ID: 397950
Cookbook: browseurl.jbs
Time: 16:10:26
Date: 26/04/2021
Version: 31.0.0 Emerald

Table of Contents

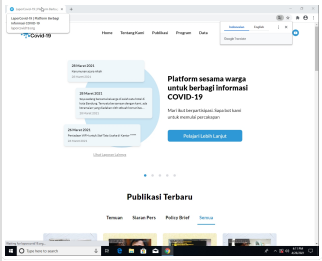
Analysis Report http://www.laporcovid19.org

Overview

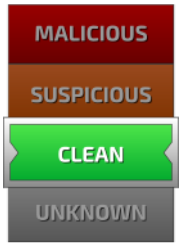
General Information

Sample URL:	http://www.laporcovid19.org
Analysis ID:	397950
Infos:	

Most interesting Screenshot:



Detection

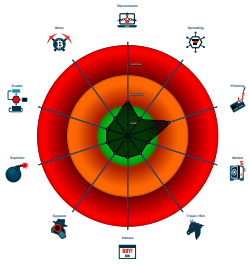


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- HTML title does not match URL
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6032 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.laporcovid19.org' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5368 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7152 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4744 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

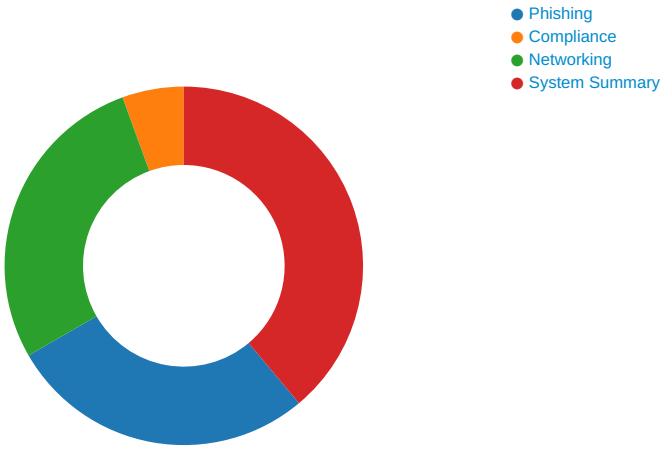
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



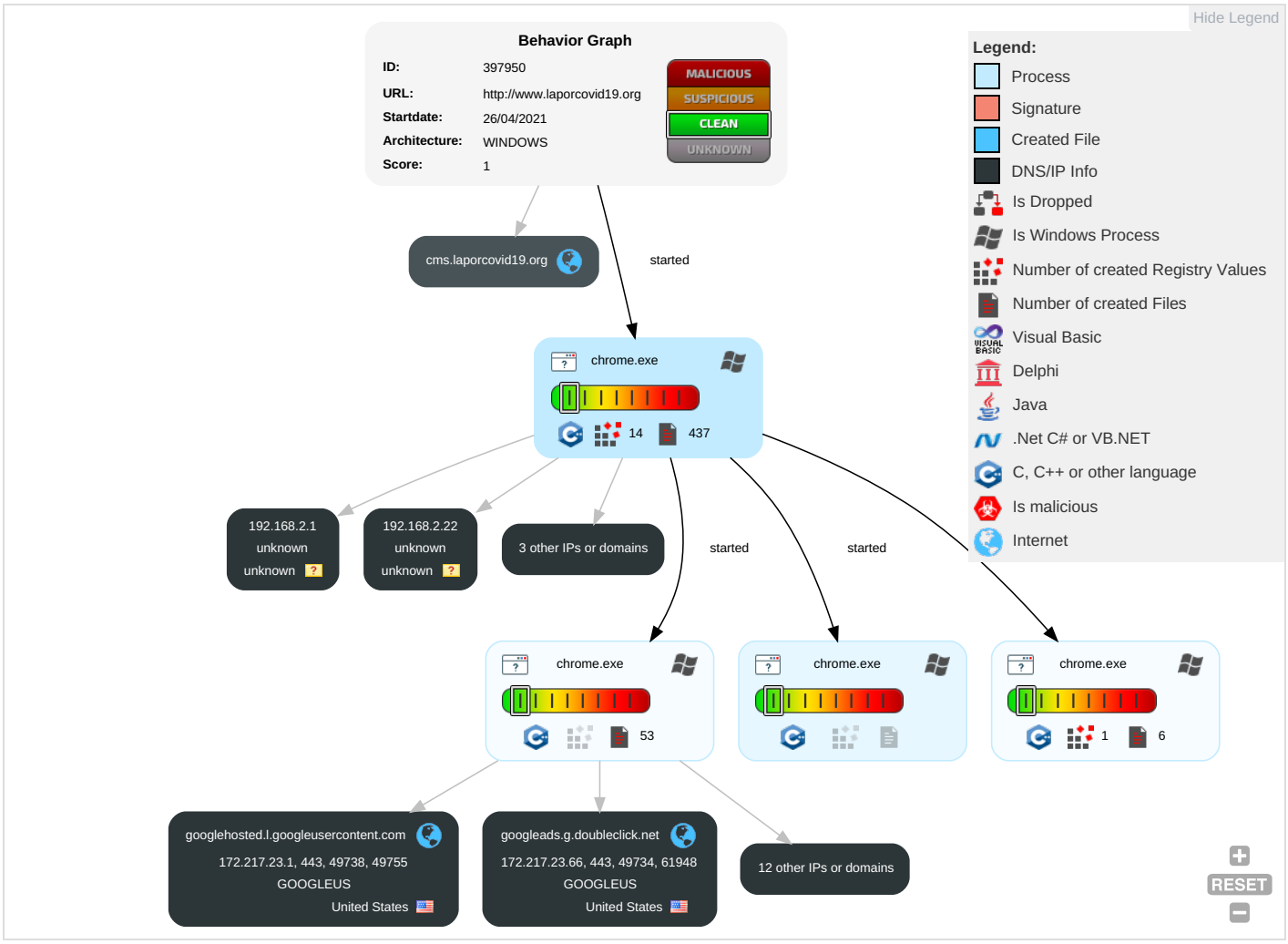
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	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
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

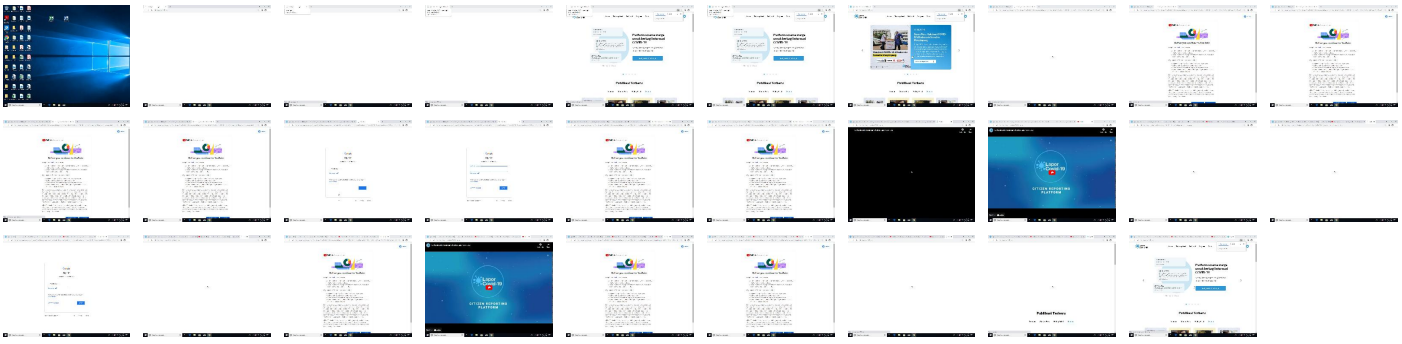
Behavior Graph

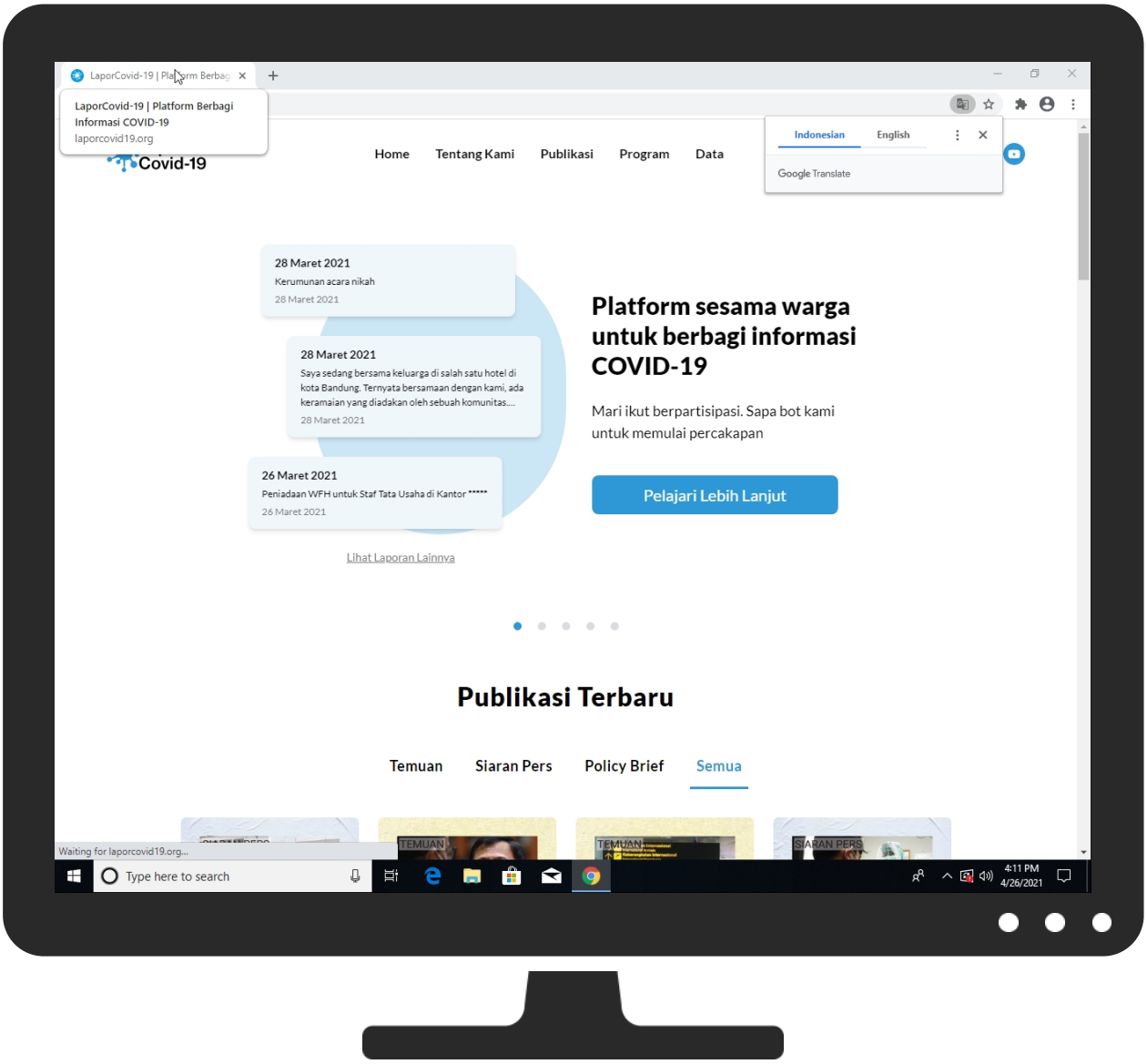


Screenshots

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://www.laporcovid19.org	0%	Virustotal		Browse
http://www.laporcovid19.org	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://laporcovid19.org/_nuxt/aa5b96e.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/14b25ad.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/3023af3.js	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://laporcovid19.org/LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.orgh	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/3LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/758f5b5.jsaD	0%	Avira URL Cloud	safe	
http://www.laporcovid19.org/	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/7f26880.js	0%	Avira URL Cloud	safe	
http://192.168.1.5:4000/	0%	Avira URL Cloud	safe	
http://https://peta.laporcovid19.org/	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/cdn-cgi/bm/cv/669835187/api.js	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://laporcovid19.org/_nuxt/7f26880.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/e89325f.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/favicon.ico	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/758f5b5.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/113a2f4.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/7cd4187.js	0%	Avira URL Cloud	safe	
http://laporcovid19.org/	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/aa5b96e.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/02731e2.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/jk	0%	Avira URL Cloud	safe	
http://www.laporcovid19.org/LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/113a2f4.jsaD	0%	Avira URL Cloud	safe	
http://https://www.laporcovid19.org/LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/d2fd471.jsaD	0%	Avira URL Cloud	safe	
http://https://www.laporcovid19.org/	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/d2fd471.js	0%	Avira URL Cloud	safe	
http://www.laporcovid19.org/23LaporCovid-19	0%	Avira URL Cloud	safe	
http://laporcovid19.org/LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/696116c.jsaD	0%	Avira URL Cloud	safe	
http://https://forum.laporcovid19.org/	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/3023af3.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/696116c.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/6ca9ecf.jsaD	0%	Avira URL Cloud	safe	
http://https://www.laporcovid19.org/23LaporCovid-19	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/71744e7.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/7cd4187.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/e89325f.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/02731e2.jsaD	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/R	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/_nuxt/71744e7.js	0%	Avira URL Cloud	safe	
http://https://laporcovid19.org/23LaporCovid-19	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
laporcovid19.org	104.21.85.166	true	false		unknown
googleads.g.doubleclick.net	172.217.23.66	true	false		high
www.laporcovid19.org	104.21.85.166	true	false		unknown
i.ytimg.com	172.217.23.86	true	false		high
photos-ugc.l.googleusercontent.com	172.217.23.1	true	false		high
consent.youtube.com	172.217.23.46	true	false		high
cms.laporcovid19.org	172.67.207.167	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
yt3.ggpht.com	unknown	unknown	false		high
accounts.youtube.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.youtube.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/embed/0rMjn0gn3-s	false		high
http://www.laporcovid19.org/	false	• Avira URL Cloud: safe	unknown
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D0rMjn0gn3-s&gl=DE&m=0&pc=yt&uxe=23983172&hl=en&src=1	false		high
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCboLp6FcRL5LbKL46sXBXlg&gl=DE&m=0&pc=yt&uxe=23983172&hl=en&src=1	false		high
http://laporcovid19.org/	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/	false		unknown
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCboLp6FcRL5LbKL46sXBXlg%3Ffeature%3Demb_ch_name_ex&gl=DE&m=0&pc=yt&uxe=23983172&hl=en&src=1	false		high
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D0rMjn0gn3-s%26feature%3Demb_imp_woyt&gl=DE&m=0&pc=yt&uxe=23983172&hl=en&src=1	false		high

