C9A870D1A17D158CAAB8B
SHA-512:	0F4D1007C9D3C5F2A796AB1A7F24185B38C411D7CCE572E6EF17108086B4BF158D79122DF3511274BDB7B25B223ED99ED829B143BDB689D9F3E665A811C7339
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:34.140 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-18:53:34.141 168c Recovering log #3.2021/05/12-18:53:34.141 168c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.52939797743357
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKIf8QPKxWStHWFvDFYtRanlHCvdrl58tyGdDmXhXpK5kt:m3VYyK08fNH1DaIv3yL6XhZK6t
MD5:	2D34F2D6A4CDF72704521A479312A5B1
SHA1:	6319FA21C9E41174384637E558459FEA22015B5F
SHA-256:	0BDAD790859A4B25439D4AE9C2B44D0EEF78FAE6CD0ADB7D15705472B034A239
SHA-512:	08F0E049C2FF79C9658BC0CC13123676B4E07370BE6F6F9E7B1EF8EE924D9E676DDD7C3B061E31C609FFA22286C6B1A4F8DEBDB69B9FBDAEC760F1FE87B94668
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/.Qh.. /.....j.....=.z-.7.K]..~..=..9.....8...A..Eo.....Y..B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d4dbbbfb0e94616_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d4dbbbfb0e94616_0	
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.554748332153876
Encrypted:	false
SSDEEP:	6:msnYeMggmVp50vlYkRVKNWYPkY9ShK6t:7MggyX0vljVKggS7
MD5:	EDCCBFB2EA1F3630F18870744A78CFD7
SHA1:	AF0ECEE229B1ADBF62AE54121E6EE53D9EA33FB1
SHA-256:	B07CF7F15472C5CB50E5D326FA345867D8FCD808B07BEB811469A099978A5AB8
SHA-512:	7F46BFB7AF47E1A370BF94DAAE81B418C22B8B3BE1D12F1657CAD21E5134D6802DD8CABC43B55E8AA029DE86340A735DBE87C155A4213A59F0B43F0EBB69B8B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....Q.e...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://4dfffgghmhkh.s3.eu-west-3.amazonaws.com/.... /.....k.....?.:7.../...M>.O./..;..Cb..a9f.A..Eo.....q.Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0df9317af40b3bb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	393
Entropy (8bit):	5.927304701259399
Encrypted:	false
SSDEEP:	6:mmkVYr8I8i8qqD2fSqWIyvgdgYOEl1ege6nCK6t/ji3/mgFEeHEl1ege6nP:fPZp8FX4da6U2U5jiP1rH6U2
MD5:	78021E3EFDA3805BA66B7A8B74660756
SHA1:	8A9BDED5A8552F56021B2C0445900B5F97FC0000
SHA-256:	FA04CA8C84E52063E0656F330B16D2B2E1B91F1B9A7D0DAE3F4D6F7D2EAC8A7D
SHA-512:	D8D89E32D4B1DEA6178D886B8A7306C5C851FC3C0F432BB2C7BED2579E5EA55E562260885000E73027B6AEFD738AD14AB138C772BF4AE6B4F65C4FBF6C505EEA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/static/ceb721f3140266a92265.js .https://bredlifeof.info/..... /.....Q.....C.....$~A./u.[n.....,..; .z..A..Eo.....?..:.....A..Eo..... /...<.5AF3E2193D542BC14160D146399B4CE23EC5541D063C8476EEFFA4E51AB4A7B3.C.....$~A./u.[n.....,..; .z..A..Eo.....X.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\14c06f6781117c4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.420032528787289
Encrypted:	false
SSDEEP:	12:TDQLzkGFhhykPpoMKl0xUDjNC1Ngw97we9EY0p5FSDGK1wu/St7:T0hQklxUDRCTFuY0MLwu/G7
MD5:	D2BA2358DB99D0717707E8E3AE7DD45F
SHA1:	FA9DEAD877EA1BB664D2E3CA0EF0BB9D085AFC23
SHA-256:	207BB9A315921ABDECE3E8451F7A6C4C5AA96C1FD78995FFD810349B35C46D51
SHA-512:	D4ABD0C59A6A08153DE00C4E1F1B88E4307560B27009D928B3974E95B2D69EC5E96F370129741CF0EED48A85C80821C3A93C6514F020FBCC32B2DD7ABC929A3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.*'.. /.....V.....o..m~v....*>...p....a..K..o..M..A..Eo.....g..-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328b75cf02d95d5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.663139498907591
Encrypted:	false
SSDEEP:	6:mcYiRDHwA7eIAX3TH5R2DAPAg8owDgjn5/m4DK6t:XDHXeB3L5gDAPbwCm+
MD5:	83E6687B1A8353FF1FB417C229D28E96
SHA1:	E27A830743EA0386D6EBA90528A4E0F1BD97EAD7
SHA-256:	5775CB8A639B8C9AEAF3FEE175ECB31A8C956A0263BF2E158A41FA3BA56A7E80

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328b75cf02d95d5e_0	
SHA-512:	4E6356E7217650C7BD46635D888C5E2C206EFEDFE2941A9B982FC486A7DFB6C8595BD99DC7A1D8EB8A2B24DD29CADD412DAFA7700B5C55DD60496A7E0685C3E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...?....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/.Ph.. /.....k.....U..0.....\.oQ.8gD.r*{.....A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a7b0a16eebe4c59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.378759360188977
Encrypted:	false
SSDEEP:	12:JLDQLH6kGFhhykPpoMKl0xUDjNC1Ngw97we9EY0p5FSDlIXN:lkShQklxUDRCTFuY0MxIN
MD5:	B4EF8529AF85D7086D32DBF49A566097
SHA1:	BB7C6C1B9D2DE094D718F7C5977D27F266D37BA0
SHA-256:	8AFB3656C5FF74E9878AE04A742F115F77BF355CC9A94B288D534650D8851CFF
SHA-512:	D6B39CDD0A0F49B61C1185911990BC005B5E26A62434DB9D64C98315649D2D04C156B1BAF443B6E14DBE832CC34B12799BB5CD5E8F04B4E023F08FF33703859
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.a....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.yi.. /.....k.....o..r&.@..I.....a._.?f..~...A..Eo.....m.9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5014fd48897e10fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3983920
Entropy (8bit):	6.304761932606532
Encrypted:	false
SSDEEP:	49152:I6puQhIwJroZsjY6UeoAQeM4hQUw2POoovwn8wDoGgFLHZg8gE8hQ7sRAfPhzPlL:roeoAQj4N+
MD5:	6FB81B5CB1FB94C26E529359811B196F
SHA1:	55A6AD1477B58B1BC3DFA713390DA7749ECA6F93
SHA-256:	1EE9B374F553883A29E0CDE0B58BAD70EE0C7B9D90431E8C60B130A63DFC700F
SHA-512:	A5D768DEDF328EC039ED9C83F6013E9B1D3784907FA6B343E39BCBACD78836D6CF71A2B6CDDF117402B275DC5934E4CD86F187980EECC11AACEE976E664081A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....n.....5AF3E2193D542BC14160D146399B4CE23EC5541D063C8476EEFFA4E51AB4A7B3.....'..G...O.....<..o.....(.....d.....<.....H.....|.....h..`.....8.....x....7.....t.....h...P%.....d.....$(.....<...x....p.....4.....$...X... .....h...L.....(.....,..4.....p.....L...0.....p.....L.....t.....X...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\781980b07f1bb38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.64892367837321
Encrypted:	false
SSDEEP:	6:mql9YiRDHwA7qYsDpNdNFvNgDgb6GXpR0QK4BK6t:RTDHXqn/xNgDMIQn
MD5:	01C095B28501B93D7FB158A3DBBE81A7
SHA1:	6A83CE16445D1411C6653131B97C7DE2E7B56735
SHA-256:	243AC3760CB1F7FEC93B2930C9B445ED8564C57E9D1494C2EF6643BE5EBBBC5C
SHA-512:	07E13EDA35FDA384FFF0DEE000572258A80E6C2C901484D3519A7EA2F91E00B25506DCD4002EA4804ADBBF319A5F79F4E4B77D218C5C826EC4A7CB779DE312E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...0.v....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/../.. /.....`Y.....5...a...S...s5.O..8O....F$.|3F.A..Eo.....Z`^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.351291403713415
Encrypted:	false
SSDEEP:	3:m+lSd7ta8RzY/VW4McTtRAJOlGQHLRSVNRFYtRTglHCU//cWUBl0iPy2wd1UmOXX:mXYI4McTDsJegDTTU/U1TrlEYK6t
MD5:	7D3E685E84F7651748948B1F3070E45F
SHA1:	D6E66B06CC1CFEF3A92A644C2A64943617FF8C30
SHA-256:	3E96CF87261E8A1CD9762D73086D761A458CE9CFEC41041CC5F5687F62509A2C
SHA-512:	BEB38B01912F5B208EAC5F1D78DE6E007690B9049CF7AE3332AD12E44826E7385540E55138066369D5376A7ED0455AE12F23B6F3F202624D1D3FA04992D0AA61
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/..,.. /.....SV.....<.S....l....*.W.U\..E?`..r.A..Eo..... ..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.503705627732891
Encrypted:	false
SSDEEP:	3:m+lSxla8RzYJb9yKIf8QPKxQBHWFvDFYtRwY8wNlHC5lldyq5EzDHz4mCl1pK5kt:mfYyK08fUH1DwY8wy5gq5EfzrmDK6t
MD5:	1E0FDD0F74E8D7D0AF3A96B253CA0277
SHA1:	32B748D5DA9AB4EE2C87DB84AEEB7E0469750417
SHA-256:	92587F54EE868FB4E272EC4890BED30F0F1B87EE84603883C45C0F09BD1F59A0
SHA-512:	4B56E8C83DF34C8691B1B6CA6933B603CBE9EAD2C276E5BC0FEA42E088DADC758CB9DEDE9C1079034F76126E767670048225E6029A412B478214E9EFD452DD 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...T....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://microsoft.com/..,.. /.....HV.....f....cB..cWhT..6..(..$....G..A..A..Eo.....2a..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff3254c380ce1732_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1103
Entropy (8bit):	4.988090591355411
Encrypted:	false
SSDEEP:	24:MjXJaGN4zXk16FHPtJ8dtUUuzi19EJkuLUkI5E/9RLFePpnS2:M9aGQXi6OdCzLJk+UkeE1nePpv
MD5:	78DE891DFC00D0BD4E25C8104CA5C944
SHA1:	C70180ACEC40BED072D1284E1505D5C27D828176
SHA-256:	DDEC4107C97E09EDD4A680A0B3B15B77B69F8A831DD0274D980042EDD7023CD1
SHA-512:	BC456CE9DD4548E983E1476286141B0D204308C7B6EC03B3F5C99898886A38AFFCEF822B0D58AA95118670B0F3474FFC4E1F0F554C060DF4893DEBC9D4C98D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742 bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19 ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645- b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1- fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9- e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0- 4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8 .https://microsoft.com/u.,..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9674958248778283
Encrypted:	false
SSDEEP:	24:t2+tYeFlfqLbJLbXaFpEO5bNmISHn06Uwz8:t2UYejfq5LLOpEO5J/Kn7U08
MD5:	5D391F388A820E316FC653196AC89A56
SHA1:	DAEB7DBB45814020E7E5F8E2354AC3A0F739FA27
SHA-256:	66BF3A741DD67462D7E3F007EB0134B890025FF51564BA74CCEED3070CE77BBE
SHA-512:	EBA159674C1CFDE3198B5EF5132A9F3E1A7629D26F7D39E5C4DEDF232235187B915A7202D3F20A5F8ADE1AA921F20EC76C9913F45CE7E4B0DCB3C7815E10BF
Malicious:	false
Reputation:	low
Preview:	.....6N..... ....