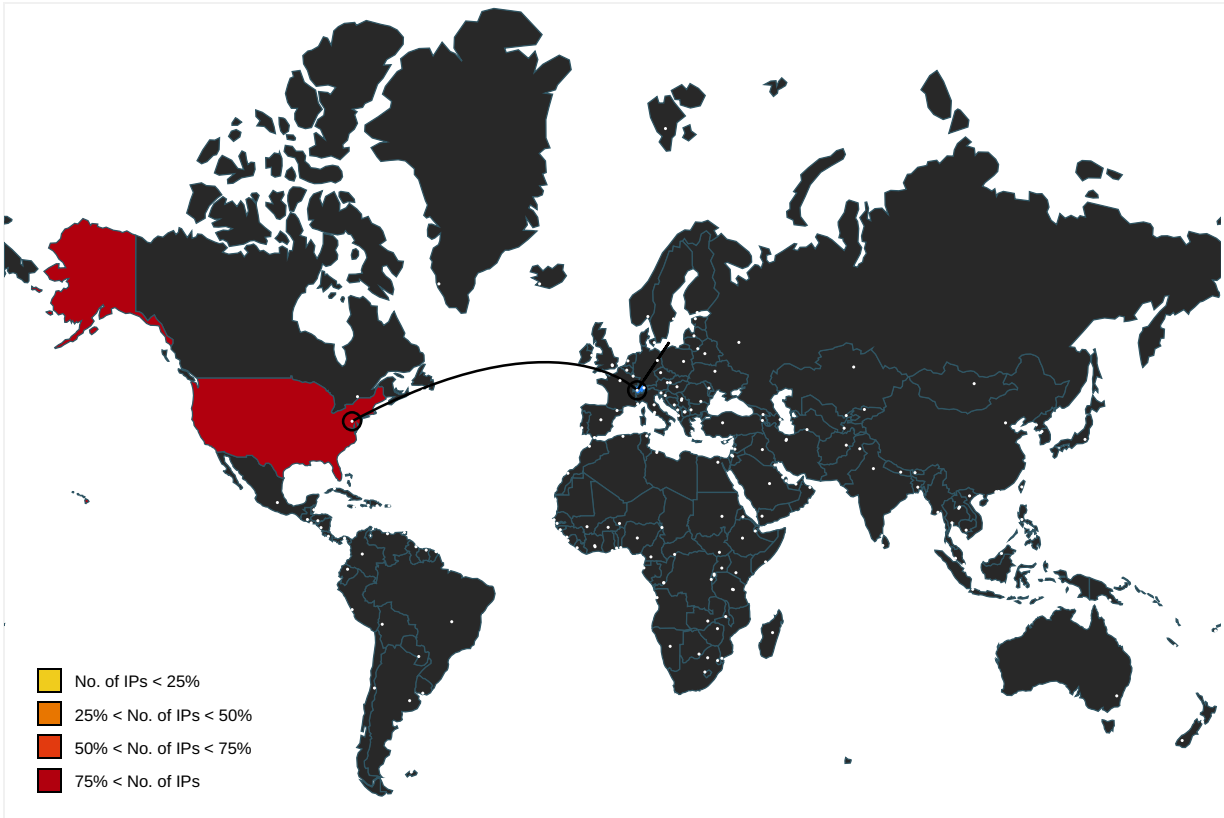
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://laporcovid19.org/_nuxt/aa5b96e.jsaD	5ae83a951500f4f1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/fa244a41/www-embed-player.vflset/www-embed-player.js	f374efe77d747fee_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/14b25ad.js	3628128b7cb7b3ec_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/3023af3.js	ad16b5408654ed52_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/LaporCovid-19	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.orgh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/base.js	ef7caa204c1b984e_0.0.dr, b06ea7729b30c0bd_0.0.dr	false		high
http://https://laporcovid19.org/3LaporCovid-19	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/758f5b5.jsaD	c4e0918b4735a4bb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCboLp6FcRL5LbKL46s	History-journal.0.dr	false		high
http://https://www.youtube.com/watch?v=0rMjn0gn3-s	Current Session.0.dr	false		high
http://https://yt3.ggpht.com	2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high
http://https://www.youtube.com	Current Session.0.dr, 2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high
http://https://twitter.com/LaporCovid	d7301d588c29468b_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/7f26880.js	b7791abd66804a67_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/favicon.ico	Favicons.0.dr	false		high
http://https://youtube.com/F	335e69ddec2b9ac6_0.0.dr	false		high
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_loginYouTube/	History-journal.0.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/embed.jsaD	b0a360ceeb8dc1d8_0.0.dr	false		high
http://https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg	Current Session.0.dr	false		high
http://192.168.1.5:4000/	d7301d588c29468b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/0rMjn0gn3-sYouTube	History-journal.0.dr	false		high
http://https://youtube.com/	baf039634a1a22d3_0.0.dr, d894af6cc49377fb_0.0.dr	false		high
http://https://peta.laporcovid19.org/	9d6d19f482de5a7d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/cdn-cgi/bm/cv/669835187/api.js	13198f6293cb0d13_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	203b75e8-1113-48ec-b3fe-db301dfe56db.tmp.1.dr, 5a4ff1d6-afe2-43bf-b831-297da7da3016.tmp.1.dr, 8bab6cfd-84f4-4ebd-9833-e78ec45f6fa0.tmp.1.dr, 2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/embed/0rMjn0gn3-s	Current Session.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlgBefore	History-journal.0.dr	false		high
http://https://laporcovid19.org/_nuxt/7f26880.jsaD	b7791abd66804a67_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/e89325f.jsaD	55474a2cdb068b88_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/favicon.ico	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/758f5b5.js	c4e0918b4735a4bb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/113a2f4.js	586efb0622951409_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/	000003.log0.0.dr	false		high
http://https://youtube.com/V	335e69ddec2b9ac6_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/7cd4187.js	a7a0299e641655a5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=zdmDRZpD7ZbTNFiazYRwzyjNaQ91p8BUX4l9osCYkShVbD8Qnx8R%2FWNGdOyE	Reporting and NEL.1.dr	false		high
http://https://youtube.com/U	f374efe77d747fee_0.0.dr	false		high
http://https://www.instagram.com/laporcovid19/	d7301d588c29468b_0.0.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/remote.js	2563e2cfdae02f95_0.0.dr, 39986ccdf0da7184_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/aa5b96e.js	5ae83a951500f4f1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/favicon.ico&	Favicons.0.dr	false		high
http://https://laporcovid19.org/_nuxt/02731e2.js	08a027927af6e12c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/jk	ad16b5408654ed52_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.laporcovid19.org/LaporCovid-19	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login	Current Session.0.dr, History-journal.0.dr	false		high
http://https://laporcovid19.org/_nuxt/113a2f4.jsaD	586efb0622951409_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_loginP-E	Current Session.0.dr	false		high
http://https://www.laporcovid19.org/LaporCovid-19	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/d2fd471.jsaD	34cadc32b20ec592_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.laporcovid19.org/	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/watch?v=0rMjn0gn3-sBefore	History-journal.0.dr	false		high
http://https://youtube.com/m	335e69ddec2b9ac6_0.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/d2fd471.js	34cadc32b20ec592_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.laporcovid19.org/23LaporCovid-19	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/0rMjn0gn3-sYouTube/	History-journal.0.dr	false		high
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_loginV	Current Session.0.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/fetch-polyfill.vflset/fetch-polyfill.jsaD	baf039634a1a22d3_0.0.dr	false		high
http://laporcovid19.org/LaporCovid-19	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/696116c.jsaD	6fdde531359d58b6_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://forum.laporcovid19.org/	d7301d588c29468b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/fa244a41/fetch-polyfill.vflset/fetch-polyfill.js	baf039634a1a22d3_0.0.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/embed.js	b0a360ceeb8dc1d8_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/3023af3.jsaD	ad16b5408654ed52_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D0rMjn0gn3-s%26fea	Current Session.0.dr, History-journal.0.dr	false		high
http://https://laporcovid19.org/_nuxt/696116c.js	6fdde531359d58b6_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/6ca9ecf.jsaD	d7301d588c29468b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login2	Current Session.0.dr	false		high
http://https://consent.youtube.com/	Network Action Predictor-journal.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=devPYgTGRqqhLtNi1soMS0b96VuZ7giiIlvn6Vz%2BvK7bmAxcuPM3Dy%2Fn6D	Reporting and NEL.1.dr	false		high
http://https://www.laporcovid19.org/23LaporCovid-19	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://consent.youtube.com	Current Session.0.dr, 2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mathiasbynens/CSS.escape).	d7301d588c29468b_0.0.dr	false		high
http://https://laporcovid19.org/_nuxt/71744e7.jsaD	9d6d19f482de5a7d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg?feature=emb_ch_name_exBefore	History-journal.0.dr	false		high
http://https://laporcovid19.org/_nuxt/7cd4187.jsaD	a7a0299e641655a5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=wyAd%2F60a7YkqKqASYrQ1Cy9E3lYScIo4MUm%2B%2F8zq%2B5s7gQpyFFmoBP	Reporting and NEL.1.dr	false		high
http://https://laporcovid19.org/_nuxt/e89325f.js	55474a2cdb068b88_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/_nuxt/02731e2.jsaD	08a027927af6e12c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.doubleclick.net	2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/base.jsaD	ef7caa204c1b984e_0.0.dr	false		high
http://https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg?feature=emb_ch_name_ex	Current Session.0.dr	false		high
http://https://laporcovid19.org/R	08a027927af6e12c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://youtube.com/Q$#	b0a360ceeb8dc1d8_0.0.dr	false		high
http://https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_loginYouTube	History-journal.0.dr	false		high
http://https://laporcovid19.org/_nuxt/71744e7.js	9d6d19f482de5a7d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://laporcovid19.org/23LaporCovid-19	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com	2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high
http://https://googleads.g.doubleclick.net	2a52b76b-550d-411b-9675-677450b0d02b.tmp.1.dr	false		high
http://https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/remote.jsaD	39986ccdf0da7184_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.1	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.86	i.ytimg.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.21.85.166	laporcovid19.org	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.5
192.168.2.22
192.168.2.30
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	397950
Start date:	26.04.2021
Start time:	16:10:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.laporcovid19.org
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@49/215@13/10

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg • Browse: https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg?feature=emb_ch_name_ex • Browse: https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login • Browse: https://www.youtube.com/watch?v=0rMjn0gn3-s • Browse: https://www.youtube.com/embed/0rMjn0gn3-s • Browse: https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg • Browse: https://www.youtube.com/channel/UCboLp6FcRL5LbKL46sXBXlg?feature=emb_ch_name_ex • Browse: https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login • Browse: https://www.youtube.com/watch?v=0rMjn0gn3-s • Browse: https://www.youtube.com/embed/0rMjn0gn3-s • Browse: https://www.youtube.com/watch?v=0rMjn0gn3-s&feature=emb_imp_woyt • Browse: https://laporcovid19.org/

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): 40.88.32.150, 92.122.145.220, 13.64.90.137, 172.217.20.238, 172.217.22.238, 172.217.22.205, 168.61.161.212, 173.194.160.139, 74.125.108.39, 216.58.207.131, 172.217.23.67, 172.217.20.234, 172.217.23.46, 216.58.207.142, 216.58.207.174, 172.217.23.14, 172.217.23.78, 172.217.22.206, 172.217.23.74, 216.58.207.134, 216.58.207.132, 172.217.20.227, 172.217.22.234, 216.58.207.138, 216.58.207.170, 172.217.23.10, 172.217.23.42, 172.217.22.202, 216.58.207.164, 172.217.23.35, 184.30.24.56, 20.82.210.154, 52.147.198.201, 93.184.221.240, 92.122.213.247, 92.122.213.194, 74.125.108.40 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, arc.msn.com.nsatc.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, r3---sn-h0jeenle.gvt1.com, skypedataprdcoleus15.cloudapp.net, clients2.google.com, r2.sn-h0jeenle.gvt1.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, youtube-ui.l.google.com, www3.l.google.com, store-images.s-microsoft.com, translate.googleapis.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r5---sn-h0jeen7d.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, static-doubleclick-net.l.google.com, r2---sn-h0jeenle.gvt1.com, skypedataprdcoleus16.cloudapp.net, r5.sn-h0jeen7d.gvt1.com, play.google.com, r3.sn-h0jeenle.gvt1.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 NtWriteFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\572e8620-2305-4508-879f-d998540bf246.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):	157171
Entropy (8bit):	6.050953668169353
Encrypted:	false
SSDEEP:	3072:dxfI3pxWj/2Cr2KuQznfv2xFcbXafIB0u1GOJmA3iuRS:fpr3ZznHaaqfIlUOoSiuRS
MD5:	5383E3C6AA2E321E09DA584908F4505D
SHA1:	8F7BFD11B91F18E19621DA8F0A950B7DF7666740
SHA-256:	66A437DD9C99445EC04130C12925D975AEF76851F9A84C3FDC2E8DF71791D4A6
SHA-512:	525D77D844CAF4355930866F4466ADD4942ABEC7FE1D8A90D727AA26F910BFDB3AD281DC8F83FC01DDDADEE89558887DF268383EBE53154CAB7DA3E0025272 1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\572e8620-2305-4508-879f-d998540bf246.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.619478678733329e+12,"network":1.61944628e+12,"ticks":97726641.0,"uncertainty":4535546.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016756115"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\616f281f-d85e-4983-af90-137857d6fdd7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7436723388799393
Encrypted:	false
SSDEEP:	384:xnp2eADJkTcyVb9ClN+r7vSa3xKUpHkRGFMrXkSYxZk4srrTCmP030G2K1OsIGNQ:JemBJCkV9wenUeAY/X26KMqWx0
MD5:	2E9370E3652F1A91873FA93951423150
SHA1:	78DB87AE3F70D50D7FBA6CA61A729660B920D4DD
SHA-256:	592A28E038B3424ADBE229854E0F170049C447DF52AD35B86CB45E87E1DEC5C0
SHA-512:	9C7332A05C8439814FBF47C5C9A70E1100407F4418BB4A7571F8F0AC128A9BE7EB2FA019AC6919D5FD59B15784ECA49C314B556B3E4C19A6D32F15E5F9DFDCD0
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...O88.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\6fb46bd4-73e1-44a3-ac33-fdf694a52947.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):	165654
Entropy (8bit):	6.081638696402161
Encrypted:	false
SSDEEP:	3072:XdWxfl3pxWj/2Cr2KuQznfv2xFcbXafIB0u1GOJmA3iuRS:Nkpr3ZznHaaqfIlUOoSiuRS
MD5:	AB9C86F64562BBEAD05F9ED64505AEC3
SHA1:	C438BE2B822D246E0D9D95A4FBD6B782633E8B85
SHA-256:	CFAAB2DA6292E01506B4590F70C9244C8CB9BC3F2277CE83D51D99CD1FD73804
SHA-512:	E1810A5136F3C521F666592AA4FD361274C9BDE088A2E3331103F009EE64B7EF66C6B58D4A5583F155FD8BA10D861725BC9D308968E198CB67FA0867FF39A243
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":1.619478678733329e+12,"network":1.61944628e+12,"ticks":97726641.0,"uncertainty":4535546.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fd65967-e7bb-4eb0-84f1-2ff565f7d946.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7434438229072184
Encrypted:	false
SSDEEP:	384:hnp2eADJkTcyVb9ClN+r7vSa3xKUpHkRGFMrXkSYxZk4srrTCmP7J30G2K1OsIGF:ZemBJCkM9wenUeAY/X26KMqWx7
MD5:	09405122D925617BE315939FE4A5A86E
SHA1:	1CFE51A718EAF738CE6CA66BAF1807F168000EB8
SHA-256:	0217CF1025EBF2BD7B279EC7419A866E4535C30AB8C6B8EC84F3B3BB415A1187
SHA-512:	457A0E1F4033A04A677E053E33D9506D3C5C22711CF1FDAAA78E56BC5D44553098D7ACEB66614C6492EF2D3BFA100081F303FCF04244B4F42D8D3746A84DAD9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fd65967-e7bb-4eb0-84f1-2ff565f7d946.tmp	
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...O88.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\723898b2-b40c-420a-94a3-60e014386e47.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):	165654
Entropy (8bit):	6.081636149134691
Encrypted:	false
SSDEEP:	3072:XLgxfI3pxWj/2Cr2KuQznfv2xFcbXafIB0u1GOJmA3iuRS:7epr3ZznHaaqfIlUOoSiuRS
MD5:	A6E3D2DD1F2835C53DF530D64CDEA714
SHA1:	B57FB0D38966DAEF97AA5EFBBA808EA5539F970D
SHA-256:	4D47F2130659CD8C18CEC68BFA707D81F7A27C96860560369634DF1FD510475D
SHA-512:	28C70281FC49079BEFC66A6E345B0239446D84EB3362DD670B7EFC9E0EEF896DBD22805782A8C65C2980BDAA77EFD1F0073943997DD4C9E224BD0BEE0EC630A
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":1.619478678733329e+12,"network":1.61944628e+12,"ticks":97726641.0,"uncertainty":4535546.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\07834de8-7029-419b-a0de-384aed9ff5fb.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):	1374
Entropy (8bit):	5.5754530979210895
Encrypted:	false
SSDEEP:	24:YI6H0UhrrfwUgf4xatSU1iaZ3kG1KU1aQvkq/HeUeXby2qUeXv4y/b7wU12WRUew:YI6UUhQUIaatSUISDKUv8qPeUer2UefQ
MD5:	481CA2B5D1239ABFF4479A6B74B80B35
SHA1:	083AE07D6640CBD9D1B48155256AC5F3E1FEF3DE
SHA-256:	CA4BD31822FC079D8BEEC3D6265FEB872734642CCB96BFB14CD92F5F853C832F
SHA-512:	5E285F0B3438EDC7B82175E8D6F219DB9776608A04E18BBD1F1E776C1FA14B2331221E4496688A82996A931F9A9E394482D8930D7ECFFFC49190FC1FC72454C5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1630365081.708151,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619478681.708157},{"expiry":1651014733.773056,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478733.77306},{"expiry":1651014688.829084,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478688.829088},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14405826-94a2-4dfa-a363-409d01905208.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1375
Entropy (8bit):	5.573592115158562
Encrypted:	false
SSDEEP:	24:YI6H0UhrrfwUgf4kgtSU1zNxXG1KU1Ekq/HeUeXby2qUeXv443b7wU1jFRUenHQ:YI6UUhQUI7gtSUtzyKUDqPeUer2UefdA
MD5:	DBF397589C3C037B11663FC16FF0DED8
SHA1:	4EFF21CD4464B543506E4E9BC8EDFAD6066903E2
SHA-256:	1043F38E4371BDE7526B238974215AD018D0D0BF7681D61AECC1AB84DFB96DE2
SHA-512:	B258B3F8AC8D3D09E167D0B2DCE4EC50847B36360F945A33CC6CDE80B22DE6254D26DDE45776F37D80330F15C11A2D618BB90EA94CDD3BB28906069F270ABD 3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1630365081.708151,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619478681.708157},{"expiry":1651014687.788723,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478687.788727},{"expiry":1651014680.608996,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478680.609001},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\16c3aa17-e26d-4c95-a953-c44f394f94ee.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):	5093
Entropy (8bit):	4.98310253313669
Encrypted:	false
SSDEEP:	96:nr96N0p8fpcVyMok0JCKL83k41pbOTQVuwn:nr8Nfpci4KMk4D
MD5:	B6421E72FD937F457BC37B3CD94FFCAA
SHA1:	A4E54833445DAD7C16919FEDBA949B20BBEC90AB
SHA-256:	938DF1939E1891F30B90D6656899C521AD4AAFE4CD1EF86B9E54981167CF5BBF
SHA-512:	9A0A48EE947F4FC25B81501DE8AE29E36AF4E6A75D9118C7533331882D55E06DA4BD1161CB25645F4A7AD770831D2A6E42518AE4A6C127CB38E653F7FB648C0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263952275977524","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_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",",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1badc00b-7dc4-484c-ab86-0826b03af8c6.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):	5757
Entropy (8bit):	5.190216763273546
Encrypted:	false
SSDEEP:	96:nr96X0H8flwo+AW0cVymok0JCKL83k41pbOTcfVuwn:nr8Nflwo+ccO4KMk4jR
MD5:	121E5F7E6D0E5A8D598B15115E55B9D0
SHA1:	DAE3FE8109B51D72D5ACA9A911AEBBFA59F38607
SHA-256:	A227D778549438B5487B1A967965130603C164700FE0DC6DA639B26C7770C9D4
SHA-512:	61470921C0EC953392FB8F3A4D98CE975105349B7E1BDFE70B41794D70B1CB1425E29F9111179E3B5F509855098DB6027ED0558E8CA148A608F6F4A3BF20AE13
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263952275977524","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_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",",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\26e32a77-9e5b-4ee5-b28d-daaaed07a260.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\26e32a77-9e5b-4ee5-b28d-daaaed07a260.tmp	
Category:	dropped
Size (bytes):	1375
Entropy (8bit):	5.578024269803528
Encrypted:	false
SSDEEP:	24:YI6H0UhrrfwUgf4TotSU1YZ3kG1KU1aQvkq/HeUeXby2qUeXv4y/b7wU12WRUenw:YI6UUhQUIztSUWDKUv8qPeUer2Uefbf0
MD5:	7D07707B1BEE8F7F7AE4E35D0C046542
SHA1:	D7218AAC4F484E475DFD317A6AA18A443971E634
SHA-256:	84B3CD61169738DEDB6A235C742001C7C243604572F975ACB02FB505D6C41E3D
SHA-512:	F7B3A07637FD8F99B57CEE228A3370EF1C04D12325035C060BDDB4210A420A335C16AD1990187BE7D18535D36D21A9CF41369991D7748C59302F42BADE902F1F
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1630365081.708151,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619478681.708157},{"expiry":1651014729.419524,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478729.419528},{"expiry":1651014688.829084,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DealM38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478688.829088},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\28c94b37-589c-48a6-809b-b5ec8949b012.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):	1374
Entropy (8bit):	5.577184274162081
Encrypted:	false
SSDEEP:	24:YI6H0UhrrfwUgf4h/tSU1ZZ3kG1KU1aQvkq/HeUeXby2qUeXv443b7wU1jFRUenw:YI6UUhQUIItSUBDKUv8qPeUer2Uefdw9
MD5:	7EAA686E563943343D75B3884781D033
SHA1:	8BE11D542AF8D7A41FF0D49F720AFAA9A0EEECF7
SHA-256:	71BE1A768E8B865AA7C0EFE4AB118EF646C86AAA31FE2505354EB10DAEA92A3C
SHA-512:	EDF36C7043366BC3A3BC3447D26A7DE5A0BC3481AED1A35953DCA38D51563C29254A6E3FC547B7721877BD03019B047D651738B73491E732358EF8D75F2B0021
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1630365081.708151,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619478681.708157},{"expiry":1651014695.78858,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478695.788584},{"expiry":1651014688.829084,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DealM38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478688.829088},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2a52b76b-550d-411b-9675-677450b0d02b.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):	4842
Entropy (8bit):	4.885825075771808
Encrypted:	false
SSDEEP:	96:JXDHzM3fu9HvmrG2rGfqrpLdGt6rs1EyLIEA4GKGyc2r7hH:JXDHzM3fu9PmrrrdFLds6rsKyLIEbVnF
MD5:	E632366B4E2905F318A32BBCC5733F24
SHA1:	77AF3AFEAAB4C590B757ACDC076F24D84D293480
SHA-256:	C7E08FC0F6CB2AFEE2F1AEB22388D87D41C6A9754723B62D46178C6497A68473
SHA-512:	F9078851B54B0907649DE273DE4B05E4CE892DB367939CBF86A6D438BD3053436D75CA41D80BACE2F73BDB9C801BEA8D41ED63771D04DB1D6DE28F5FC6A798ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.laporcovid19.org","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13266544278533355","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13266544278895764","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13266544278895766","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r5---sn-h0jeen7d.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13266544286696488","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.googleusercontent.com","suppor

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\544876ea-5734-4db6-b4ae-aa5040b74848.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\544876ea-5734-4db6-b4ae-aa5040b74848.tmp	
Size (bytes):	1375
Entropy (8bit):	5.572027782432224
Encrypted:	false
SSDEEP:	24:YI6H0UhrrfwUgf4RUtSU1dZ3kG1KU1aQvkq/HeUeXby2qUeXv4vU7wU18aRUenHQ:YI6UUhQUIptSURDKUv8qPeUer2UefPwd
MD5:	EAF84C51E56439543DCBE9FF4B67B7AB
SHA1:	7BE1D894C067178BF189DD4165933212EF4777BF
SHA-256:	8E3DD358FEFD715D780FCD05AF4D509D083843B5C432D42205F22E312F62BD1E
SHA-512:	A9FFED6201016FC812119BB812B3D7BD8FBEAA474720B995DF72FA2E593442AB185254E853F6DFEAD5CB0D31DC69BD9D5A8EB104722308D7DBF2D2CC2BCB9 11
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1630365081.708151,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619478681.708157},{"expiry":1651014708.610117,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478708.610121},{"expiry":1651014688.829084,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1619478688.829088},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a4ff1d6-afe2-43bf-b831-297da7da3016.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a903268-934e-4f5f-b2a5-afd4a0801f23.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):	5744
Entropy (8bit):	5.189320800545943
Encrypted:	false
SSDEEP:	96:nr96X0X8flwo+AW0cVyZok0JCKL83k41pbOTcfVuwn:nr8fflwo+cc/4KMk4jR
MD5:	AE0AD4D24947B9836656C4BD6925DDC2
SHA1:	213C5F2B6DECB4740D38701AABBD725492B677E9
SHA-256:	EE86C285CB40180C60276337921444FF7037382ECB9E5B5E4E6FCB1DAAEEE1E3
SHA-512:	E855E2ED7D0E1EAB259D8D7BD8868F354A14E4B9C01102BF59C6F8EE3E67670CB3862193E98F3350507D3B198B9F6B33E49E0C90926C1FE4E9E3AAFF0C9F62F 9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263952275977524","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91a2cabf-004c-455c-95e3-9b4b74e5bbc3.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):	5757

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91a2cabf-004c-455c-95e3-9b4b74e5bbc3.tmp	
Entropy (8bit):	5.190337620048109
Encrypted:	false
SSDEEP:	96:nr96X0H8flwo+AW0cVytok0JCKL83k41pbOTcfVuwn:nr8Nflwo+ccj4KMk4jR
MD5:	8D13F9A6CAF3378E89F5F10D61A4DBEF
SHA1:	3E99B2E0497E390C946C41542D16155C3CB2940A
SHA-256:	C7967B9D1821195AFD2151477FC006B4FBAE54BCC0331925274CD40D94046378
SHA-512:	A712FBD503D68947F23A04B67CB8DC644ED4FC62686CD18956A68C3CF8D690990A65F8A0865B7C6CBCD01C16ECF5BFBD9E200719B6D57D28A517FDA2C6E0D A9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263952275977524","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9d5e2239-056d-4c6c-ae34-73af599a2700.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):	5.577408098971342
Encrypted:	false
SSDEEP:	384:5pZt1LlW5X51kXqKf/pUZNCgVLH2HfDNrUbIq8/4U:tLlK51kXqKf/pUZNCgVLH2HfhrUN8/T
MD5:	5B15A9BE6A515D0075D78EAA8E3B3ACE
SHA1:	0FDEF6211390D7E0EF9B11575541D10F3F2CC095
SHA-256:	A9DC2FB94AD8C84887166EACE148AB1EDBC4115432D7AB196E668CF4719CA93C
SHA-512:	C624BF7F69581C470917E4B6BF85B8953C25E32854F7D291422BD9FC2F1173A7019AD87CCC48A48F3E90DA7417BA7B82399926347AAD9FE76214335ACF32EC39
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":"13263952275733776","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.288092919369606
Encrypted:	false
SSDEEP:	6:mR7CN+q2PWXp+N23iKKdK9RXXTZIFUtp07ZdjZZmwP07EnBVkwOWXp+N23iKKdKT:ICIva5Kk7XT2FUtp4/Z/P4EnP5f5Kk73
MD5:	8CBC4B69C3E5E20BB1C225E2AC031539
SHA1:	189EAD9D7F2F09F282E3CABBC9CB2F239FCF96F1
SHA-256:	B63B43C961DDB85D767F9ECD9515869CE4CE6A8FFDBA6F5F36DC793AB58BE31C
SHA-512:	6089A5F7E9F15D4B8A7D023F8D1E6F467EB1A0F6D30BDC8902AA098101D099764FB58C43E5CCDBC3BDC3623D453C31D473C5ABE5702ECC4361B30E0EAAF384 D8
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.545 868 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/26-16:11:27.573 868 Recovering log #3.2021/04/26-16:11:27.574 868 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.249036821062639
Encrypted:	false
SSDEEP:	6:mR7iHN+q2PWXp+N23iKKdKyDZIFUtp07nZmwP07mgd3VkwOWXp+N23iKKdKyJLJ:Iiova5Kk02FUtp4n/P4JdF5f5KkWJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
MD5:	759EE168DC279111CF574BEF7069A312
SHA1:	7303E0F907535C017C1B5E3CABA46CF79DF22719
SHA-256:	0F3E0F23A2F1F96FC16836A6841C4E4F75F1650500EEF2EE47C84DB4836EEDE8
SHA-512:	84552E32AFA784BF5C5DAB215C78FDC9A235923EB29BC4D9C7BBB960171C2E78155216CD37B73913CC0CD665E87BB39AD73612519AF28AC92F9F8E1EA68D65E
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.541 1768 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/26-16:11:27.542 1768 Recovering log #3.2021/04/26-16:11:27.546 1768 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\08a027927af6e12c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1240
Entropy (8bit):	5.500568821797075
Encrypted:	false
SSDEEP:	24:36dk7ja+lKFmKm+LP/8vHorvaVNm7/YMkcxntfdk1:36Im+Oj/8HKvf/ocHfo
MD5:	539D0C842BD4AD9EEC90F9894268E8B3
SHA1:	97D1DB92EFD295F12A6119F492AED9B5DCC604E5
SHA-256:	BBA7A917F91CB3F2928217C1D3C33758BC6A55A9DD7C0D1F3D87E44FEFE2E54A
SHA-512:	4A5C74557F8FD3101B379F23A2F0CEA54AE8EE8F339A8BD16A7F14BBF24B2A680E0AA8D03F532A27DC188AF9A38D3562F6C69BA8325599ED15D4985A6096A1DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...f.5...._keyhttps://laporcovid19.org/_nuxt/02731e2.js .https://laporcovid19.org/R...~./.....7T..J?*@.gW|..h3PJ..]..|,.g....A..Eo.....5.....A..Eo.....R...~./.....'.....O.....m.....8.....(S....`.....L`.....Qcj.....window....Q.P.|....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....0..b.....f...C`....C`....C`....C`.....(S.....Pc.....push.307aF.....Qb.....307.E.@.-....8P.....)...https://laporcovid19.org/_nuxt/02731e2.js...a.....D`....D`....D`.....4...`....&...&..q.&.(S....Pc.....push.382a....$.....Qb.....382.E....d.....@.....&.(S....Pc.....push.383a1.....Qb.....383.E.d.....&.(S.....Pc.....push.452a.....8..I*.....@.....@.....@.....@.....@..... .....Qb.....452.E.d.....@.....D`....DI]d.....q...K`....D.Q.H.....&....&.(.....|.&.-...(...&.z...&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d8bd6ed36d52d11_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28321
Entropy (8bit):	5.593841284668421
Encrypted:	false
SSDEEP:	384:f18w3lVFTb/YCVd/1QUvzUfCZmIz8U0CERiGq079wcqlHmpz:ewp/tVd/KUvrZdoZqgdkmpz
MD5:	33409DEF5B38C453F4230FC8D15CF4D3
SHA1:	413B9F68D1DD5E2C8F689FCF433EE0F8E7E00E51
SHA-256:	024D497C498C70DD6C4A1A9C9944BBCB217A98F9CEDC36EC393F14DB41C86F98
SHA-512:	D434E21D765630E20D103C0C55BC8827FE3726BB1A149B5902EB4760095811939173644D4EEDE4D29F0CA98440E4EA7B90B53B838606B986D1FC7583D56185E3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en.kUju4RKWvZk.O/am=A4O4YYMCNAAIQAAAAAAAAACgESRAIfU6CP8/d=0/ct=zgms/rs=ABkqax2U4h6etIF89B-4_q5CH43h9ykl6A/m=sy2h,i5dxUd,m9oV,RAnnUd,sy2d,sy2e,sy2f,uu7UOe,soHxf .https://accounts.google.com/..J.~./.....N@.o._O.....g...s.Y%ld+H.A..Eo.....w/.s.....A..Eo.....'.'.]....O...`l...R.....\.....(S.P..`Z.....L`.....Qb..'...._G...(S.....`p5.....L`.....E.Rc.....F.....Qb....._.....Qc.....window....Qb.M.....kZa...Qb.....jZa...QbJ.r....mZa...Qb... ....nZa...Qb2"ML....oZa...Qb.....lZa...Qb..?D....qZa...Qb..\...rZa...Qb..E....zQ....Qb.....AQ....Qb.....sZa...Qb.P.....vZa...Qb.=.....BZa...Qb..1.....yZa...Qb.u.....zZa...Qb&\V....xZa...Qb.....AZa...Qbzj.g....DZa...Qb".`.....EZa...QbF.s.....tZa...Qb...n....FZa...Qb.'.....CZa...Qb&%.....uZa...Qb..C.....wZa...Qb.F....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13198f6293cb0d13_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.5830644577610915
Encrypted:	false
SSDEEP:	6:mRXYcr77lrLvrbBlg2lPcwMhmSahythK6t:l/hfbz9cwMlawt7
MD5:	0CF791535938742CF3098BB3494CE8AF
SHA1:	8605FE637E4669133286E36B9F58820D3BF737CD
SHA-256:	ED2783ED9E80B5675378AF7541DD8280C33C4E791E9657E57086F51EFB0F220E
SHA-512:	0A1A687DD78AD9718CD2B56524A1CB730AAF4F512B04610F32BEF4B99F96887E800829ED218662613C406D74E71606577C84EBC99236172F72ED975208E6AA88
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13198f6293cb0d13_0	
Reputation:	low
Preview:	0\r..m.....V.....+$...._keyhttps://laporcovid19.org/cdn-cgi/bm/cv/669835187/api.js .https://laporcovid19.org/H...~./.....Sy..R/.).d..=]..W.a..jx..r...A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2563e2cfdae02f95_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.9421164786614336
Encrypted:	false
SSDEEP:	6:mmkIEYGLUxGBzib0vT2buGguGhrHlgKktKP6REw+0xWDK6tC0RgMoC7Y2uSmjvRX:kSGBibw6buGguG9FqqLl1Y0aMoYYbVjO
MD5:	7AA92D939C2F251374D16E8ED8A56AEF
SHA1:	FA6B1A4D1132B83C068B5482B933CA5893C23338
SHA-256:	95C7CF008C4C6A101D162DBED7F6DF38E0292CF25B643C7E25C53D8358CE562B
SHA-512:	B36E8DDF5F1B5DB31BAE3494F5C9BF9FE4FBB6397C23CB49B4C9B423E7B901E41E56167A824B58FD0C6ACF21C8D102B66F3450A833EDFBFAE6CE6BB987A98B8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...7....._keyhttps://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/remote.js .https://youtube.com/..!.~./.....Q>....0...+ AD.m...B...jR....Y.A..Eo.....A..Eo.....!.~./.hv..E62F691C5B14FE4A5A061BC3D1A3F3085F91676B841F89CC10E134759AD728C4Q>....0...+ AD.m...B...jR....Y.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\335e69ddec2b9ac6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1144
Entropy (8bit):	5.43509781557958
Encrypted:	false
SSDEEP:	24:IQAlOoh7mo1qQA/5ooCQAfOoGCQAEo8CQACoeA:SIW7mGQ/53Y29YEvYCi
MD5:	C38E77C9DC59E97B37B535CDD4189E2C
SHA1:	B37182286F2B897A56D2D624EC183A4BC8D12452
SHA-256:	3C36D7C2742DD3CCCC6B38F9E202385642DEF973EFA02CB2728B6981C0E50A47
SHA-512:	2CCA59D194CC7B8D587CF17AEABDF6CC003960AA4459D8F5AB54A3ACC0171F09999379CBD0E388C066E932EACA84D6C0F32B9591171C9C98718A0D837B7453
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/V.&.~./.....~.....1@dbM..w./.61...wt...R..u.AU...A..Eo....._..+.....A..Eo.....O.).~./.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....hq.....0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/F..~./.....r.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....}.....A..Eo.....0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/m...~./.....P.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....3I.....A..Eo.....0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/....~./.....@.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....(.....A..Eo.....0\r..m.....P...E@S.....keyhttps://www.gstatic.com/cv/js/sender/v1/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\34cadc32b20ec592_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1264
Entropy (8bit):	5.565744620791901
Encrypted:	false
SSDEEP:	24:fneO6cYwhtzKmq3/NXNlRbYOhr/aVNm7/YMqcp5Ge/:z6/wC9NlKOd/f/Ocp5j
MD5:	F1C435ED16BDE4B3002FD1E2C0E4E417
SHA1:	2CC2565FAF5C8E7E21E031270A6BB5D732D2B880
SHA-256:	E4F58D90DC1C1A0CBC35C5B9D973B1C099398F711518DCFE91ED51C0EE5711D3
SHA-512:	64E5EACEDA28D24D2B769CD74764781590CFD09DAD8078AA03024D97956F930F531DECEFDDBB75BFF7787A8C58D5A1B5E87AAD0B685CEF5BE6E9E4717E4E14F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...>....._keyhttps://laporcovid19.org/_nuxt/d2fd471.js .https://laporcovid19.org/,...~./.....=.....*...b...t..A..l..N..d.=...A..Eo.....A..Eo.....~./.....'.....O.....JN.....X.....(S...`.....,L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...l....push.....`.....L`.....`.....Ma.....`.....0..b.....B...C`....C`....C`h...C`.....(S.....Pc.....push.289aF.....Qb.....289.E.@.-....8P.....)...https://laporcovid19.org/_nuxt/d2fd471.js...a.....D`....D`....D`.....@...`....&...&..q.&.(S.....Pc.....push.346a....$.....Qbh.....346.E....d.....@.....&.(S.....Pc.....push.347a1.....Qbl.....347.E.d.....&.(S.....Pc.....push.436a'.....L..q?.....@.....@.....@.....@.....@.....@.....@.!."..@.... ....Qb.....436.E.d.....@.....D`....DI]d.....1.....K`....D.Q.H.....&....&.(....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3628128b7cb7b3ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	30192
Entropy (8bit):	5.536017712024051
Encrypted:	false
SSDEEP:	384:cUMPuAxMSZfqMtmbp6pzJBkHnf0R90fzqh3/JJRkPsWN3+0kd3Kd9oQ9ZicMcjd8:7gdMSZSR15F3dZp2mYtKBdbgAUrB
MD5:	98DD076A13DB59AEB4690647CEE5194D
SHA1:	83E09213541EE3387C36FFF6266BC33829D44B46
SHA-256:	B89179FA6F13850648EDDAC7B96E05C898FB1B099B86662401BD9F2AC1B7AA53
SHA-512:	A831C036DE412DE52AD3E443B6DCD9FF1A95D5216A168A3FC9438F4E9D446D1816565BC75C256E7B2963DAD3DCD25B1DCB385FDCDC11CA135530BFED14A8FFB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://laporcovid19.org/_nuxt/14b25ad.js .https://laporcovid19.org/....~./.....*.....\....5.8..@$...4..p...Y.\\...A..Eo.....G.H.....A..Eo.....'..0....O....`t..[7.....D.....H.....(S.i...`.....9.L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....`.....L`....Eu.....Ek.....E}.....Eb.....E|.....Ec.....E.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\39986ccdf0da7184_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96016
Entropy (8bit):	5.687144208055971
Encrypted:	false
SSDEEP:	1536:29Sv0IeGI9VvKqqvK8idykLSxwNjrAOnUhUuy96o43mFxYmkq9yOKe8M:Y/5bqv+0kL4wxrv2UF9R4ukq9yON8M
MD5:	F2F3CC11F9D56F2187408327954C6CDB
SHA1:	6270B415A903AD705593F02514A3FC8F012188B1
SHA-256:	B448034514721B27A5B348831249682B4508CB64387E14EA8623CF6F46A5FA3D
SHA-512:	43A42E91795FE293F6AE0193BA9C1499453A02FC8F5F36E05ECB1FACADF09B220D30F4AB19594D05AB51857FDD7FAC7D2486D0630B5F4202D37234869EDFAAEB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....E62F691C5B14FE4A5A061BC3D1A3F3085F91676B841F89CC10E134759AD728C4.....'.....O ....u....U.....;.....`.....0.....(S.4..`$....L`.....(S....;.`.u.....L`.....m.Rc2.....Qc..h.....window....Qb.....aKa...Qb.[.W....D4....Qb.....E4..Qb.^.]....F4....Qb.g.....bKa...Qb...m....cKa...Qb.....dKa...Qb.....eKa...Qb.V.....G4....QbJ.....fKa...QbJnc.....gKa...QbF.:.....hKa...Qbf.|.....iKa...Qbb.E.....jKa...Qb~.....H4..Qb.....I4....Qb.2.-....J4....QbJ.U.....kKa...Qb...O....lKa...Qb..Fz....K4....Qb..p.....L4....Qb._.....nKa...Qb.....oKa...QbJ.N.....pKa...QbB..h....M4....Qb.0.....N4....Qb^ \<....O4..Qb..o.....qKa...Qbn.....P4....Qb.1.7....Q4....Qb.....rKa...Qb..J.....R4....Qb.....sKa...Qb.).....tKa...QbRO.....T4....Qb.....U4....Qb.....uKa...Qb.....vKa...Qb.....wKa..QbF;.....xKa...Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ae0c9815dce8653_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.591004607727542
Encrypted:	false
SSDEEP:	6:mB/lXYGL+MIwJJer1pealgo2hdLmmK4KDK6tWB/lXYGL+MIwJJer1BlgK4hdLmm7:Slwve5NihdPG1ElwveRTuhdPR
MD5:	42602404F0B9F06BDE6BFF897FB45B48
SHA1:	D11F6F3B38CB449B06609C7F01BAE0942BC397B5
SHA-256:	74B85DE17CE8F35CD968BCD10C04BFB506146C8861196DB0A0171EB6B182B747
SHA-512:	20204138F5F6BAB8D8945D483353AD02ABB4F099CDC7B316332FA8440C87120546332920DF1DB9D02EEF1A4E8E1CAE674DF21F9041818FFF694FD0E416135E47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...6\+....._keyhttps://www.google-analytics.com/analytics.js .https://laporcovid19.org/.[..~./.....x..?.....u.(A4....:....A..Eo.....A..Eo.....0\r..m.....L...6\+....._keyhttps://www.google-analytics.com/analytics.js .https://laporcovid19.org/...~./.....%.....x..?.....u.(A4....:....A..Eo.....J.!&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3edafc1cfda525f9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	137424
Entropy (8bit):	5.909814387544524