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):	13148
Entropy (8bit):	3.2391284310325714
Encrypted:	false
SSDEEP:	384:imbLFkWskDOkn8XZm3IljrkWukKIkd8TZ0Tlj:BCRXh
MD5:	E3AB1E616A83C7D9C12559701B563FFB
SHA1:	4948BA9409A4728DD92A8C37F618541BB8E965AE
SHA-256:	BEF1998F3A850B2AC4BF5A50714B1AD7F9C1806FAE9CFE1A68BC3F5E05F07A6D
SHA-512:	35669478227DCBE6A7D7C05EE153EC06BEF84FE1F854D6DEEB3E17C887929721256158D198B4A42BA6EC5FBDA961444D89330541B990B3DF43F8AE3174D979F
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...a82040d5_43d7_4b51_ad48_41137073e3e9.....W..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....https://www.bredlifeof.info/....H.o.m.e. .|. .r.e .M.i.t.t.a.n.c.e.....h.....`.....+d,....+d,...X.....p.....@.....h.t.t.p.s.:././.w.w.w...b.r.e.d.l.i.f.e.o.f.. .i.n.f.o./.....@.....8.....(.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&..... .....N.o. .o.w.n.e.r.....1.....c

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.194995718858655
Encrypted:	false
SSDEEP:	6:mXUwL+q2PcNwi23iKKdK8aPrqIFUtp8URz1ZmwP8URlLVkwOcNwi23iKKdK8amLJ:scvLZ5KkL3FUtp8M1/P8+54Z5KkQJ
MD5:	E42DFDC337EC0683A620FBEE3B98428E
SHA1:	E8F2482A9FD52467FE370D6774217F12B8DAB994
SHA-256:	D7C40DDAC7F098248A05BD938D46A65733B183690AF0BE6CA52C8EBA2197DF9C
SHA-512:	3125ABFF0BDADDF3E5E6C6125E0270891AD0169D472C315730B6E789C7AB4B0FFA7F3EC60AC3AF97AD994DA071E2314B3645FA42A7F2BE00350593FAF0717CE 4
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.526 15e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/12-18:53:13.527 15e8 Recovering log #3.2021/05/12-18:53:13.527 15e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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

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):	328
Entropy (8bit):	5.241439323633344
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SSDEEP:	6:mXYFijIq2PcNwi23iKKdK8NIFUtp8YBZmwP8YDiPkwOcNwi23iKKdK8+eLJ:sYFWIvLZ5KkpFUtp8YB/P8Yi54Z5KkqJ
MD5:	E5E5B96839F1083818EC118D7A051870
SHA1:	5AC62384A9A16A366D1249446C276CA0AD8A6D15
SHA-256:	A573E7FDE264BF3BE908183DE28CEB6124385FD122A926A36C970948E9E7B0FE
SHA-512:	A91AFC3FE7EA12EC8B2566CB658554E0F61340627781AB8BF1DA6C70CEA4088CCAB7CE7BE15721685CC5ED1FE802780D4FBA1F8405DD53B30116CE5D89FEA(BC
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:16.031 1394 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/12-1 8:53:16.032 1394 Recovering log #3.2021/05/12-18:53:16.037 1394 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\comput ed_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=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECROfI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\c omputed_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=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq 4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQ RpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl 32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc="," eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKn MKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9u qQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	30720
Entropy (8bit):	1.3037468526226759
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SSDEEP:	96:yBCVAAQ09016CQU2SC7h0909090M090o3QOLBBqyw:IJ4934C494BA/
MD5:	8F299C0466039CA4712B0D44715A2916
SHA1:	4BF5B74B4F5D78ABAA495C5359F678E3B36A7FC5
SHA-256:	F77B6A6D84324D78ADAEFA1AD190456347C61D84EA2907587729A6B8C4F998B7
SHA-512:	FF3003496BB6A50C19B8096A2313C9537AA876BFB30C762A3BA99D3435FC6D16C821F32C419590F52A72ACE925B98B28DE899371AB342F969E439D4CC1738CA
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):	31888
Entropy (8bit):	0.7276616172452409
Encrypted:	false
SSDEEP:	24:ayoKyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwE3H5HIT5YtsaDc90R4sBwTnNGwUo:roKdBmw6fUL3H5AOtjI90R4RGwYf34
MD5:	4D21E8AA5AA5753BACC11076BA716ECA
SHA1:	EEF68506605A4497A405510B6D125B3CA3B7D2F2
SHA-256:	E40EF6755EC3930311B036E0C3C31D4AD226A90B6C743594DFCB9517E8BEB90C
SHA-512:	639D9F4B9068D1444C5051B3DD000FA80220F80984D5269EA83A4E787F3EC8E09643F46D78B275E110DA51604F280D2ECBA2A663C4424BBAFE357E659DF2A285
Malicious:	false
Reputation:	low
Preview:	.....].I..... ....