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3edafc1cfda525f9_0	
Encrypted:	false
SSDEEP:	3072:P8ujC831LE3Z4uJ5b1qv2ZENZS1zzAauSG:UuJE3uuD1qv2Zwauh
MD5:	C22AE8546864F054C3FD48168016E2D2
SHA1:	812E4EE442E6392EDF22A719A4723B7BF4B1FBD0
SHA-256:	3B304537BC9383E27BAFF37C6839A34AF5AD507C25D28FE5E7F32C383455FBC2
SHA-512:	9DFDE791A558E14524A71CF13C3D32136DB145365E0DCC9E1FBD5F8CFCF6363E7CD1187997B05789C87A139BCE990EE8581273C153A6027A01EF251099D20DF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...t).....82D7D516690FCBDF6A2D0A6BB3430ADBBE92548B646C3538D4F35C809C223979.....'.....O)...X.....Q.....l.....H..... .....(S.<..`2.....L`.....(S....Q.`0.....L`.....m.Rc2.....Qb.x.....aa....Qb...N....ca....Qb.).....ea ....Qb&.....fa....R....Qb^.8.....ha....Qb*-.....ia....Qbn..,....ja....QbB.;.....pa....Qb.....qa....Qb.(]b....ra....Qb.H.....sa....Qb.....w.....Qb.9.....ta....Qb.v.....ua....Qb>..U....va....Q b...W....wa....Qb.(.....xa....Qb./.q....ya....Qb.G.....za....Qb:..%....Aa....Qb.@.....Ba....Qb.,.....x.....Qb.....Ca....Qb...F....Da....Qbf.....Ea....Qb*2.....Fa....QbZ#.F....y.....Qb .....z.....Qb...7....A.....Qb.M.m....Ga....Qb.....Ia....Qb.....Ja....QbF..,....Ka....QbB.o.....La....Qb.X.O....Ma....Qb.@.....Na....Qb.UH.....Oa....Qb..Dc....Pa....Qbb.....B.....Qb&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\55474a2cdb068b88_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10120
Entropy (8bit):	5.57978223435895
Encrypted:	false
SSDEEP:	192:yNDYwRloZ4e5DmPeSCTjhkzcOp0IS9WXBJ0pCH0z29G2ZLWagl6:yGwRaZ4eyPeSPzPp0IlXAa06g2ZUl6
MD5:	2C986EE2A8CF3B34B0731D9E16DF0916
SHA1:	74D38263283BFCA41E4CF0C68A446E85972D4422
SHA-256:	F1FF697BBC8584F0FC5FAB36E7C0EE53A49F761503A208EB783339D057B6372C
SHA-512:	8B2D5B185A574DA1AA26CA1C66275A36786C57B61E3B2F19CB2FC7DC738192BB47D81633934EDC4D54978A9E9DDC4F8F7CFD635A52578CF0931DE0B4728725 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...Ti....._keyhttps://laporcovid19.org/_nuxt/e89325f.js .https://laporcovid19.org/...~./.....-.....?eBzx..W...{.].l`6T.....A..Eo.....B'.....A..Eo..... .....'..|....O.....&..T.. .....d.....(S.i...`.....\L`*.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma....L....`.....bD..... .C`....C`....C`F...C`J...C`L...C`N...C`P...C`\...C`....C`....C`0...C`....C`....C`2...C`N...C`.....(S.....Pc.....push.109ay...j.....d.....@.....Qb.....109.E.@.-....8P.....)...http s://laporcovid19.org/_nuxt/e89325f.js...a.....D`....D`....D`....9...`....&...&.....D&.(S.....Pc.....push.110aw.....q.....3...L..... ....!.!....!."...."."...."."...."."...".#....#.%....%.%....&.&....&.,.....,@..@.@.A....A.B....B.C....C.D....D.G....G.I....I.L....M

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\586efb0622951409_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2352
Entropy (8bit):	5.515441908680556
Encrypted:	false
SSDEEP:	24:3KVpOgvTFLxZsnlddduIKm8yqvfkapvpWu5AHwlx87+lOQvtToPd4eT6Jky4NDS:aVpOgrpvU0iyyfjtnoM4d4pJQDIVeACK
MD5:	3AE2AE6523382B28C2948945CFE9E130
SHA1:	974FA507CA6F9C9D7EED18AE0D8742B9F04671A7
SHA-256:	B6050A238ED9CD149D869B16E26CA55A94D51022DC88723826819098343BFB69
SHA-512:	8325F24C65EAD7C84C21E7B3696D191A9A8AACC5F541B877C9575BE7154E811BA374C6C8F21CBB398EBA456634DE9A6FB73472CCD62112434CF69C4BF85FB0 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...`<....._keyhttps://laporcovid19.org/_nuxt/113a2f4.js .https://laporcovid19.org/,...~./.....N.....&..T..y..lu...A.s.K.j.../`.k!.A..Eo...../..|.....A..Eo..... ...,...~./. .....'.....O.....8..R.....L.....(S.4..`$....L`....(S.-..`....|L`:....`Rc,.....Qbr.P.....e.....Qb..9....t....Qb..X....n....Qb&{yq....o.....Qb.....c....Q bj}.r....f....Qb.....v...f$.....I`....Da.....(S.....Ia....7.....Qb.....r.....@.-....8P.....)...https://laporcovid19.org/_nuxt/113a2f4.js...a.....D`....D`....D`....T...`&. ..&...&....&..!.&.(S...`,....L`.....M...QcZ..9....splice....Qb^7.O....s.....K`....D...P.....&...&.(...i.....&.%.*..&..&...&.(...i...'%.*..&..&...&.%.*..h..Q...&.%.L.&..+.%..8..&.(...&.%.v.& .M.&...&.Z.....&...&..*..&.-...]...&.%.L.&....%...,Rc.....`....Da..... ..f.....@..".....A.d.....&.(S.....Ia....o.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58e056af14dcaf2e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1090
Entropy (8bit):	6.205956364310571
Encrypted:	false
SSDEEP:	24:tww7tIO+V8N384KumZkC0o+GGz8/At4gWRsi:tN7mOG34XCBpY8oWgti
MD5:	3B154D605400383A60489CCA40646E53
SHA1:	645F5553BAC07450FC40FEA0F087FD3749ACE0C6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58e056af14dcaf2e_0	
SHA-256:	FB20DDF1E1E420CEE96FA9E06009DC7656655AA17CF617F275BC3A2EB4CA0ABB
SHA-512:	879E978EE9DECDD99D92665228AB7771D76E6094EBF8E2C936D89BEE003F9C69AFCB91782582E233C1BF2961497288BBF43FEFCB71B87565FFB486A59E97129
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:...~..-...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en._7XOn5LT8K8.es5.O/ck=boq-identity.ConsentUi.ICiqwhtLDUE.L.B1.O/am=CwAQ/d=1/exm=A7fCU,BVgquf,CBlRxf,COQbmf,EFQ78c,GkRiKb,HDvRde,HLo3Ef,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,MpJwZc,NpD4ec,NwH0H,O1Gjze,O6y8ed,O8k1Cd,OmgaI,PQaYAf,PrPYRd,QIhFr,RMhBfe,SF3gsd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,UgAtXe,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,YLQSd,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,blwjVc,byfTOb,e5qFLc,fKUV3e,fkuQ3,gychg,hc6Ubd,iTsyac,iWP1Yb,lPKSwe,lsjVmc,lwddkf,n73qwf,o02Jie,pB6Zqd,pjICDe,pw70Gc,rE6Mgd,rHjpXd,s39S4,tfTN8c,w9hDv,ws9Tlc,x60fie,xQtZb,xUdipf,xiqEse,yDVVkb,zbML3c/excm=_b,_tp,mainview/ed=1/wt=2/rs=AOaEmlGYzwwl0jD2icWkrkQ2y_vxK_G8ag/m=i5dxUd,m9oV,A4UTCb,RAnnUd,uu7UOe,UMu52b,nKuFpb,soHxf,EGNJFf,iSvg6e,uY3Nvd,hZ9Bt .https://youtube.com/...~./.....0.....2B..g.t.(7...l#...A.SQl..N.P.A..Eo.....W .....A..Eo.....~./..B..B26E78B31044C962DB3C2B4E93BA00

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ae83a951500f4f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4472
Entropy (8bit):	5.33337613942187
Encrypted:	false
SSDEEP:	48:n2gi/Vnjf2NgMCUW39uC1H+FJZFKsPqSETMpBUVTXw/wE+3SlQlt6kl1T:nwfMVW3kC1G3oquQBUC/L+WQH6klh
MD5:	E4B4E99A9463413C0C9AD18AA9C7E0A4
SHA1:	5D5687397A61DF36BC139450943A3CF89231CF83
SHA-256:	75CC7DC0D6BC2884DBBD12005FD3594351888999B995B2287594F1CA7DA8331C
SHA-512:	56689F18B7D3CE45F298F581A58A5BB34E79416DC9BE7E23D8B0F469A374F90E93B66458AD6CF4AE1E824058458004472C4FD97EBD0A3019DD146C0513806669
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....S....._keyhttps://laporcovid19.org/_nuxt/aa5b96e.js .https://laporcovid19.org/l...~./.....22..kCKJ..sXD.0..\..Q..''1.I.....A..Eo.....U8.E.....A..Eo.....'.P.....O.....p.'`.....(S.e...`.....L`F.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma....0...`.....b|.....C`....C`....C`....C`....C`4...C`6...C`8...C`:...C`<...C`>...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`(...C`*...C`,...C`....C`0...C`J...C`....C`.....(S.....Pc.....push.252aF.....Qb.....252.E.@.-....8P.....)...https://laporcovid19.org/_nuxt/aa5b96e.js...a.....D`....D`....D`.....`....&...&..A.D&.(S.....Pc.....push.253a.....Qb.....253.E....d.....@.....D&.(S.....Pc.....push.256a.....Qb.....256.E.d.....@.....D&.(S.....Pc.....push.257a....a.....Qb.....257.E.d.....@.....D&.(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b7afd9443462a0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4700
Entropy (8bit):	5.705238086682577
Encrypted:	false
SSDEEP:	96:dPVo8wgBKG4YzSLVP3kBjkXzI3Fm/hUUhrxpi:dPq8wcOLJ6GI1yBI
MD5:	F7289BB27749E09E0ADBEB704E5A2E10
SHA1:	D623FC5152B4C3F4558965EA7D9ECC348FC45943
SHA-256:	6609FB8C6DB491F237089CC253611C98868F951BC041A8EF9FB202F0155775C4
SHA-512:	D2D1E3A582B8FB8927115A3300ED61E5CCAD74C34764DE7140DC0C2BE521071401B9E64A2727599A00ECD09AB8BB2B3E5B4358E1823BC36E22F553933A66A98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,.J...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en.kUju4RKWvZk.O/am=A4O4YYMCNAAIQAAAAAAAAACgESRAIfU6CP8/d=0/ct=zgms/rs=ABkqax2U4h6etIF89B-4_q5CH43h9ykl6A/m=sy35,sy36,sy37,sy39,sy3a,sy4x,pwd_view .https://accounts.google.com/..L.~./.....H.}.....0[..@(W.....}G....%&...A..Eo.....W.9.....A..Eo.....p;....O....@...3.....0.....(S.P..`Z....L`.....Qb...'...._G...(S.%..`.....1.L`.....DRc.....Qb.....q3a...Qb.....yT..c$.....l`....Da:....v....Qb...0....k.....Qb.l%1....sy35.(S.....Pb....._.pTaQ...l...l..a..@.-.....P.q.....https://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en.kUju4RKWvZk.O/am=A4O4YYMCNAAIQAAAAAAAAACgESRAIfU6CP8/d=0/ct=zgms/rs=ABkqax2U4h6etIF89B-4_q5CH43h9ykl6A/m=sy35,sy36,sy37,sy39,sy3a,sy4x,pwd_view..a.....D`....D` ...D`.....l...`2...&...&..q.&....&.(S.....Pb....._.qTaz.....l....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d55f8929805159e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15415
Entropy (8bit):	6.024029734795529
Encrypted:	false
SSDEEP:	192:jBaJh6Bmu4GqRzOMeHsaT/P+q0mRr52xwLXBpBYPBiOC40IBjYqe3G4gDr7m3fNv:jBaSBOtOMU/2ZmieFpSpdleWHDW3f009
MD5:	0905D862160727BA767C02674F8F13F9
SHA1:	51379644AA807C1057D032A7B848D6CDF4B049DD
SHA-256:	D3F4C92921BAAAF49D6D8673456B3A7065822C8903DAAC2721BAF5769E6CC0B1
SHA-512:	1446A8BD0E19720F5DD28D9A6E48A0247C7C77D39B5309375474BC112D50C30531750C0D592737E4574DB531D2FEBFA8BFCC531A4C472AC5F43E92C779225AD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d55f8929805159e_0	
Reputation:	low
Preview:	0\r..m.....W...B.*}...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en._7XOn5LT8K8.es5.O/ck=boq-identity.ConsentUi.lCiqwhtLDUE.L.B1.O/am=CwAQ/d=1/exm=A4UTCb,A7fCU,BVgquf,CBlRxf,COQbmf,EFQ78c,EGNJFf,GkRiKb,HDvRde,HLo3Ef,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,MpJwZc,NpD4ec,NwH0H,O1Gjze,O6y8ed,O8k1Cd,OmgaI,PQaYAf,PrPYRd,QIhFr,RAnnUd,RMhBfe,SF3gsd,SdcwHb,SpsfSb,U0aPgd,UMu52b,UUJqVe,Uas9Hd,UgAtXe,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,YLQSd,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,blwjVc,byfTOb,e5qFLc,fKUV3e,fkuQ3,gychg,hZ9Bt,hc6Ubd,i5dxUd,iSvg6e,iTsyac,iWP1Yb,lPKSwe,lsjVmc,lwddkf,m9oV,n73qwf,nKuFpb,o02Jie,pB6Zqd,pjICDe,pw70Gc,rE6Mgd,rHjpXd,s39S4,soHxf,tfTN8c,uY3Nvd,uu7UOe,w9hDv,ws9Tlc,x60fie,xQtZb,xUdipf,xiqEse,yDVVkb,zbML3c/excm=_b,_tp,mainview/ed=1/wt=2/rs=AOaEmlGYzwwl0jD2icWkrkQ2y_vxK_G8ag/m=Wt6vjf,_latency,FCpbqb,WhJNk .https://youtube.com/...~./.....4...}.p.^7..)x2.u...."b...A..Eo.....#z.&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6fdde531359d58b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9912
Entropy (8bit):	6.1687857500402705
Encrypted:	false
SSDEEP:	192:PobkiQDmMqhwl6v23SB4QLpm6F3YXDhYV19Gept10wxZHuJvk23rQ3KWKzMtY:wbTihqHvOSnLplpqlYUept10wxZHmcgP
MD5:	6635476AEFB22B8FA505C6D489991EC6
SHA1:	DA37E3F20C250BCB9415CEC4CDFA04C7DCCDCDF5
SHA-256:	25765D4FB70EC597FA9ECFF66C9B16A65E1EA2E68231DDAAC44594F6030815B5
SHA-512:	7AFCF2D435F840BC1D8966E40D451E10293E47923547F6C147A75CB592AD37E84A15B93BB511FB663E9073E888C7426734BC6B57E20EAE67E7E16987F60A69D2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://laporcovid19.org/_nuxt/696116c.js .https://laporcovid19.org/<...~./.....)..AX.RSY8Dm..*q....-.hN?...A..Eo.....m".^.....A..Eo.....'.....O....H%..a.Ne.....(S....`.....,L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....0..b.....`..C`....C`....C`....C`.....(S..`.....(L`.....`.....La.....`.....Lb.....I...S...Qc..=.....locals....Qc...i....exports..a...Qc:>de....728e466a...a.....Qd.u.....sourceMap...H..K`...D.!.0... .....y.&.]...&.s..1z...&..&.z..%&..&.(...1.....&.%.1...%.1...'..%.(.....(...&.-...%...&.]...&.(...&...&..&.}..)&.'..[.....(Rc.....Qb.....304.`.....Pc.....push.304a.....e.....Y..8P...P.....@.-....8P.....)...https://laporcovid19.org/_nuxt/696116c.js...a.....D`....D`&...D`.....0...`....&...&..q.&.(S.0..`....]..K`....Df.... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75802e05d48dc972_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.899097195962414
Encrypted:	false
SSDEEP:	6:mfUXYcrJ3r1nlg9f/J+ZH/hnVhK6t6w0lQRmSwA25jtfh+ZH/hnp:tnd3343QV7Ew0K3lGBY
MD5:	45EFB38FD8E55371F6F86E8FF6B13419
SHA1:	C679277DCFEF907D4C2075B740B5EB2402D45204
SHA-256:	19328B30ED50F740D95433F152F4A7673C93704CAA01003A22A3ED84F9716D19
SHA-512:	9FFD40F98C144B72F67E148D6602F9AA032973D481A45E55CD2D2B80976B57900A91E8E128436AE5E31819DFA60342A35A70CF77E81CDBA1A428DEF0729197BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://laporcovid19.org/_nuxt/6ca9ecf.js .https://laporcovid19.org/....~./.....3.1.-...L/4:.....|n.(!.,..X=..A..Eo.....M.%.....A..Eo.....~./.....54C7FEAD779E671152EDB9AF60425DEAAB5EFDF7C875114E3E81E7187FF9BB32.3.1.-...L/4:.....|n.(!.,..X=..A..Eo.....<Xt.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\777a12b5f6b0e6a5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1004
Entropy (8bit):	6.270627164445414
Encrypted:	false
SSDEEP:	24:Aww7tIO+kzBw1pJJkpbQ8ugTbZAmLAB4bd78Z8el:AN7mOlByvJd8ugVAvB4bd78Zj
MD5:	FE6FA6679158F1CCBB9BAFA3FB96A426
SHA1:	172DAC6FA32ECB08FEC09D9C98D27A572F270E91
SHA-256:	01425FC5D49D7DEFBA034F538716229336B7A6DEFA0220AB4B16E3160DED656F
SHA-512:	65FF5448B8ECDF9A3D6F774477AFEC4222AA63630158F0ADE69E9269FA42B7D44791D297916B20F7666161B4CE745B1129CB1757D4FC4D7A4B03A999639D2305
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\777a12b5f6b0e6a5_0	
Preview:	0\r..m.....G....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en._7XOn5LT8K8.es5.O/ck=boq-identity.ConsentUi.lCiqwhtLDUE.L.B1.O/am=CwAQ/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,mainview/ed=1/wt=2/rs=AOaEmlGYzwwl0jD2icWkrkQ2y_vxK_G8ag/m=n73qwf,ws9Tlc,lZT63,e5qFLc,GkRiKb,UUJqVe,O1Gjze,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,WO9ee,O6y8ed,NpD4ec,PrPYRd,iWP1Yb,MpJwZc,O8k1Cd,NwH0H,OmgaI,HLo3Ef,x60fie,xiqEse,XVMNvd,L1AAkb,KUM7Z,rE6Mgd,s39S4,lwddkf,gychg,w9hDv,RMhBfe,SdcwHb,aW3pY,YLQSd,PQaYAf,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,CBlRxf,MdUzUe,xQtZb,lPKSwe,QIhFr,JNoxi,pB6Zqd,rHjpXd,yDVVkb,SF3gsd,iTsyac,hc6Ubd,KG2eXe,SpsfSb,tfTN8c,o02Jie,VwDzFe,zbML3c,HDvRde,Uas9Hd,BVgquf,A7fCU,UgAtXe,pjICDe .https://youtube.com/..}.~./.....!.mr..w.&8.Y.K...!....(5.../.A..Eo.....p.....A..Eo.....}.~./. ..12A058AFF5FC490823B1D68425BE1BEEF57B0082E71C3ED078A0B01112D84C0F.!.mr..w.&8.Y.K...!....(5.../.A..Eo.....'L...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\783a744b2b46364f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	324296
Entropy (8bit):	5.858619097301141
Encrypted:	false
SSDEEP:	3072:dRkepZTiz/gjUeVyJL9X4VnlNPg5SM0pD39e8R43lXxlJunT4GE/Mi:U+VuclN3be8e/unTFi
MD5:	EED6747A0CF8D3AB4F30292DC73F2267
SHA1:	4642E3BCEE544FEF8B5EEAA8208A8A866EFA34C8
SHA-256:	E095B4122C479D8A39F5F1319FF91100634FD0D9B52E6D98F6A152346336DCCF
SHA-512:	8167C932773870A61B9DA73D2D60BA0776AC1DF285899FF583905822FE1BAE7AE34EAFFE6244277038AAF7CA16762103375881AC366D8FAB3E2D318C91C45117
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....gP....12A058AFF5FC490823B1D68425BE1BEEF57B0082E71C3ED078A0B01112D84C0F.....'..[....OS.....j..a.....(...t(.....0...`.....l.....p.....(S.l..`..... L`.....Q.`.[.l...._F_installCss.....Q.....tr....KL4X6e{background:#eeeeee;bottom:0;left:0;opacity:0;position:absolute;right:0;top:0}.TuA45b{opacity:.8}sentinel{}..... Q.p.k.....default_ConsentUi....(S...).`.....u(L`6.....Rc.....X.....Qb..v...._.....Qc:.?7....window....QbV.s.....CC....Qb^.....IC....Qb.\ky....gx....Qb.....lx....Qbj.....TE....Qb.U.....UE....Qb.....Eu....Qb...[....ZB....Qb.....$B....QbB.....aC....Qb..).....Vu....QbRw(8....Yu....Qb.....Zu....Qb^..K....bv....Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85cda9ce55047d7d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	82608
Entropy (8bit):	5.7097809247126365
Encrypted:	false
SSDEEP:	1536:3ZqtgwRZmFrFHDGf+c5vL21NqRNUxc4lqW43i/:pjwqFtDG3561NqHGci1X
MD5:	A236A2BEAB224D8DF2D10BF745980515
SHA1:	9787214527E331C7B5D4A1C9694CEC203EC98073
SHA-256:	0091B7CB891BECD57F49679FF19394191CE9DB0461D47C2CFC735EA8938A49C2
SHA-512:	321F751888C317683F54DBA389ADFBE5F773DB593ADD8A9F8A8307A2C8418743AF581DBC529443A6F6A6E54D4A056614E12298F13EBC3FEFB676A2F7D33CA38
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...&.4M....B26E78B31044C962DB3C2B4E93BA00EF32DD953D141309178552775A274A16A9.....'..3....O....xA..3.z.....H...h[.....T.....(S.l..`..... L`.....Q.`.[.l...._F_installCss....0Q.....#....fb0g6{position:relative}sentinel{}..... Q.p.k.....default_ConsentUi....(S...i[.`.....L`.....Rc.....Qb..v...._.....Qc:.?7....window....Qb...T....OM....QbJ.....NM....Qb:.....QM....Qb6.d.....RM....Qb...:....SM....Qb.,=.....PM....Qb.....UM....Qb*..|....VM....Qb...5....WM....Qbj./.....XM....Qb.....YM....Qb...1....aN....Qb.o.....gN....Qb.!N.....dN....Qb...>....eN....Qb".....cN....Qb..+`....fN....Qb&.....iN....Qb..E]....jN....Qbz.....ZM....Qb.jy.....kN....Qb.....hN....Qb..b....$M....Qb...+....bN....QbZHcz....lN....QbR.&q....mN....Qbj.e.....qN....Qb.....uT....Qbv .>....vT....Qb*-.=....wT....Qbj.%t....xT....Qb6|.|....DT....Qb&..4....FT....QbvU.....CT....Qb"`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99746ad493b8171a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7312
Entropy (8bit):	6.16820905797584
Encrypted:	false
SSDEEP:	96:HZYKHvIwRw11xrJRUXvGeic2qRN92qRBZkkGrlejaOhVbOhhLuuuhfVR7flOibn9:WKPi1xrJiXvpi0xZrGRe4YPR7fJt3kG
MD5:	22CC03EBB12E54D9718893BC913C6C95
SHA1:	D0C4FC9F4E4FFCFACCBD01E5BF3B5E16982BABAE
SHA-256:	2E719CEA610316AD17710F28164DB66BFB23072A50C3138C7905515E0E399308
SHA-512:	B53B196C8C466E136B4A06E06AD3F5FFB6F1EE945731A5A6E00C0253170CAB3D3EBA9F26924E96E99FC4918CA4FA4E303890A69A272B9155D5738B3891BC894A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99746ad493b8171a_0	
Preview:	0\r..m.....H...G..M...._keyhttps://laporcovid19.org/_nuxt/1725d6d.js .https://laporcovid19.org/....~./..... .....N@E..6|!0.m.9.9./.....g.....A..Eo.....3K.$.....A..Eo..... .....'.....O.... ...8M.Z.....d.....(S....`.....L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....0..b.....^. ..C`....C`....C`~...C`.....(S...`.....(L`.....`.....La.....`.....Lb.....I...S...Qc..=.....locals....Qc...i....exports..a...Qc.b/c....2afd8572...a.....Qd.u.....sourceMap...H..K`. ...D.!.0... .....w.&.]...&.s..1z...&..&.z..%&..&.(...1.....&.%.1...%.1...'..%.(.....(...&.-...%...&.]...&.(...&...&..&.}..)&.'..[.....(Rc.....Qb.....303.`.....Pc.....push.303a..... .....e.....Y..8P...P.....@.-....8P.....)...https://laporcovid19.org/_nuxt/1725d6d.js...a.....D`....D`$...D`.....(...`....&...&..q.&.(S.0..`....]..K`....Df.... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9d6d19f482de5a7d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6080
Entropy (8bit):	6.06336924751808
Encrypted:	false
SSDEEP:	96:G9xDvXh6XK0vGxu2qXdNalS6O7dMFUONWI0OTLOkEjde399pg/Vx:G9xbx6a0vkibGodqzWJEzEjde37pgr
MD5:	844BACF7A61CFE4C2077E0C9FD4A5BF1
SHA1:	C8C62231CEB02FA3CEA4F3A7CDC3CF9B239FECC3
SHA-256:	22F7E3092794951BB6A8E87B4023D5B4C64A50127DBEF0BE468E9F9E5D7F9E94
SHA-512:	01C0289F72B53F21B719B71F8B27A2EC890340DAC90D08DDA6BDC82E7E87704C34D60D3C509A790B8F31F6D0DBB25518F7C24DCC544A246AC1E69A9A1B0B51 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....(.Y...._keyhttps://laporcovid19.org/_nuxt/71744e7.js .https://laporcovid19.org/....~./.....O..C....9....d.C."..cp.}3..A..Eo.....Z.....A..Eo..... .....'.....O....P...]..... .....(S....`.....,L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....0..b.....b...C`....C`. ...C`....C`.....(S...`.....(L`.....`.....La.....`.....Lb.....I...S...Qc..=.....locals....Qc...i....exports..a...Qc..W.....f9004148...a.....Qd.u.....sourceMap...H..K`....D.!.0... ..... {.&.]...&.s..1z...&..&.z..%&..&.(...1.....&.%.1...%.1...'..%.(.....(...&.-...%...&.]...&.(...&...&..&.}..)&.'..[.....(Rc.....Qb.....305.`.....Pc.....push.305a.....e.....Y.. 8P...P.....@.-....8P.....)...https://laporcovid19.org/_nuxt/71744e7.js...a.....D`....D`(...D`.....$...`....&...&..q.&.(S.0..`....]..K`....Df.... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7a0299e641655a5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3024
Entropy (8bit):	5.229580175214515
Encrypted:	false
SSDEEP:	48:hYiiyXA7E/HdYnkJTPiJGFBZoj86lOgnb/sOX9PnYECKKsmQdm/kgI1xCW2:2/GHdYwT0kAYGpWDxym/rI1cX
MD5:	0DCF19876846831A7E4F3B17C5DA74DC
SHA1:	2204B39932D830049FC3409E4DE6F6B2913596EF
SHA-256:	D624B23030DD585D09A85B6D8314D18C4114BD14796874107CE4713910E57C3D
SHA-512:	A57F83CB4A77A9EAB31D4C424BD74AA3E832EAB0E94072D66D9C9DE38F8C45A87BFB9EBEC1B84DC671409DC0FEA5B9D83862580E0E3A6856A5B9CCCEC6CA BC84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...g=1...._keyhttps://laporcovid19.org/_nuxt/7cd4187.js .https://laporcovid19.org/.;..~./.....j....3Q...s.?K{.k..V..-.....0.A..Eo.....>7.*.....A..Eo..... ....;..~./.....'..%....O..... t.....(S.....`N....pL`4.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....bX.....C `....C` ...C`&...C`t...C`~...C`....C`....C`2...C`4...C`6...C`8...C`:...C`<...C`>...C`@...C`B...C`D...C`F...C`H...C`V...C`.....(S.....Pc.....push.263aE.....d.....@.....Q b.....263.E.@.-....8P.....)...https://laporcovid19.org/_nuxt/7cd4187.js...a.....D`....D`....D`.....`V...&...&..1..D&.(S.....Pc.....push.264a.....Qb .....264.E....d..... .....&.(S.....Pc.....push.272a.....J....Qb@.....272.E.d.....@.....D&.(S.....Pc.....push.275a.J..lK....QbL.....275.E.d.....&.(S.....Pc.....push.314ayK

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad16b5408654ed52_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9072
Entropy (8bit):	6.211431475499401
Encrypted:	false
SSDEEP:	192:WaP4/PB6V8/McYAyGnDZo4H+k+l0Hq5HLPImVR/Ba5s:WZpKFynmX0HA1Bms
MD5:	679801C688CD1A249EED0D5E9346A062
SHA1:	9C51311E3AB2E4A5AA9FCD0830D0EE9433DEF41F
SHA-256:	E20CE9A11D7AF895A4F9CD8B37C8DAA5E4071B8266759CA9702AE5F7F911A9D7
SHA-512:	E678318D0974FE4E2E92D848E319C2248D5891428C522DEF43F202165838414C04E43BFA9F2C06BAFFF6E59D2F316F84A1EBCE6185D862964E543AE555A85DB8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...h..^...._keyhttps://laporcovid19.org/_nuxt/3023af3.js .https://laporcovid19.org/jk..~./.....Aa...@.QD.....}.../.....N...A..Eo.....u.....A..Eo..... .....'.9.....O....''...T.M.....(S....`.....,L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....0..b.....\...C`....C`... .C`|...C`.....(S...`.....(L`.....`.....La.....`.....Lb.....I...S...Qc..=.....locals....Qc...i....exports..a...Qc>O.}....6158975e...a.....Qd.u.....sourceMap...H..K`....D.!.0... ..... u.&.]...&.s..1z...&..&.z..%&..&.(...1.....&.%.1...%.1...'..%.(.....(...&.-...%...&.]...&.(...&...&..&.}..)&.'..[.....(Rc.....Qb.....302.`.....Pc.....push.302a.....e.....Y..8P ...P.....@.-....8P.....)...https://laporcovid19.org/_nuxt/3023af3.js...a.....D`....D`'"...D`.....,...`....&...&..q.&.(S.0..`....]..K`....Df.... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b06ea7729b30c0bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	447
Entropy (8bit):	5.914878755270058
Encrypted:	false
SSDEEP:	12:3GBibw6IguGgtTQbhLZt0nMRpEMjVn6qM/8L:2AIAYUhLyMRSMpTZL
MD5:	A44FEAD4857CF0DBD6FF3A8196A1F0ED
SHA1:	8A1A33EF91D4BEBE57AD9DE4D71FD66F6139BCED
SHA-256:	85B4F75BD29539B4B3FC6835239B1E80431596C31F3F1B7E529F0F17FDCF2941
SHA-512:	18625F8FA33E96D4EE458780992B3D7BDA0F04C9885BF8A6E783E69E4A2D170E4DA4D8E1CEB1703F641C2AC5669529042952AE6EA7F0F343CC462EAD0B49A2AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....._keyhttps://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/base.js .https://youtube.com/....~./.....KG.....J.&.....%.=10.N.....A..Eo.....;.....A..Eo.....~./.....KG.....J.&.....%.=10.N.....A..Eo.....i.....~./.`s..91ACA30B3303BEB921AC6960851E60E0433AC21DA220D93F37C3A81E5EEE7569KG.....J.&.....%.=10.N.....A..Eo.....p.[*L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b0a360ceeb8dc1d8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23708
Entropy (8bit):	6.161519177683994
Encrypted:	false
SSDEEP:	384:9l+YRgyq+e8jtYWbF3nq6qQjbnjcQFPfdZ1U9MhzZEbwDfD2M:bG+1jtfJnqxUvtdZ1jzCg
MD5:	A105F2271458DEA0ADF4D8FC6470C13A
SHA1:	9A45FC0B8E60D523428121D1243548C2B4126FB1
SHA-256:	3758CCE0877FE2F99DBB8EAC71C495A5FB6742ED2DD3A794F85EE18E652C5DE5
SHA-512:	4CB7A66B4D341A394DB7B691E8FAF23F8499CF7AAB9AD278CD05C8FD321F2EB35C5D26BA0FC13F3A1046912334BDB10E19794CA2DA7FACE77EB64DB9FFC4A294
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....C....._keyhttps://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/embed.js .https://youtube.com/Q$#.~./.....^...`.A.....=...u.. ..+.A..Eo.....E.i.....A..Eo.....'.ha....O.....[.....(S.4..`$.....L`.....(S.=..`2.....L`.....Rcf.....*.....Qc..h.....window....Qbv.&%....aJa...QbR.D.....m3....Qb..*.....n3....Qb.4J.....o3....Qb.e.....p3....QbBM.....cJa...Qb*..k....q3....Qb.....dJa...QbV_.q....eJa...Qbv5.v....r3....Qbf.=.....s3....Qb..<... .t3....Qb.5.....u3....Qb.....v3....Qb..13....w3....Qb.{.....gJa...QbFs.....x3....Qb.....fJa...Qb.....bJa.u$.....I`....Da.....(S.....!a:...w.....@.-....XP.Q.....J...https://www.youtube.com/s/player/fa244a41/player_ias.vflset/en_US/embed.js..a.....D`....D`0...D`.....-....`....&...&....&..a&&.(S.(..`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b7791abd66804a67_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3320
Entropy (8bit):	5.170001927157235
Encrypted:	false
SSDEEP:	48:CIIoM0y72sN9tSGF9muMMDkeLSqhc/AWcQq0TKj:ZIm87oGF9HRv2q6/xaTj
MD5:	C5F7CE05A169583177673C91D12E6370
SHA1:	9427887EDD122D84C94E172B9670A06EB19D47DC
SHA-256:	B042C297CD91AC79F2FC6D2CEDFE79239D7DB7ACA275240C6F28F1CBDCC1F15D
SHA-512:	FA92908904188C637FAE94BDE9FA9ACCADD74003FA1466F87750142E7705C21FF58B17C36B855320557AB68EEA57425197916BDDC5835241B06B0BEACF622F4E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....5s....._keyhttps://laporcovid19.org/_nuxt/7f26880.js .https://laporcovid19.org/....~./.....i|I.....kPK.!.=..2.g...^+Lb....A..Eo.....Ek.....A..Eo.....~./.....'..3....O.....8.....<.....(S....`.....xL`8.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...I....push.....`.....L`.....`.....Ma.....`.....b`.....h...C`j...C`l...C`n...C`p...C`r...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`L....C`N...C`P...C`R...C`....C`.....(S.....Pc.....push.308aE.....Qb.....308.E.@.-....8P.....)...https://laporcovid19.org/_nuxt/7f26880.js...a.....D`....D`....D`.....`T...&...&....&.(S.....Pc.....push.309a.....Qb.....309.E....d.....&.(S.....Pc.....push.310a....~.....Qb.....310.E.d.....&.(S.....Pc.....push.311a....@.....Qb.....311.E.d.....&.(S.....Pc.....push.312aM.....Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\baf039634a1a22d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4303
Entropy (8bit):	5.598609732288287
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\baf039634a1a22d3_0	
SSDEEP:	48:mJZzgShY1NvBj1voQlW194PCQxd6s4pN8WilHTTJXNXP41ibl8d3UMOxsnGU9Ap7:mJZ7Y/ZpBcwCQd61NJzHXgrd3nOx3RSc
MD5:	5861D98F52D86D4B59B44FE2A33E9838
SHA1:	659267903562DB94D525F4A4C47D9C0DA2A635A0
SHA-256:	13A02AAF17C8A76EA47AA41021EF570EDF787C266D5FBDAFF7E23CA97B6BEA42
SHA-512:	4067A0D8EB9C6D3F0931C33E2CC5F989BF1F37049FF4818F00EF66E70ABA015C3AFECEE998BCFB7C07321746155A365EFF6C73E8437F46D348752C8202D8A7B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...NFh....._keyhttps://www.youtube.com/s/player/fa244a41/fetch-polyfill.vflset/fetch-polyfill.js .https://youtube.com/.[..~./.....5...T{!..X4.spl.;z..%.....A..Eo.....N.....A..Eo.....[..~./.....5...T{!..X4.spl.;z..%.....A..Eo.....[..~./.H.....'._!....O.....H.....(S.@..`<.....L`.....(S....`r.....L`l.....RcL.....Qe..O.....normalizeName.....Qe.....normalizeValue....Qc.6.....Headers...Qc..,....consumed..Qef.....fileReaderReady..QgbgA....read BlobAsArrayBuffer.....Qe.U.>....readBlobAsText....Qc.....support...Qc..Z....methods...Qe..1....normalizeMethod...Qc.K.....Request...Qc.....decode....Qc..\G....heade rs...Qc>.\.....Response..Qeb?.Q....redirectStatusesn.....I`....Da....nB...(S.....Iax.....@.-....`P.q.....Q...https://www.youtube.com/s /player/fa244a41/fet