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):	5.265820614392633
Encrypted:	false
SSDEEP:	6:mX2ScM+q2PcNwi23iKKdK25+Xqx8chI+IFUtp8ZSJZmwP8X3cMVkwOcNwi23iKKN:sVcM+vLZ5KkTXfchI3FUtp8ZSJ/P8ncQ
MD5:	33F2AC85207EBF42C844189B7A097581
SHA1:	F86E3A55AD0171B4A9D5488E3084630EE6375A56
SHA-256:	00D20DE72019B7FCDAB103169AA0210B3167BD01A1E8522982E9ABB2774150FF
SHA-512:	E15BC4354250DF901DD982D43AE46EBA97CED89081B8CAAACA721B874FF53B8F75FA4AA7C3D5D4C2510CA424ABF10A741DB315C051CA1A78A2E7997931F534C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/05/12-18:53:34.003 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/12-18:53:34.004 168c Recovering log #3.2021/05/12-18:53:34.005 168c 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):	5.2287822508401
Encrypted:	false
SSDEEP:	6:mXeEcM+q2PcNwi23iKKdK25+XuoIFUtp8kS3JZmwP8ELcMVkwOcNwi23iKKdK25y:seEcM+vLZ5KkTXYFUtp8kEJ/P8AcMV5M
MD5:	7DC2E126B6B2235B02CB394C209FA4C6
SHA1:	79A1A89F549A4A156448E32E03F25B68F39FD62A
SHA-256:	670A60850FBABE69F18CEC05708DADC84F1353F156A250699C5828BCAFCF358B
SHA-512:	66BDE825B9BAA6DC24723BE7C4FE43FD9CD6397B09448744B95E101F3A437958063175A52B2564DFEB948D8677FD2155BD613079C10F4DF55DF68D23955C233A
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:33.253 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/12-18:53:33.295 168c Recovering log #3.2021/05/12-18:53:33.296 168c 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):	5.259248563018129
Encrypted:	false
SSDEEP:	6:mXrN+q2PcNwi23iKKdKWT5g1IdqIFUtp86ZmwP8Bd3VkwOcNwi23iKKdKWT5g1Iu:sMvLZ5Kkg5gSRFUtp86/P8rF54Z5Kkgk
MD5:	16CB9BA2064E42B4621C1805B1F9E4C1
SHA1:	1F07E7050A88A01A9E21BBD57D017F439086412C
SHA-256:	5C1D24E25A5A158D800E353CA682847FF6D75AAE204B12CE906806E8B502B896
SHA-512:	4B4612F2AC6F6845774B38C84F6B22C70C976973410E087FAF3D39439A26576F6120F52FE0499CFBC5212E4FDEBFE329C4990959D203BBDBF036EFC817AD03A6
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:31.054 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/12-18:53:31.055 1bb8 Recovering log #3.2021/05/12-18:53:31.056 1bb8 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):	147456
Entropy (8bit):	0.38571892656198664
Encrypted:	false
SSDEEP:	384:tLKmXx/7ztZdXlA0b7gtZdXFb0b7ICrZBldb:BjOSdb
MD5:	68B31D008ADE792342E29D8189ACBE1F
SHA1:	574824BB5A2A76BC4AAD6686DD02357447DAFCC7
SHA-256:	DD56F36EABC985A239632C0A81EAA4B872A857E40CB603DD48B59A9BD1E17D8D
SHA-512:	37D3C487BF21F23C55B2C0DDBAF9EC7C25B514F126C32A02D285DD0FF4EFDE56B044D2D87E54839309B190CCBC6BDD2888979EEE2C52A3EC3C7D42D4CF2FA9
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	474
Entropy (8bit):	5.1434054160745495
Encrypted:	false
SSDEEP:	12:HDqpaTD3W58UdRe+Ly6sV8tm/JaFBk778B/xgs+Tc+f5:HOoD3Gu76se4eY78BJgs+Td5
MD5:	A4855F8E2B87EF711E5825346D2A0267
SHA1:	3751C61AEF0D4396219CBF9DFBE5750C6B3F4181
SHA-256:	004F9CC94E28293B623A40EAA59F5327AA77B089DDD7876733175FCA8B69BBA9
SHA-512:	BFAACEF142D1635EEEA041AD15F4BDD9485C8FFEA83C069313CA75CA78F1CE1AA9DDF7819E037D32BDB8368E39AC25C5647EFE900756368C20D0523D06C2FD8
Malicious:	false
Reputation:	low
Preview:	......"2....bredlifeof..home..https..info..remittance..www*J.....bredlifeof.....home.....https.....info.....remittance.....www..2.....a.....b.....c.....d.....e.....f.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....w...:8.....BU...Q..... .....*.https://www.bredlifeof.info/2.Home | reMittance:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150364
Entropy (8bit):	0.2865895612910949
Encrypted:	false
SSDEEP:	192:WHKoTyN7kXT/3P0b71tZdXT3/3yotZdXTbhVb3N:WHKo07kXrf0b71tZdXz1tZdXnhZd
MD5:	17D4D6A6DAA9783C543064A3C72E6047
SHA1:	B73C9B3623669D9E27D4316B5C2B6C76ACA8B670
SHA-256:	BC1AF75B1CD46540B080C302BD00D732E845E6C8E217BFC6A40C0E5E47D56294
SHA-512:	3619218C2FB07A74BFD07A8DE6F86C6E45A6440A863832C75CFA3C146FD75A5E754EB7D02C022F0EE9D388ABB95A2F868D70A6677495748D3AE1E31D96C5FB3
Malicious:	false
Reputation:	low
Preview:	.....dW..... ....

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):	3149
Entropy (8bit):	5.52515433003837
Encrypted:	false
SSDEEP:	48:OdtI6hOr8b8jGPha7RMs8dbDBRZbQSefgGRNrS0U9RdiN9l:O77Yr8ha7RM/dbDBRZbQ5fgGrrS0H
MD5:	DE536815556473FF8F9843CEBDC9017D
SHA1:	0A13A7C5E0C25A651B5419163DD45331A78C9427
SHA-256:	62688B574F78609796EF7470A668ED6037C2CAD4AF0192039D24AB0FCB75D741
SHA-512:	4655B76E8C809602A3DAA9E9F12611A3457A8DE610404383E6214449A9636B76D95E3B5D95CE942D878A9D0B46673D4658C812B5ED57D9235125BDEAF441894C
Malicious:	false
Reputation:	low
Preview:	ex.,...*..... META:https://www.bredlifeof.info.....a.-_https://www.bredlifeof.info..web-store-stateQ.{"cart":[],"currentOffer":null,"discountCode":null,"cappedQuantityWarning":null}.....,.....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..552371000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-12 18:53:35.40][INFO][mr.Init] MR instance ID: 2871a6ae-4248-4b9e-82e8-3643b47797c2\n","[2021-05-12 18:53:35.40][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-12 18:53:35.40][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-12 18:53:35.40][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-12 18:53:35.40][INFO][

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):	5.18713453686808
Encrypted:	false
SSDEEP:	6:mXSDiq2PcNwi23iKKdK8a2jMGIFUtp8SNrZmwP8SWibkwOcNwi23iKKdK8a2jMmd:sSDivLZ5Kk8EFUtp8Sd/P8SWib54Z5KV
MD5:	7CE1DDC8827CF78EF098233EA8D475DF
SHA1:	C37CB1B17EE0DC09556207FABF9B456D11AC5171

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SHA-256:	D3237D0444696F9973B3C2A0C0E425E7758D9D858E82A0A266A6D5951251C562
SHA-512:	0131EE100C43C2B6CA80DFA40DCD9412C9699AAAEB0A46C710C0B7CABC7BB4583F355759299C412AF867E3D05DAADE75F50165E4DE943F95172CCC75F9FE7 3C
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.326 6b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/12-18:53:13.328 6b0 Recovering log #3.2021/05/12-18:53:13.331 6b0 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):	1.3396676716768625
Encrypted:	false
SSDEEP:	384:HeRTJVPJRTJIfKRTJcvfRQT/+jRQG6mxJjRQ6/:HWH/0y4c+GmxJT
MD5:	BF75C0BDFC052A2B5DB837DAF1E427B4
SHA1:	5EFD551072F84D487B5EADBF5BFACDBAD7DD8828
SHA-256:	6E028FC67A8ECA8847DCD4803519EF77B4DDBF78CA662ED018C863CBF30BD883
SHA-512:	2EAB88A01D6A63A6531025A0BD595D4CF11982AACA0192FEE92CF86F6A2C4741650119C617BBA865890B5A31F080D8C2BCF291081DFBEDF225D638F9E430AAE 6
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):	1.1729284957960142
Encrypted:	false
SSDEEP:	384:4yUuhRTJUiTiRTJAStCMtRQVys7jRQPiN:FUKDWX0gutN
MD5:	E0A00CF5BE7C5ADF2C7A0A46BA755D7A
SHA1:	C4305D96B0AD471CFFE4B3C117C3217651D54122
SHA-256:	8DAA55B672B5DA6AF5CBB384931FCE72D4D1396FFFCE5D157C6EB961E648CBB0
SHA-512:	A3D3BF53F0D467A4862A3D62F934A1F0282C792479B09348DA9E4ED9523DF043867856AFC3F720E8C2C776AA6F27EC0D36698EA9F39ACEFD2F748BB54A0944A
Malicious:	false
Reputation:	low
Preview:	....

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):	342
Entropy (8bit):	5.193138709357016
Encrypted:	false
SSDEEP:	6:mXUQQIlL+q2PcNwi23iKKdKgXz4rRIFUtp8U0z1ZmwP8U0lLVkwOcNwi23iKKdKt:svQIlvLZ5KkgXiuFUtp8jz1/P8jz54ZR
MD5:	97016AF6DC24F305BC4FED771B9354A3
SHA1:	D2BD21F60AD47455DCCA6AB24C1DF0192C66E8D8
SHA-256:	E6E84CF6B85E86BEAD64B3854501DBBCE80E7B5E0D41F0163730622D9A4C801E
SHA-512:	84BE990D3F92B7D6EE03D16F344A31F80CEA8604AB6C169B2320B599F31FAE1867912F586021C3497EAA3FF5C43B713489B393FD09A9DC69BDDEA40E9AF8C5C 5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/05/12-18:53:13.560 15e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/12-18:53:13.562 15e8 Recovering log #3.2021/05/12-18:53:13.562 15e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.8613684550215958
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzPb2dWY2x:wIElwQF8mpcSg
MD5:	CE3B119D32B38366CAFB5BB21699C9DD
SHA1:	D263330CC7C7298A6E79FD0BDA7E5AE7BA3EDD54
SHA-256:	EA49C6A3B82B39A643FF9C681BCC44917075F2B4DE39ED3703091994A82CFF83
SHA-512:	F76A9ED39E8973FC04E5223A9C25A60B52EDBEE3C3DB053215709BD7EC67C00EA73689296D20E5874A6F884DA30F47E5FAFD2BFECAB335167626D9AC487C01D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6262534477889092
Encrypted:	false
SSDEEP:	48:WxQ5s2cMeqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUX4:VEhIElwQF8mpcS8
MD5:	671D39C04C8E3A129B94CF4022AE220C
SHA1:	3D9B448EB2050E8FEACE748B1D4F98B342E0144C
SHA-256:	46EBBCC8A5FE01FF721939A5450875A4593AC5E5B44778FE3E6A262A34D77173
SHA-512:	BF0E4E3463D9D34AB3BA6538F509B1C704F8868AA89A06046690BE066400ECC952137F1C443A65789996E71CEA74FD5F320F2BB9A7FC7CBF3685B0EF41CF4F15
Malicious:	false
Reputation:	low
Preview:	.....Tt..... ....

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):	95
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Entropy (8bit):	5.181666912092966
Encrypted:	false
SSDEEP:	6:mXXjIq2PcNwi23iKKdKrQMxIFUtp8a9ZmwP8aPkwOcNwi23iKKdKrQMFLJ:sXjIvLZ5KkCFUtp8a9/P8aP54Z5KktJ
MD5:	4E93FBE35E21A3B913A26E47B0679CC1
SHA1:	FF63F454E8F4161A49F34415688C171A876148FF
SHA-256:	C177059DD3C754E5298BE1D538133B2D92AC7E21D45E0CB73A30CAE2A2400891
SHA-512:	554D383A72DCDA156EB37044DE9EF13A8AC0A36A5510D9D9ED7363E853B13959C0C89BB7E71BCF6A3D8C3C305BD7D81E007D5588210655789AF9CC7B2B6A9A 0
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.438 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/12-1 8:53:13.439 15a4 Recovering log #3.2021/05/12-18:53:13.439 15a4 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
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.15832694299888
Encrypted:	false
SSDEEP:	6:mXOi+q2PcNwi23iKKdK7Uh2ghZIFUtp8bfQZmwP8oKtVkwOcNwi23iKKdK7Uh2gd:sOzvLZ5KklhHh2FUtp8bfQ/P8bT54Z5m
MD5:	941FC7F1B198CF05BF71386AD5C9F8D3
SHA1:	49B11CAC916E6165B26474DE70E9A4A8776A0C5C
SHA-256:	78CF2BD9292240FE016BA40D273A6F97BF6FA1E4D7E033B0E1DF055BBBAB66F3
SHA-512:	70763BB16F105EC57CE7B3DACC886FDED2154B03C8E02B769056C36B4B761E5E406677EC62C801164D7CA6B663EE3A76379AB2DBC97A28440070AAC42B7B33 C
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.234 15a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/05/12-18:53:13.235 15a8 Recovering log #3.2021/05/12-18:53:13.236 15a8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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):	438
Entropy (8bit):	5.282480035812205
Encrypted:	false
SSDEEP:	6:mXxpq2PcNwi23iKKdKusNpV/2jMGIFUtp89jZZmwP8oPkwOcNwi23iKKdKusNpV0:sxpvLZ5KkFFUtp8pZ/P8A54Z5KkOJ
MD5:	65577D1DA207A11F72B03ECB5860B7A9
SHA1:	4E37933DD54E7E8E566DE16492FC9F14A673E785
SHA-256:	A3C8B3C7562B4D0DD2BE5D9A564F15E329E01512BC4B258E123ED3E6F50FF4B9
SHA-512:	8746DB5E137BC32247ECA1B857FDE10D5D327C9580170E29772E7BAF82F7E891A9D9D35386F80CE24E62070A36118B0E7DF11D2CF9F496E8BE5FDF45FE697F9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Preview:	2021/05/12-18:53:13.497 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-18:53:13.498 15a4 Recovering log #3.2021/05/12-18:53:13.499 15a4 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):	5.301211922709334
Encrypted:	false
SSDEEP:	12:sxG4vLZ5KkmiuFUtp8lU9/P8lUP54Z5Kkm2J:ql5KkSgaJuo5Kkr
MD5:	354295B23E81B84E9FA6599C01AE3D2E
SHA1:	DBF7A3CCDC724A069723B31E667ED90CAB7248F0
SHA-256:	5C62D4E8845CB3662AF033B3A63906E8C6AD9225E86C8310D66890946F7E8476
SHA-512:	5D7444BBD8FB127C21B512BE37773FBFAE37C3F061A0918222D3F76D4DE2163CC1ED6373F19616B972E7D2953A17343B9E6966920776D3DEC2DA14FF7D100A7
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.565 cf4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/12-18:53:13.569 cf4 Recovering log #3.2021/05/12-18:53:13.569 cf4 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):	426
Entropy (8bit):	5.213118416744271
Encrypted:	false
SSDEEP:	6:mXb1lL+q2PcNwi23iKKdKusNpZQMxIFUtp8811ZmwP8vlLVkwOcNwi23iKKdKusx:sb1IvLZ5KkMFUtp8+1/P8vz54Z5KkTJ
MD5:	4CAA93B33E8783E36B41FB8B05B05BBF
SHA1:	20511673772448C272CA2AC8414DA6B77C946092
SHA-256:	AB194437F5E5EB23A83FB9991A3C3AA5B41F6E45E8A6B0BC9BBA9B779CC1A8AB
SHA-512:	EAE3DFD0D3F096BAA22817302343A0F1D680B0A5629028BACD8809E72EF7B809AAA1102EC1C041D0235D02F09B963E8F31157827B8F78CB2775BC4986E791AA(
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:30.280 15e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/12-18:53:30.281 15e8 Recovering log #3.2021/05/12-18:53:30.282 15e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\abd2dcd5-17ca-4b4a-8b6d-f696cf779a5f.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\abd2dcd5-17ca-4b4a-8b6d-f696cf779a5f.tmp	
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\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.198020166388796
Encrypted:	false
SSDEEP:	12:sEjvLZ5KkkGHArBFUtp8E3/P8EM54Z5KkkGHAryJ:Hl5KkkGgPgIo5KkkGga
MD5:	FB3064A454962B764ED61DA1F9ACCADA
SHA1:	613C9BBD80FF2BB99F13CBF29823A87DFA5DE171
SHA-256:	33F771F17029188816D417F72887E371C0554816432533BEFEF03DA4F947D98F
SHA-512:	68616DD5A985B4C1E5432E45238D9AD105BB372D77DC674DFEAF5FDDF869D4DC363154A7F8AEB7AAFEA35E6C59E3D2BC8D137A650E900C057BD94F4A4C7CE56
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:31.933 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-18:53:31.934 15a4 Recovering log #3.2021/05/12-18:53:31.935 15a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.239149324750957
Encrypted:	false
SSDEEP:	12:sENvLZ5KkkGHArqiuFUtp8EY/P8E/f54Z5KkkGHArq2J:tl5KkkGgCgYxo5KkkGg7
MD5:	E74DED88F10E4B234995BBA9D66BFD08
SHA1:	CD2E0B7D8FB63A394AB5C5507100D08842538E93
SHA-256:	80FE06145EFFB62AD4496E2273DDA1879F441EB41FA77EB6AF74CCE06B93BA17
SHA-512:	68ADF46D879732D398B7674189F00D1F1624F76079A77C91E22932621999BD69D20EDBE8DA52E2AC2B3BD0F28F7F71D9618ED5F12CDAADEDB51C8245ABAFC94
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Preview:	2021/05/12-18:53:31.947 7a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/12-18:53:31.954 7a4 Recovering log #3.2021/05/12-18:53:31.955 7a4 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):	5.208092808833178
Encrypted:	false
SSDEEP:	12:spvLZ5KkkGHArAFUtp8DC/P8nURF54Z5KkkGHArfJ:El5KkkGgkgOUBo5KkkGgV
MD5:	7BE1BCAD038073A5E6B221C377BB6DB1
SHA1:	7D456D5E15937105B699D674870A8B3F8C9AC55F
SHA-256:	158F2E4F7F4EB03618F0A2C7390110ADBCCCFDF808EBCAD81576C04B54DCE6BC
SHA-512:	74D30450703DC6BFA683270C0E7B85579AF181B5DBB1B59581DB925207892E9427736E827D75DE7EF41105EF180C560124BC0FA6F81C7D20F86568773FC9979B
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:47.407 cf4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/12-18:53:47.409 cf4 Recovering log #3.2021/05/12-18:53:47.410 cf4 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\a89915ff-cacb-48a9-96ae-3c2ace19d5ad.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.260704953275551
Encrypted:	false
SSDEEP:	6:mXzW39+q2PcNwi23iKKdKpIFUtp85HS3JZmwP8l2GN9VkwOcNwi23iKKdKa/WLJ:szO+vLZ5KkmFUtp85yZ/P8v3V54Z5Kk7
MD5:	33922B54E5B2DA3A0F286E636EDF523F
SHA1:	EE9047D70AC0F8171EECB2ADCC000DAB9CB71B24
SHA-256:	AC1E3B82E27B7C1F879C7998554FC8B4F5A237211AABC7FE82029F5B2CCD8721
SHA-512:	E10F0D36F70795C158282F188886016DBA12657E7F115A7974CC1B1658AE5412CC2538446A47866B6CECD3538D4CDF464366E54C7892BD20CD9C9C59FC1B14D
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:13.245 16bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/12-18:53:13.250 16bc Recovering log #3.2021/05/12-18:53:13.251 16bc 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):	410
Entropy (8bit):	5.319460199409376
Encrypted:	false
SSDEEP:	12:sCOvLZ5KkkOrsFUtp85Z/P8w54Z5KkkOrzJ:gl5Kk+gMHo5Kkn
MD5:	4CF964197DD2D26608AA8E929BDA1FA0
SHA1:	1E8DB4753DA9CD518225C040963E9842C4BEAC13
SHA-256:	FC87C876E1BB2C86D92230736C2475DFEF24F41D9097EEE478904976E88B0211
SHA-512:	67F69B697FCE76F844085C355194EFE3D71D746ABB52D1BAF193B8EACCDEBCE5BCD11F5F5E08BF0D19CFDD1ECE862495CD01EAD5C35D73AEA6A9E7F34881 B9B
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:35.387 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/12-18:53:35.388 15a4 Recovering log #3.2021/05/12-18:53:35.389 15a4 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):	84
Entropy (8bit):	5.094775120629743
Encrypted:	false
SSDEEP:	3:pv7wlhFjfjllDUgoazvZlz5ttszvH:pzQDfbtRPI
MD5:	B75ED224F0D100AB8341296B044E1C22
SHA1:	C0D197CB565B765B8C879FDD7A7EF0E4F59DC819
SHA-256:	26A3B1FD0687E9EC0956F2C847F91EB8870BE0FC218F1761772B3CB27AC85957
SHA-512:	BF1F215D36DF8F6AB7C63E898A70BDE301239E624ABCFA209B4AD06BF1F94EA43AE2A04F6C5C470AB0C912C5975620B45AED284E4E1A5009D4D918AF6154CE 98
Malicious:	false
Reputation:	low
Preview:	....M.[.....^c7TI.j.....X...q.....e..K.>...../.-..)...."..,.I.....I..JOw..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bb3d3b44-00f5-4c44-8a70-3893966c8164.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):	19181
Entropy (8bit):	5.570170056026729
Encrypted:	false
SSDEEP:	384:suntpLl1zXf1kXqKf/pUZNCgVLH2HfD+rUAVHGqXKICo4RZ:FLlpf1kXqKf/pUZNCgVLH2HfirUApG6i
MD5:	F546EC45BCC69C37307EB9C819A5114B
SHA1:	081649322AFFF99D1920FAF3DA84CDF287C8BFCC
SHA-256:	96CC62B32965E2F9E5E13A0A6AE2230CAC122FB35FCA55A3A78E044BE5BE35FC
SHA-512:	CA32A71843FAAB580FC7E4CB92761CF93C7BCEC795B5C43B4CE691B0B366198D9EBD21D91325CF2538CBCD08FAFBD7D450397949CCCE09CA8210BE3F9C678 C0
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":"13265344393250038","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\bdbe1232-1289-4776-9e62-d5b97fc29e10.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5794
Entropy (8bit):	5.200823896738687
Encrypted:	false
SSDEEP:	96:nG3hhs12tsYVGik0JCKL8kKkx1xbOTQVuwn:nyhu2tsY8k4KvKkxz
MD5:	4F0E2CE5AB6F91FDD98DDE04DDD79249
SHA1:	2AA45C58AB659E2C1C06A6B2AAC7936751B99111
SHA-256:	BEDFFD969501B5BCCABD5E13DA33E614235C1995183BFBF1C7D27449910075EF
SHA-512:	AD651FC2ED5C4E158F36A0FA1F749CB00848F90443DC22B106BC6E90AB19780D1FEE1801AF31CC292E620FBE3D2ABE6C4DDEC4B8CC67C5F3F738C5F00EE25 93
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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\c5e69d7c-330b-44b3-980e-a55c57a6f44e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577055123767945
Encrypted:	false
SSDEEP:	384:sunt8Ll1zXf1kXqKf/pUZNCgVLH2HfD+rUBXfIbo4d:QLlpf1kXqKf/pUZNCgVLH2HfirUBgboi
MD5:	3CF6F1A034F3AAB6F8B8143D217E3F49
SHA1:	85F3438018A43C0EFDEF4587FAB79711F3C0F04E
SHA-256:	A28326FA28646124735A7E351627CBA46FC6B79D794594EE85BB434D0878AEFE
SHA-512:	8E05028809562DA3296243F5F0655890A4A86CFE765371313A7BBAF539A620F41673AC4087D9B198205942C05B15BEE8956C17A5396BCC3906E38F8D2BD87F50
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":"13265344393250038","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\d30a0184-0f95-43c5-9818-a0fc24cf7416.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d30a0184-0f95-43c5-9818-a0fc24cf7416.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5768
Entropy (8bit):	5.198604262900556
Encrypted:	false
SSDEEP:	96:nG3hP/12tsYVZik0JCKL8kKkx1EbOTQVuwn:nyhl2tsY3k4KvKkxs
MD5:	F15011B638D9BB16E46F6F030A50F632
SHA1:	530FF4C521DC5D9BC5380476F59AADEAF3CE3582
SHA-256:	B5489E2C9D41260B3D527E86CA066860D0AB6AD5C649BE37C632B764B1461F80
SHA-512:	4A3652BF69E9698A065A34E6584D827B3B594AA3F3A89D684117573DD7FF6C3C97D5849672D9EB05B4145CCB57A6E5B5BFDA896B259C9697C2D436116CEBA70
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.509908250129215
Encrypted:	false
SSDEEP:	3:tUKCDfQ6LIj1Zmwv38DfQ6LXTsSVV8s8DfQ6LXTsSVWGv:mXJLIJZmwP8JLDsSVVv8JLDsSVtv
MD5:	15C5E758E3AE0252A68E45D8660712F3
SHA1:	713517CDE5E215684BD4BD7F0E8C3E4556D403E1
SHA-256:	8B3D709C0D7B4D8D1DC555DDE0EE4852C995FE159B7229941BA83489FCA203D1
SHA-512:	3F66BB2C421D6919ED5DDBEE5A7285E873309C6AEA8263C9A5F1CC703639E13E22B0334DD762A34C273213464FB7DB6DF51BB151E144A0D87B54790178CF5AE
Malicious:	false
Reputation:	low
Preview:	2021/05/12-18:53:24.254 168c Recovering log #3.2021/05/12-18:53:24.356 168c Delete type=0 #3.2021/05/12-18:53:24.356 168c Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dc9139bb-3de3-4c9e-b75f-6afe2dfa69ba.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):	1545
Entropy (8bit):	5.568944815251771
Encrypted:	false
SSDEEP:	48:Y8BUAVwUz6UUhvMSUoKUevGUeiU64CpwUWUev2:rBUfUmUUSSUoKU/UHU64dUWUl
MD5:	F07521DB36CD38675B36967597C2DA21
SHA1:	5BE8ECCB63F6B9EDF4D1A8428D59440517C54F78
SHA-256:	6AD64C159DB42AE927D81C57C5D28F6680DE666A454DCAA8AE9B2C3BB3EB8790
SHA-512:	33DBA51F06C8AB4222BFC910F67CB2D8A3E24ECFB64376C0E80AC9362ED06BE1CE183F9F9BBB84165020051E462F11984157AE87BFA6B4AE3C02EB2E050E0AEA
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1652406846.784934,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870846.784939},{"expiry":1636650811.7257,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870811.725704},{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1652406846.569183,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620870846.569187},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de064d0f-dc33-47f2-9cc2-fb890febd9ba.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):	5768
Entropy (8bit):	5.198631225566995
Encrypted:	false
SSDEEP:	96:nG3hP/12tsYVcik0JCKL8kKkx1EbOTQVuwn:nyhl2tsYmk4KvKkxs
MD5:	3FBF3C49EEDC5FDF0AFA322C98FD9461
SHA1:	127DAD1535D7AC8BA39D512934B1463DB911F250
SHA-256:	27B856F6D6659779D42F4A930CC2DDD0B8F593C2F3988A0AF4B6895AC242E915
SHA-512:	CDEB6FB6DB578B20FA5F1C94DDC71EF1A497DB7135DF0E9A45A0C7820ACE35D66939108975BF0A024277876BA016D711F48BF7CCDE69F9E16CF6C0502D98D5D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265344393483203","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\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):	5.250897776321817
Encrypted:	false
SSDEEP:	6:mXGdIq2PcNwi23iKKdKfrzAdIFUtp8AdZZmwP8z3PkwOcNwi23iKKdKfrzILJ:sG2vLZ5Kk9FUtp84Z/P87P54Z5Kk2J
MD5:	0B4FD8BD1EF1A483A5BB6035715A0EEA
SHA1:	525AE80C218E0C79A4AF47F204FD679AC14364CC
SHA-256:	0C86F3E9B617B7F9D2FED0E0B9D4692A5657B9DA3E48A10921036DCEB1768D3C
SHA-512:	562111AE58CCCAA4C417952FBF126A99217C4C69259DBA1D91B6F2F7527EC0B6D9AC98D4F66D8FD99CB215126FA568FA4FC0CCF5D48C557451EE046983F431
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/05/12-18:53:34.280 7a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/12-18:53:34.286 7a4 Recovering log #3.2021/05/12-18:53:34.287 7a4 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\b8dab316-e31d-451c-881f-3fffd91cfec2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7492880326805356
Encrypted:	false
SSDEEP:	384:dn+ltzoibgz7VU6poNJrCvNX3mpnCHTeGatrYLxtxm3fj+r8dmsPoHDtJD9mOzD1:da2R1K7gDnawerRXUOln72TKVbBpl
MD5:	2F8F45A6D36F365231B387886F7794C1
SHA1:	6FAA0F27521056C65E589DFFA45E193CD04A4279
SHA-256:	6B8D493EB385D7BEFC7914CC16E3618D5B48E5FE95BEEA7488220FE662DE37F9
SHA-512:	90B733BAE17FCDEBE3E3334090A05EA60CFBAFDCB5E605C9906503B599D8A005B5C4E3C0108EEB3412EDBF37D214AA5E03326B11B83DF5D612E23D2EAA7E2F67
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....98.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\c2113ef5-7069-4cf5-9b0f-9d49eb0d981b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724

C:\Users\user\AppData\Local\Google\Chrome\User Data\c2113ef5-7069-4cf5-9b0f-9d49eb0d981b.tmp	
Entropy (8bit):	3.7488610282735757
Encrypted:	false
SSDEEP:	384:zn+ltzoiHzcpoNJrCvNX3mpnCHTeGatrYLxtxm3fj+r8dmsPoHDtJD9mOzD5NI1D:y2R1K7gDnawerRXUOIn72TKVbBpq
MD5:	D7F191174BF1ADA5331F9EC7B0E936D8
SHA1:	A9BDC9838BFD587084EE9C377279CD5D6FB2EB2F
SHA-256:	53656738832D6230E5CD8EB54ECB095F332664FF64C6C8BE7A8BC13A1BAFCAF8
SHA-512:	7BDC7B2380E81E1028D8ED49BCBFC2508201D433A6F6530FCB7A4670F918E7B3DA94BCD174A8788F50FC49602ABF34145ABE9E38B9C5763BDAC34C5437B6AAB
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....98.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\d028659d-ed6c-4205-b933-02e5be6a2232.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):	168898
Entropy (8bit):	6.079942931581325
Encrypted:	false
SSDEEP:	3072:OkUbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:dUiyDhXHwbtgbV/njhcI8II6Ri
MD5:	E741BE1DF2E8BD663F2651EDE0938821
SHA1:	B4E4AEC7E2A1757504E1A39A11AEDD4A69D8BCDB
SHA-256:	56D38A7BDE0E4DDC6847FB26EC3D3DE35E2BD578653D7E1D8438B342A07EA89C
SHA-512:	53982203AF11B0880F8B89F510267ECF619B0D5DF2AC63F2F19F97AC6E3DF03A06F8DBC3332F02565C95D1444F9E04ABB221D56A6542C279EB8CFDB43F5C2EF
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909260519"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\de23baa0-d7e1-449f-be06-e1b8c6cf7746.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):	168898
Entropy (8bit):	6.0799422655318835
Encrypted:	false
SSDEEP:	3072:OkFbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:dFiyDhXHwbtgbV/njhcI8II6Ri
MD5:	240725213CA5E73D2962247D80A16B93
SHA1:	F37BB5C0C6C755F9C0289875DD38D54506995A07
SHA-256:	55840A8114BD4EDEFF9A1B4D20ED4C92577CDA957B7E0919476EAFF593F94876
SHA-512:	C8DB99AA12C0A5BF90E168CF1B7885476295E47457287504ED8B20DAA8C56936050E04F404BACC7BAB030262F2F098E48C99C8D153C5B45AC890F7C59A8C508
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909260519"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\fbdf428a-6c36-45c0-bd0f-110fbd0ca4c8.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):	168897
Entropy (8bit):	6.07994079920717

C:\Users\user\AppData\Local\Google\Chrome\User Data\fbdf428a-6c36-45c0-bd0f-110fbd0ca4c8.tmp	
Encrypted:	false
SSDEEP:	3072:3kKbYjw5DhcuwTcwLfSpvdLBALA7bV/nYorVcI8XIssElYTRi:0KiyDhXHwbtgbV/njhcI8II6Ri
MD5:	A8A7438F293E740E090FE239A34BFCB4
SHA1:	7BC7439BDA0C6CB62B26985934FEBBBB0ECABD0E
SHA-256:	262377893B36EA6C902E9B0923548A1ADB3867E06EFBFFE0DFE9783A5C745D1F
SHA-512:	1741001309CC147A0763E22D6656F6B83A2921C7DB6EBEBBB8BDDD4FFC312C77EE9AC9BF799E041B66310A7B74241CC475A0D34C19A9276B0BC1B5E08ABCB97A
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":1.620870796662304e+12,"network":1.620838398e+12,"ticks":109657559.0,"uncertainty":4778640.0}},"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\074a9540-96f8-4196-9d68-c6d1eb3e8847.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\1a5e0603-3c9e-490b-a20f-df9da55775df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.:.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\a5183b88-3250-4c2e-8c73-d675bc9df0ae.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

C:\Users\user\AppData\Local\Temp\a5183b88-3250-4c2e-8c73-d675bc9df0ae.tmp	
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	38454
Entropy (8bit):	4.5899002289059005
Encrypted:	false
SSDEEP:	768:PdKZ5q5Qttz5cROj3EQIkuYaa3YAuFcfrt2srSAX1RQ/ZLkl5SwsoHT:PA5ptz5nIkuYH3YAuFcfrt2srSAXKE
MD5:	58CA6BF02E3EB6FCBCD922261FDF2BA7
SHA1:	FC912B6E328718B0400FB837E8AEBF2DF7D91CBB
SHA-256:	0A4ABA3CF8049883E2A0F7CB057774D651DA0129653044D5DBEA6ADC882B028E
SHA-512:	C80D1B824EBB8C75C63E015912D919CCB526ED5C8DF82EBDFAF5F2310EAB448CB7514DB7AB24A405CFAADB9C1B9406ADBAD27B75713664795D7A71A03B62D15A
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 12f5620983023193b3f9183b74f824d57f4d23bf2e36a5da0f436e13cf566c2f f4d466a7202313bfe573845eb5c8a4907f62b73d26e033b9bc1d1a63904346fa.SERVER_HANDSHAKE_TRAFFIC_SECRET 12f5620983023193b3f9183b74f824d57f4d23bf2e36a5da0f436e13cf566c2f fc916c69ae6a2100af0eff4fc261c5256c217a829d5992a10c82d1c8ecc7922c.CLIENT_HANDSHAKE_TRAFFIC_SECRET 7e5d23ed1a2a4b0f87de50a561f4de48c3bf20b119157178d617455ca9b3a6ec 66734cc513e59af139bcb8112fe411bf90ef5b046f1dc22a382fc895a79eabc0.SERVER_HANDSHAKE_TRAFFIC_SECRET 7e5d23ed1a2a4b0f87de50a561f4de48c3bf20b119157178d617455ca9b3a6ec 88a4335f344d669851cecb338f7164a92b71b830a1039fd7bf132ef720dd4c78.CLIENT_HANDSHAKE_TRAFFIC_SECRET 6d7727ecfa83927d8cfdfcf8259bf32982dc12896f98e7528a5a41e86b522ef1 966301b66c9e8bc42e9a395a7e3da631dca635ea579b84428e92d6799e59de3a.SERVER_HANDSHAKE_TRAFFIC_SECRET 6d7727ecfa83927d8cfdfcf8259bf32982dc12896f98e7528a5a41e86b522ef1 46e3e4ddb0bf5c2302dc6ac3d1a201e398f1716f6887350b57aa0e0e8670918d.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\cdcecb74-35f2-4b7c-af73-59c0b0a0f709.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
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..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir6128_1573894603\1a5e0603-3c9e-490b-a20f-df9da55775df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6128_1573894603\1a5e0603-3c9e-490b-a20f-df9da55775df.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6128_1573894603\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205l7": {.. "message": "....."... },... "1213957982723875920": {.. "message": "..... ... .?"... },.. "1282768764603190 75": {.. "message": "..... ..."... },... "1428448869078126731": {.. "message": ".... ....."... },... "1522140683318860351": {.. "message": "..... ...."... },.. "1550904064710828958": {.. "message": "...."... },... "1636686747687494376": {.. "message": "... ..."... },... "1802762746589457177": {.. "message": "..."... },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

Static File Info

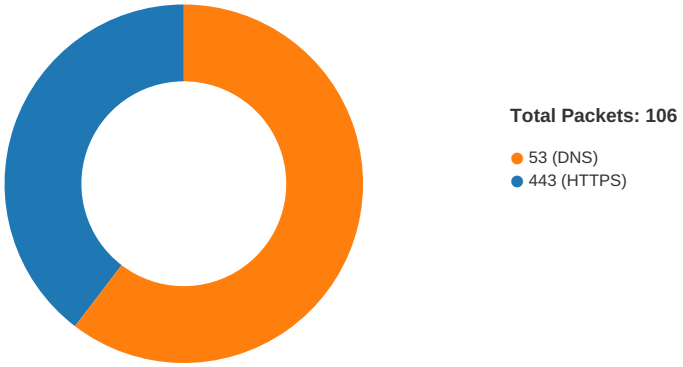
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-18:53:33.485975	TCP	2515	WEB-MISC PCT Client_Hello overflow attempt	49759	443	192.168.2.7	142.250.186.74

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:53:17.992695093 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:17.993630886 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.055995941 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.056113005 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.056476116 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.058494091 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.058607101 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.058866024 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.119705915 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.122148037 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.122175932 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.122189045 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.122196913 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.122262955 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.122303009 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.123245001 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.123613119 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.126310110 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.126339912 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.126360893 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.126374960 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.126432896 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.126468897 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.127480030 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.214811087 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.214890957 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.320874929 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.322170019 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.322956085 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.385828018 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.388607025 CEST	443	49712	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395572901 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395622969 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395647049 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395673990 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395699978 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395709038 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.395723104 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395733118 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.395747900 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395771027 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.395771027 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395792007 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.395797014 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.395832062 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459148884 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459172964 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459197998 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459222078 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459245920 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459275961 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459280014 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459305048 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459306002 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459325075 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459330082 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459355116 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459378958 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459379911 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459405899 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459422112 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459433079 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459458113 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459480047 CEST	49711	443	192.168.2.7	52.49.20.157

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:53:18.459485054 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459511042 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459521055 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459534883 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459561110 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459569931 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459587097 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459611893 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459624052 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.459635973 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.459681034 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.514643908 CEST	49712	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.522934914 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.522978067 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523005009 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523036003 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523051977 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.523061991 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523078918 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.523087025 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523113012 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523139000 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523140907 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.523166895 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523184061 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.523194075 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523217916 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523241997 CEST	443	49711	52.49.20.157	192.168.2.7
May 12, 2021 18:53:18.523264885 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.523294926 CEST	49711	443	192.168.2.7	52.49.20.157
May 12, 2021 18:53:18.599297047 CEST	49718	443	192.168.2.7	151.101.2.79
May 12, 2021 18:53:18.599965096 CEST	49719	443	192.168.2.7	151.101.2.79
May 12, 2021 18:53:18.601314068 CEST	49722	443	192.168.2.7	151.101.2.79
May 12, 2021 18:53:18.603071928 CEST	49724	443	192.168.2.7	151.101.2.79
May 12, 2021 18:53:18.644690990 CEST	443	49718	151.101.2.79	192.168.2.7
May 12, 2021 18:53:18.644792080 CEST	49718	443	192.168.2.7	151.101.2.79

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:53:06.224049091 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:06.273742914 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 18:53:06.464854002 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:06.525661945 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 18:53:07.231760025 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:07.285341024 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 18:53:08.395788908 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:08.447257996 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 18:53:09.765147924 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:09.819205046 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 18:53:11.333652020 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:11.382453918 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 18:53:12.569169044 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:12.619544029 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 18:53:14.159445047 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:14.208255053 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 18:53:17.465817928 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.519301891 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 18:53:17.859427929 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.862492085 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.864494085 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.867660046 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.869437933 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:17.923377991 CEST	53	54008	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:53:17.926397085 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 18:53:17.928765059 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 18:53:17.936623096 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 18:53:17.991483927 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 18:53:18.365539074 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:18.424855947 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 18:53:18.539072990 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:18.539879084 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:18.540122032 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:18.566504002 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:18.596487999 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 18:53:18.596992016 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 18:53:18.597192049 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 18:53:18.625682116 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 18:53:19.395512104 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:19.444369078 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 18:53:20.800745010 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:20.853432894 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 18:53:20.973082066 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:21.107646942 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 18:53:22.216025114 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:22.265618086 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 18:53:23.405275106 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:23.456126928 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 18:53:24.976188898 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:25.033334970 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 18:53:25.486066103 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:25.546245098 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 18:53:31.495099068 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:31.516266108 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:31.519586086 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:31.557226896 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 18:53:31.571254015 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 18:53:31.574374914 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 18:53:31.694355965 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:31.743096113 CEST	53	60599	8.8.8.8	192.168.2.7
May 12, 2021 18:53:32.386960983 CEST	59571	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:32.446584940 CEST	53	59571	8.8.8.8	192.168.2.7
May 12, 2021 18:53:33.357029915 CEST	52689	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:33.434721947 CEST	53	52689	8.8.8.8	192.168.2.7
May 12, 2021 18:53:34.045320034 CEST	50290	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:34.096841097 CEST	53	50290	8.8.8.8	192.168.2.7
May 12, 2021 18:53:34.889273882 CEST	60427	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:34.949284077 CEST	53	60427	8.8.8.8	192.168.2.7
May 12, 2021 18:53:35.180433035 CEST	56209	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:35.237835884 CEST	53	56209	8.8.8.8	192.168.2.7
May 12, 2021 18:53:35.684349060 CEST	59582	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:35.745563984 CEST	53	59582	8.8.8.8	192.168.2.7
May 12, 2021 18:53:35.916655064 CEST	60949	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:35.965446949 CEST	53	60949	8.8.8.8	192.168.2.7
May 12, 2021 18:53:39.080028057 CEST	58542	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:39.128834963 CEST	53	58542	8.8.8.8	192.168.2.7
May 12, 2021 18:53:45.536283970 CEST	59179	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:45.587306023 CEST	53	59179	8.8.8.8	192.168.2.7
May 12, 2021 18:53:50.337038994 CEST	60927	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:50.385914087 CEST	53	60927	8.8.8.8	192.168.2.7
May 12, 2021 18:53:51.839994907 CEST	57854	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:51.888791084 CEST	53	57854	8.8.8.8	192.168.2.7
May 12, 2021 18:53:58.452924967 CEST	62026	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:58.529781103 CEST	53	62026	8.8.8.8	192.168.2.7
May 12, 2021 18:53:58.920938015 CEST	62468	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:58.982783079 CEST	53	62468	8.8.8.8	192.168.2.7
May 12, 2021 18:53:59.667813063 CEST	52563	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:59.668751001 CEST	54721	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:53:59.669322968 CEST	62826	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:59.673036098 CEST	62046	53	192.168.2.7	8.8.8.8
May 12, 2021 18:53:59.728410959 CEST	53	62826	8.8.8.8	192.168.2.7
May 12, 2021 18:53:59.736048937 CEST	53	52563	8.8.8.8	192.168.2.7
May 12, 2021 18:53:59.742613077 CEST	53	54721	8.8.8.8	192.168.2.7
May 12, 2021 18:53:59.746110916 CEST	53	62046	8.8.8.8	192.168.2.7
May 12, 2021 18:54:00.441657066 CEST	51223	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:00.499841928 CEST	53	51223	8.8.8.8	192.168.2.7
May 12, 2021 18:54:00.578771114 CEST	63908	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:00.639125109 CEST	53	63908	8.8.8.8	192.168.2.7
May 12, 2021 18:54:03.030932903 CEST	49226	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:03.098017931 CEST	53	49226	8.8.8.8	192.168.2.7
May 12, 2021 18:54:03.977631092 CEST	60212	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:03.978408098 CEST	58867	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:04.038233995 CEST	53	58867	8.8.8.8	192.168.2.7
May 12, 2021 18:54:04.050685883 CEST	53	60212	8.8.8.8	192.168.2.7
May 12, 2021 18:54:05.608027935 CEST	50864	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:05.608860970 CEST	61504	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:05.609661102 CEST	60231	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:05.667481899 CEST	53	60231	8.8.8.8	192.168.2.7
May 12, 2021 18:54:05.668458939 CEST	53	50864	8.8.8.8	192.168.2.7
May 12, 2021 18:54:05.669218063 CEST	53	61504	8.8.8.8	192.168.2.7
May 12, 2021 18:54:06.087532043 CEST	50095	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:06.148927927 CEST	53	50095	8.8.8.8	192.168.2.7
May 12, 2021 18:54:13.578208923 CEST	59654	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:13.646811008 CEST	53	59654	8.8.8.8	192.168.2.7
May 12, 2021 18:54:14.059211016 CEST	56822	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:14.116309881 CEST	53	56822	8.8.8.8	192.168.2.7
May 12, 2021 18:54:14.233237982 CEST	62572	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:14.290529013 CEST	53	62572	8.8.8.8	192.168.2.7
May 12, 2021 18:54:14.861850977 CEST	57179	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:14.923655033 CEST	53	57179	8.8.8.8	192.168.2.7
May 12, 2021 18:54:20.044581890 CEST	56124	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:20.059781075 CEST	62287	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:20.074142933 CEST	54644	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:20.117120028 CEST	53	62287	8.8.8.8	192.168.2.7
May 12, 2021 18:54:20.150470972 CEST	53	54644	8.8.8.8	192.168.2.7
May 12, 2021 18:54:20.150501966 CEST	53	56124	8.8.8.8	192.168.2.7
May 12, 2021 18:54:20.849330902 CEST	59159	53	192.168.2.7	8.8.8.8
May 12, 2021 18:54:20.910062075 CEST	53	59159	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:53:17.859427929 CEST	192.168.2.7	8.8.8.8	0xe7b4	Standard query (0)	www.bredlifeof.info	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.539072990 CEST	192.168.2.7	8.8.8.8	0xd444	Standard query (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.539879084 CEST	192.168.2.7	8.8.8.8	0x2ebf	Standard query (0)	jimdo-storage.freetls.fastly.net	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.540122032 CEST	192.168.2.7	8.8.8.8	0x8c27	Standard query (0)	fonts.jimstatic.com	A (IP address)	IN (0x0001)
May 12, 2021 18:53:20.973082066 CEST	192.168.2.7	8.8.8.8	0xef5d	Standard query (0)	www.bredlifeof.info	A (IP address)	IN (0x0001)
May 12, 2021 18:53:24.976188898 CEST	192.168.2.7	8.8.8.8	0xd9	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
May 12, 2021 18:53:25.486066103 CEST	192.168.2.7	8.8.8.8	0x1e5f	Standard query (0)	4dfffgghmhkh.s3.eu-west-3.amazonaws.com	A (IP address)	IN (0x0001)
May 12, 2021 18:53:31.495099068 CEST	192.168.2.7	8.8.8.8	0xf704	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 12, 2021 18:53:31.516266108 CEST	192.168.2.7	8.8.8.8	0xeab2	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:53:31.519586086 CEST	192.168.2.7	8.8.8.8	0x7512	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 18:53:34.889273882 CEST	192.168.2.7	8.8.8.8	0x950d	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 12, 2021 18:53:59.669322968 CEST	192.168.2.7	8.8.8.8	0x9581	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 18:54:03.977631092 CEST	192.168.2.7	8.8.8.8	0x8d48	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.044581890 CEST	192.168.2.7	8.8.8.8	0xf0b4	Standard query (0)	www.bredlifeof.info	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.059781075 CEST	192.168.2.7	8.8.8.8	0x73b6	Standard query (0)	fonts.jimstatic.com	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.074142933 CEST	192.168.2.7	8.8.8.8	0xf508	Standard query (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.849330902 CEST	192.168.2.7	8.8.8.8	0x41f4	Standard query (0)	jimdo-storage.freetls.fastly.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	www.bredlifeof.info	web.jimdosite.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	web.jimdosite.com	dolphin-renderserve-prod.jimdo-platform.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	dolphin-renderserve-prod.jimdo-platform.net	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.49.20.157	A (IP address)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		54.246.199.25	A (IP address)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.16.206.246	A (IP address)	IN (0x0001)
May 12, 2021 18:53:17.991483927 CEST	8.8.8.8	192.168.2.7	0xe7b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		34.248.153.214	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.596487999 CEST	8.8.8.8	192.168.2.7	0xd444	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.2.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.596487999 CEST	8.8.8.8	192.168.2.7	0xd444	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.66.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.596487999 CEST	8.8.8.8	192.168.2.7	0xd444	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.130.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.596487999 CEST	8.8.8.8	192.168.2.7	0xd444	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.194.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.596992016 CEST	8.8.8.8	192.168.2.7	0x8c27	No error (0)	fonts.jimstatic.com	f2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:18.597192049 CEST	8.8.8.8	192.168.2.7	0x2ebf	No error (0)	jimdo-storage.freetls.fastly.net		151.101.2.79	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:53:18.597192049 CEST	8.8.8.8	192.168.2.7	0x2ebf	No error (0)	jimdo-storage.freetls.fastly.net		151.101.66.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.597192049 CEST	8.8.8.8	192.168.2.7	0x2ebf	No error (0)	jimdo-storage.freetls.fastly.net		151.101.130.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:18.597192049 CEST	8.8.8.8	192.168.2.7	0x2ebf	No error (0)	jimdo-storage.freetls.fastly.net		151.101.194.79	A (IP address)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	www.bredlifeof.info	web.jimdosite.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	web.jimdosite.com	dolphin-renderserve-prod.jimdo-platform.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	dolphin-renderserve-prod.jimdo-platform.net	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.16.206.246	A (IP address)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		34.248.153.214	A (IP address)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.49.20.157	A (IP address)	IN (0x0001)
May 12, 2021 18:53:21.107646942 CEST	8.8.8.8	192.168.2.7	0xef5d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		54.246.199.25	A (IP address)	IN (0x0001)
May 12, 2021 18:53:25.033334970 CEST	8.8.8.8	192.168.2.7	0xd9	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:25.033334970 CEST	8.8.8.8	192.168.2.7	0xd9	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 12, 2021 18:53:25.546245098 CEST	8.8.8.8	192.168.2.7	0x1e5f	No error (0)	4dfffgghmhkh.s3.eu-west-3.amazonaws.com	s3-r-w.eu-west-3.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:25.546245098 CEST	8.8.8.8	192.168.2.7	0x1e5f	No error (0)	s3-r-w.eu-west-3.amazonaws.com		52.95.155.72	A (IP address)	IN (0x0001)
May 12, 2021 18:53:31.557226896 CEST	8.8.8.8	192.168.2.7	0xf704	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 12, 2021 18:53:31.557226896 CEST	8.8.8.8	192.168.2.7	0xf704	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 12, 2021 18:53:31.571254015 CEST	8.8.8.8	192.168.2.7	0x7512	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:31.574374914 CEST	8.8.8.8	192.168.2.7	0xeab2	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:31.574374914 CEST	8.8.8.8	192.168.2.7	0xeab2	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 12, 2021 18:53:34.949284077 CEST	8.8.8.8	192.168.2.7	0x950d	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:53:34.949284077 CEST	8.8.8.8	192.168.2.7	0x950d	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 12, 2021 18:53:59.728410959 CEST	8.8.8.8	192.168.2.7	0x9581	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:53:59.746110916 CEST	8.8.8.8	192.168.2.7	0xcfce	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:04.050685883 CEST	8.8.8.8	192.168.2.7	0x8d48	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:20.117120028 CEST	8.8.8.8	192.168.2.7	0x73b6	No error (0)	fonts.jimstatic.com	f2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:20.150470972 CEST	8.8.8.8	192.168.2.7	0xf508	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.2.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150470972 CEST	8.8.8.8	192.168.2.7	0xf508	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.66.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150470972 CEST	8.8.8.8	192.168.2.7	0xf508	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.130.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150470972 CEST	8.8.8.8	192.168.2.7	0xf508	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.194.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	www.bredlifeof.info	web.jimdosite.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	web.jimdosite.com	dolphin-renderserve-prod.jimdo-platform.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	dolphin-renderserve-prod.jimdo-platform.net	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.16.206.246	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		54.246.199.25	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		34.248.153.214	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.150501966 CEST	8.8.8.8	192.168.2.7	0xf0b4	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.49.20.157	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.910062075 CEST	8.8.8.8	192.168.2.7	0x41f4	No error (0)	jimdo-storage.freetls.fastly.net		151.101.2.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.910062075 CEST	8.8.8.8	192.168.2.7	0x41f4	No error (0)	jimdo-storage.freetls.fastly.net		151.101.66.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.910062075 CEST	8.8.8.8	192.168.2.7	0x41f4	No error (0)	jimdo-storage.freetls.fastly.net		151.101.130.79	A (IP address)	IN (0x0001)
May 12, 2021 18:54:20.910062075 CEST	8.8.8.8	192.168.2.7	0x41f4	No error (0)	jimdo-storage.freetls.fastly.net		151.101.194.79	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 12, 2021 18:53:18.691216946 CEST	151.101.2.79	443	192.168.2.7	49718	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:53:18.693104982 CEST	151.101.2.79	443	192.168.2.7	49719	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:53:18.693291903 CEST	151.101.2.79	443	192.168.2.7	49722	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:53:18.693937063 CEST	151.101.2.79	443	192.168.2.7	49724	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:53:21.249480009 CEST	52.16.206.246	443	192.168.2.7	49734	CN=www.bredlifeof.info CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 15:49:09 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 15:49:09 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 12, 2021 18:53:26.771344900 CEST	52.95.155.72	443	192.168.2.7	49742	CN=*.s3.eu-west-3.amazonaws.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Aug 28 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Aug 27 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 12, 2021 18:53:26.771614075 CEST	52.95.155.72	443	192.168.2.7	49743	CN=*.s3.eu-west-3.amazonaws.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Aug 28 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Aug 27 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:53:35.071875095 CEST	152.199.23.37	443	192.168.2.7	49770	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.072092056 CEST	152.199.23.37	443	192.168.2.7	49769	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.325793982 CEST	152.199.23.37	443	192.168.2.7	49772	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:53:35.332716942 CEST	152.199.23.37	443	192.168.2.7	49773	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.533154964 CEST	152.199.23.37	443	192.168.2.7	49775	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.537758112 CEST	152.199.23.37	443	192.168.2.7	49776	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:53:35.714345932 CEST	152.199.23.37	443	192.168.2.7	49777	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.715466976 CEST	152.199.23.37	443	192.168.2.7	49778	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 12, 2021 18:53:35.895198107 CEST	152.199.23.37	443	192.168.2.7	49780	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:53:43.702076912 CEST	52.16.206.246	443	192.168.2.7	49796	CN=www.bredlifeof.info CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 15:49:09 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 15:49:09 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 12, 2021 18:53:45.513624907 CEST	52.16.206.246	443	192.168.2.7	49805	CN=www.bredlifeof.info CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 15:49:09 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 15:49:09 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 12, 2021 18:53:52.822266102 CEST	52.16.206.246	443	192.168.2.7	49822	CN=www.bredlifeof.info CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 15:49:09 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 15:49:09 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:54:15.961910009 CEST	151.101.2.79	443	192.168.2.7	49895	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021	Sun May 29 20:19:36 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:54:16.369847059 CEST	151.101.2.79	443	192.168.2.7	49898	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021	Sun May 29 20:19:36 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:54:16.370721102 CEST	151.101.2.79	443	192.168.2.7	49897	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021	Sun May 29 20:19:36 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:54:20.284327984 CEST	151.101.2.79	443	192.168.2.7	49910	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021	Sun May 29 20:19:36 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 12, 2021 18:54:20.946614027 CEST	151.101.2.79	443	192.168.2.7	49912	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021	Sun May 29 20:19:36 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 18:54:21.123662949 CEST	151.101.2.79	443	192.168.2.7	49914	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6128 Parent PID: 160

General

Start time:	18:53:12
Start date:	12/05/2021
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.bredlifeof.info/'
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: 5172 Parent PID: 6128

General

Start time:	18:53:14
Start date:	12/05/2021
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=1576,19381948695824494,2468386753968997499,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1772 /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