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bcb193756032fcc9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	44775
Entropy (8bit):	5.712654970711178
Encrypted:	false
SSDEEP:	768:/iQsWjdpgU9rH3V1ypooWcBipKos+COhlRip4ZljE2aWqAKXf:/jftPMTIpXs+bnZVL
MD5:	FD9E890A46B48D822C523DE9BAA41252
SHA1:	23F88A69E9710EACFAA4F165F321695D336364C9
SHA-256:	7C11D9F712960C65A59B2859C34EB31C3371FCDDC28E5C5AF0731BE076BEE98C
SHA-512:	1896EA2F55FC7BE5273DCF17224D93E9B52CFC8F3B2D110ED5FE1B068BB04CD247810BD4D324323250D46E33712EBA12B8E20A87DD00CCA73ADB4C482C0307 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.E....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en._7XOn5LT8K8.es5.O/ck=boq-identity.ConsentUi.lCiqwhtLDUE. L.B1.O/am=CwAQ/d=1/exm=_b,_tp/excm=_b,_tp,mainview/ed=1/wt=2/rs=AOaEmlGYzwwl0jD2icWkrkQ2y_vxK_G8ag/m=byfTOb,lsjVmc,LEikZe .https://youtube.c om/..}.~./..... ...;....Q4y.MY..r1....DO`.>l....A..Eo.....D.....A..Eo.....'.l.....O.....).....`!.....$.....(S.\..`t.....L`..... Q.p.k.....default_ConsentUi....(S...a!.`xB.....Y.L`.....].Rc.....Qb..v...._.....Qc:.?7....window....Qb.c}....zv....Qbz~.y....Bv....Qbj1.....Iv....Qbj.....Cv....Qb.....Ev....Qb .Y.....Dv....Qb.....Hv....Qb.....Fv....Qb.kv]....Jv....Qb6O.S....Lv....Qb>.....yv....Qb.....Kv....Qb.....Gv....QbB..e....Wy....Qb.SD&....Yy....Qb.'J.....Zy....Qb.....Vy.... Qb.M.o....bz....Qb:Dk.....Zx....Qb..D.....iz....Qb:.."....jz....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4e0918b4735a4bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6184
Entropy (8bit):	6.092902477593095
Encrypted:	false
SSDEEP:	96:haGhdYnCXKCvGsd2qRP2qRLvsyMlXO78nLgweOCTZQarDxvuhSyRc1pg/raaGl:AGhdqCaCvFpszvLr0Fxvuxopg2l
MD5:	389701249626B5DC7A17769BAD10B345
SHA1:	11ABEFC1D6DA19E470412B60B2BF7DC79CBA22EE
SHA-256:	372F27A7A8AB08C95757B74EB80284CF5C88C9130D7395CBC867354AB0E44775
SHA-512:	6CA6434CBF64032D2606E1352FA6760BEB86E0A0E912AFA5E9E5A8FD6BC7D81D941C1D72E8FEE1B3CE70D1EEA4E1E046E72A2DC507D2E7DA9F111D02DC1BE 081
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H.....)._keyhttps://laporcovid19.org/_nuxt/758f5b5.js .https://laporcovid19.org/....~./.....0.....".IJJ.]&..9....8.S....t.!Dj..A..Eo.....Y.....A..Eo..... .....'."....O.....(S...`.....,L`.....Qcj.....window....Q.P.|.....webpackJsonp..Qb...l....push.....`.....L`.....`.....Ma.....`.....0..b.....d...C`....C`. ...C`....C`.....(S...`.....(L`.....`.....La.....`.....Lb.....I...S...Qc..=.....locals....Qc...i....exports..a...Qc..ch....7000707c...a.....Qd.u.....sourceMap...H..K`....D.!.0... ..... ..}.&.]...&.s..1z...&..&.z..%&..&.(...1.....&.%.1...%.1...'..%.(.....(...&.-...%...&.]...&.(...&...&..&.}..)&.'..[.....(Rc.....Qb.....306.`.....Pc.....push.306a.....e.....Y.. 8P...P.....@.-....8P.....)...https://laporcovid19.org/_nuxt/758f5b5.js...a.....D`....D`*...D`.....$...`....&...&..q.&.(S.0..`....]..K`....Df.... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d7301d588c29468b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195912
Entropy (8bit):	6.350495458551198
Encrypted:	false
SSDEEP:	1536:KqUwGXmBjaNVLo9xOv2n/WVyY0vVFLqwUeNw9Bes0VEL46XHk/Wtz8GAfo7ev0BV:hfjTkSesV29Bes0Cpwmz8GesBV
MD5:	418A3B6502B2576A15B850A76895C9BC
SHA1:	10FF42C2D4A3E76B727F82070C0E3703966AFAF8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d7301d588c29468b_0	
SHA-256:	EBCE6CFE4DD3388E7C79FF016FF7E818981103290C333A20D7D7662BD87064F3
SHA-512:	CB250A78F99D70770E1A53929BD45203A92BFDD013D4DEA110842C53546D1FDB2901DA7570C31736C0005194A0CE78BCFA027576A40F63BAC322C2041992CDE
Malicious:	false
Reputation:	low
Preview:	0\r..m......@.....f.....54C7FEAD779E671152EDB9AF60425DEAAB5EFDF7C875114E3E81E7187FF9BB32.............'.C@....O2...L.................T..................4..<........................(S.....`@.....L`T.....Qcj.......window....Q.P.|.....webpackJsonp..Qb...I....push.....`......L`.......`......Ma........`.......`......L`.......`......Md....Z...J.......L....9...b............C`....C`....C`*...C`,...C`....C`0...C`2...C`4...C`R...C`Z...C`^...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`L...C`....C`....C`....C`....C`....C`....C`.....(S.q..`.....Y.L`.....i.Rc............P.....Qb..X.....n.....Qb&{yq....o.....Qb.(J.....l.....Qb^.F.....d.....Qb.......c.....Qb.V.....m.....Qb.Q......h.....Qbj}.r....f.....Qb.r9m....x.....Qbj.......w.....Qb.......v.....Qb.._.....y.....Qb........C.....Qbn....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d894af6cc49377fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37593
Entropy (8bit):	5.884675430635726
Encrypted:	false
SSDEEP:	768:Zpt309Zxu4oj5fBnZXBo7gIMRYN7ATfBOSgvwRM4K8U:zW4ZXBKglYN0TJgvwC9
MD5:	BA068B56DC579A38F740280B4FCFDFDE
SHA1:	C7B31280AF237F5F7B87F0443CF3CCB768DF3E14
SHA-256:	D9D2289538C2FCD1C88AE108B4F2AD43842B617BD3A845CF3F661F240337E71E
SHA-512:	1829C34BD567FCF98081F3F7888F7240B089BF91016F5A711C5691E0C292468473F81664199E90D38899D1ACC191B222290D57A480F8DCA695C41601F3DBBA11
Malicious:	false
Reputation:	low
Preview:	0\r..m......e....@....._keyhttps://www.google.com/js/th/hlLHYuMj9gNC5zTdq--KBNr5YWNPOXBLIpYMmShXYzs.js .https://youtube.com/+z$.~./....................>...w....D.I........M+..:.b....A..Eo......j4BN.........A..Eo.................+z$.~./.....................>...w....D.I........M+..:.b....A..Eo......<..p.....................'.......O.........G#.....................d................(S.<..`2.....L`.....(S...`.....<L`.....LRc"................QbNN.\....N.....Qbb.......B.....Qbrj......L.....Qb..f.....X...d...................I`....Da.........(S.(.`....]..K`....Dd.............%......,Rc.................!.`....Da,...F...........@.-....XP.Q.....K...https://www.google.com/js/th/hlLHYuMj9gNC5zTdq--KBNr5YWNPOXBLIpYMmShXYzs.js.a........D`....D`....D`.....(...`....&...&....&..!.&.(S....`.....,L`......Qd..|.....trustedTypes..Qd...a....createPolicy.$..a..........Qd.'r.....createHTML..C..Qd>m......createScriptC..Qe~n......createScriptURL.C..q.......1.. Rc.................Qb... ....Z...`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e51c4f1931fed3e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7240
Entropy (8bit):	5.81430998398458
Encrypted:	false
SSDEEP:	192:6Dd+vMhNEOD7ufYPI7kfFBzpPQR+uf4QOJEEhkShOucpixhHqjfz+C:6zNHW/Q9xgrOeECS1coOh
MD5:	1616D6C3C29AD989CA4A92547C3C01BE
SHA1:	36C793566C6F6180CA0723221F2D9A20FE49E8C3
SHA-256:	35479798009CDC11457C195B58B74F92C644A5C49C6C3D148F0998D6595BAD01
SHA-512:	278CCDDC51B35FD2E5E09CC6EF319EE2E77B9DDA15C9A89D0D1A3085D8C8E63B6D6869D9907BB83E391DEC310040587745495A61E564893AAF14383C851CAE 2
Malicious:	false
Reputation:	low
Preview:	0\r..m............I....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en.kUju4RKWvZk.O/am=A4O4YYMCNAAIQAAAAAAAAACgESRAIfU6CP8/d=0/ct=zgms/rs=ABkqax2U4h6etIF89B-4_q5CH43h9ykl6A/m=NpD4ec,SF3gsd,O8k1Cd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,otPmVb,rlNAl .https://accounts.google.com/=.E.~./......................mLl...)....../Y.-T.Q/.".br..:...A..Eo........7.........A..Eo................................'.*.....O........0..h...........x........................(S.P..`Z.....L`.........Qb...'...._G...(S....`......L`v....dRc.................Qb........_.....QbJ.{.....Yyb...QbfhJ.....Zyb...Qb........$yb...QbZ.?.....czb...Qb..$3....bzb...Qb.=.%....azb.g$..............................I`....Da:.........Qb...0....k.....Qc..{.....NpD4ec....Qb.{......l.... Rc.................Qb.@Af....e...`..........Q.`...2...._DumpException....Qc..+....SF3gsd... Rc.................!.`.......Qc........O8k1Cd... Rc................`.......Qc.0}.....YLQSd.....QbV^......Gs....Qb>..4....Yw...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ef7caa204c1b984e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	947208
Entropy (8bit):	5.778770957623711
Encrypted:	false
SSDEEP:	12288:vpMdrGHVolk5yxdBy1evzLr3n1ZBTH9uO2BkAxt:GGulk5AdBBr3n1fbc
MD5:	8789BADF5FDF8E067465F7FCE3F8C1FF
SHA1:	EBEC28C4C4C7A2FDA428CB734178C58E9CB86BCC
SHA-256:	8D98E3BFA8116576FF13403BFB1B4BEBADA48D3430D15590E0EC97940D5F6B22
SHA-512:	336CD73CAC47686ABCF5F34D6181557919C03630D85B0E3EEEA4A180D5050C13714C13FB25E304636AB76B0647754D8B3BC1905C1A1ECE49750360EB9B2816A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ef7caa204c1b984e_0	
Reputation:	low
Preview:	0\r..m.....@.....jr....91ACA30B3303BEB921AC6960851E60E0433AC21DA220D93F37C3A81E5EEE7569.....'..1....O.....o..M]].....}..... ....$..... .....X.....\.....`....#..<.....3.....(S.D..`D....L`..... L`.....Qd.~.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f374efe77d747fee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	459
Entropy (8bit):	5.9128923206533
Encrypted:	false
SSDEEP:	12:U/GBiblsPjcRsGguGhYwAcCWwN0GZ1bbkw:UOTP7GAKw1BwNJZ1Uw
MD5:	3CBCBE402CE251D44A773140DE67B075
SHA1:	ED3F0CED16D0C67BBA83946CF0534331F52446C8
SHA-256:	483E2E203BA774D532EB4DD6CD19A168B5844408BB13116B6687A777BEE58221
SHA-512:	4AA1652B50453B5797B8F1C4FC3A5C7DCA25506EC01D4EA19B952CBC3C5421981B94663EF324BCE591EAC129F07A675DD845DB631F2F94A6EE64BDB66475D7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....y...._keyhttps://www.youtube.com/s/player/fa244a41/www-embed-player.vflset/www-embed-player.js .https://youtube.com/U\..~./.....E.j....d. ....h.g.M.?.!u..6....7.A..Eo.....Y.DW.....A..Eo.....U\..~./.....:.....E.j....d.....h.g.M.?.!u..6....7.A..Eo.....U\..~./.(...82D7D516690FCBDF6A2D0A6BB3430ADBBE92548B646C3538D4F35C809C223979E.j....d.....h.g.M.?.!u..6....7.A..Eo.....W.4.L.....

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):	2.6223023968497845
Encrypted:	false
SSDEEP:	96:dNwFXOXwv5zVzowWnzkx0hsj23hFNnZOLQXM+:duoAv5R8lkqsKNZJM
MD5:	7A4EE6652A2D29560AAC9EA91CD433D6
SHA1:	E28404861D9AD1FF195343B8341D34C592742F79
SHA-256:	EE49F9FBD3D3717740D2B1D383E7EC53EF3E59EAC2384B9591FAFD3B5900064F
SHA-512:	78E585F08439E5D62FDC8609C0A6446622C02919B525FB221B6AC54704BFC738ACBD45A9F69C122F9DB0D6F378DE0A5A294996C18B32742AF0FA74FBE1E7304
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):	0.9674639951076403
Encrypted:	false
SSDEEP:	24:Y6cLgAZOZD/+3qLbJLbXaFpEO5bNmISHn06UwG68:V8NOZ+3q5LLOpEO5J/Kn7Um8
MD5:	4852A4A6E1C48F33041846B79DFAD1CC
SHA1:	89FA70594C17A91F17B99DC911B6EF79AA8E8E4B
SHA-256:	633DDD8D3A2C65BE4AB97303974293C4E48A1B0D73CCA07121CCD1ED35EC0EE2
SHA-512:	CF5DC17A37B6213E978C41BD5A39E182F5FF0ED45051C1AEC882775F67644E1EE969500C83AE4C3102E3A5FF620317CFCB0DBADE8FC16DB8765373DDB22C7D1
Malicious:	false
Reputation:	low
Preview:	....

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):	44216
Entropy (8bit):	3.800990157682822
Encrypted:	false
SSDEEP:	192:3az4eZx2XTTjT905BtA6BtabsjbSe3rn7fhl38uQ5sWrT9lO+qwcBlABtPP3Sq36:KIs6eHutzqq1EF
MD5:	05F885D46B65DDAA2FEDD58137342356
SHA1:	CE585519731A9122452E9D16916DB70DD6514515
SHA-256:	CF14B614A3BE61D27BD81FD10FA99367835D4D468FDB1C4A6A204B599226A199
SHA-512:	B1CD833C07D6D3D0C8929E771528D68AC0F37EC9294520F00C2E2949900E0CA893985605757EC9E7496FE98132443B66048AB8D319AAA5FBB79FF497D4146B25
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...55dbc929_d11d_4572_996e_e0949b99b7c7..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://laporcovid19.org/...3...L.a.p. o.r.C.o.v.i.d.-.1.9. .|. .P.l.a.t.f.o.r.m. .B.e.r.b.a.g.i. .I.n.f.o.r.m.a.s.i. .C.O.V.I.D.-.1.9.....x.....h.....`.....uC.....uC..... ....(.....:.....h.t.t.p.s.:.//.l.a.p.o.r.c.o.v.i.d.1.9...o.r.g./.....o".key".5579.205{.....8.....0.....8..... ..... ..... .....X.....h.....`.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.153788802341355
Encrypted:	false
SSDEEP:	6:mRUyVq2PWXp+N23iKKdK8aPrqIFUtp0U4gZmwP0UzIkwOWXp+N23iKKdK8amLJ:Luva5KkL3FUtpbB/PbM5f5KkQJ
MD5:	508F29CC91FFFB279CAE3999F4D22E09
SHA1:	7F84657A860C08AD1A55CA1D232AA7C5676C5C60
SHA-256:	6B2F952E36CB1F183F5F91D3BDDA114A965EE6C74E7018F84DA2A5BCAB8DC9A8
SHA-512:	7626A29134A17B3BD8E0328B399A918907D5F352CAA23B24AC65BA06DEF2E28315A7429A223240EF9E7EB4F537E1A13EEB50304AD9BA1B27A5027814560B1201

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:16.020 ff0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/26-16:11:16.022 ff0 Recovering log #3.2021/04/26-16:11:16.023 ff0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
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):	320
Entropy (8bit):	5.191390780423364
Encrypted:	false
SSDEEP:	6:mReKjZAVq2PWXp+N23iKKdK8NIFUtp0eg4AgZmwP0eg4AIkwOWXp+N23iKKdK8+Q:46va5KkpFUtpR/PL5f5KkqJ
MD5:	42184ABC6B25B010DC501DFF1A8A030A
SHA1:	06F7C026C6E4F0D3F9A6A616D68E6CF213A765BE
SHA-256:	5E93621D8DFABE0990FF9F4CDAEBB432EFAEE6E8CD302AB72B5FEF209186FA06
SHA-512:	73ADD857B6FDCC9ED425E3C781BF7A6F3DCFE690DCEBDB0A88AE565A17316AD5389C9332AD614ECECFF5118CD65C68F655B380A46A89746F0E24E69D0EF6859
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:18.169 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/26-16:11:18.171 1440 Recovering log #3.2021/04/26-16:11:18.171 1440 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	63488
Entropy (8bit):	2.9343666673644524
Encrypted:	false
SSDEEP:	192:mH4hAFY2YeTKM1VwTmO6P1dmsHXzCvPo1sfgVAnTmIwjMx6PMxprxwgVAnTmVKY4:04hAFY+TJsc1dlHXSiyTbiMWT8To
MD5:	9F4371C3E31DC8D5BEACBFAC004821AF
SHA1:	1DE4CCFA677F9CF686B131D80EF79D641F53DCFB
SHA-256:	C03F88051C69ADED85657003646B7FD8FED85D6AD04AE9894414F6B0CD4416E5
SHA-512:	2BDA97AD2BADFB4581BC46E5CB2775E61AA123ABF4E37B6B14F9E91AC26290E5AE7379F408A9EDDC6DBE81BAFD498CDD8FBA1E41C41675C784441744C14F6CA0
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):	57608
Entropy (8bit):	1.7679803773566882
Encrypted:	false
SSDEEP:	192:mLtRXTLtPc/06PiTmvwdZMx6PAgVAnTm0:mrLhc/zsAM9ETh
MD5:	F7E36209B09783018DE2C984498E677A
SHA1:	C4EB3151FACDD1A516D33E756FE91BB8BB90AF98
SHA-256:	C2FFD58D407AC031DB121ADDF6D7052EA436385082FA57CC97AE86D2947C631E
SHA-512:	57BC916401EE2697FFCFD9371411BF09B157293E1A74B387BE321C23C21F39644CA7D51E3A32C7942698A6A784B9024319604769DC1097E7FBAB02B480BF25E7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Preview:	.....v..6..... ....

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):	369
Entropy (8bit):	5.322424136862454
Encrypted:	false
SSDEEP:	6:mR7cm73+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp07VZmwP07ITd3VkwOWXp+N23U:IcRva5KkTXfchI3FUtp4V/P4IP5f5KkI
MD5:	87A63D3CC924176B0FD5EF9640915AFB
SHA1:	9B18D7CDA4E579A950CAD61C600080218CE2596C
SHA-256:	4F9ADF3AE0DC048BDF5222A31920C0A466BFE653A9A6E2FFC1A736FC5798E813
SHA-512:	C6D2BE73ED2F45D31EEF167E2BC40DF1B3600BA5943B5A450E60DAA9DBDD0DC6AFA2DFA24E919018B30CA6530A2E6B25F64A340FC253029EBDAC8304A20951B
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.496 868 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/26-16:11:27.533 868 Recovering log #3.2021/04/26-16:11:27.534 868 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):	355
Entropy (8bit):	5.254052627471852
Encrypted:	false
SSDEEP:	6:mR7cdu+q2PWXp+N23iKKdK25+XuoIFUtp07cdBZmwP07cdbVkwOWXp+N23iKKdKl:Icdfva5KkTXYFUtp4cdB/P4cdB5f5Kkl
MD5:	149FCA0627A5AABC0C6493851B7E5404
SHA1:	2BD05ADCF3D7261786D25A52D886AF8BB56461F9
SHA-256:	CF8E65E0686A242803C00C6F85057B0DC0FE1E819F750E2D4B9E139F5511A3CC
SHA-512:	C15CD7775E1D0DB707BD37046F3BC1952F376444BB44BC8A725C40469118052EE00AA7B7F9C3DB4EB5111C18C413956D5D27B83EDCEE44E9A5851DF6CE5A535
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.485 868 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/26-16:11:27.486 868 Recovering log #3.2021/04/26-16:11:27.488 868 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Entropy (8bit):	5.258807124452385
Encrypted:	false
SSDEEP:	6:mR7adp+q2PWXp+N23iKKdKWT5g1IdqIFUtp07adaUZmwP07adS7VkwOWXp+N23im:IZva5Kkg5gSRFUtp4S/P4Vh5f5Kkg5gZ
MD5:	A6405CBA8C2578826BE92DC2F5967DB5
SHA1:	6B9ED05E3ADF2B907AF92053F3D94F1E2CDE4500
SHA-256:	7BBF1816EF3537F5FD5DCE0F1EFE497DB48443E5816C5CF5D70F67493319B6DE
SHA-512:	5115AB91ED9C4DC5AF065FE65A2F6B8F85F9CA2B883E57E800440AB46764729B4F9C25A64352F33FBBD2AC360B5BC4C9CC8EBEDDFDE7A820CA3B1845362434AC
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.284 1768 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/26-16:11:27.286 1768 Recovering log #3.2021/04/26-16:11:27.287 1768 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):	1.4624950307850333
Encrypted:	false
SSDEEP:	192:uRyNBL2nBrM/10WRINQBL26a3V+rQZy/10WRttQBL2essaPVws1tgRGQJbxQBL2+:5ReoScO4UmiYcpUUjjZm
MD5:	26D785A245F9CE552CE52CB9EBB7F2DB
SHA1:	171EB95C57C3DD004C37B2668E3762042911795C
SHA-256:	AB964958070198D738FE80F5FCD65D4CD6FA7C067967B10ED74B2A894AA9D5DC
SHA-512:	74CA58A69056C008A71DC1BF75EFCC26148D392800B33BFF75F608D5675FA2BA2685DA5A3069BC0B702EBC1918E81E5216831E8A21147201285FE6E9C9174C15
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1188
Entropy (8bit):	5.783239560763552
Encrypted:	false
SSDEEP:	24:Ft5zhizVXCMTSaQ5/5S5oa6y6q1VS5IdUVS5Bb/S5Z0Bh:Ftp4spva6yp60Bh
MD5:	26E323FEBADA8CA6FC162835EF2F382B
SHA1:	1575B529A0BA616887444E91E6550CE115EA1DFC
SHA-256:	1B8CA51BF26B61B7A962CA7855EC026AB8496B338D95B9A0873DA9E5887A62E9
SHA-512:	753F40C25E4DE6E91646ADADD7C09F4993549CB454C6D9029AB8521C6838B318EC2782A51D903597D42B2B1DBDCA1934733D28FD4B06EB9D1D389A40571F73F
Malicious:	false
Reputation:	low
Preview:	....."\....19..berbagi..covid..https..informasi..laporcovid..laporcovid19..org..platform..http..www*.....19.....berbagi.....covid.....http.....https.....informasi.....laporcovid.....laporcovid19.....org.....platform.....www..2.....1.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....v.....w...:.....B..... .....*.https://laporcovid19.org/23LaporCovid-19 | Platform Berbagi Informasi COVID-19:.....:.....s..... .....*.http://www.laporcovid19.org/23LaporCovid-19 | Platform Berbagi Informasi COVID-19:.....y..... .....*.https://www.laporcovid19.org/23LaporCovid-19 | Platform Berbagi Informasi COVID-19:.....t.....

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):	171396
Entropy (8bit):	1.210383873773922
Encrypted:	false
SSDEEP:	192:uwRy6BL2QsaurM/10WRIqQBL2XV+rQZy/10WRtnQBL2HVws1tgRGQJlTUjjxQBLf:uzCeDOc6TU/6YchjyU9z
MD5:	56D9A62CB8FB49C39BCEE1F49D5EDCA4
SHA1:	F28B385991A34FC11499B901B92F66F9DF760D3C
SHA-256:	AEB0A9FB60B76932066FBE8DBE4C7A1068377C3833AC9EE4D5D0388247C1A85C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
SHA-512:	F7E5DDDE0F1B961612A631BF9A3D45521C93B2B3F2E5B0D3725005E4363A915D5816A16D64640B1488E5CF0FF7AEDCC4CDD071CFB5A410C05A516DAB10162BC
Malicious:	false
Reputation:	low
Preview:	..."}..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3906
Entropy (8bit):	5.636205936934856
Encrypted:	false
SSDEEP:	96:eZJui+EsGG4xGa7VGMxKdbJMBJRJJubQ5fgorS0NmQeTz3:v/GG4xGyVGeKdNMBJRJJuE5fgsK
MD5:	01C68ADDC72AF109308BF11B06C5B8FC
SHA1:	4A35AC1E9E103696714E374EA7B9F1B84EC4072C
SHA-256:	F1DAF1F738FBC8113FEEBC350B8B37AB59A64B24D25DCA688611C19E34CCBE8A
SHA-512:	A510C2810472463497EF75AE9087E870F9DCFF121F739E474EA206491C3EECD4A8C5FEEED0ADD3A14C79B5EA0AFDA822CE16F7A4B05CFB6F84B3298C4416D9D
Malicious:	false
Reputation:	low
Preview:	}...f..*.....META:https://www.youtube.com.....5_https://www.youtube.com..yt-remote-connected-devicesB.{"data":"[]","expiration":1619565083143,"creation":1619478683143}.-_https://www.youtube.com..yt-remote-device-idd.{"data":"a62b275b-0876-41fb-a4bd-1a566a70a02e","expiration":1651014682872,"creation":1619478682872}.._https://www.youtube.com..__sakq/.D..... META:https://accounts.google.com.....#_https://accounts.google.com..promo..{}.#_https://accounts.google.com..__sak.....1.....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..712232000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-26 16:11:33.13] [INFO][mr.Init] MR instance ID: 554a44

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.213939434195221
Encrypted:	false
SSDEEP:	6:mRujyq2PWXp+N23iKKdK8a2jMGIFUtp0Zvt/1ZmwP0Zl2RjRkwOWXp+N23iKKdKw:xyva5Kk8EFUtpO9/Pm2RjR5f5Kk8bJ
MD5:	0453413484EB43F1464B38F685799941
SHA1:	396CD17859D1A9AC805030BD2611DDD5317ED81E
SHA-256:	67DB31257F722FC4E994663B3CD28A631485260FD65470FAA73A241C8F9F77C9
SHA-512:	4A64A1AFDFAFD0DF8290E0FF7A93E251808FB72AADA947F9EF68DA4EC10426D357972460737B767579E884BF288FEEF3E2A8E4776F8BBE5E5405D5FB3176E26(
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:15.799 1454 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/26-16:11:15.800 1454 Recovering log #3.2021/04/26-16:11:15.801 1454 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):	98304
Entropy (8bit):	1.3274470630274688
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWO6Hzx1TOqAuhjspnWO5HHNkDSDOqAuhjspnWOq3AV92HHNkDI+Hzn:HB8rn3ZgQFe4FxmNPV3SxPVyxP6Yj
MD5:	2D8EBB9009ADD600CCFD85054FB0F405
SHA1:	6D3B5ECFAC2FC3057865F19E550D09A2B2532587
SHA-256:	97E3E06332FC5A7A3206286B93259A558BC5A7F4E7F8310C5E50C6E042CC6BBD
SHA-512:	D0AF975F0A019029DC52D7D944ADF5A2E2CD50F61D79452239FF60C3AE42A7C657A4EF6BA3E130A10BED52B3F53B55A3943A0E707886F77E03CFAEFDA2A673(7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	102688
Entropy (8bit):	1.2273824242455025
Encrypted:	false
SSDEEP:	96:iQUOqAuhjspnWOXkOqAuhjspnWOBgHHNkDw0OqAuhjspnWO5MmHzx8EOqAuhjsp5:Fy+idzS3C2FtyoT3yi7PV3ZLmAPVfCs
MD5:	5BD7CDA559DB3DBE8F8EBC3840C32B5F
SHA1:	FAE09442871D40D0CE6BCD6754009BB5AD958141
SHA-256:	835E5C938BA371F96553EDC05960CFC83D1263C264E4C9A1B57283B4B54DBFC0
SHA-512:	F49091C1BD9B5AB9F0538537FBF36AFC0824262804BAE6E009818736314C3E44593E95C408E2580661345855C18E8968889B2B87FCC240B3301A04357CFD4BFB
Malicious:	false
Reputation:	low
Preview:	.....U.o..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.17364816513066
Encrypted:	false
SSDEEP:	6:mRUZAVq2PWXp+N23iKKdKgXz4rRIFUtp0UvAgZmwP0UYNAIkwOWXp+N23iKKdKgi:L6va5KkgXiuFUtpbh/PbU5f5KkgX2J
MD5:	D9BFF6C7D7F0E6098A0A99A29AE379C2
SHA1:	7CFB04F8525A681F8CEFBA67BFB53F2C6E10C8FE
SHA-256:	AD9A3FAFB40928DD4C41BC242CFB31AD886FE11934CBE47104C7B3CE480A8642
SHA-512:	02DAD88AF472A3CC3722967C0089C3A75A9B03E0BE81F3E535A6568C98F1FCA94970446F652FB058D371261AD7BA300167F5ED09645206B5779E50FAE46A17A4
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:16.041 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/26-16:11:16.047 1440 Recovering log #3.2021/04/26-16:11:16.048 1440 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.6481234388495065
Encrypted:	false
SSDEEP:	96:wIElwQF8mpcS6q8Vs/mZq8x0lH8VJVvbh1:wIElwQF8mpcSJ84H8QMJZd1
MD5:	EC1CEAF091591BACE64E6D831F196F64
SHA1:	F3C6C318857EF78B9F80CF106283286A84145B9F
SHA-256:	F1474CCB33786E2AA02A0F10DDDF5656755DCCE0B98D4FDC43A7398E0D59908E
SHA-512:	DD3F901521911F934B4E18AC8D79663E7ED7F98E303C4817A7179F8F32FC88F2A72104B6DB5A68E545D6BDD86FCE99F054DB6B68E024122362F6F410CA07F27F
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Size (bytes):	29252
Entropy (8bit):	0.6280695547400827
Encrypted:	false
SSDEEP:	48:r8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU0At4:r8hIElwQF8mpcSAAy
MD5:	D6E1063DECB82AD445209AEDC59BD252
SHA1:	1E6EDD198EC57FE17AF2B408F9B2A16B46E628FF
SHA-256:	23120AE683630EEAEF191D6B84A55074786CF126D7E47EF20583797B4C386A62
SHA-512:	1E3A9C7B650698E341DD939E2C36A7D39AB5E4C3A233C0FEC4A3660AF34E2547163709D3E2B1F27C60A2D4250D2FCD0B66F3DC90299B05ACEACA71DAB31141F
Malicious:	false
Reputation:	low
Preview:	.....42l!..... ....

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):	2990
Entropy (8bit):	4.4672470928175105
Encrypted:	false
SSDEEP:	48:7uG1KnPfQ8kn6AJ5Rh/5zp5l4M3xqoSRwzIIQwc3Lqz38gR0MezMVUBR38qlD0Rb:i9Pfyn5Jl/LP4HIdP8bEyBLFC
MD5:	4929BA33C1CCC62166DE3E2F20C5F476
SHA1:	277A7FB4FE94D260F5F89DB32E5E3650EC153B51
SHA-256:	EAB89A2F0AE9A7602F2AAED5ED6989B4495570C3FAAF432B650C3F7AAA18D8F3
SHA-512:	B15B03B93DFC9A0533675145F3AEC18BB82E1E526FC12DF7402297F3FF2491D75E4007066E1E6DC29F3CFE7B7C3E3FC3981761C40C385B650ED53BE60A64362
Malicious:	false
Reputation:	low
Preview:	..&f.....f.....next-map-id.1.Gnamespace-55dbc929_d11d_4572_996e_e0949b99b7c7-https://www.youtube.com/.0sQe.....map-0-yt-remote-cast-installedR{.".d.a.t.a.".:.".f.a.l.s.e.".,.".c.r.e.a.t.i.o.n.".:.1.6.1.9.4.7.8.6.8.3.3.1.5.}..!map-0-yt-remote-fast-check-periodb{.".d.a.t.a.".:.".1.6.1.9.4.7.8.9.8.3.1.4.2.",.".c.r.e.a.t.i.o.n.".:.1.6.1.9.4.7.8.6.8.3.1.4.2.}...map-0-yt-remote-session-appf{.".d.a.t.a.".:.".y.o.u.t.u.b.e.-.d.e.s.k.t.o.p.".,.".c.r.e.a.t.i.o.n.".:.1.6.1.9.4.7.8.6.8.3.1.4.1.}...map-0-yt-remote-session-nameV{.".d.a.t.a.".:.".D.e.s.k.t.o.p.".,.".c.r.e.a.t.i.o.n.".:.1.6.1.9.4.7.8.6.8.3.1.4.1.}...map-0-__sak.g.....g.....g.....g.....D..f.....next-map-id.2.Gnamespace-ac50ba8f_8085_4e88_832d_bdb5fd5706db-https://www.youtube.com/.1j..(|.....map-1-yt-remote-cast-availableR{.".d.a.t.a.".:.".f.a.l.s.e.".,.".c.r.e.a.t.i.o.n.".:.1.6.1.9.4.7.8.7.1.2.2.3.5.}...map-1-yt-remote-cast-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2148255068198015
Encrypted:	false
SSDEEP:	6:mRUN4q2PWXp+N23iKKdKrQMxIFUtp0aLJZmwP0IFIDLDkwOWXp+N23iKKdKrQMFd:p4va5KkCFUtpfLJ/P9cLD5f5KktJ
MD5:	F5E6A2FB85F98103D0F3F0305736B4AC
SHA1:	2C7EA3B82DAA64FAD4E044F594C6389CFAF2A4D2
SHA-256:	0E65795A9B4416A157DF5F603FA576997485388FD4242D28BD8C0B419B432F21
SHA-512:	2132437B77789DDBBF2EFEADE2A71DE1305DAC6105BE567D4F4715164A5F54C042D1CD356F6D519F2CA83C8B5D91830EA2E466A1959EE4276D93A6147B58BDC
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:15.934 14f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/26-16:11:15.936 14f4 Recovering log #3.2021/04/26-16:11:15.937 14f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.181006546683084
Encrypted:	false
SSDEEP:	6:mRNoyq2PWXp+N23iKKdK7Uh2ghZIFUtp0VV11ZmwP0KlRkwOWXp+N23iKKdK7Uh9:4va5KkIhHh2FUtpm1/Pjz5f5KkIhHLJ
MD5:	8EC0D3A1BFE6F1727EF56F47C7263B70
SHA1:	ADB492F0E8DCE569E382B4132A7BA728AA694F56

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	883669640CD591FE0FF3ECB2813A9E41D84EE2BAE70292D147ECA03F95E70283
SHA-512:	A2083FA15D353AD4E5E6FB1540E13CFFEA95DABCB0754406710DB72C0B1D9B0560A905CFED3425AD648FB213E7B89AB4DC079D98FA4DE6DDD6B79EB9AF43A F09
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:15.734 15a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/04/26-16:11:15.737 15a0 Recovering log #3.2021/04/26-16:11:15.738 15a0 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\8bab6cfd-84f4-4ebd-9833-e78ec45f6fa0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.266400083848141
Encrypted:	false
SSDEEP:	6:mROL4q2PWXp+N23iKKdKusNpV/2jMGIFUtp0MFIDLJZmwP0MFIDLDkwOWXp+N23e:j4va5KkFFUtp9FInJ/P9FInD5f5KkOJ
MD5:	20182C7209B039B84A4352636BFDD0A1
SHA1:	A7CCD3BCEEBB3183658E5B5B238D9BC830177671
SHA-256:	27B88B376F144755363B4772F6F4E8BD5E1F90B358AF2EB669A9A2B1CABBFC7F
SHA-512:	DFEB71FB901619FC03A7E73C8B52CDFB87464828CEAF74C5CB4120F06890040D3DCB2C2702E689DE598B20F5E85139B36EE277ADB2C6739C846898171BEC496
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:15.990 14f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/04/26-16:11:15.991 14f4 Recovering log #3.2021/04/26-16:11:15.991 14f4 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.234609585886892
Encrypted:	false
SSDEEP:	6:mRURVq2PWXp+N23iKKdKusNpqz4rRIFUtp0UEgZmwP0UKYIkwOWXp+N23iKKdKua:Lrva5KkmiuFUtpbt/PbK75f5Kkm2J
MD5:	87BEB552B3543AF8CA96D4705E70BE6A
SHA1:	2BEDFB9817D72002F57B90422DDA5D7D5BE44B24
SHA-256:	F13D6C2EDD603DF85949926E9759703E26F0C63F1886F8381EF5D2903D959718
SHA-512:	3786A1ED2FA8934376262120722C3FFCDDF70D2C1F31C0B6996B6EDA66F4607EB86265B2E247313A8EF67ACDA2586DEF56F10DC43146D75A1A569268380319AA
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:16.036 ff0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/26-16:11:16.040 ff0 Recovering log #3.2021/04/26-16:11:16.043 ff0 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):	418
Entropy (8bit):	5.235437028378594
Encrypted:	false
SSDEEP:	6:mRe2N+q2PWXp+N23iKKdKusNpZQMxIFUtp0vWZmwP042NVkwOWXp+N23iKKdKusx:du+va5KkMFUtpGW/PuV5f5KkTJ
MD5:	6E63DF540ABFEF70E88DE0572FADBECF
SHA1:	40DC4BC116ED16D1A8442CAC50290E6352049737
SHA-256:	0C7D178CD0B7829A25E1EBBEF70347278FB7963151730E84AD8ECE82A961941C
SHA-512:	7E82E3154254699109A9D6FECBFAAB1D61A11E66773CE64066D4690D6771ACA21FA474493D1E8433FBF86327A84A7BC15A9BA96FC0165026C7F98FDA823AD8D
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:32.611 143c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/04/26-16:11:32.612 143c Recovering log #3.2021/04/26-16:11:32.613 143c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\203b75e8-1113-48ec-b3fe-db301dfe56db.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\203b75e8-1113-48ec-b3fe-db301dfe56db.tmp

Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.187358980325512
Encrypted:	false
SSDEEP:	12:IMAva5KkkGHArBFUtp4uR/P4r5f5KkkGHAryJ:Ipa5KkkGgPgW/9f5KkkGga
MD5:	1D063E6AEAE8B8741B7ACF63C3B62BD5
SHA1:	597DDD70406C05181676C4A86BB7F37EDC7136AC
SHA-256:	49EA98F1E0E8A71A386C7DCFCD0CE9EED77E681126516E02D3241B0C0DA710E0
SHA-512:	3AE7065AB953CE0D042AC7EED7A163397AAE3F65EC72167F554ECF5CC94294921F9611F297527EA7D817FD0608FB37A1FD08D09B1885F888E2FA835525B6F8D8
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.157 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/04/26-16:11:27.160 1440 Recovering log #3.2021/04/26-16:11:27.161 1440 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.198189177991581
Encrypted:	false
SSDEEP:	12:IJAVva5KkkGHArqiuFUtp4Ig/P4kFODI5f5KkkGHArq2J:Ie5a5KkkGgCgWIdkFODSf5KkkGg7
MD5:	4EF7CAAA90EA074EB3BAE0262CDBAAC1
SHA1:	31A880A091219504C2DD42A02E46E7920036D8AC
SHA-256:	856FF1935ED65A54E7CD240B1DD712880C8E90AC9D9D766E54BCFD0A50EB403C
SHA-512:	DE7928A6038CE493A98FB82F2B2FFE08F0815AD25740785CE2CF0538C0ABCA379EF4B5B8632148E7BA927D5A0C3A3AC246AD1B4A19B597956731DB606B144B3
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:27.159 12e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/04/26-16:11:27.162 12e0 Recovering log #3.2021/04/26-16:11:27.163 12e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.209698636609536
Encrypted:	false
SSDEEP:	12:9+va5KkkGHArAFUtp1W/P4V5f5KkkGHArfJ:Ka5KkkGgkg3f5KkkGgV
MD5:	3A8A090E90D46F88EEF005C185EE0FE7
SHA1:	C1848640BCB214D4B82E5D2092D88318D8EE8552
SHA-256:	38F5FF6C4C5A9746025D8591772469D17D00D7F859F6DE5B84F0B2E1C80627B6
SHA-512:	D534866B00E2623FB958AA8176CC2F31000884741D074DE8FA636DB0CFEA15BDBA7AC2AE40C1E99CC1DC199F0CFFE94F233F2D7585A5B76005D6F8FB012969 F
Malicious:	false
Reputation:	low
Preview:	2021/04/26-16:11:42.392 143c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/04/26-16:11:42.395 143c Recovering log #3.2021/04/26-16:11:42.395 143c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	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):	324
Entropy (8bit):	5.233063363776056
Encrypted:	false
SSDEEP:	6:mRmZq2PWXp+N23iKKdKpIFUtp0oFZZmwP0MzkwOWXp+N23iKKdKa/WLJ:/va5KkmFUtpFX/PV5f5KkaUJ
MD5:	ABDA053F5847172752A1BA3107D62B13
SHA1:	A42952AEE782C1FFD0465CBECDFA157CB9A7BDCB
SHA-256:	CEB1CA795DB2F440F5A84D136DFBF9420A58BF4040158E91A320822F314310EC
SHA-512:	E1391D7D9D4D3620DA0CC829920EE6019E24D2F48A6CC6F84FAA1C094B7E326B92CC7DFE25835871FD68428BE8BA95E99865D445CAE75AAEE3C542E20E2E24 1
Malicious:	false
Reputation:	low

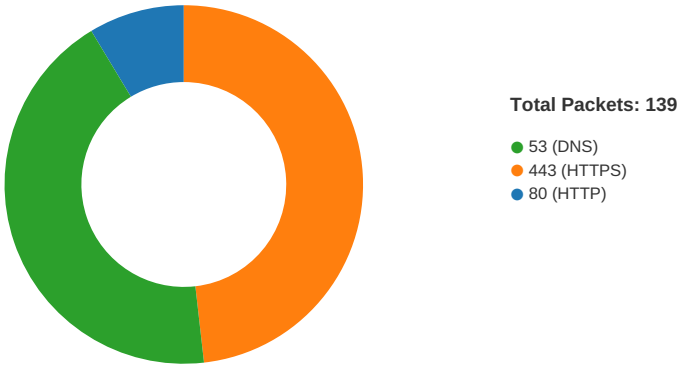
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Preview:	2021/04/26-16:11:15.740 1514 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/26-16:11:15.741 1514 Recovering log #3.2021/04/26-16:11:15.743 1514 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:17.956604004 CEST	49713	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:17.957660913 CEST	49714	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:17.978903055 CEST	49715	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:17.997590065 CEST	80	49713	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:17.997714996 CEST	49713	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:17.998105049 CEST	49713	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:17.998428106 CEST	80	49714	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:17.998536110 CEST	49714	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.019844055 CEST	80	49715	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.019982100 CEST	49715	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.038847923 CEST	80	49713	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.075934887 CEST	80	49713	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.086030960 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.116863966 CEST	49713	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.127134085 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.127290964 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.127573967 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.168572903 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.172250986 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.172276020 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.172456026 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.206969023 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.207127094 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.207313061 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.247960091 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.248003960 CEST	443	49716	104.21.85.166	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:18.248116970 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.248754978 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.249114037 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.290033102 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.726849079 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.767518044 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.913230896 CEST	49722	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.954232931 CEST	80	49722	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:18.954355001 CEST	49722	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.954968929 CEST	49722	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:18.995834112 CEST	80	49722	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.009372950 CEST	80	49722	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.018758059 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.050527096 CEST	49722	80	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.059823990 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907294035 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907315016 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907327890 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907340050 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907356977 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907373905 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.907397032 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.907440901 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.908142090 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.908210993 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.908272028 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.910634041 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.910648108 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.910731077 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.910832882 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.910846949 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.910896063 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.911319017 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.911335945 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.911410093 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.912303925 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.912322044 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.912384033 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.913307905 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.913330078 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.913388014 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.914223909 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.914247990 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.914330006 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.915200949 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.915241957 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.915302038 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:19.916172028 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.916186094 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:19.916249037 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.000714064 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.001043081 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.001369953 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.002223015 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.002248049 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.002551079 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.003019094 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.003349066 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.004004002 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.041572094 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.041836977 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.042288065 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.042999983 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.043086052 CEST	443	49716	104.21.85.166	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:20.043428898 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.044003963 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.044147968 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.044883966 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.050729990 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.050762892 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.050822020 CEST	49716	443	192.168.2.3	104.21.85.166
Apr 26, 2021 16:11:20.050949097 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.051098108 CEST	443	49716	104.21.85.166	192.168.2.3
Apr 26, 2021 16:11:20.051163912 CEST	49716	443	192.168.2.3	104.21.85.166

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:10.305567026 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:10.316595078 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:10.369375944 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:10.375905991 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:11.089426041 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:11.138045073 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:12.942015886 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:12.990761042 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:14.440002918 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:14.491719007 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:15.998919010 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:16.056324959 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:17.733961105 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:17.734795094 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:17.740048885 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:17.745044947 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:17.791481972 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:17.797128916 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:17.813255072 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:17.823292017 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:17.872000933 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:17.949769974 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:18.229167938 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:18.297732115 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:18.405082941 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:18.472944975 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:18.735228062 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:18.831397057 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:18.880167961 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:18.906120062 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:19.619596958 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:19.668240070 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:19.704932928 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:19.770606041 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:19.999855995 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:20.007463932 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:20.018019915 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:20.065215111 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:20.075444937 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:20.107152939 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:21.152419090 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:21.211210966 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:21.403882027 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:21.452456951 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:21.486826897 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:21.554701090 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:21.642712116 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:21.702086926 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.273463964 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:22.289685965 CEST	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:22.331089020 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.354566097 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.416172981 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:22.476591110 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.538629055 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.548015118 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:22.595837116 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.595858097 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.596688986 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.598033905 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.598606110 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.598623991 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.666994095 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.669522047 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.669919014 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.673449993 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.701518059 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.702270985 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.703066111 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.704168081 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.704487085 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.704533100 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.737507105 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:22.739557981 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:22.787422895 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.794755936 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.798986912 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:22.805620909 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:22.842775106 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.874902964 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.875880957 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:22.876851082 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:24.915813923 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:24.973217010 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:25.659749031 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:25.828749895 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:26.128010035 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:26.193336964 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:27.488528967 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:27.553153038 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:30.952255964 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:31.012572050 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:33.027091980 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:33.091964006 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:34.162034988 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:34.210654974 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:34.249118090 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:34.297722101 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:37.705658913 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:37.774703026 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:38.380377054 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:38.429270029 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:41.346719980 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:41.395289898 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:41.439409018 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:41.486922026 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:41.507014990 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:41.552464008 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:42.507384062 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:42.569520950 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:43.605137110 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:43.653923035 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:44.941863060 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:45.019830942 CEST	53	54833	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:11:46.539143085 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:46.589792013 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:49.242043972 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:49.311592102 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:49.318015099 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:49.319031000 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:49.411217928 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:49.489450932 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:49.502466917 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:11:49.503519058 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:11:49.678627014 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:49.736440897 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:49.736480951 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:49.936810970 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:49.936908007 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.236829042 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.236865044 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.553982019 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:50.554157019 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:50.554210901 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:50.556255102 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:50.622406960 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.625478029 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.626173019 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:11:50.633981943 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:50.664923906 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:11:55.611023903 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:55.659832001 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:57.161945105 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:57.211705923 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:57.753109932 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:57.801816940 CEST	53	61633	8.8.8.8	192.168.2.3
Apr 26, 2021 16:11:57.967529058 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:11:58.016226053 CEST	53	55949	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:03.761154890 CEST	49342	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:03.821454048 CEST	53	49342	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:11.803293943 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:11.873209000 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:11.879122019 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:11.879996061 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:11.881448030 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:11.968169928 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:12.012408018 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:12:12.042416096 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:13.067615986 CEST	56253	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:13.116424084 CEST	53	56253	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:15.714713097 CEST	49667	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:15.776711941 CEST	53	49667	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:16.143584967 CEST	57069	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:16.203469038 CEST	53	57069	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:16.396656036 CEST	57659	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:16.463165998 CEST	53	57659	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:16.590090036 CEST	54717	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:16.647353888 CEST	53	54717	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:16.705197096 CEST	63975	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:16.764995098 CEST	53	63975	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:23.155167103 CEST	56639	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:23.327833891 CEST	53	56639	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:25.023231030 CEST	51856	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:25.120950937 CEST	53	51856	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:26.160160065 CEST	56546	53	192.168.2.3	8.8.8.8
Apr 26, 2021 16:12:26.220160007 CEST	53	56546	8.8.8.8	192.168.2.3
Apr 26, 2021 16:12:26.804209948 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:26.824008942 CEST	61948	443	192.168.2.3	172.217.23.66

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 16:12:26.867944002 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:26.899553061 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:26.900576115 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:26.901475906 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:27.093414068 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:27.161964893 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:12:27.167222977 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:12:27.167256117 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:12:27.167685986 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:27.200737953 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:27.269588947 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:27.276878119 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:27.277761936 CEST	443	61948	172.217.23.66	192.168.2.3
Apr 26, 2021 16:12:27.280750990 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:27.712970018 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:27.757180929 CEST	443	62479	172.217.23.86	192.168.2.3
Apr 26, 2021 16:12:27.784121037 CEST	62479	443	192.168.2.3	172.217.23.86
Apr 26, 2021 16:12:41.844825983 CEST	61948	443	192.168.2.3	172.217.23.66
Apr 26, 2021 16:12:41.914108992 CEST	443	61948	172.217.23.66	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 26, 2021 16:11:17.734795094 CEST	192.168.2.3	8.8.8.8	0x7f94	Standard query (0)	www.laporcovid19.org	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:18.735228062 CEST	192.168.2.3	8.8.8.8	0x1506	Standard query (0)	laporcovid19.org	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:20.018019915 CEST	192.168.2.3	8.8.8.8	0xf816	Standard query (0)	cms.laporcovid19.org	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:21.403882027 CEST	192.168.2.3	8.8.8.8	0x4cf1	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.273463964 CEST	192.168.2.3	8.8.8.8	0xeb13	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.289685965 CEST	192.168.2.3	8.8.8.8	0xc857	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.737507105 CEST	192.168.2.3	8.8.8.8	0x3	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.739557981 CEST	192.168.2.3	8.8.8.8	0xcaa6	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:25.659749031 CEST	192.168.2.3	8.8.8.8	0x8cf3	Standard query (0)	cms.laporcovid19.org	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:26.128010035 CEST	192.168.2.3	8.8.8.8	0x6576	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:27.488528967 CEST	192.168.2.3	8.8.8.8	0xd75f	Standard query (0)	consent.youtube.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:41.486922026 CEST	192.168.2.3	8.8.8.8	0xfe60	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Apr 26, 2021 16:12:23.155167103 CEST	192.168.2.3	8.8.8.8	0x91bf	Standard query (0)	laporcovid19.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 26, 2021 16:11:17.949769974 CEST	8.8.8.8	192.168.2.3	0x7f94	No error (0)	www.laporcovid19.org		104.21.85.166	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:17.949769974 CEST	8.8.8.8	192.168.2.3	0x7f94	No error (0)	www.laporcovid19.org		172.67.207.167	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:18.906120062 CEST	8.8.8.8	192.168.2.3	0x1506	No error (0)	laporcovid19.org		104.21.85.166	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:18.906120062 CEST	8.8.8.8	192.168.2.3	0x1506	No error (0)	laporcovid19.org		172.67.207.167	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:20.107152939 CEST	8.8.8.8	192.168.2.3	0xf816	No error (0)	cms.laporcovid19.org		172.67.207.167	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:20.107152939 CEST	8.8.8.8	192.168.2.3	0xf816	No error (0)	cms.laporcovid19.org		104.21.85.166	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 26, 2021 16:11:21.452456951 CEST	8.8.8.8	192.168.2.3	0x4cf1	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 16:11:22.331089020 CEST	8.8.8.8	192.168.2.3	0xeb13	No error (0)	googleads.g.doubleclick.net		172.217.23.66	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.354566097 CEST	8.8.8.8	192.168.2.3	0xc857	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 16:11:22.794755936 CEST	8.8.8.8	192.168.2.3	0x3	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 16:11:22.794755936 CEST	8.8.8.8	192.168.2.3	0x3	No error (0)	photos-ugc.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.23.86	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.22.214	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.22.246	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		216.58.207.150	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		216.58.207.182	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.20.246	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.23.22	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:22.805620909 CEST	8.8.8.8	192.168.2.3	0xcaa6	No error (0)	i.ytimg.com		172.217.23.54	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:25.828749895 CEST	8.8.8.8	192.168.2.3	0x8cf3	No error (0)	cms.laporcovid19.org		172.67.207.167	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:25.828749895 CEST	8.8.8.8	192.168.2.3	0x8cf3	No error (0)	cms.laporcovid19.org		104.21.85.166	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:26.193336964 CEST	8.8.8.8	192.168.2.3	0x6576	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 16:11:26.193336964 CEST	8.8.8.8	192.168.2.3	0x6576	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:27.553153038 CEST	8.8.8.8	192.168.2.3	0xd75f	No error (0)	consent.youtube.com		172.217.23.46	A (IP address)	IN (0x0001)
Apr 26, 2021 16:11:41.552464008 CEST	8.8.8.8	192.168.2.3	0xfe60	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 16:12:23.327833891 CEST	8.8.8.8	192.168.2.3	0x91bf	No error (0)	laporcovid19.org		104.21.85.166	A (IP address)	IN (0x0001)
Apr 26, 2021 16:12:23.327833891 CEST	8.8.8.8	192.168.2.3	0x91bf	No error (0)	laporcovid19.org		172.67.207.167	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.laporcovid19.org
- laporcovid19.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	104.21.85.166	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 26, 2021 16:11:17.998105049 CEST	1097	OUT	GET / HTTP/1.1 Host: www.laporcovid19.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Apr 26, 2021 16:11:18.075934887 CEST	1099	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 26 Apr 2021 14:11:18 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 26 Apr 2021 15:11:18 GMT Location: https://www.laporcovid19.org/ cf-request-id: 09b01e3f8f0000c29aec378000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=blHd7%2FggvWNzew4g%2FMtBU28%2BZlziNujCAZZfPmonh2a2VRt1Zero%2Fk26tWeKNzwd7uNkFI9fEOYW7tPwQC4QMbRmoZlfaqsk6Tvz7eXiCuJOBg39Fg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 64606645be1dc29a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

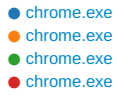
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49722	104.21.85.166	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 26, 2021 16:11:18.954968929 CEST	1865	OUT	GET / HTTP/1.1 Host: laporcovid19.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Apr 26, 2021 16:11:19.009372950 CEST	1866	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 26 Apr 2021 14:11:19 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 26 Apr 2021 15:11:18 GMT Location: https://laporcovid19.org/ cf-request-id: 09b01e434b0000dfcb31885000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=PC%2FeSw0kjHHXsPnRwKJKJ7iKz9lOFKtWImCSTGlOGcnFy6OUff3QCtC0F%2BTaZKUM8EVdyZFjs59g6iSecyTKcoOcVKvqs5w%2FqV7KEbK2a7H%2B"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Vary: Accept-Encoding Server: cloudflare CF-RAY: 6460664baaafdfcb-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6032 Parent PID: 2124

General

Start time:	16:11:14
Start date:	26/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.laporcovid19.org'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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: 5368 Parent PID: 6032

General

Start time:	16:11:16
Start date:	26/04/2021
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=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 7152 Parent PID: 6032

General

Start time:	16:11:23
Start date:	26/04/2021
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=audio.mojom.AudioService --field-trial-handle=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5720 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 4744 Parent PID: 6032

General

Start time:	16:11:25
Start date:	26/04/2021
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1636,11939290187013884241,7043982140473784357,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4708 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly