ID: 341595
Cookbook: browseurl.jbs
Time: 15:17:49
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report http://www.covid19-siparadigm.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 46
No static file info 46
Network Behavior 46
Network Port Distribution 46
TCP Packets 46
UDP Packets 48
DNS Queries 49
DNS Answers 50
HTTP Request Dependency Graph 50
HTTP Packets 50
HTTPS Packets 51
Code Manipulations 51
Statistics 51
Behavior 51
System Behavior 52

Analysis Process: chrome.exe PID: 4720 Parent PID: 3572 52
General 52
File Activities 52
Registry Activities 52
Analysis Process: chrome.exe PID: 5968 Parent PID: 4720 52
General 52
File Activities 53
Analysis Process: chrome.exe PID: 6172 Parent PID: 4720 53
General 53
File Activities 53
Registry Activities 53
Disassembly 53

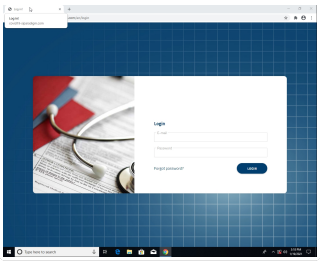
Analysis Report http://www.covid19-siparadigm.com

Overview

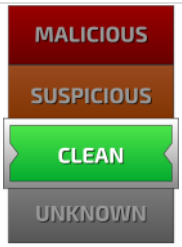
General Information

Sample URL:	http://www.covid19-siparadigm.com
Analysis ID:	341595

Most interesting Screenshot:



Detection

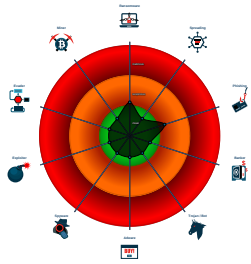


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4720 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.covid19-siparadigm.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5968 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,1923756594479640155,10121834588426309513,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6172 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1592,1923756594479640155,10121834588426309513,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3936 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

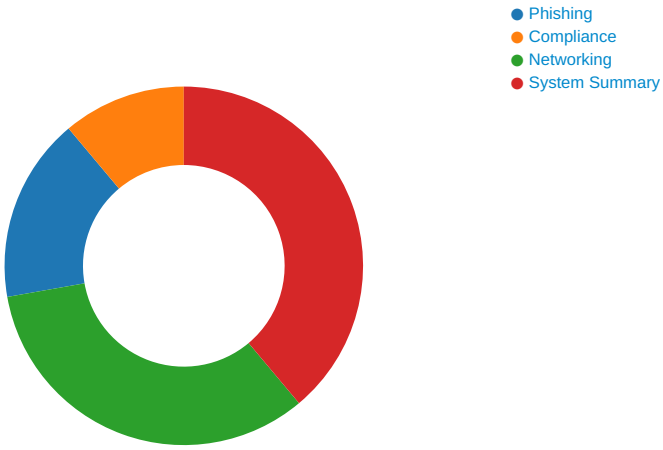
Yara Overview

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.

Compliance:

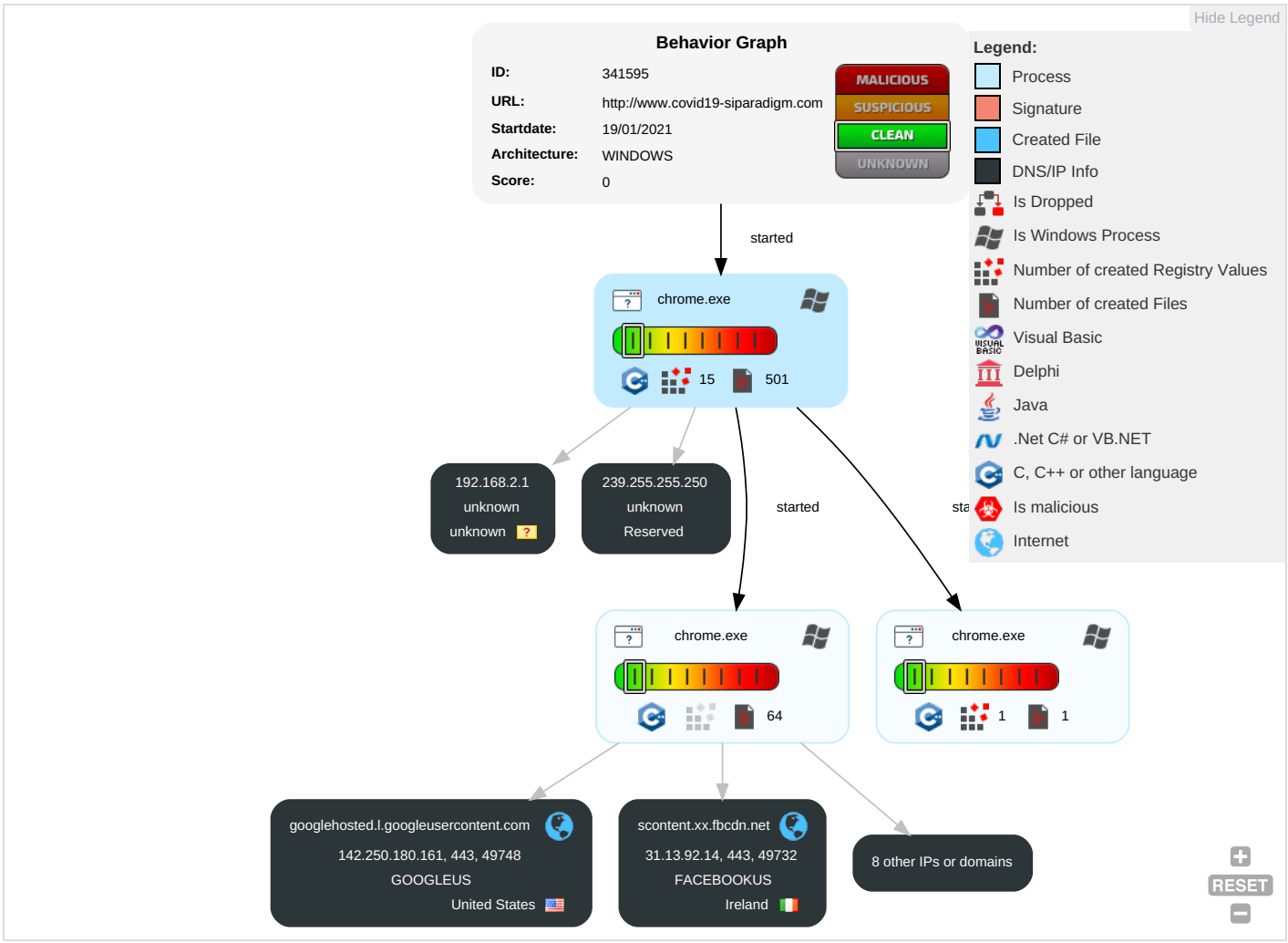
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
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	Devic Lock
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	Delet Devic Data
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		Carri Billing Fraud

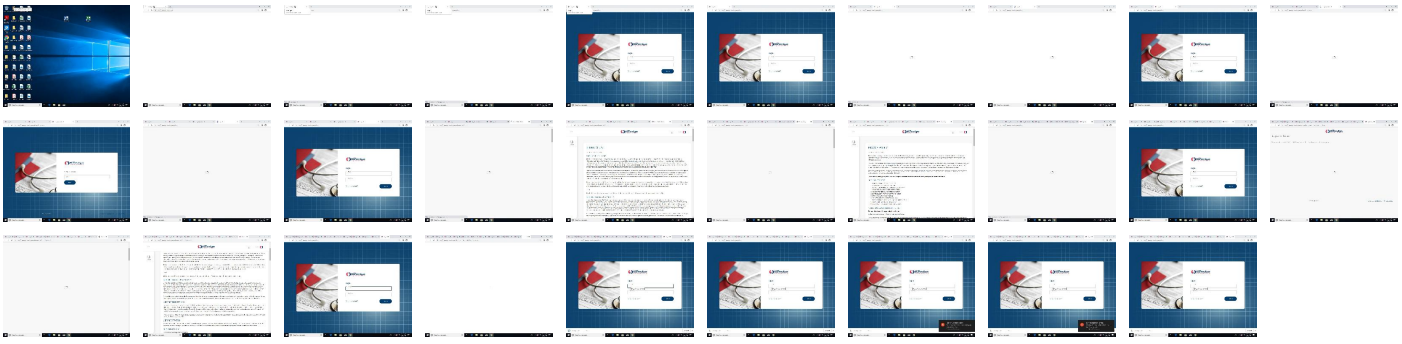
Behavior Graph

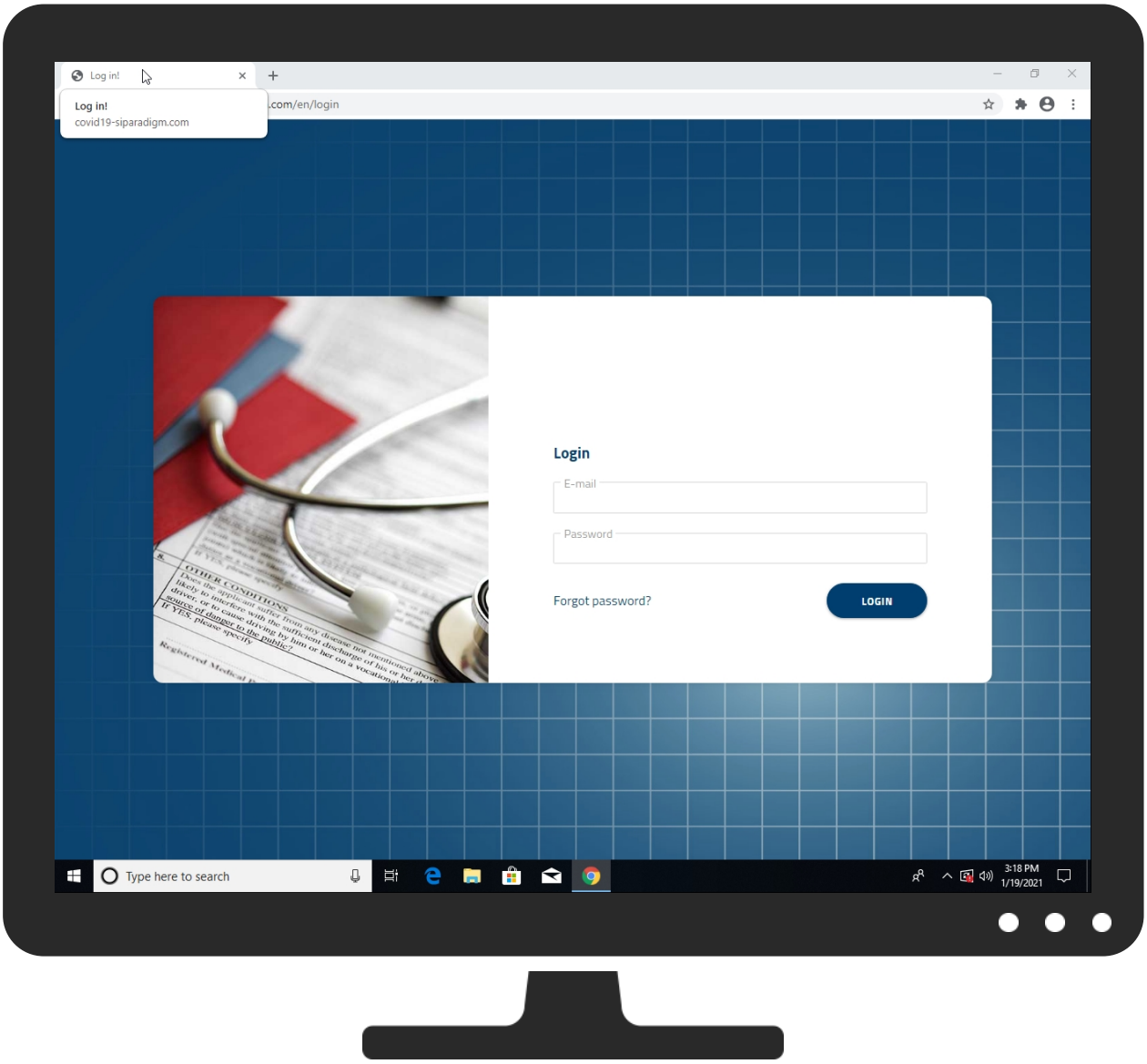


Screenshots

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.covid19-siparadigm.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.covid19-siparadigm.com/en/terms-conditions#supportTerms	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3a	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/forgot_passwordForgot	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.covid19-siparadigm.com/en//	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/Chart.bundle.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/owl.carousel.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap.bundle.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/Log	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.barrating.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/fullcalendar.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/loginLog	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/neovare/templates/dore/menu.html.twig4	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/dashboard/	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.validate/jquery.validate.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/privacy-policy:	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/p	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/X	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/l	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/o	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/y	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/a	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/fullcalendar.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/login2	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/custom_libraries/google/googleAnalytics.jsaD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/moment.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/kbPX	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/terms-conditions9	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/custom_libraries/select2/select2.full.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/Z	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/chartjs-plugin-datalabels.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/V	0%	Avira URL Cloud	safe	
http://www.covid19-siparadigm.com/)	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/I	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/K	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/terms-conditionsTerms	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/dore-plugins/select.from.library.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/perfect-scrollbar.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://www.covid19-siparadigm.com/Log	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/%o1Y	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/gn4Y	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/wm	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://www.covid19-siparadigm.com/N	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.barrating.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/typeahead.bundle.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-datepicker.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://www.covid19-siparadigm.com/L	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/terms-conditions#supportM	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://www.covid19-siparadigm.com/2	0%	Avira URL Cloud	safe	
http://https://covid19-siparadigm.com/4.2Y	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3a	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/en/print/printer-driversLog	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3	0%	Avira URL Cloud	safe	
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.validate/jquery.validate.min.js?v=1.5.3aD	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
neovare-alb-285209131.us-west-2.elb.amazonaws.com	54.149.7.8	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.161	true	false		high
www.covid19-siparadigm.com	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.covid19-siparadigm.com/en/privacy-policy	false		unknown
http://https://www.covid19-siparadigm.com/en/terms-conditions	false		unknown
http://https://www.covid19-siparadigm.com/en/login	false		unknown
http://https://www.covid19-siparadigm.com/en/terms-conditions#support	false		unknown
http://https://www.covid19-siparadigm.com/en/forgot_password	false		unknown

URLs from Memory and Binaries

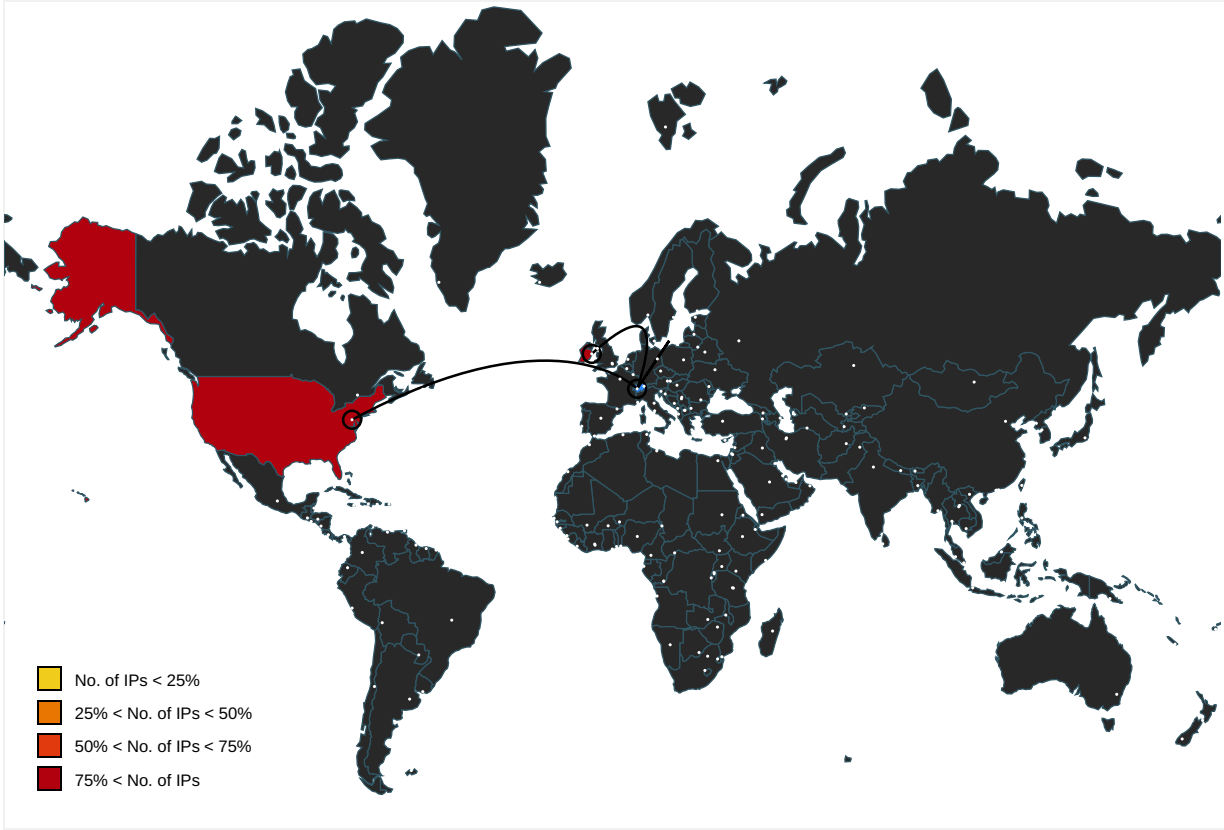
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.covid19-siparadigm.com/en/terms-conditions#supportTerms	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3a	0f8167173cfdde1f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3	0d400fb19bd41030_0.0.dr, 9acb17b07b2d71aa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/forgot_passwordForgot	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en//	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/Chart.bundle.min.js?v=1.5.3aD	bead25964382b68f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/owl.carousel.min.js?v=1.5.3	3f6da823cbffbfab_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap.bundle.min.js?v=1.5.3	13490cf906b3f6b4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3	f5d363064ecce588_0.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.covid19-siparadigm.com/en/terms-conditions	Current Session.0.dr	false		unknown
http://https://www.covid19-siparadigm.com/en/Log	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3	e508f5ea9c0d214f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3aD	cb4433fb907e1cce_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.barrating.min.js?v=1.5.3	eab3f5e80b9c9c0b_0.0.dr, segui sym.ttf.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3aD	b6971dcab2beb1fe_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/fullcalendar.min.js?v=1.5.3	44fe39ce09791f8c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/fbevents.js	5070c80b4ccf8e9e_0.0.dr	false		high
http://https://www.covid19-siparadigm.com/en/loginLog	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/neovare/templates/dore/menu.html.twig4	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3	5715a7ebf0b01a60_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/dashboard/	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3aD	ae1ae1891fb3d2d1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	4b5facdb-31a7-4891-a848-bbaba79dbb46.tmp.1.dr, 77c0f0b7-2265-4d58-a575-a81b60cf8a8b.tmp.1.dr, 2d8d8b34-9f68-42d1-97aa-7079ad4b874a.tmp.1.dr, f66901d8-3c23-49e1-9963-5d3530b85794.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://momentjs.com/guides/#/warnings/zone/	bead25964382b68f_0.0.dr, cc19588327582ba6_0.0.dr	false		high
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.validate/jquery.validate.min.js?v=1.5.3	0f85719212f732a4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.jsdelivr.net/	Network Action Predictor-journal.0.dr	false		high
http://https://www.covid19-siparadigm.com/en/privacy-policy:	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/	000003.log0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/	80754dd448f8c9bf_0.0.dr, 5070c80b4ccf8e9e_0.0.dr, 3b834dbee20d78d5_0.0.dr, cffccb8fdc29a204_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/privacy-policy	Current Session.0.dr	false		unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3aD	f5d363064ecce588_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/p	3b834dbee20d78d5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3aD	d629d47e5b296288_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3	0f8167173cfdde1f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/X	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/l	3b834dbee20d78d5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/o	cffccb8fdc29a204_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/y	3b834dbee20d78d5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3aD	0f8167173cfdde1f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.jsdelivr.net	4b5facdb-31a7-4891-a848-bbaba79dbb46.tmp.1.dr	false		high
http://https://covid19-siparadigm.com/a	cc19588327582ba6_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3aD	5715a7ebf0b01a60_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/fullcalendar.min.js?v=1.5.3aD	33c51cdee04606bd_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/login2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/custom_libraries/google/googleAnalytics.jsaD	e47734d8b5f45427_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/moment.min.js?v=1.5.3	cc19588327582ba6_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/kbPX	13490cf906b3f6b4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com	000003.log3.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/terms-conditions9	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3	b774c64f3d731ee5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3aD	e508f5ea9c0d214f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/terms-conditions#support	Current Session.0.dr, History-journal.0.dr	false		unknown
http://https://www.covid19-siparadigm.com/custom_libraries/select2/select2.full.min.js?v=1.5.3aD	e3a093248cd06e5f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/Z	cffccb8fdc29a204_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.covid19-siparadigm.com/dore/js/vendor/chartjs-plugin-datalabels.js?v=1.5.3aD	6edbfff5c06531e4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://momentjs.com/guides/#/warnings/min-max/	bead25964382b68f_0.0.dr, cc19588327582ba6_0.0.dr	false		high
http://https://covid19-siparadigm.com/V	5070c80b4ccf8e9e_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.covid19-siparadigm.com/)	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/I	3b834dbee20d78d5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/K	3b834dbee20d78d5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/terms-conditionsTerms	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/dore-plugins/select.from.library.js?v=1.5.3	5058f561f02561cd_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/neovare/templates/dore/menu.html.twig	Current Session.0.dr, Favicons-journal.0.dr	false		unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/perfect-scrollbar.min.js?v=1.5.3aD	1e110aee5bf277be_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3aD	b774c64f3d731ee5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.covid19-siparadigm.com/Log	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/%o1Y	0f8167173cfdde1f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3	80754dd448f8c9bf_0.0.dr, cb4433fb907e1cce_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-siparadigm.com/gn4Y	f5d363064ecce588_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/signals/config/3692194074184385?v=2.9.32&r=stable	3b834dbee20d78d5_0.0.dr	false		high
http://https://covid19-siparadigm.com/wm	096e1f9b7eb0d642_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3aD	3b88956e8fa6bdcd_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.covid19-siparadigm.com/N	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3	ae1ae1891fb3d2d1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.barrating.min.js?v=1.5.3aD	eab3f5e80b9c9c0b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/typeahead.bundle.js?v=1.5.3	6c180cd76b238e73_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-datepicker.js?v=1.5.3aD	7355060daeeb1408_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://momentjs.com/guides/#/warnings/js-date/	bead25964382b68f_0.0.dr	false		high
http://www.covid19-siparadigm.com/L	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3	309cb9bdfb34402c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3aD	9acb17b07b2d71aa_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/terms-conditions#supportM	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3	3b88956e8fa6bdcd_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3	d629d47e5b296288_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.covid19-siparadigm.com/2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/forgot_password	Current Session.0.dr, Favicons-journal.0.dr	false		unknown
http://https://covid19-siparadigm.com/4.2Y	fc55e55442907e54_0.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3a	309cb9bdfb34402c_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/en/print/printer-driversLog	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3	b6971dcab2beb1fe_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.covid19-siparadigm.com/dore/js/vendor/jquery.validate/jquery.validate.min.js?v=1.5.3aD	0f85719212f732a4_0.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.13.92.14	unknown	Ireland		32934	FACEBOOKUS	false
31.13.92.36	unknown	Ireland		32934	FACEBOOKUS	false
54.149.7.8	unknown	United States		16509	AMAZON-02US	false
142.250.180.161	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341595
Start date:	19.01.2021
Start time:	15:17:49
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.covid19-siparadigm.com
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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@52/278@5/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.covid19-siparadigm.com/en/ • Browse: https://www.covid19-siparadigm.com/en/forgot_password • Browse: https://www.covid19-siparadigm.com/en/ • Browse: https://www.covid19-siparadigm.com/en/terms-conditions • Browse: https://www.covid19-siparadigm.com/en/privacy-policy • Browse: https://www.covid19-siparadigm.com/en/dashboard/ • Browse: https://www.covid19-siparadigm.com/en/login • Browse: https://www.covid19-siparadigm.com/neovare/templates/dore/menu.html.twig • Browse: https://www.covid19-siparadigm.com/en/terms-conditions#support • Browse: https://www.covid19-siparadigm.com/en/print/printer-drivers • Browse: https://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.88.21.125, 216.58.198.13, 216.58.208.174, 142.250.180.110, 74.125.104.87, 173.194.188.234, 142.250.180.67, 216.58.198.42, 216.58.206.78, 142.250.180.106, 216.58.207.35, 173.194.187.106, 216.58.209.42, 216.58.206.74, 216.58.205.74, 142.250.180.74, 142.250.180.138, 142.250.180.170, 216.58.206.42, 216.58.208.138, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 51.11.168.160, 92.122.213.247, 92.122.213.194, 8.248.113.254, 8.248.147.254, 8.253.207.120, 8.248.149.254, 8.248.115.254, 52.255.188.83, 51.103.5.186, 142.250.180.99, 142.250.180.131, 52.251.11.100, 20.54.26.129, 2.18.68.82, 173.194.163.76, 74.125.173.199, 51.104.144.132 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, clientservices.googleapis.com, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, r6.sn-4g5ednls.gvt1.com, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r6---sn-4g5ednls.gvt1.com, r5---sn-4g5ednsk.gvt1.com, ris.api.iris.microsoft.com, r1---sn-4g5ednle.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, par02p.wns.notify.trafficmanager.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, r5---sn-4g5e6nsr.gvt1.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, redirector.gvt1.com, r1.sn-4g5ednle.gvt1.com, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, r2.sn-4g5e6nzz.gvt1.com, dualstack.f3.shared.global.fastly.net, r5.sn-4g5ednsk.gvt1.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, r2---sn-4g5e6nzz.gvt1.com, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, r5.sn-4g5e6nsr.gvt1.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found. • VT rate limit hit for: http://www.covid19-siparadigm.com

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\0f6a744d-2618-4d76-b412-ccee604e1ae2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	100932

C:\Users\user\AppData\Local\Google\Chrome\User Data\0f6a744d-2618-4d76-b412-ccee604e1ae2.tmp	
Entropy (8bit):	3.747390384391337
Encrypted:	false
SSDEEP:	384:nfgF1Bf42fgjLVkq54NZryvdn3mpDiHfAaG5i9rIbRZux3ClWLvTurshmc/43JpT:P+2BNtdW+keXhMrYfHinKB3d2L
MD5:	FF7AB06038DC9942750F059DBFD61B2D
SHA1:	AD387EE4EF112D9C14D901F4F9EFC59C845C6A21
SHA-256:	7E2967CDACDAF1D75E5D969F4EEEAC77581A4DA29B0F9BCC0F8F25FCE9B82C4A
SHA-512:	B3475DD8D0FDF557756295E5663704E6AF104FEA56143845333D89DCD3ECBF7BFE2B85826ECAC6E10AFC1184D5A451940FEBE253FFFAC52199AF49922F4FE06
Malicious:	false
Reputation:	low
Preview:	@.....*...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...7/8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\2df45a7a-fbee-4587-9213-3e2325caf150.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.7473307069204456
Encrypted:	false
SSDEEP:	384:nfe1Bf42rjM54NZryvdn3mpDiHzaGq9rIbRpxWLvTurshmc/43Jph2OHfJNs1xoO:62BNWvW+keXhrrIfTinKB3d2F
MD5:	D77ED0A73C147784BE6B7ECE12C33410
SHA1:	F7D9C72585E46D4C60EA8C9FB1D0EAF101CC51DC
SHA-256:	FE30F2267754F82019F30C4A9D929BAD1B3B98AB1FC1317C45252831D652133E
SHA-512:	BF98568AF84D33458383494CBA669136086EAEEBA6E4AF2D4B809894C1520A2E8839B56BE326E253407A1FF7421ABB8230789AA44F2EE8990DAD56A499ADF7CE
Malicious:	false
Reputation:	low
Preview:	.g.....*...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...7/8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4d7eb0b0-28d6-4777-bfbe-09017606a10a.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):	358658
Entropy (8bit):	6.028594308216096
Encrypted:	false
SSDEEP:	6144:tVCpuN9msDwjWCuG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxins:tVoqmsDRNGNPUZ+w7wJHyEtAW9
MD5:	57625A92D99F084A3077BE9B1A8F258F
SHA1:	0882E852E2D0B38533D5834998F0938343F259AD
SHA-256:	89A9A391F71BFDB101D0EADEAFCD1EB6A7ADF5D2B845A30F8E4831D1534DC53A
SHA-512:	20BE9BE312481D2245FF9EADA35B5C49B16DD94A20848F8A739F402B83F98BE7DFBCDED54EF5AA002F490DFE5EF7DA3F7840985F8E3E201E9CF8CB5D6DB76E 36
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":1.611098330850985e+12,"network":1.611065932e+12,"ticks":163802962.0,"uncertainty":4528918.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OU Dn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfi V1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488917169"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\50725408-24e6-45c2-beae-ce173f59608b.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):	358744
Entropy (8bit):	6.028713910868493
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\50725408-24e6-45c2-beae-ce173f59608b.tmp	
SSDEEP:	6144:EVCpuN9msDwjWCuG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxins:EVoqmsDRNGNPUZ+w7wJHyEtAW9
MD5:	E3E0D4C380FF8179FDC6A6239E5E1D55
SHA1:	45FFDD425C18DCA1764A82C11A7CEF8C6D863449
SHA-256:	6E47DF7C416FBEA3F22CE7C3CFF8C793769CF509CA0C5E0D62AE4F27867761A0
SHA-512:	F60F1700C2426566A0846828A0FE4E50C17B058C7C44213FCA68C21E61771C4C6111F1D8629BB185EE057ECF6A9304F018B888285E3C22EFB42D26D3A959092D
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":1.611098330850985e+12,"network":1.611065932e+12,"ticks":163802962.0,"uncertainty":4528918.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488917169"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\635cd82d-b6d7-4ef0-b0b6-86c968668c55.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):	367136
Entropy (8bit):	6.05024678432094
Encrypted:	false
SSDEEP:	6144:0VCpuN9msDwjWCuG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxins:0VoqmsDRNGNPUZ+w7wJHyEtAW9
MD5:	3FC719FFFA92ADA8D892DC75826E1029
SHA1:	F343053D87FD70A5770FA85FA5145E9367355B4B
SHA-256:	6F558EDB098C335F3E142B50329FF7F044EC17CC821CE7B1069E7585515EF725
SHA-512:	F4C0A0E1F584B53E3A6D1791BB5E01538DCF110FFFC812082547A048D84F7C9BFE294059D7D2CF81325C4E42EEDE24F8391B637606C9FD04575FCFAD64C0B0A
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":1.611098330850985e+12,"network":1.611065932e+12,"ticks":163802962.0,"uncertainty":4528918.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\654e5574-c7ad-4c63-b300-eafea78d3455.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):	367135
Entropy (8bit):	6.0502468698344565
Encrypted:	false
SSDEEP:	6144:ZVCpuN9msDwjWCuG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxins:ZVoqmsDRNGNPUZ+w7wJHyEtAW9
MD5:	B53F264020FE188D8473EBC2600E425C
SHA1:	DC14C3C247D25F204C10FF993A0994E89ED1DDBD
SHA-256:	E9B732E52496B3F25E633E0E10590FD0D1C527ECECB2E89F0D22F7EA600D81CE
SHA-512:	B8B1B78A2863E2F5FD0E3035253552AF4136C3F7125850FE9E08387131AD28AD22942E06BDDD730634E21AA5C17066FD03AAA26D8BFFAA780E478841D510571B
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":1.611098330850985e+12,"network":1.611065932e+12,"ticks":163802962.0,"uncertainty":4528918.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6555e513-ee92-4bdc-b997-96f82bf7f375.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):	367136
Entropy (8bit):	6.050247040745096
Encrypted:	false
SSDEEP:	6144:eVCpuN9msDwjWCuG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxins:eVoqmsDRNGNPUZ+w7wJHyEtAW9

C:\Users\user\AppData\Local\Google\Chrome\User Data\6555e513-ee92-4bdc-b997-96f82bf7f375.tmp	
MD5:	37D3C1BAB261DE7A308DF2AE5FC6EA96
SHA1:	830DEC7DA6AE76B96F3582917097F384C8D87F4D
SHA-256:	2CB8860EC03DF3CC8BA9CCAF7A3E896AA9A4527CA48BCFC8565989C1F9A99F70
SHA-512:	4C85AD728B64123E995E494B02194AC79D98B00D5BB01B669DB6E11783E94501B206B22044F020A06D2B4307D2C60BE78497BE87FD2CC148B8F86355572CB449
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":1.611098330850985e+12,"network":1.611065932e+12,"ticks":163802962.0,"uncertainty":4528918.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMtttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\90f5ae0f-5d0c-4d1a-8e99-ebb76ea46fcf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	101652
Entropy (8bit):	3.7473637822626755
Encrypted:	false
SSDEEP:	384:3fgF1Bf42fgjLVkq54NZryvdn3mpDiHfAaG5i9rIbRZux3ClWLvTurshmcI643Jt:f+2BNtdM+keXhMrYfHinKB3d2P
MD5:	B76925BC234012E14D35205480C30F53
SHA1:	1DF008482768E05D768DB8924EE3972273AD1BB2
SHA-256:	F2D6CE621CB20708125409A522087ADF0DA53753EB1771FAA498C9F672A24593
SHA-512:	3DB8117B9D45A92203ED7661D656F0DD10F65272856BDA90A36B5DB54360F111F4FB8F63E85CEFEB9FC0BA7BCB9621AE258D31EF0D3BF0B74A1EE7E90215E5E
Malicious:	false
Reputation:	low
Preview:	.....*...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...7/8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000001.dbtmp	
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000002.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1062
Entropy (8bit):	5.7979976976593655
Encrypted:	false
SSDEEP:	24:3qdLqdNB/rUtQpqd3qdqB/rUtq+FlU+FrV8y9gg:3qdLqdNB/rUyqd3qdqB/rUx9Ay/
MD5:	956EE887F16D4EDE2CCD852561D99121
SHA1:	12CBD0DFC77241AAE0C24C96FC9087B8807CC461
SHA-256:	31674B6CE1EA4139F9EFDC641403DD1AA27EE1A2D8189BA50D8869F7C8A130AF
SHA-512:	7914E5D448960BDD505CFEDF186527FE1255DC67D6AD96B245FBF703C4A57D9D7ABE984B8B2AFA8CBABD5F52FD6DB175E7FEE57E6F1282B12323095E86E2EE 0A
Malicious:	false
Reputation:	low
Preview:	..&.....-download,81e32542-ef88-4c06-80bf-6bf8cb8b8bc4.....$81e32542-ef88-4c06-80bf-6bf8cb8b8bc4....."...Ghttps://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv...."Ghttps://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv*.0.B."116-5b8c3461d1d80"J.Wed, 13 Jan 2021 07:41:58 GMTP..Z.text/csvb.text/csvj.....r.....x.....G.e.s.....-download,81e32542-ef88-4c06-80bf-6bf8cb8b8bc4.....$81e32542-ef88-4c06-80bf-6bf8cb8b8bc4....."...Ghttps://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv...."Ghttps://www.covid19-siparadigm.com/bulk_import_template/bulk_import.csv*.0.B."116-5b8c3461d1d80"J.Wed, 13 Jan 2021 07:41:58 GMTP..Z.text/csvb.text/csvj`\...+...C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.D.o.w.n.l.o.a.d.s.\.b.u.l.k._.i.m.p.o.r.t...c.s.v...r`\...+...C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.D.o.w.n.l.o.a.d.s.\.b.u.l.k._.i.m.p.o.r.t...c.s.v...x.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39d66010-e9d3-4e26-a930-346afc9ebe47.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):	24073
Entropy (8bit):	5.533374932916279
Encrypted:	false
SSDEEP:	384:jO9tFLlVTXp1kXqKf/pUZNCgVLH2HfDGrUeHGxHG6nTmAns4i:+LlRp1kXqKf/pUZNCgVLH2HfCrUOGlGl
MD5:	75312E1C35CBC8365297C5DA33C49324
SHA1:	4E31C0D65AC30EF2237175F10826104FFDE86340
SHA-256:	CEC2E91644DE9AAA52EC05F953A67A2344CE7F759054B1345A0BBA4B0D1A43F8
SHA-512:	A05FDF973D16C13F225554583C5CA25A80F16FD64735B1AC3E18C4E42109B1D313EB60FF187448FFC80132F4E82D7CC4FD186FFA24E864EE2E7A0DE5879C032
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":"13255571927871692","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b5facdb-31a7-4891-a848-bbaba79dbb46.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b5facdb-31a7-4891-a848-bbaba79dbb46.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3316
Entropy (8bit):	4.895100276072814
Encrypted:	false
SSDEEP:	48:YALteBdpNntwTXDHz5s/TsERLsXsXsOyKsS3zs0MHl6bsMTkqssd5KWqxsxMHqz6:2lNnOTXDHzEVVfjBGl6zjzKlCGdGmUhS
MD5:	C50DEFA80FCDBFDB4EAA0FAE7930F7DB
SHA1:	8984043B9BA216CAAB62A0D343AFDC1246382628
SHA-256:	3E40B6F561331A2366687A4B130080801C2F0FE6D488280B446E8F94B652F1C1
SHA-512:	E3B2D45BAF63FA2199E788C3D7045E8CF1C7A63CF5446AE93BDD855F679B14A1B7DF885D3A83631012DF1AA277CDCCA6907E7D5A5AE577CEAAF62594F18CA0 2A
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"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},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258163930755727","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258163930762966","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\57156c9a-f8a2-4f7d-8462-2dab1be7df88.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):	1709
Entropy (8bit):	5.599599342618852
Encrypted:	false
SSDEEP:	48:Yc6UUhcovdUokEUoLUoTp+KU9TkUoraUeywU9PhUeSUoU:yUUaoVUolUoLUoTUKU9TkUoraU+U9pUw
MD5:	551C61A89F7E973E7058F0111006332A
SHA1:	AD74A39659B2EC87D87C8E2EFD42ABA5CAF05B4B
SHA-256:	0933CFF2EE8D36348B4CE1821C285C5E314BE2A96EF6900E82903B69C5B16CB4
SHA-512:	668AA2619C3BD9807DAF62BFCF6135C6FB717E8CDEC280D64E3DEBD168576F0ED1E8D5B3D84B309C363D7B8570997AACC442B795D1EC46ACDD72DB495462E BD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1626823161.036503,"host":"RFlsnWZhYYUhthkBPLLnKDkgwkESVHqFwryRmK4ve6o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611098361.036509},{"expiry":1642634362.04191,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611098362.041914},{"expiry":1621984733.465122,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611098333.465127},{"expiry":1642634333.735783,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611098333.735789},{"expiry":1642634347.077709,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\644ccd0b-d376-44b7-b34e-58b7da57c714.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):	5714
Entropy (8bit):	5.1919458347302205
Encrypted:	false
SSDEEP:	96:nBVIpA4dCyIy5aAVuxk0JCKL89kr1fi/cbOTQVuwn:nBV/4RV59g4KKkrBiu
MD5:	4B517C3F3101D43FD9B23FB8C3AC13BA
SHA1:	319D33602532D4FB3763D3606FF16A9AD8154481
SHA-256:	249D6B40DAE83F86A4FF9E5733053F5E9A4DC17B44F08CA7E8E5A20813DA7F83
SHA-512:	4C28F28441F817B83E861B589C1634871AF994331F56154C3FEF65A81A3042E1723ED1A555DDA65D475684536ACB4AAF7A518FA1E765D10B3FD78AF067F97F5A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255571928124502","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","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","1501624"],"daily_received_length":["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\7f70746a-9f30-49fe-b0a0-aad771eb2170.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f70746a-9f30-49fe-b0a0-aad771eb2170.tmp	
Category:	dropped
Size (bytes):	22614
Entropy (8bit):	5.535709931511721
Encrypted:	false
SSDEEP:	384:jO9tFLlVTXp1kXqKf/pUZNCgVLH2HfDGrUqQHGonTmABs4O:+LlRp1kXqKf/pUZNCgVLH2HfCrUdGonQ
MD5:	FB309DAB403E4ABE18A4695A2D7371D1
SHA1:	4C2DE041A336476F65FC6E6B83839D5051F7CA37
SHA-256:	F0289E3BCF07B7B673D32976F462DC0798B5E8B876AF664E434F1D20C90D8C78
SHA-512:	CB33F4D49F1CAC5D1B0E0262BE3F8B3F99E92302218BA4E5F3A56C39AD53C5811809C93B8A988B3070B517BE9EFEDB01E3B242829E1559910A6C183874EB93B B
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13255571927871692","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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):	340
Entropy (8bit):	5.145673679818619
Encrypted:	false
SSDEEP:	6:m0fQwv+q2PN723iKKdK9RXXTZIFUtpBfQwXhZmwPBfQwX1VkwON723iKKdK9RXXH:5mvVa5Kk7XT2FUtpph/Pp75Oa5Kk7XVJ
MD5:	9048F684AD3FD7BCED867DE6F4016F39
SHA1:	701534068933FE90E4CF140DD12FA608606E83A2
SHA-256:	2A0FD6B32BE6E997273C028E5F35423545AEB4754537B7C13CA637D73740E1D9
SHA-512:	AB222757CD0DD7CAE9F80310A88B0C57BE23782953EC9A231C82A9C0F15E17034173A35A3394FB5C222B34BB283D88A13FDC02BBD40F23B1D7DD2E15B97395A 1
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.821 1008 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/ 01/19-15:18:59.823 1008 Recovering log #3.2021/01/19-15:18:59.823 1008 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik eDatabase/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):	324
Entropy (8bit):	5.136599890018571
Encrypted:	false
SSDEEP:	6:m0fQg9+q2PN723iKKdKyDZIFUtpBfQDj3JZmwPBfQGF9VkwON723iKKdKyJLJ:5YvVa5Kk02FUtpps9/Pp35Oa5KkWJ
MD5:	58FFB325BDDB99D4A72E0E91D6614005
SHA1:	B3D10789B6DA16ED55DD16B48CEF8DDC52097CD8
SHA-256:	CA86348BA72BF790A6CF941011AE6AED07A8641F8C9FF221A44654433C1E3653
SHA-512:	5A274C1377368067CD57FF02D4086A910E167DDF4C39F32B91A747D8B2CAA42A5962D456577E92653B7877F2B924FCE61683D5DF35EE8A6A49011A241E68524B
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.815 1588 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/19-15 :18:59.818 1588 Recovering log #3.2021/01/19-15:18:59.819 1588 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\096e1f9b7eb0d642_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.970555647967523
Encrypted:	false
SSDEEP:	6:miYGLiZeEE9OHgE6DgCm1rygrVK6tVuJS9QZ6Ak644+W1rygr4:OMEjZ9bXbHuPUB648XM
MD5:	8CA1A707E94D5E2C4624F521968FB326

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\096e1f9b7eb0d642_0	
SHA1:	9B76C2FC4B873A4B5099100C87F26900E6B50405
SHA-256:	3BCD51444EBD06269004FF29474A4F1C739574698358D59548306460ED225F71
SHA-512:	7A9FB2AA1A0215EB8801286DB4B8F8110670ACB9FDE21287A22CB4223258015370F8E494FB69B86D94A4976C9E415A5A87CA8588B4FB2895BCBE5DFD8A4B60FB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...ym....._keyhttps://www.covid19-siparadigm.com/custom_libraries/google/googleAnalytics.js .https://covid19-siparadigm.com/wm]X../.....Os.|....{q.`.....N-..D...D.A..Eo.....G.....A..Eo.....wm]X../..$..94ADAC47C6C937561890EEB78C4B531D0BA687048CB1F2D925AAC300780C50CC.....Os.|....{q.`.....N-..D...D.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d400fb19bd41030_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.971303934687809
Encrypted:	false
SSDEEP:	6:mszn YGLiYW91IvdTJVbH2XTaJSMSFhI/7K6t35DwWDkOpPd1/O0TAF1MSFhI/JQt:7zSY21wTJVzCMSFhYx5DHj1WJF1MSFhz
MD5:	22C53D20754EAA4D7374AC9B0D526160
SHA1:	D4DE61A7FE9A767C629128D1CB9AF1B78732A8AE
SHA-256:	001A1EF50D0410683DE4F20FAD06CF36054D8F4EEB3F886272AA74E4AFC7F604
SHA-512:	C5B1AEABB8A5575186A5814BE8368B3687AB024D05DFAF55E56546201F9D9CBE99436E7EF12A3B5965A29D2FDCDEDFB347F27A46AC2C466344AE3C28B5F9369
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...;*T....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3 .https://covid19-siparadigm.com/.o4Y../.....".."..dSw.-p.....J.~..#..".f....A..Eo.....,.....A..Eo.....o4Y../.....2A6F5473B73140B84D8B94AFAFEDE53685E01B5EDD9713424B5D721468C97218"..dSw.-p.....J.~..#..".f....A..Eo.....q..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f8167173cfdde1f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16645
Entropy (8bit):	5.775096426183475
Encrypted:	false
SSDEEP:	192:HEN3r2t8wv6fRDgAh0m3jCzl0U0f73GNQy43iiOIe6ZDQvnU+opmXw9ZQAkWd47j:HK6tJoaQ3DJOvbo3QAmeaWghNya
MD5:	EAECEDC0C3AC7253C78823E94936255C
SHA1:	5FCD14EFC7F810512EFAE69D66B2C0FEDDF83CE3
SHA-256:	CA00E1E7E597FC97F3DEC90756BEAAB4D1AE3345CF0406DA5CDE3AE3FC01F0AE
SHA-512:	A0CD5D9E87CB8D41CC3DD5353CD73ED8D786BA10867FFD188C278092B91B9D4BD89D51A3BD8AFF618165C89746A2AD115418934CF955A13ADAA5F3929C107AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....Rd....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3 .https://covid19-siparadigm.com/%o1Y../.....J.....[oK.,....:[c._V...GLg.%i.l.#.A..Eo.....1.....A..Eo.....'.....O....h?.....<.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@.....exports...Q.@*.$.....module....Q.@..k.....define....Qb..4-....amd...Q.@z..Q....Cropper...K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....l`....Da.....e.....`...p...@.....@.-....TP.A.....H...https://www.covid19-siparadigm.com/dore/js/vendor/cropper.min.js?v=1.5.3a.....D`....D`....D`.....E....`....&...&....&.(S....`.....L`.....Rcd.....Qb"C.9....n.....Qb.....h.....Qb..@e....d.....Qb...f....k.....QbJh.....T.....Qb."......W.....QbN.....N.....Qb.....E.....Qb&..b....H.....Qb^.F.....L.....Qb^.....O.....Qb.:.....z...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f85719212f732a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19101
Entropy (8bit):	5.401813987278068
Encrypted:	false
SSDEEP:	384:Wiehqda+leDofZ8YN/uhjVz9WgjtrZCp9D9M2GqO/W6FDXqCFkG2:PEfQNqjVz9VVCROqO+i6p5
MD5:	99DFFBE1FCEB7E30EE0928970EC38BB1
SHA1:	8E3C8103395CE98419112B3AF51C2A5CC37E30CF
SHA-256:	D8163D38FDF36A91AC5197EDA07ECC7A930AFF1F95C7074E31D15B16B83917B8
SHA-512:	D32C9B61A9F093EEB5FD5606F1DE453CEE2ACE97B467210AE0D2FDC7680D0A056987ACDA3953698549E44125D95FD920BB2F2C745894B57D76F7D46BE19791CA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f85719212f732a4_0	
Preview:	0\r..m.....I...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/jquery.validate/jquery.validate.min.js?v=1.5.3 .https://covid19-siparadigm.com/.4Y../..... .....@..k...h..i...Z.;[..XB.....A..Eo.....e.....A..Eo.....'.7_....O.....H...`.....h.....(S.8..`(.....L`.....(S...`.....(L`.....Q.@..k.....de fine....Qb..4-....amd.....`.....M`.....Qcj..T....jquery....Q.@*.$.....module....Q.@.....exports...Q.@...o....require.....Q.@.{.....jQuery....K`....D\| .....s.....&.(.....&.z..%& .^.....?...s../...&.(....$...&....&...&.]...&.]...&.-...%.....&.] vendor/jquery.validate/jquery.validate.min.js?v=1.5.3a.....D`....D`<...D`.....`....&...&....&.(S.!..`.....U.L`.....@Rc.....M....O...Qb..{.....c...b$.....I`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13490cf906b3f6b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	57486
Entropy (8bit):	5.900254968712421
Encrypted:	false
SSDEEP:	1536:hTWKmJVxwDxGupLsM8k5IwJqVomjGTiQg55B:h/CV2D4M8kHgVoDiDB
MD5:	B5C5D6323CB7624D1C5840AD339D0006
SHA1:	2EBF4E057EB6FA9DFDD8776B4109B2E8B6E2D170
SHA-256:	40852A1BB47894FD3C7D8F9C16C060ABCD7A4A934685CE8E870F640005731374
SHA-512:	1A24927E05053A935F51B4FAE232A0086E882A42FAF982FCEAA254D94F0889305AC68EA657E94F6485B7DDACFDA86DF07BE2836FFA72AF83E76252FC5A16B581
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...yI.c...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/bootstrap.bundle.min.js?v=1.5.3 .https://covid19-siparadigm.com/kbPX../.....8..... I.... ....t.1.<..2..R.<..A..Eo.....or@5.....A..Eo.....'..2....O.....L.....(S.<..`4.....L`.....(S...`.....0L`.. ....Q.@V.....exports...Q.@.{.F....module....Qc~.f(....require...Qc.....jquery....Q.@.{Oq....define....Qb.#J.....amd.....`.....M`.....Qb.._.....self..Q.P"......bootstrap.....Q. @.U.....jQuery....K`....D. .....s..$...s.....&....&...&.]...&.^.....G...s.....&.(.....&.z..%&.^.....#%.'.....&.~&.-...'.(...&.^.....(Rc.....I`....Da....t.... ..f.....`...@...P..... .....@.-....`P.q.....Q...https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap.bundle.min.js?v=1.5.3...a.....D`....D`....D`.....`L...&...&....&.(S.....`.3...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e110aee5bf277be_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7103
Entropy (8bit):	5.705805608553843
Encrypted:	false
SSDEEP:	192:/m7YaQRWbU/g2Eaz++wuqgucl7ocfpPbjy:kYahbnoz+EZun7owbO
MD5:	A1C4DE339B1C430C847476EFA6E884AE
SHA1:	84E3C465C40229DE4CFCD18DC79D88BA15A0E99C
SHA-256:	BECA677E8407491D9DE0DB6C8F3C3FB233D23605879FA4795E4827DB125BE6BE
SHA-512:	59D87124615CF46E962F946FF4CA29A54E8F3EAC6C9993C8F20A0144ECB4FCF59345D2DB22B351FE5D2CDEB84A330BFE6FB7623EF4EB0553E2D2DFBB637A2B CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....N....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/perfect-scrollbar.min.js?v=1.5.3 .https://covid19-siparadigm.com/.i1Y../.....9.....*(...q.. m..bQi.H.`..$.q....F.A..Eo.....^W.....A..Eo.....'.rF....O.... ....d.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@.....exports...Q.@*.$.... .module....Q.@..k.....define....Qb..4-....amd...Q.`r.....PerfectScrollbar..K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da..... ...e.....`...p...@.....@.-....`P.q.....R...https://www.covid19-siparadigm.com/dore/js/vendor/perfect-scrollbar.min.js?v=1.5.3..a.....D`....D`(...D`.....a....`....&...&....&.(S....`. .....L`.....Rcx.....4.....Qb.....t.....Qb.%I.....e.....S...Qb..d....r.....QbB.%.....I.....Qb"C.9....n.....Qb.....o.....Qb.,.....s.....M...Qb..{.....c.....Qb.....h.....R....Qb..@e....d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\309cb9bdfb34402c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4129
Entropy (8bit):	5.59259583804122
Encrypted:	false
SSDEEP:	48:W2bT0uVllPCW2KKZyokBZhgwke3CGoaXAPHtSaZhLe9Kp3SKJs2d8XrrTh:W2zpCW2KKyoqgwk+NoYMHQGeUp3SV2dg
MD5:	03ACC9694774275F887EAF0E10973F8D
SHA1:	B8657B086483761FD207FAF47D5E2C8D6DD6887A
SHA-256:	89A7A35F0EDDAA085CAD533BAF50C4525FC56FC7754F7F44C571110014CC03C4
SHA-512:	52E9C23B3934D38AA15ECBA63547AA0E377CFF0D8CAA3E0DD88158060F94D666EB7ECD70F8846F6D3EC6FAFFDF707DF1BE187AB6E9CD2C8D8471F8B8E8867 5F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y...ho4....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3 .https://covid19-siparadigm.com/.k1Y../.....D.....6...c. ....vo.....P!J...).....A..Eo.....A..Eo.....k1Y../.....'.."....O.....~.4.....(S.<..`2.....L`.....(S.A..`:.....L`f....pRc4.....M....O...Qb..{. ....c.....Qb..@e....d.....Qb.%I.....e.....Qb~.....f.....Qb.....h.....S.h$.....I`....Da.....E...(S....Ia`.....@.-....`P.q.....T...https://www.covid19-siparadigm.c om/dore/js/vendor/bootstrap-tagsinput.min.js?v=1.5.3a.....D`....D`,...D`.....`j...&...&....&....&.(S.....Ia.....d.....@.....d.....@.....D&.(S...Ia....+..... .d.....@.....d.....@.....D&.(S.....Ia5...V.....d.....@.....&.(S...Ia`..:.....Q...d.....@.....&.(S.....IaD...~.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33c51cdee04606bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	187880
Entropy (8bit):	5.664950920516537
Encrypted:	false
SSDEEP:	3072:CRLuNK6HpnRMVEyG1r+FYraGUY7jT1KY8PkY36:WCfUK+F5GUYn8Pjq
MD5:	153B7A3C58FCA7C420F4FC7DC9F19A5C
SHA1:	D9C030C60D7C129462AD5BAB0F6592A178458BBD
SHA-256:	DD1563C3D7B25EE3032AC1F7EDA5CAF2413F30936F31639D39952EC225C409A5
SHA-512:	233A28FB1C52B54D3936B79C17877303594AA6AC77F9A79D0123B7E36F2261C3A3C406A1833A1EBCB631B4CC6862B465DC3CDA80625AF30C7E71F979C26A178
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...<].]....DF69C6724371D53BE4D38FC8EEB360197AF4D2685D38381CC37795EB68ABFE11.....'..C....O>... .....E..... .....H.....h.....x.....4..... .....(S.H..`L.....L`.....(S..`p....0L`.....Q.@.. .....exports...Q.@*.$.....module....Q.@...o....require...Q.@..l.....moment....Qcj..T....jquery....Q.@..k.....define....Qb..4-....amd.....`.....M`.....1...Q.P6.....FullCalendar..Q.@ .{.....jQuery....K`....D.!.(.....s..;...s..4...&....&...&.]...&....&...&.]...&.^....&.-...%..x...s.....&.(.....&.z..%&.^.....T...s..4...&....&...&.]...&....&...&.]...&.^....&.-..!%...(..#&.(..%& .^...'&.-..)%.....(Rc.....I`....Da...*.....i+.....`...@...p...0.....@.-....\P.a.....M...https://www.covid19-siparadigm.com/dore/js/vendor/fullcale

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b834dbee20d78d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2717
Entropy (8bit):	5.823311486753731
Encrypted:	false
SSDEEP:	48:YpX49e1W549TW149sWG490WjX49cWC49CWv49VWA49xW+49DWM34947WDf49Z5:TmJnmroSEi4bZ
MD5:	757F75562EDE6A18DEF40551F62BBC5F
SHA1:	79B7F05226CDCF40F342070139976AD0DA867B78
SHA-256:	CA44207BCA5A2593D786FE8D7D463FD7A3AC156826C05BE41E6AE52B706C488E
SHA-512:	6C9436B8DE7DB7438535FD8DAF52279251FB37A551E759BDB68E0EBD64FD53DF3B6F66A2E764B249E2C1E2801A4A695A4FFABF2A3FF181B2ED7713146FEE950C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...%2P....._keyhttps://connect.facebook.net/signals/config/3692194074184385?v=2.9.32&r=stable .https://covid19-siparadigm.com/y.`X../.....O..... (.Q,..sf..H$...=..R.X4..,.A..Eo..... .....A..Eo.....0\r..m.....s...%2P....._keyhttps://connect.facebook.net/signals/config/3692194074184385?v=2.9.32&r=stable .https://covid19-siparadigm.com/K..X../.....O.....(.Q,..sf..H$...=..R.X4..,.A..Eo.....,.....A..Eo.....0\r..m.....s...%2P....._keyhttps://connect.facebook.net/signals/config/3692194074184385?v=2.9.32&r=stable .https://covid19-siparadigm.com/..3Y../.....O.....(.Q,..sf..H$...=..R.X4..,.A..Eo....."".....A..Eo.....0\r..m.....s...%2P....._keyhttps://connect.facebook.net/signals/config/3692194074184385?v=2.9.32&r=stable .https://covid19-siparadigm.com/ ..Y../.....?.....O..... (.Q,..sf..H$...=..R.X4..,.A..Eo.....j.....A..Eo.....0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b88956e8fa6bdcd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4390
Entropy (8bit):	5.723687697606077
Encrypted:	false
SSDEEP:	96:q2rP76IY2aGrszY7xECqK5Isy2yHDfg+mGWjN:f76I7HKkEIN
MD5:	16CA76DDEBC33FC0239DEECD11B2E0D1
SHA1:	7F61130917984F9F6EEA28BD99616F39433666F7
SHA-256:	B2ECBC7844BE0BE035A1B224D6F253B36A071C78E78FD5E550BD69F6164AFA69
SHA-512:	8958030A71E193AB800A31581EF3494C89BCB0661F0853C546732FFD73F2954048335FE528BCC1DF5876906D3A157431FC0D59F6A95D5D1C4C193DDFBA220D13
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3 .https://covid19-siparadigm.com/.i1Y../.....:.....r..U...n.. .JB.....Z..8.t?.>.[.A..Eo.....!R.....A..Eo.....i1Y../.....'.....O.....q.Z.....(S.8..`(.....L`.....(S.l.`.....$L`.....Q.@..k.....define....Qb..4- ....amd.....`.....M`.....Qcj..T....jquery....Q.@.....exports...Qc...o....require.....Q.@.{.....jQuery....K`....Du.....s.....&.(.....&.z..%&.^.....$...s.'.....&...&.].....&.]..... (Rc.....I`....Da.....e.....P.....@.-....`P.q.....Q...https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-notify.min.js?v=1.5.3...a.....D`....D`*.. .D`.....`>...&...&....&.(S..`P.....L`>....@Rc.....Qb.....t.....Qb.%l.....e.....Qb.,.....s...b$.....I`....Da....p?...(S.....la.....q.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f6da823cbffbfab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f6da823cbffbfab_0	
Entropy (8bit):	5.606621290739067
Encrypted:	false
SSDEEP:	6:mFYGLiYW917b//PdTJVbHr/JBVTP43bK6t:3Y21fHdTJVzvdGN
MD5:	A0D98B12CE9B006983F6E46AA8C2B5C6
SHA1:	8939DBB305A1B27512339CFDA04FEB0D3B9AB38F
SHA-256:	7E984DF620C9D51EC6A293A6D3D512B482708884A52DBDCD1F17B3436FAD5ACD
SHA-512:	181AA63A002DA0EF4AB73DF8FCEB30DD37048B3936EF6B968F6A68F287455AE9BD17F9BE682E422627A1367590219A826FC1F77263139C7816428A67DEE53A8D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r.....K....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/owl.carousel.min.js?v=1.5.3 .https://covid19-siparadigm.com/.{4Y../.....~..M.c..VFLI V.^.bl.>^.b.....A..Eo.....3b.n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\44fe39ce09791f8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.994561374824214
Encrypted:	false
SSDEEP:	6:m4YGLiYW91MPTJVbHdZ9/hFJfc/Ux/YhK6tMR86wDT2oqlWZocjLFJfc/Ux/6R:cY21MPTJVzb9H1PxsGRrwDColjR1PxK
MD5:	1B424E0D2651E9959F745196143CE2B5
SHA1:	7E2C6FBD43C5841F1462EA726D3C81732D9538D6
SHA-256:	220DA75EE934C9D1B6DB2B9206514B58C662ED9C6C2C8C80CDE3DFAF0157C578
SHA-512:	59852E06FC3F9ADEF2D74AF2F6E5767741E50B9016B4D83F88E5CFD9AAAEEBE5C8917EA98DFDCD38F99AB39F1DBDF0ED5DFDED4472FCB92D697BBC543640 301
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...9.G...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/fullcalendar.min.js?v=1.5.3 .https://covid19-siparadigm.com/.4Y../.....<.....5cb.....-s! =..4P...8.~+q...A..Eo.....a'.....A..Eo.....4Y../.@...DF69C6724371D53BE4D38FC8EEB360197AF4D2685D38381CC37795EB68ABFE11....5cb.....-s!=..4P. ..8.~+q...A..Eo.....%.?'L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5058f561f02561cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	948
Entropy (8bit):	5.226596076882446
Encrypted:	false
SSDEEP:	12:l6blIaL40zlfJjFcIc0jBFGcg41YO3of8FNXmUS/YEO3ltFKCUi0enmJne/lJFLN:m1Jp/jBkcgqY0Dm5AE2oq5/lPmVroA9+
MD5:	D23467D9C42410F15BEF59BCB5BFCD88
SHA1:	0E79B2CC60D6AA26DBE5EB8753D2132F776D886F
SHA-256:	DC598C66BC5B4ED298270B93F791D802FF1DDB629546495E2160ADFB96F5ED5A
SHA-512:	CBC6AB5F5F94B90AB3689BC0188A682828E4ABBEB0D7377E27530B15AA819A34392013718CB634B888B15EA9BD8C7ED35CEA39375E654AF58793D9ECF7F9158 B
Malicious:	false
Reputation:	low
Preview:	}o1Y../.p.....'.[.....O....0...+.{.....(S.L..`P.....L`.....(S.....5.a.....a..... Qfb.....selectFromLibrary...a....V.....~q..... ...."...."..$....$.%....%.'....'.(....).)....).*....*.*.....+.....d.....d.....!."....d.....$.%.....d.....&.&.....d.....'.(.....IE.@.-....dP.....V...https://www.covid19-sipa radigm.com/dore/js/dore-plugins/select.from.library.js?v=1.5.3..a.....D`....D`4...D`.....d...`....&...&..A...D&.(S.....a.....a.....a.....a.....Qb.4BK....fn.....a.....az...Y .....d.....+.,.... ...IE....d.....D`....DI]d.....1...K`....Dm.....&.....-.....&.(...&.....&.-...'..%.....$Rc.....`.....Ib.....,.....c.....P.....d..... .qN .....`M.h.,.[..f....^...A..Eo.....|.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5070c80b4ccf8e9e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2150
Entropy (8bit):	5.635742276678037
Encrypted:	false
SSDEEP:	48:BvKpqULvKenLvKMBLvKVpLLvKkbLvKXuLvKTaLvKKPLvK+3LvKjj1:BvyvZvhvavDv9vNvVv1v
MD5:	8AA0CBA0576D20B4D5A73F291CA9DD43
SHA1:	BAF0BA86BCF2FFB3C7ADD6DB11FB4E1369E9F9AB
SHA-256:	3597A62E1B6810A55E6447DE9EE4AAA82614790799C062A8E27F1451C23EC71B
SHA-512:	A4B417FD3C1574D85DEC9E35189D2EDB4AD6E8AB88BF3616EA825AFADF776AF60BA2F0A8D579C2D940D167F7B03B40FEE3521E3871A40DA8B376DDD840488 73

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5070c80b4ccf8e9e_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...@....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://covid19-siparadigm.com/...X../.....y.....F.0.?....f...n.;..h}.>...5.0.A..Eo..... ..A..Eo.....0\r..m.....S...@....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://covid19-siparadigm.com/.0Y../.....F.0.?....f...n.;..h}.>...5. 0.A..Eo.....r.....A..Eo.....0\r..m.....S...@....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://covid19-siparadigm.com/.w.Y../.....m.....F.0 .?....f...n.;..h}.>...5.0.A..Eo.....>.....A..Eo.....0\r..m.....S...@....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://covid19-siparadigm.com/V..Y../... .....".....F.0.?....f...n.;..h}.>...5.0.A..Eo.....V.O.....A..Eo.....0\r..m.....S...@....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://covid19- siparadigm.com/..Z../.....T.....F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5715a7ebf0b01a60_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29358
Entropy (8bit):	5.951379760880098
Encrypted:	false
SSDEEP:	384:6vU+2hxoKwGmg38RxL1B65XJ2zmNpNw8uHVi7eQ7TcJ0dfzacgYZVCSeYV:6M+2PoKgS8Rh1BeWm/bY0d7abScSh
MD5:	9D2E0CB3778BDF3B90BBCEAC316DB8F2
SHA1:	9D0C371BD352E2E09B6D79AA1C3B604D00939A30
SHA-256:	F9166A38A26F449E7BEF8560F5AD5E5AB5ABFF203BAF36687109AFF8AEF16197
SHA-512:	44991CC2D38C1447F3B818F09409F181DA6F58F7985C29A071CBE5E98B1675EA3EA90D1A6BB555228716F4BE2D9A7A0C95A5B57EC15B5F29A8048B1C1A275EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....L....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3 .https://covid19-siparadigm.com/.n1Y../.....B.....3wU.y.. .>N..FE3.X.?..._...1...A..Eo.....x.....A..Eo.....'.....O.....q...#.....\.....(S.a...`x....-.L`.....TL`&....(S.....Ia0.....(Qh..J.. ..._possibleConstructorReturn..E.@.-....XP.Q....I...https://www.covid19-siparadigm.com/dore/js/vendor/dropzone.min.js?v=1.5.3...a.....D`....D`....D`.....]....`....&...&..!.&.(S ...`.....4L`.....DQo...W8...Super expression must either be null or a function, not .....Qc.....create.....a.....Q.C.,.a.....C...H...G.E.G...U.....K`....D.a.0..... .%.s...%.....&...&.%.R4..&.%.e.....&.(...&.%.'....(...&.}...&.}..)&.%./...%./...Z.....-...%..(...&.(.....&.(...&.Z.....%.-...%.....(Rc.....Qd.<.o...._inherits...`....Da..... ..f..... <.....&....`...`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c180cd76b238e73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7354
Entropy (8bit):	5.644510331087169
Encrypted:	false
SSDEEP:	96:828WiWQOPV28W6SS+9KIhjfHp+it9qte4RJ7GYHKGzVS0fKemHIFNfr5AyWN:rZQX19KIBd9aJ5VSmP7fr5AJN
MD5:	D0EC5694B110C49E9C4263F2BD86D080
SHA1:	3BCA18AE8D3005A8133B567F16031FE5BF3AE223
SHA-256:	E793FE57BCBEFDCCD167CAFFA8FA83BFF51E6BA4BA1376C440B19D3FFEBD5941
SHA-512:	3EA6C247BACCFAA78CAB89036B1563355989DEC359E71EF5FE0DEB4FCB663989C93DEBA7A86453628169A4197FB831E3E3B5D08B887FA3159B4A8C4803B4CCA0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r.....@....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/typeahead.bundle.js?v=1.5.3 .https://covid19-siparadigm.com/.j1Y../.....K.....^...h.ED/..*. ....; .8Q.....A..Eo.....A..Eo.....'.e2....O.... .....m.....(S.<..`4.....L`.....(S...`.....0L`.....0Rc.....QcJ/^W....factory.`....I`....Da.... <.....Q.@*.$.....module....Q.@.....exports...Qc...o....require...Qcj..T....jquery....Q.@..k.....define....Qb..4-....amd.....`.....M`.....(S.....Ia.....I.....@.-....\P.a.....M...ht tps://www.covid19-siparadigm.com/dore/js/vendor/typeahead.bundle.js?v=1.5.3...a.....D`....D`2...D`.....``...&...&....&....&.(S.....`.....e.L`.....@Rc.....Qd.....Typ eahead.....Qb..E.....old.b$.....I`....DaX....d...(S.....q.aS...?.....q.....d.....@.....a.....Q.C..Qd.S<.....setDefault..C..Q.@.. K....select..C..Qc...i....updater.C..Qd..... ..s

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6edbfff5c06531e4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6419
Entropy (8bit):	5.598362019429096
Encrypted:	false
SSDEEP:	96:i2hMHRVXd42hAEnr3dbYOeS2EyAP+TuJEePkIQ4MlKgW3oFs6V99xY8X:FMrXdP7nr3dbYtEVP96esIQ4zroVN5
MD5:	F52260512F2D1B3444FF1DA488602DB8
SHA1:	076EAD1A39DF1D8535211CCB07148149D4BD20CC
SHA-256:	8BECC04EA9813BBB3C124734D62FFE908FD02DA52B8A5CE8E02BC122560D4D54
SHA-512:	5E674C882DF13739B687858A9A27E0EA07922E6E603174B1B9B37895D6E98FC8406C507F94CA5F940D1DF8E97A2A0A64073466D0220BF8B34CBE3BD581069033
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6edbfff5c06531e4_0	
Preview:	0\r..m.....{....w!3...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/chartjs-plugin-datalabels.js?v=1.5.3 .https://covid19-siparadigm.com/.e4Y../.....tZ&.&.....[$s...L....p.n.o.A..Eo.....A..Eo.....'..!....O....p...1.kg.....P.....(S.<..`4.....L`.....(S.x.`.....(L`.....Q.@.....exports...Q.@*.$.....module....Q.@...o....require...Qc..Z.....chart.js..Q.@..k.....define....Qb..4-....amd.....`.....M`.....Q.@..:....Chart.....K`....Dx.....s.....s.....&...&.]...&.]....0...s.....&.(.....&.z..%&.^.....(...&.].....(Rc.....I`....Da....2.....e.....`...p...0.....@.-....dP.....V...https://www.covid19-siparadigm.com/dore/js/vendor/chartjs-plugin-datalabels.js?v=1.5.3..a.....D`....D`6...D`.....`L...&...&....&.(S.=..`4....9.L`.....RcP..... .....QbB.%.....I.....S...Qb..d....r.....R....Qb..@e....d.....Qb.,.....s.....Qb...~....v.....O

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7355060daeeb1408_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18678
Entropy (8bit):	5.790963212971315
Encrypted:	false
SSDEEP:	384:bTZQmXU6Dr/ALXl76y+fqpDPKOzF7RqZMlZ2vIl:fymE6Dr/qXlWyggDPKOZ7RqZMTYa
MD5:	5D0111B4800C0B37059E151C00E908F6
SHA1:	E6EB7A4C1A54F1C71E2C4107E2071FF7E4FC2E7F
SHA-256:	F5494A1170A291CF30D01D4348BCDC4288B1E6B056B0ED19AB0BF58B06C9B2DB
SHA-512:	F4009C10D0E74CB50B2FEF330FFABACBCB6B311284503D94EE20E8739BB460A321A282D4D66468721EC2CB296201CA670483ACB869521987F5ED1D3092E090A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....y.$...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-datepicker.js?v=1.5.3 .https://covid19-siparadigm.com/.j1Y../.....@.....h..k.C..&oZ&w.....X[F./...>..3.A..Eo.....@.....A..Eo.....'.....O....HG..._GR.....(S.8..`&.....L`.....(S.p.`.....$L`.....Q.@..k.....define....Qb..4-....amd.....`.....M`.....Qcj..T....jquery....Q.@.....exports...Qc...o....require.....Q.@.{.....jQuery....K`....Dv.....s.....&.(.....&.z..%&.^.....'...s.....&...&.]...&.]....&.].....(Rc.....I`....Da....T.....e.....P.....@.-....`P.q.....Q...https://www.covid19-siparadigm.com/dore/js/vendor/bootstrap-datepicker.js?v=1.5.3...a.....D`..D`....D`.....-....`....&...&....&.(S.)..`.....y.L`.....RcT.....".....Qc.[.....UTCDate...Qc2,nc....UTCToday..Qd."......isUTCEquals...Qdru.....isValidDate...Qd.~.....DateArray...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80754dd448f8c9bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.905370372135123
Encrypted:	false
SSDEEP:	6:mz9YGLiYW918NSlYTJVbHky+llgbjsvRK6tZ90gWcF2nLfUYttxbjsnl:fY213lYTJVzk8MvigM9zx2
MD5:	081D5C151D0D2B201FFE129AD366D346
SHA1:	C6DD006B29EB3F470ABD308C31CFB3B8BE6DB63C
SHA-256:	04A8E8A024032962C87389BE52839855636C89AAB02D28D047C6284E496B6408
SHA-512:	97F42396963854723740369425 0BBC310D9182C7F72F98332DF52C113EF3691CD6970C174F4C4F888C843CEF30F0B888A56CED8A4205A43A3B9007C4E738CE13
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....C-....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3 .https://covid19-siparadigm.com/.VX../.....Z... ....#2.....K...5/N...N.-FW.A..Eo.....$G.....A..Eo.....VX../..x..2D4A001FAC82E20BA3FD0EAB38AB13C23AECAFD24448E858BC951CD8C6590D72Z... ....#2.....K...5/N...N.-FW.A..Eo.....UL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9acb17b07b2d71aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	117400
Entropy (8bit):	5.810149319474973
Encrypted:	false
SSDEEP:	3072:X5+hb05FS63uNxiWJdSbZ7XbxSCbUfljDSj:BFj3Sjd8RXblj
MD5:	0DF114FC78EAC47361F95FF767EFF6B5
SHA1:	6778B0D43008B388084D44D1785B0432D9AF7DDC
SHA-256:	B47C2391D0273E5A1668F4B2D70D3CEE52E245A19E5769806EDF90B76ED8DFC5
SHA-512:	F56F989669E381CAE66630C9BFAB019DEB595405B89C77285F0F4FCD327058394538FE9AE023F35C66B495967FF28F132B597EA1D5CFE601D8F6CD7A3FC097F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....i.....2A6F5473B73140B84D8B94AFAFEDE53685E01B5EDD9713424B5D721468C97218.....'.h)....O*... ...R..... .....x..... .....H.....(S.)...`.....L`@....(S..`.....4L`.....0Rc.....Qb.....h...`$...l`....Dal.....Q.@..k.....define. ...Qb..4-....amd.....`.....M`.....Qcj..T....jquery...(S.....Ia.....I.....@.-....XP.Q.....K...https://www.covid19-siparadigm.com/dore/js/vendor/datatables.min.js?v=1.5.3.a.....D`....D`....D`.....`....&...&..a.&..A.&...(S.....5.a.....a.....a.....Q....a.....a.....Q.@*.$.....module....Pc.....exportsaN.....I.....!.d.....&.(S...y...`.....L`.....Rc<.....Qb...f....k.....Qb. .....G.....Qb.....E.....QbN.).....X.....QbV2.0....I.....Qbr0.)....Ca....Qb.oA.....db....Qb.,Z....eb....QbZF.R....fb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae1ae1891fb3d2d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae1ae1891fb3d2d1_0	
File Type:	data
Category:	dropped
Size (bytes):	2738
Entropy (8bit):	5.999251017345734
Encrypted:	false
SSDEEP:	48:zpl9ldwJTYApeuwpiMVRpbRTs+CKRr2xN4v6hlaMnA1wMP4oLP:zp0JTvpXSP9IMr+N66vA1wMw8P
MD5:	CBEA26479DC4732603DC290A12D5034B
SHA1:	450E49019C532829ACA2BB743C273D636F88C46D
SHA-256:	D727F6910A2A8F0147545F2327AE2F1BCCCF4C652AB4EB2D626A236AB37CA6D4
SHA-512:	14F6ABF1EC53443524ED260482F9C9F66509750AEB5B9EBA35A33DF01EC78371F773741AF7056CCA2A1427E05926E03C42DE59EC5B9BB5D9665A2A5DE292F87
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...>* s...._keyhttps://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3 .https://covid19-siparadigm.com/..VX../.....).)....{..UZo.q...^...Um.L. A..Eo.....q.....A..Eo.....VX../.....'.....O....H....i.....(S.@..`<.....L`.....L`.....(S...`.....XL`(....0Rc.....Qc..A.....callback`.....QdF Ea.....loadStyle...`....DaP.....Qc.J.....document..Qd.A.....styleSheets..M...rT.. QfB.-....getElementsByTagName..Qb.Xr....head..Qeb..G....createElement.....Qb.7.G.. ..link..Q.P6.:;....stylesheet....Qb.....rel...Q.@.....text/css....(S.....Pd.....link.onload.a....3...I..A..@.-....LP.!.....=...https://www.covid19-siparadigm.com/dore/js/scripts.js?v=1.5.3...a.....D`....D`....D`.....(...`....&...&..1.&....&.(S....`....hL`0....HRc .....QdZs.=....direction.....Qc.{b....radius...$QgZ..:....onStyleCompleteDelayed..c$..... .....I`....Da6.....(S.....lay.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6971dcab2beb1fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7408
Entropy (8bit):	5.459982066966103
Encrypted:	false
SSDEEP:	96:02oeQh072ICWV59RZz94yhfnvjaIWsWSD92r7QzBsS1jSunBAIfk:OeZmWVr77t+Itf0r7QzuS1BBBk
MD5:	8B19259DD7E3B5B64DF62E54047DC00D
SHA1:	5675E1827D15D5B32028772CDA167B6C3D26D49D
SHA-256:	AF3592A4C24FBDD91403A170DC21F31B368648F5EC77AD50B660DDF76BEC7C7B
SHA-512:	518D414D1005FD5235F8D159A9290D458DA4EC1923C5216D88ACD06ACBA6FA61B8746BE10633ACE6B95DFE8613122F97B9611463905D2EA4A2EC670AED89D81
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....G.X...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3 .https://covid19-siparadigm.com/.i1Y../.....F.....N.^...w:+.....Aj. .u..h;B.A..Eo.....f.....A..Eo.....'.(V....O....X....4.....0.....(S.8..`(....L`.....(S.p.`..... L`.....Q.@..k.....define....Qb..4-....amd...Q.@.....e xports...Q.@*.$.....module....Qc.-.2....window....Q.P.M.s....noUiSlider....K`....Dv.....s.....&.(.....&.|.&.^.....+...s.....&.\..&.-...%.....&.\..&.-...%.....(Rc.....I`... .Dav...h.....e.....P.....@.-....XP.Q.....K...https://www.covid19-siparadigm.com/dore/js/vendor/nouislider.min.js?v=1.5.3.a.....D`....D`....D`.....i....`0...&...&....&.(S.. ..`.....=.L`.....Rc.....j.....M....O...Qb..{....c.....Qb..@e....d.....Qb.%I.....e.....Qb~.....f.....Qb.....h.....S...Qb.....j....Qb...f....k.....QbB.%.....l.....Qb2.....m.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b774c64f3d731ee5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9594
Entropy (8bit):	5.781549012955561
Encrypted:	false
SSDEEP:	192:Qq8U69alOpIDaXix7SQU6UFkV2eFSj+hK+h2enmmFoPPtAdIPL:Q7T9uOpIDacSVelSiK+oemwWAdIPL
MD5:	D722C506E764AD2D17776DB1E856D16A
SHA1:	A0AEE04E43267E344CB742BE20C503EA13880787
SHA-256:	E0F4ED9CD1D5561F5F81C0E24C2488B4029970A507891180E0E8E9F77E5BE829
SHA-512:	CC3B2F9B1F8869F0FA21081AABD61D6F23F467F60536EFB16B819260E760066731D0C8932A5FC101823BD9DAADA26CB630CB5A86E2FB35F4D0610B0E47281E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....s./...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3 .https://covid19-siparadigm.com/..4Y../.....C.o_.3..y..HZ.('..J>6;p-f&...A..Eo.....7.....A..Eo.....'.2.....O.....#....j.....@.....(S.8..`&.....L`.....(S.p.`..... L`.....Q.@..k.....define....Qb..4-....amd...Q.@*.$.....modu le....Q.@.....exports...Qc.-.2....window....Q.@RrP.....Sortable..K`....Dv.....s.....&.(.....&.]....0...s.....&.(...s.....&.\..-.....&.\..-.....(Rc.....Qez.....s ortableModule..`....Da.....e.....P...`.....@.-....TP.A.....E...https://www.covid19-siparadigm.com/dore/js/vendor/Sortable.js?v=1.5.3...a.....D`....D`....D`.....`.... &...&....&.(S.!..`.....L`.....Rc.....x.....Qcv..7....dragEl....Qc..7.....parentEl..Qc.@N.....ghostEl...Qc.(/.....cloneEl...Qc.76S....rootEl....Qc.*:.....nextEl....Qd...M....lastDo wnEl....Qc.?/L..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bead25964382b68f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202528
Entropy (8bit):	5.634914580006736

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bead25964382b68f_0	
Encrypted:	false
SSDEEP:	3072:Aza242h7WisVTwltIMVr7DAGZv9BCQ6iBS9ENF:GoOJsVElmOAoVBdrS9Er
MD5:	419451BBD47AAAFAB8244D3F95937D91
SHA1:	2883E12D517A887540B6A26E8AA40761842CF56F
SHA-256:	C38D8824CAC44FB2856DC58BDFC62ACAFB9B3897B745817EC8CA41DF645A8728
SHA-512:	F9BF5DB08446E5E259891AD14AB04D0800B07BAEB35AD3D6573957857F488634728A0D911E8226E877222B78FA8933080BB3ED1F487E1FCA1C75D37603506F7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....':....89F51944D0CA34E09756755EFA5A35764141BA89BB64487B4A4A96FC8DECBDDF.....'..8....OA...H...;17:.....(.....$.....H.....(.....t...\|.....(S.8..`(.....L`.....(S...`.....(L`.....Q.@.....exports...Q.@*.$.....module....Q.@..k.....define....Qb..4-....amd...Qc.-.2....window.....Qb*%.R....self..Q.@...:....Chart.....K`....D.....s.....s.....&.\..-....S...s.....&.(.....&.|.&.^.....1...s.....s.....s.....%.&.\..-..!.....,Rd.....I`....Da.....$..g#.....`...p...0.....@.-....\P.a.....M...https://www.covid19-siparadigm.com/dore/js/vendor/Chart.bundle.min.js?v=1.5.3...a.....D`....D`....D`.....`p...&...&....&...(S....`t.....L`.....(S.x.`.....L`.....PRc$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb4433fb907e1cce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96424
Entropy (8bit):	5.826126893566232
Encrypted:	false
SSDEEP:	1536:Xyp1jLsZbR5XTNozFnugbobEDpIjgoEkFnw5O4u:5Vv6nugf1SgUFnw5OV
MD5:	3283FFA3A0A0B8D6A4C42EE94317AFAA
SHA1:	4EBF6E030F2167E170C539A23291330B6ACA10B2
SHA-256:	3D3D56EC212EB7DD16A04E8803C3807F6050EFF7267C7E14A25A4509A81486E0
SHA-512:	96A9FC52EFBB26FC59B71EC533659F061BB9F35B14EFFD249EAA51F118340C549B52E15471751EBCD114B522E8BE01342CECD08125F78A75122EEBF24CC9CC57
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...b..`....2D4A001FAC82E20BA3FD0EAB38AB13C23AECAFD24448E858BC951CD8C6590D72.....'..S....O!...Pw....7e.....H#.....,.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb..i.....t...`....I`....Da....j.....Q.@.{.F....module....QcV.....exports..Qc.J.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....\P.a.....M...https://www.covid19-siparadigm.com/dore/js/vendor/jquery-3.3.1.min.js?v=1.5.3...a.....D`....D`....D`.....Y....`....&...&..!.&....&.(S...I#..`FF.....L`.....Rct.....2.....Qb..W....e.....Qb".b....r.....S...QbBO.....o.....M...Qb.....s.....R....Qb&.....l.....Qb&.....c.....Qb.o.....f.....Qb.....p.....Qb.-Z%....d.....Qbn.R.....h.....Qb.....y.....Qbf.....v.....Qb...k....m.....Qb."..... x.....Qb.....w..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc19588327582ba6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	49148
Entropy (8bit):	5.9626171878292595
Encrypted:	false
SSDEEP:	768:XA9QwFYnHouXuSIHI0ty3fCcEm0GAc4FcDm/FyXdjIsY6Lf:XgYHou90InqcEtGuFcDSbAf
MD5:	C48B111A9780A805074672796A3CDCFF
SHA1:	D405320120019FD5B998E3D7C94F3042963DF6F4
SHA-256:	AC319F9A4D8B238BAC304CAE6DD1D6F01CAC25D97052827B8552B581EF9BEF29
SHA-512:	C7B8D9477428B93D3A51891D5D2D1B6A956A86DDA6B387F9DF349FDF2D0B4DDD825042D198BDEE86FAE44C296B316EC89BF6129E1559280E3A9889A591A137AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....F.K...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/moment.min.js?v=1.5.3 .https://covid19-siparadigm.com/a|SX../.....V?..3../..Qk.b*8.^.....C"...A..Eo.....D.....A..Eo.....'.....O....8....{>.....$.....T.....(S.<..`4....L`.....(S.l.`.....L`.....Q.@V.....exports...Q.@.{.F....module....Q.@.{Oq....define....Qb.#J.....amd...Q.@...C....moment....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....I`....Da....(.....e.....`...p...@.....@.-....TP.A.....G...https://www.covid19-siparadigm.com/dore/js/vendor/moment.min.js?v=1.5.3.a.....D`....D`....D`.....`\|...&...&....&.(S....$.`.G.....%.L`.....y.Rc8.....Qb..W....e.....Qb..i.....t.....Qb^..}....n.....Qb.....s.....S...Qb"..b....r.....M...QbBO.....o.....R....Qb&.....l.....Qb.-Z%....d.....Qbn.R.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cffccb8fdc29a204_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2140
Entropy (8bit):	5.622560920606455
Encrypted:	false
SSDEEP:	48:iL8coL8BfoLF11oL8oLGoL1oL6AoLLoL2poLb:iLwL8BgLFMLZLHLSLgLcLLL
MD5:	1B6A8329377603B711C0509EE802DA94
SHA1:	1B9911F1ACAE66A27C13CC9922ADF53E22D64AC6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cffccb8fdc29a204_0	
SHA-256:	D273CD4F3E14D72445EE2C3268EA3E7CA32A177F8FC7457953B96E4AFAC49F2C
SHA-512:	394307D6A5E92C31D48C8FE80F89EF7649FBE8AD66E95223249E837196579A268788E7216024DDAEF298EB9EDDF80549CB9B5D2C2714609599B5BACD6DA735B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....!U...._keyhttps://www.google-analytics.com/analytics.js .https://covid19-siparadigm.com/.8cX../.....;.....Y."Z.g....@..&Y.'.4j...vF...A..Eo.....D..@....A..Eo.....0\r..m.....R....!U...._keyhttps://www.google-analytics.com/analytics.js .https://covid19-siparadigm.com/...X../.....Y."Z.g....@..&Y.'.4j...vF...A..Eo.....t.....A..Eo.....0\r..m.....R....!U...._keyhttps://www.google-analytics.com/analytics.js .https://covid19-siparadigm.com/Z.3Y../.....Y."Z.g....@..&Y.'.4j...vF...A..Eo.....*.....A..Eo.....0\r..m.....R....!U...._keyhttps://www.google-analytics.com/analytics.js .https://covid19-siparadigm.com/...Y../.....Y."Z.g....@..&Y.'.4j...vF...A..Eo.....8H.-.....A..Eo.....0\r..m.....R....!U...._keyhttps://www.google-analytics.com/analytics.js .https://covid19-siparadigm.com/...Z../.....c.....Y."Z.g...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d629d47e5b296288_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26897
Entropy (8bit):	5.632150240246757
Encrypted:	false
SSDEEP:	768:y9hX3Y5DG58YIbQqjusRk6k8vBQUZcpKnv08BZyA5jUWG:y9hX3Y5DG58YIbQqjusRk6rvBQUZcpK6
MD5:	9650310175892FA7512E72D58716CBFC
SHA1:	5679E4FDA5EB67E8509743D01DE097348C77BB41
SHA-256:	BC01C1978C7BDC6BF40AC6B2BBF811CDC896EECCF502629C208D87AC019C7824
SHA-512:	F01A1278BB599B33CD293FBF87012893ED714EF0AF39EA51061135FB7FB7EFF40AE6CF62BB7808DD94FF2CCBCF7B298C15F5BC62BF888ABF7D654DA7DDFF46 82
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3 .https://covid19-siparadigm.com/zm4Y../.....;=T.).VW.fY..c...{.^..3*DX..0....A..Eo.....ad.....A..Eo.....'..W....O....`g.....(S.8..`(.....L`.....(S...`.....(L`.....Q.@.....exports...Q.@*.$.....module....Q.@..k.....define....Qb..4-....amd...Qc.-.2....window.....Qb*%.R....self..Q.P.....ProgressBar...K`....D.....s.....s.....&.\..-....S...s.....&.(.....&.|.&.^.....1...s.....s.....s.....%.&.\..-..!.....,Rd.....I`....Da....4....$..g#.....`...p...0.....@.-....XP.Q.....L...https://www.covid19-siparadigm.com/dore/js/vendor/progressbar.min.js?v=1.5.3a.....D`....D`8...D`.....`r...&...&....&.(S.U..`d....`L`,....0Rc.....M.`....I`....DaF.....(S.x.`.....L`.....TRc&.....Qb..@e....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3a093248cd06e5f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64396
Entropy (8bit):	5.7264134983707775
Encrypted:	false
SSDEEP:	1536:yfpbhUw3zTqfrPSlH/pGEVmRo5HGMlbnUaPVXXWs6e:6X3yIH/pGEvmMlzUaPZX/n
MD5:	17275F664457F0FDAD1411714F87C706
SHA1:	970EA364E3EE7BE256E767C48369AF7965071468
SHA-256:	2F025F422950B36E1E7B748CB198C1CD133FCBC5AD7D2A8830DDECB97CF43DC1
SHA-512:	DF6F1F2313E74BA70A2D48925F3C828297B5ECF9E1C3E280046C5F1C5AC14132D24E194C1EE04BB8B132C0C8903345B85B5FC29671AFD9EFC9E0B9F63ACB54B E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...g....._keyhttps://www.covid19-siparadigm.com/custom_libraries/select2/select2.full.min.js?v=1.5.3 .https://covid19-siparadigm.com/.Q4Y../.....E.....\..8...qE..5).BD;.W.H..).H$.O.A..Eo.....A..Eo.....'..-....O.....S%.....8.....h...\.....(S.8..`(.....L`.....(S...`.....(L`.....0Rc.....Qb"C.9....n...`$...I`....Da.....Q.@..k.....define....Qb..4-....amd.....`.....M`.....Qcj..T....jquery....Q.@*.$.....module....Q.@.....exports..(S.....5.a....(.....!....a....".....a....!.....q....a.....a.....a....a.....a.....a.....a.....Pc.....exportsa....?...I..!..@.-....dP.....W...https://www.covid19-siparadigm.com/custom_libraries/select2/select2.full.min.js?v=1.5.3.a.....D`....D`....D`.....`....&...&....&....&.(S.`..`|....$L`.....0Rc.....Qb..@e....d...`$

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e47734d8b5f45427_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75096
Entropy (8bit):	5.705474693208933
Encrypted:	false
SSDEEP:	1536:5y9B50lUQR7mFbbOyRJ9++RL6hdwjbpOyUchPzbCn:5Q7/QdmJdJfL6PEbpOyUibbCn
MD5:	F5124CC235CD4350DE2A810300047BDA
SHA1:	92600FB7774858F394911AB4EFC557E26D9EB49E
SHA-256:	9168E51B2E4148DBC1B3736AB6616F8FE5E869FB338360799DD07A4F08AD3ED8
SHA-512:	BD202A76ACAF00BC108707727D3AC30CE7EB41D52C52E8C5D055E43520955E15624F62C5114585836981C8E0B6C39C5271676BCDBD929BCCA5706AE5491BCF2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e47734d8b5f45427_0	
Reputation:	low
Preview:	0\r..m.....@.....\.....94ADAC47C6C937561890EEB78C4B531D0BA687048CB1F2D925AAC300780C50CC.....'..p....O.... $...../..... .....d.....(S.0..`.....L`.....(S.../.`.^.....L`.....u.Rc.....Qb.0N....data..QbFm1x....ba....Qb..Zt....ja....Qb^@.....na....Qb^.....ra....Qb.....s a....QbR..%....qa....Qb...[....pa.....Qb...Q....ta....Qb.X.....va....Qb..>....wa....Qbf.....xa.....Qb.`.....ya....Qb.....za....Qb..l.....Aa....Qb.....Ba....Qb.Tk.....Ca....Qb~.....Ea... .Qbz.....Fa....Qb2y.....Ga....Qbn.a.....Ha....QbR.&.....Ia....Qb...e....Ja....Qb*.....Ka....Qb..*....Da....Qb.W+.....La....Qb._.....Ma....Qb.;.....Na....Qb6..W....Pa....QbV. %.....Qa....Qb.nb....Sa....Qb.~.....Ta....Qb".Fv....Ua....Qb.....Va....Qb.G.(....Wa....Qb...D....Xa....Qb...k....m.....Qb..>Q....Za....Qb.....zb....Qb...k....Ab....Qb.,|p....Bb....Qb&.. .....Cb....Qb.h.....Db....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e508f5ea9c0d214f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9178
Entropy (8bit):	5.821352431032633
Encrypted:	false
SSDEEP:	96:b5ZJ9fHlYCZMi58FcbEtaSCtajDEXrI9/mao0EuPt2uhs/nIxkk6RnzMnS+f2r3J:NNMoSZDEXrI9/NPx4Rn4+r3MJ/kRCE
MD5:	932D130FAC8C06A4AD271F87B7F33852
SHA1:	7918ADA6B33C2D3CD95F79CBD50AFB24F5C942C9
SHA-256:	699FFC411E68239BE4267370E83AFB11C21D141DCCEB227F0679E6A811E1773A
SHA-512:	0EF1201FA271595005106968732651CCB0D9236775B8F128D78729E9F3B3C20C8993978B14A330EE456C3A00C465B0F38A7354969DA769CD9B481B2B67E849D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....T~....._keyhttps://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3 .https://covid19-siparadigm.com/.{SX../.....n.NWZp.`...l....g.t.r. }.`i../.A..Eo.....i..&.....A..Eo.....'.....O....H"..qy."....(S.U...`d.....L`.....L`.....Qc.....gender...(S.....Ia....3....$Qg>.....checkInputGener AndDOB...E.@.-....TP.A.....E...https://www.covid19-siparadigm.com/dore/js/dore.script_min.js?v=1.5.3...a.....D`....D`....D`.....M...`....&...&.(S.....5.a.....a.....Pd.....fn.addCommasa.....IE.../d.....&.(S.@..`:.....L`.....0Rc.....Qb..W....e...`$...I`....Da>...<.....Qb.....fn...(S.....a.....q....a.....a.....Pd.... .....stateButtona.....d..wV..... ..I.....d.....Qd...7....stateButton...K`....Dj.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eab3f5e80b9c9c0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3020
Entropy (8bit):	5.383824194767987
Encrypted:	false
SSDEEP:	48:BjKmry9iQE2W/PN72+KJcUPKI71/onRnQsIsU4o+PcBk:0GiE2eK+IcaKIB/onRQMU4o+d
MD5:	7555857CCAA4E75FEDED28DBA500A4D5
SHA1:	DCBA02CCD1D247AA01876B321766FB6FC20A8158
SHA-256:	E07DFB87BE7C798A2BD85B3470824D788FE99C194F70B061B56F30E4D3F4F923
SHA-512:	E32E75B19265B7B634C688D73C8D416DF967F4BD5E67C637262F59630ED4877857EB2597B8FAF7FF25CE6ADE3A8E583FD4DB2ECEE9CFEB422D252BD1371B69 3
Malicious:	false
Reputation:	low
Preview:	Qj1Y../.....'.....O....H...;;.....(S.8..`(.....L`.....(S...`.....(L`.....Q.@.+.3....define....Qb..f.....amd.....`.....M`.....Qc..Q.....jquery....Q.@.b4|....module.. ..Q.@.p.....exports...Q.@NK.J....require.....Q.@.l.....jQuery....K`....D| .....s.....&.(.....&.z..%&.^.....?...s../...&.(....$...&....&...&.]...&.]...&.-...%.....&.].....(Rc..... ..I`....Da....<.... ..f.....P.....@.-....`P.q.....Q...https://www.covid19-siparadigm.com/dore/js/vendor/jquery.barrating.min.js?v=1.5.3...a.....D`....D`(...D`.....`h ...&...&....&.(S...`.....@L`.....8Rc.....Qb.....t.....Qb...X....e...a$.....I`....DaN....-...(S.<.`.....L`.....(S.....Ia..... ....!....!.#....#.%....%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f5d363064ecce588_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6111
Entropy (8bit):	5.59513144059266
Encrypted:	false
SSDEEP:	96:h2A8Ka92Y7bQkV7E1OoSBBYt1c29RegKndmGTE/dnvU4igtUYPdz33+Zv:n8K+wK6RegKcX/5U4igdrK
MD5:	6EF31F2CF3723F74E25FE07BF2660FBC
SHA1:	BF4DD0FEF0A7FF4269C6DD5F74FB5B2371D068F3
SHA-256:	C2CB1E3D6E375D96E1CF36EDD89C5F2B4575F0192CA6F54E9B06C4E88172EFCD
SHA-512:	07599C028237D001EE2239301A83F17D7B08CCCBC893E4B25E5E52700048F9CFA158E5C4B4BE031C7DCE730DA0D1B2C3E262EB7FB8F57B06A1CE2AEF6EDE00 4F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f5d363064ecce588_0	
Preview:	0\r..m.....o.....*...._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3 .https://covid19-siparadigm.com/gn4Y../.....X.c.N..u^ .....L...TDio.A..Eo.....$.....A..Eo.....'.....O....H..... .....(S.P..`X.....L`.....(S....`x.....L`Z.....RcD.....Qb.....t.....R....Qbf..Y....y... ..Qb.....E.....Qb...~....v.....Qb.:.....z.....Qbb.x....C.....Qb.%I.....e.....Qb2.....m.....Qb.....q.....Qb.,.....B.....Qb.....A.....Qb"C.9....n...l.....l`....Dal. ..b%...(S.\.`p....L`.....Qe.e.....addEventListener..Qd...I....attachEvent...Qb..Z.....on....K`....Dq(... .....(.....(...&..&.'..'..'..W.....(...&...&.%.4..&.Z.....,Rc.....`....D a....,.....A.....c.....P.....@.-....XP.Q.....J...https://www.covid19-siparadigm.com/dore/js/vendor/mousetrap.min.js?v=1.5.3..a.....D`....D`:...D`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fc55e55442907e54_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.91647621370238
Encrypted:	false
SSDEEP:	6:mAEYGLiYW91SNuaCdTJVbH5Mrtq/W5LCei4O/bK6tm7NnHvA/W5LCei4:znY21S1wTJVz5gtqiLCrP/N6tvAiLCr
MD5:	49D6E0E033FBE0F5A59C016AEF097372
SHA1:	7D151362650FBC028D603D9A0C2619EE49B7E11F
SHA-256:	B4468689D659068486824FDFA1D860F637B751516F32A231A6E95EF83371B307
SHA-512:	FE58F03924BFB4571967ADA6DB98CC016F9E0FD96E57E32372EAF8A007582D0E1959A735250413D3EA8A2BE14C548D82F9CED17CF65E44575DED21B75B871C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://www.covid19-siparadigm.com/dore/js/vendor/Chart.bundle.min.js?v=1.5.3 .https://covid19-siparadigm.com/4.2Y../.....J..C._..{.....#... ..s.S.D.].5c...A..Eo.....A.....A..Eo.....4.2Y../.x...89F51944D0CA34E09756755EFA5A35764141BA89BB64487B4A4A96FC8DECBDDFJ..C._..{.....#.....s. S.D.].5c...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.3255571079538795
Encrypted:	false
SSDEEP:	24:Ml/dIKlF1r2lFUzFB0pKvpb5bOccDSgOSa/re/V926K:GrfpB0mb5BgOS8rOV926K
MD5:	7E16BC08929378D6E79F3DD657DECB4F
SHA1:	FBAD1F019752C2E7125E19673613E280B5B309D4
SHA-256:	750BF761FFA3823CA456CD479D5BBBE11B1978CA0C7FC41E26A5C91AD70C2A89
SHA-512:	48A68B9BAA3F23A69DC0F4EE69E72A513EC990C5051C079B601B1A512752840255039BBE4203F3D1989F7545E9031119D25DBB1BE33766B4E9B046C442F6FC41
Malicious:	false
Reputation:	low
Preview:	.....- Koy retne....$.....K.....x..M.;...[../.....)....[../.....L..pP...[../.....F....3@.Z../.....q-{...@.Z../.....C.%..@.Z../....._n.$...@.Z../.....y..9.D..2Y../..... ....2...q..@.Z../..L.....N.c..@.Z../.....s=O.t.@.Z../..'.....b)[~.).@.Z../..j.....#.m?@.Z../..Z.....0....@...2Y../.....1e....n@.Z../.....T~.BT.U...2Y../.....a%.a.XP..2Y ../.....s.#k...l@.Z../.....<.g..@.Z../..B.....2Y../.....@.Z../.....,@4....0..2Y../.....`.....W@.Z../..t.....Us@.Z../..J.....n..;..2Y../.....w.[....@.Z../.....' T...4w.@..Z../..&.....~..3D.@..Z../..z.....B.~..n.@q\X../.....@q\X../.....O!.....@..Z../..%.....+X'.X..@..Z../.....I.@..Z../.....H.Mu.@q\X../...../...3.^j.../..... ....^}.Np...^j.../.....[../.

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):	24576
Entropy (8bit):	2.279951971336689
Encrypted:	false
SSDEEP:	96:dNwTvXwn7ghOXcAl71kgB3/alKuAHfKYNwDvX3MvM8ZITUN/alKuA5nd:duT47YsvaMPyYuDPNC7aMPv
MD5:	725FB9EE1D772AA650C6F3997FE4D44C
SHA1:	BCF14F602FC023729552C3A65A7F6770A157668F
SHA-256:	AB0FD9BB7EF8DB46821A0810F97D6D0FD2C88DF16DA1C415357764BBA944666A
SHA-512:	2C6F145F6CF657E956D091030586E491F3CDB4BAE5AAE936811ECD1A8208F430D4D52F04D236D58A2CCF361F7D4C6F27A3D3F4DA449CA8B6267F1E1323A630F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.625389181765293
Encrypted:	false
SSDEEP:	96:v/a3cNwWvXwn7ghOXcAI71kgB3/aw8AHfKIMNwc:3a3cuW47YsvawRyIMuc
MD5:	6C6565ECA0F85BA00F8B803D794093B7
SHA1:	D33FFEDFF54E0C170F91A58E6E3A89E7826010BA
SHA-256:	D1EAB4C20343154CF77A8448181B57DAEB922F4B7BEF958155991B5AA2E146FB
SHA-512:	F29E94DDAFF8DCE3C46FCD76B76435EEF263762D8C63F982D6DAA04A3342DCC89FF614451FDC0D1CF97766BC149A1650F4684A24CD1A6191FF53A15AE9D6B74
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):	11772
Entropy (8bit):	3.220737141436446
Encrypted:	false
SSDEEP:	96:34EpVApWDKKbXYaPZVCmYVN1xZwkOnV/YVBZ0IhqJ:3FVGMzYACjN7Zw1VqBZ0IUJ
MD5:	4E0A3ABCB943C3FE92B1C803D3A45335
SHA1:	DA0433B119A477D297BF1EB3E71DE8ABC35DEC12
SHA-256:	E8A1263A37A08810422D02CEB1F81C24DF0E12C72BA80117A99D1C8469FBD644
SHA-512:	8B350570CBB5D042AE5ECF6F9FCB98312251162FED2A5E31A8D6B16FB2AE8BC2BC5490E56BAE62735EC2AFE98099C19EA7530F61D596FE260770302B3A5403FC
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...4b71f4fa_ca68_44ee_9645_b33c2c4ae784..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....Y..T.....+...https://www.covid19-siparadigm.com/en/login..... .....h.....`.....I.....I.....^...+...h.t.t.p.s.:././.w.w.w...c.o.v.i.d.1.9.-.s.i.p.a.r.a.d.i.g.m...c.o .m./.e.n./.l.o.g.i.n.....8.....0.....8..... ......"...http://www.covid19-siparadi gm.com/.....!JX../.....!.....

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):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.................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):	326
Entropy (8bit):	5.195463797415433
Encrypted:	false
SSDEEP:	6:m0fPEUQTpDM+q2PN723iKKdK8aPrqIFUtpBfPNpgZmwPBfPeHDMVkwON723iKKdr:5PEdpDM+vVa5KkL3FUtppPNpg/PpPADJ
MD5:	1B13B2EFF43DDB75AC2C13A635960DE6
SHA1:	82E5F52C3F9BFE9D46C5FCFB910DF59FE9AC3B9C
SHA-256:	AC263B3B5F40E7D0B1E7269DE6A322269B8FC0F606BBC7F609579B1409CA2C5D
SHA-512:	7E1602AD626174F74331B132061467BB7538A772CDDD0BB7B53C084C0E0FA38B1E3450127CB9A9E3081084AF8F70C5F10CE03283B341CDC2BC82876D64B23E1
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:48.162 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/19-15:18:48.163 156c Recovering log #3.2021/01/19-15:18:48.164 156c 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Reputation:	low
Preview:	.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):	326
Entropy (8bit):	5.167265942053141
Encrypted:	false
SSDEEP:	6:m0fQBmdDM+q2PN723iKKdK8NIFUtpBfQBFHgZmwPBfQBGDMVkwON723iKKdK8+ed:5YmdDM+vVa5KkpFUtppYFg/PpYGDMV5m
MD5:	5B05C9C20A41D72746C07455143A1067
SHA1:	259743264109491DA235D613F1A8B8EA7AFDD146
SHA-256:	A249AF01E652DFDD204EBA3491082A737604A35B120DD30B43DA62C7EB98A241
SHA-512:	5F4AF8821B66C7C7F3E198DF241A60C81596AD99D71D8061162A6241BD95A72E1915E19B12AA3E061C18DB9F78C8570B290EB71A03516961BCD22844D324CAE
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:50.269 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/19-15:18:50.271 156c Recovering log #3.2021/01/19-15:18:50.272 156c 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\1.0.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_2_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
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):	40960
Entropy (8bit):	1.8286106398166337
Encrypted:	false
SSDEEP:	96:yBCaUupU6qBESRMIcXdgF5XG1lyjcQg58gRo:IcOSRMh+FFGm
MD5:	F56A4543A949488023807F69C7744C9A
SHA1:	F5DFB00D780AB0C987774D5471B4F3285D943F85
SHA-256:	5B345A823A2AAC249CAF4430DD77BA5EF2570A8F23280C16010EDFD029A1CD42
SHA-512:	7DFA178036B00774311524CB6D1D6A6C62AB49A944C0720959B16C75B50CBA20D336973EE3BE377B05A790FDC21597A6549805AE53DA96D2EA3BABD17751718
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):	43740
Entropy (8bit):	1.0149059213580645
Encrypted:	false
SSDEEP:	48:CFidBmw6fUI3a+JXm6jJPD08l8fKiJ+rslFehgi8:kidBC27Iwdys3Qgx
MD5:	B4B68D3724E858D1F115A893C87E6AEC
SHA1:	B56914CB04F06F4A4A493A6B766F97E094EA697A
SHA-256:	05E18D4FCD130F4A6B645C67100E9F668CC3C705CB6FF24907D91638D6E0C6A5
SHA-512:	B2423AAB140B4DEEA5E985DDA1B6BEB877E946AC0C4ACEFCEEE9F3CD248555A7BE8F397BE180301ED052AB4B0F8D548614527EA7528989B655AA91E22F750B4B
Malicious:	false
Reputation:	low
Preview:	.....[f.a..... ....

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):	378
Entropy (8bit):	5.233818137313146
Encrypted:	false
SSDEEP:	6:m0fQA39+q2PN723iKKdK25+Xqx8chI+IFUtpBfQHdJZmwPBfQFfF9VkwON723iKG:5xIvVa5KkTXfchI3FUtppw/Pp4ft5Oak
MD5:	CFECFC02CCF8C0709A9246608D139180
SHA1:	C967ADD668528EA33B0706558151BE4F9E34305F
SHA-256:	1FCD7B7350F0CD76F6FB512369B649C58B223DD39E117B26E1B1E7156CFD94D9
SHA-512:	42960D6644A2FC98BFC88ABAAEFEF7C4FC2CA4E611DAD5181885E290B146A2E403EA2FE662A8C533F942A74921A0ED625250B6C481C7706609546401D60DD9D
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.563 1588 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/19-15:18:59.760 1588 Recovering log #3.2021/01/19-15:18:59.762 1588 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):	364
Entropy (8bit):	5.174537150039634
Encrypted:	false
SSDEEP:	6:m0fQ8Kt39+q2PN723iKKdK25+XuoIFUtpBfQpJZmwPBfQ6z9VkwON723iKKdK25y:5KIvVa5KkTXYFUtppl/PpFn5Oa5KkTXp
MD5:	4D76B584204D8949A1155EB59AD26D34
SHA1:	C9F504AAFD9C9F94D991AAEC3A44755D4368352F
SHA-256:	F1D543C55617C0F48321D41E40345D1FE62D538554B6D2A69403402FF09B50DD
SHA-512:	C42F5EF0C7BC81B9CE6B746477F2A272395AF39AE7C1E7FF906BA3622CF2C30D8ED8B65BF4E0B22A4C54983BAB817437B627A22BC530B3E6D723DD9A9659273 8
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.421 1588 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/19-15:18:59.434 1588 Recovering log #3.2021/01/19-15:18:59.440 1588 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):	336
Entropy (8bit):	5.171846702688673
Encrypted:	false
SSDEEP:	6:m0fQH+q2PN723iKKdKWT5g1IdqIFUtpBfQLU5ZmwPBfQzM33VkwON723iKKdKWTk:5tvVa5Kkg5gSRFUtppp5/PpbF5Oa5Kkn
MD5:	E1B82CC94B13CBF5DAB02CCD733F0B28
SHA1:	CEACAC0E8741D33B5CCB216DEE6E9CA19F680177
SHA-256:	79E16C29DFC32E2D057721686EC410B5092076D617CA0804BFC3D6DC7475A829
SHA-512:	352181AD27572C1A5738B8DEAF95C98DAFDEF91A45B52B2261B5B029981C77B17136D530F3EB4C27F6B77AEF1C8A9CCEA6E7AD6193CAE37D494573AF30726D 9
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.239 1008 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/19-15:18:59.270 1008 Recovering log #3.2021/01/19-15:18:59.278 1008 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):	159744
Entropy (8bit):	0.5684439188088497
Encrypted:	false
SSDEEP:	192:r82Dg+d82nmbd82hSQ8+bd82U3haWy+bd82Cri:rr/MQk0UWvOi
MD5:	E60F06ADEEB417EEB5AA0B38F982E14A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA1:	B0ED4DD50474ACCAE218F568B08202A91CBA3B1A
SHA-256:	9B7D5917A10002A3AA9754520481CA5A92EDEEBB58DA03093CFEF462B96CE243
SHA-512:	1CE1EB82203CB5B1EE41BB6F89AA4CCC9677268DB823659371606FC34BBAD52CEEEB9A69DF5E38E8A73BD539161D392CB8E95628A1E27420AA7935AC31695AC3
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):	804
Entropy (8bit):	5.472406840150314
Encrypted:	false
SSDEEP:	24:Xu3HnZiBw1XTWD7onP1ZtVsgz+due09IQauaMeBX:eh1DWD7oP1wuva3X
MD5:	45FB6B1AE3FF8B0F1AB5C1215C103305
SHA1:	0579BD2157BFA7000C826511EC739D4ADB45EDF8
SHA-256:	FC481DCF1935C8FEAB990CA1B2E6333B89BC2F87DDC58D41FB23D0BF7175807A
SHA-512:	EDCD255D618BDEFA7ADA7B6E4EEBAB9DB2620A3AE3FEC82092827983B3D9800C33F1F725DBD15324631EE14A73C77AA5A49838C730E5CE0F0CB1EE98BB1E4541
Malicious:	false
Reputation:	low
Preview:	....."B....com..covid19..http..in..log..siparadigm..www..https..en..login*j.....com.....covid19.....en.....http.....https.....in.....log.....login.....siparadigm.....www..2.....1.....9.....a.....c.....d.....e.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....v.....w...i..... .....B.....M..... .....*"http://www.covid19-siparadigm.com/2.Log in!:.....S..... .....*#https://www.covid19-siparadigm.com/2.Log in!:..... [..... .....*+https://www.covid19-siparadigm.com/en/login2.Log in!:.....J1.....#&....

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):	0.41129379003952987
Encrypted:	false
SSDEEP:	96:ardgq82Fd82lEc9bd82zazvqQX/8+bd82Ir:aBgq82Fd82lEObd82za7nX/8+bd82E
MD5:	86008DF81961D19D29C195F7A43F9C27
SHA1:	0D30F85AAE0A2A20B972F13E1D0DAE50B9DE7445
SHA-256:	8E3B428C8C3AEEA624F5996F1096007CA61DABECD86B7B130ECA5651A51497AF
SHA-512:	BCC4113E46CFA815FEC34CE251B1E99246BD3935ED4F1433B4A2FC35A1E426BD32EE90D77FDF4704F19934BA1C02FDE18EB4068E11BCE55419803454CA497259
Malicious:	false
Reputation:	low
Preview:	.....f.T..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	46
Entropy (8bit):	4.1429146733542535
Encrypted:	false
SSDEEP:	3:tUKGKh4/Hv7WFv:mK4H7g
MD5:	6CD4371471D5E90EB14714F9BB143E3F
SHA1:	AD3E1C92824AA8E100BFD214717F7E2B3CA77434
SHA-256:	F88DE467BFD40B656EAC57590E0EF425403F2F7766869F1E28AC949E9679E9E8
SHA-512:	0176CB9E17A14F704A439C05DF825C6F80BCC3040DE89122B037CA6C631B6006E68B8419B54567D4DD46BF55775BCE0DE0CDF3925FFFDD3F3B0B4A3CE6986F7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\LOG	
Preview:	2021/01/19-15:19:41.058 1838 Delete type=3 #1.

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):	3214
Entropy (8bit):	5.513838961679599
Encrypted:	false
SSDEEP:	48:LGUt69KGzR1a7VMY8dbXe8qbQSefgGMcNrS0U9RdiN9YQ:byTa7VMTdbXe8qbQ5fgGM8rS0iQ
MD5:	DFF73A33A313C5850849840FD9DEBEFC
SHA1:	0D519E1DEC034C240B1B0C502A8DA0A8B4601D82
SHA-256:	DEF8EFB793D9E00873766F76D3F8730EF9C0188D85F1E9DFB6D776EB27BE2B5D
SHA-512:	FCFDBAAE1F8712B1DDBC30F9F9759B3960DDE4F3048CB4FB3EC4586051B19C67D7B39749174B95FFC47AFF39D4955687A4F9C80EE4C52901B455F0DE3185F42
Malicious:	false
Reputation:	low
Preview:	...J...*.....'META:https://www.covid19-siparadigm.com.....F.3_https://www.covid19-siparadigm.com..dore-direction..ltr.0_https://www.covid19-siparadigm.com..dore-radius..rounded./_https://www.covid19-siparadigm.com..dore-theme..dore.light.blue.css..T.....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..623746000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-19 15:19:05.05][INFO][mr.Init] MR instance ID: 6f220513-0222-4bb4-a4e0-08de1558eb87\n","[2021-01-19 15:19:05.05][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-19 15:19:05.05][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-19 15:19:05.05][INFO][mr.PersistentDataManager] rem

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):	338
Entropy (8bit):	5.16770985012303
Encrypted:	false
SSDEEP:	6:m0f0JsMM+q2PN723iKKdK8a2jMGIFUtpBf0cmZmwPBf0NF9SMMVkwON723iKKdKw:50eN+vVa5Kk8EFUtpp0cm/Pp0X9iV5OR
MD5:	E371EC4A8E32CC66C3C1009D376CBB62
SHA1:	DD4C40AC70EA2E24A0B74EDF3973D92AF1C72C91
SHA-256:	075434E5AF8A3AA64B15838CCB21AC231156736B98EEDA153096EE2E08178FDB
SHA-512:	AF2093F914C628F687B58F03FB74A4EFFF6F6C7AAA13A5445DC434A09503CC361163987F33C156FC7AD20852A5786B8A22292ECB29F8D540F86FBCD4D3A36583
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:47.918 181c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/19-15:18:47.922 181c Recovering log #3.2021/01/19-15:18:47.923 181c 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\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\MANIFEST-000002	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\MANIFEST-000002	
Entropy (8bit):	4.948758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVqU0blS:oO7iblS
MD5:	22BF0E81636B1B45051B138F48B3D148
SHA1:	56755D203579AB356E5620CE7E85519AD69D614A
SHA-256:	E292F241DAAFC3DF90F3E2D339C61C6E2787A0D0739AAC764E1EA9BB8544EE97
SHA-512:	A4CF1F5C74E0DF85DDA8750BE9070E24E19B8BE15C6F22F0C234EF8423EF9CA3DB22BA9EF777D64C33E8FD49FADA6FCCA26C1A14BA18E8472370533A1C65D D0
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	1.20571062447832
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOQyOqAuhjspnWOrzj1ACOqAuhjspnWOPOqAuhjspnWORQ:HRMMP1A8a4Q
MD5:	0A7F5A7D6399D53A02A6F88B2AF0A155
SHA1:	9505947E5EEC915592B56D6874174E60A1AC7803
SHA-256:	4262B305DA18DB2B915E9BECAF5BDF718D96B4D7A643EAE7B5C5B9DAEF19EC71
SHA-512:	ACCA413DAD50370598A43D8DAE7FF90D4DD403C93C98C9958955990BB5BEF5CF5B129997DD9BAF803E6342BE3A3A2F5770D6129083ABEDAFFCA28B3726972D 6
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	51344
Entropy (8bit):	1.1078444961065843
Encrypted:	false
SSDEEP:	96:8YUOqAuhjspnWOXkOqAuhjspnWORXEB0OqAuhjspnWOnzj1KBEOqAuhjspnWOt:/yaig0BS0P1KBCi
MD5:	7EB2EBC4C0BABC5528EAEBB63CE91864
SHA1:	32D0A66118CBE2AE1A7F9E00874E33EBB5704808
SHA-256:	8D4762D137FFF0D91A997E2CEDD64337BF754F769ACE115D673EBBC181A8B1B6
SHA-512:	58E4C63BD6BB0008D106A3120BFD3F4FC7596B5B6FC4450C98A7C3BDA047F12CE79529B99DADCE0684DF68034C0C7C29FD792B3E8D68E8190D2F02C6D44026 6
Malicious:	false
Reputation:	low
Preview:	.....4..... ....

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):	340
Entropy (8bit):	5.1847017228291605
Encrypted:	false
SSDEEP:	6:m0fPNGpDM+q2PN723iKKdKgXz4rRIFUtpBfPdpgZmwPBfPMDMVkwON723iKKdKgi:5PN0DM+vVa5KkgXiuFUtppPHg/PpPMDq
MD5:	F936E8D4DF6F95E54C9148E786E87579
SHA1:	F812E7434C441EA58B31210AFEFAE30087468034
SHA-256:	5FD386ACE414327857F2B226930CCC686814669E9FB75216E47EC9A6034E3E94
SHA-512:	4CDEB5823EF5013EA3FC2BA5493EB02BBACDA676A8112BC7879232E683BF002C247E8CA757E7043A8C47EF3F9C98E9DBF71B5C4A768B5D2A9048AA0EE319C2 49

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:48.180 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/19-15:18:48.181 156c Recovering log #3.2021/01/19-15:18:48.182 156c 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):	1.229414896598868
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUuszC3+bl1EIot:wIElwQF8mpcSLpUIElwQF8mpcST
MD5:	242CA5D0EDCD45B997E4D6780285C677
SHA1:	C4CE2C05B4CF6EABFB9299388FAA4A065B52F057
SHA-256:	064866ECB2B1D72B6205CF9BF66E5734B8CD6A025949CC8ECC5465D5F6EF4191
SHA-512:	0B85AA8D24A03201FE3FE1802C5D0BC3B3265577BC7727D703579022C8CDD64096358256CABC1485DFECAEA2A22F8CA0408250D756BD8A2E315F005A59E3908
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29776
Entropy (8bit):	1.1247716285126008
Encrypted:	false
SSDEEP:	48:q8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUxd+bWqUIopy:q8hIElwQF8mpcSMWxIElwQF8mpcSS
MD5:	3073267A61E93183AD33B0A0F73B4C6B
SHA1:	18B38005350E68FEDDE23EC91420450356C42D91
SHA-256:	0E3FDFD29FA756779DCFC256745B35983A37583EC4339F3B14BF887DE681D31F
SHA-512:	04F0C9ECE5D09867F859BA67689B379065BDE25A75AFBF91FAAAFD5A539299A602AD130BB829CE7B2547400531AFB0ED9C9B23F617DB03C37025A747C0636FAA
Malicious:	false
Reputation:	low
Preview:	.....h..... ....

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):	1456
Entropy (8bit):	5.279802118391218
Encrypted:	false
SSDEEP:	24:73LMRddshDTXk8k8u6X3VvQQ0OeiI/VclfoKct203ApKF2cfIpjgDlVA/+/:73A7dOTS6li/G5oKt0KjgzA/+/
MD5:	75690A92842B4BA73A25A86D888A7736
SHA1:	21D39B4FD5FF34EE60CD8CA5DEA34DA2A24CDE93
SHA-256:	D2AE4AC2D5AD40076F6C1F6030984A785677068F88250C87C487E5060916114E
SHA-512:	15A8A821D6CB750228B43B941B76F259305151563B28D8E27A4B29AA565158064151C9B5DED74E807E156A5E090460E9F670BA319E2E1A01D3866263A07549D1
Malicious:	false
Reputation:	low
Preview:	..&f.....~)Aiq.....next-map-id.1.Rnamespace-4b71f4fa_ca68_44ee_9645_b33c2c4ae784-https://www.covid19-siparadigm.com/.0j.P'q.....next-map-id.2.Rnamespace-fce80598_503e_49bc_a08c_e2c5926509e5-https://www.covid19-siparadigm.com/.1. ....%..q.....next-map-id.3.Rnamespace-fd3eba87_f801_40ff_90fe_020765612ab3-https://www.covid19-siparadigm.com/.2Y.T.q.....next-map-id.4.Rnamespace-34741d93_4934_443f_bed7_72fb0f1f5a77-https://www.covid19-siparadigm.com/.3/UJ+q.....next-map-id.5.Rnamespace-8da8b069_6df1_41ae_83b6_386848390483-https://www.covid19-siparadigm.com/.4..>.....-ny.q.....next-map-id.6.Rnamespace-c725595a_724f_44b3_9b43_d26943c16b40-https://www.covid19-siparadigm.com/.5k..q.....next-map-id.7.Rnamespace-c9913414_a1a3_415a_8c84_b6d65f512d40-https://www.covid19-siparadigm.com/.6.,..q.....next-map-id.8.Rnamespace-e7f519a6_3c9a_4b15_

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):	326
Entropy (8bit):	5.154685922690209
Encrypted:	false
SSDEEP:	6:m0fP2+q2PN723iKKdKrQMxIFUtpBfP22ZXZmwPBfP2kqkwON723iKKdKrQMFLJ:5P2+vVa5KkCFUtppP221/PpP2kq5Oa5N
MD5:	84B67A917EC7F7916A14C52CE6DDC2E0
SHA1:	B20471C0FB633E6887D52A652BFEA5063DBD35E9
SHA-256:	DF8993A918D3E6A454CD51486C75F57F9B5E82F0CC4E249C1F88455B6E3FE792
SHA-512:	834A4F9E009FF875BE29120199E7E88393EFA5179A41B6C834B4C159B9E3A6C0A1A2958C629ABB1BA49E53F06C62300F9E336FCC723CFB7A2C0479F814026F41
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:48.096 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/19-15:18:48.097 1834 Recovering log #3.2021/01/19-15:18:48.098 1834 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):	354
Entropy (8bit):	5.175407782128074
Encrypted:	false
SSDEEP:	6:m0f0h2t+q2PN723iKKdK7Uh2ghZIFUtpBf0tXZmwPBf0A9VkwON723iKKdK7Uh2w:50pvVa5KkIhHh2FUtpp0tX/Pp0AD5OaI
MD5:	E6E06734732F8F436CD1BD5387808F72
SHA1:	D59B8D69A0F12252126FF0562641D3D304044439
SHA-256:	B32D8FDA195DE914B99B134FD777CF815DFE74FA07FC85F02C95B918715793EE
SHA-512:	5F53E1BADEA49E03D1E86611E6738758BCC49924E53C982EBC471C6D22537ED719B56ACD2E347D036A361FF2A7A9522D2DCE838B134DBC61C650D3A46AB9F5A
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:47.867 1098 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/01/19-15:18:47.873 1098 Recovering log #3.2021/01/19-15:18:47.874 1098 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\2d8d8b34-9f68-42d1-97aa-7079ad4b874a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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):	436
Entropy (8bit):	5.244737676654673
Encrypted:	false
SSDEEP:	12:5P4SDM+vVa5KkFFUtppPd0g/PpP3DMV5Oa5KkOJ:RVVa5KkfgTNCOa5KkK
MD5:	E3D718463B7DEA0D7E8ECB5C9329D3AA
SHA1:	BF1F9BAFAFF22A380065E21911D68E96B249253B
SHA-256:	88609943B4DA07D4B8DF627D1F6837D8F1CDB772D9272D0B1AC4709AE045CD17
SHA-512:	AAFC588E4E5666AC79EDF5B05547816A391ED81742E1509FB28F54DC27434F5B9EF62FC954202419C44C9F252FA722A695FF0C3D16DA7D0AC08FFBA2904722E
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:48.141 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/01/19-15:18:48.144 156c Recovering log #3.2021/01/19-15:18:48.145 156c 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):	438
Entropy (8bit):	5.2917900712857895
Encrypted:	false
SSDEEP:	12:5PSvVa5KkmiuFUtppPE/PpPk5Oa5Kkm2J:R4Va5KkSgTEOOa5Kkr
MD5:	E4DB62D75C0049AD47E7DDA230254E6B
SHA1:	1342C0F9AFBB69306B90F6908B0C9F07F4D444D1
SHA-256:	FC2CB4DF7C27EF1260CD4D6B22F7044529213B7C8D9BB0E6A9B350113C138F24
SHA-512:	7407A75A1BA8BD2797EA91C17409AAD6BDBDA0D8AE4A34230A03A7BFE15BB2BA1933F49C699E57FBF84C798757DDA66F474CBDFBBC0B4203BBE2066CB908E 69D
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:48.176 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/01/19-15:18:48.177 1834 Recovering log #3.2021/01/19-15:18:48.177 1834 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.225111654656264
Encrypted:	false
SSDEEP:	6:mZT3+q2PN723iKKdKusNpZQMxIFUtpuUSXSZZmwPumiVkwON723iKKdKusNpZQMT:k+vVa5KkMFUtpOm/P/iV5Oa5KkTJ
MD5:	1F45B0290E42579AAB2C9EA046A1D63E
SHA1:	F8B81CABC07327AB11ABDFE5AC0D263141A98B79
SHA-256:	9D99005617AC38591B09DAED7E9E155C034A0FEDB6ECEA61669462C97629E71F
SHA-512:	87F0C5CE14087BC3B324F14022AC44AF03B233E252403CAAA6B8ED05BE70535D311D8C1DCC14E39A7A8AEF53B27BA1EF3E4E2ED2546D4E66AC55AC20F5610E49
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:19:04.293 182c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/19-15:19:04.294 182c Recovering log #3.2021/01/19-15:19:04.295 182c 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\77c0f0b7-2265-4d58-a575-a81b60cf8a8b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
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):	436
Entropy (8bit):	5.17287977989268
Encrypted:	false
SSDEEP:	12:53vVa5KkkGHArBFUtppW/PpMSRP5Oa5KkkGHAryJ:JVa5KkkGgPgMOa5KkkGga
MD5:	28C0D430447AF40D124D09E9F59EC565
SHA1:	517BF7D83EC3053CBAFDA126A28A9B44B2F4D169

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA-256:	C0F2D53D062DD6A90306C3214058C9AFBE640B434487EC4074D0ED836417EED1
SHA-512:	3DE5D423378F857D30FEA2525E56D9FF201CD233E1E7F6592A16089DE4B0CD7C9AD6414A66479FE63803985BBCC76E9AADE2D29F904746EADFE2396642A3EDI 1
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.505 1844 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/01/19-15:18:59.509 1844 Recovering log #3.2021/01/19-15:18:59.511 1844 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.17374659681653
Encrypted:	false
SSDEEP:	12:52vVa5KkkGHArqiuFUtppRT1/PpMSW5Oa5KkkGHArq2J:6Va5KkkGgCglwOa5KkkGg7
MD5:	7CA22760D5186E2BC5FF419D13D3AB0A
SHA1:	429D35D768320A18990B56FE95F86004C1CBA59A
SHA-256:	72903AAA4515734B11A019D7AD61661F6E6C091710F725141D88F177B2E5DCC5
SHA-512:	9BAFB852E6CF8D6744A92751A53DFF35A072E365D04B69C7395F357B1E83F55096BC2E46525CD753EF2C16DEAF399CD3A010FBF052516A08D04E6AFAC72DF8F D
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:18:59.505 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/01/19-15:18:59.509 1838 Recovering log #3.2021/01/19-15:18:59.511 1838 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....

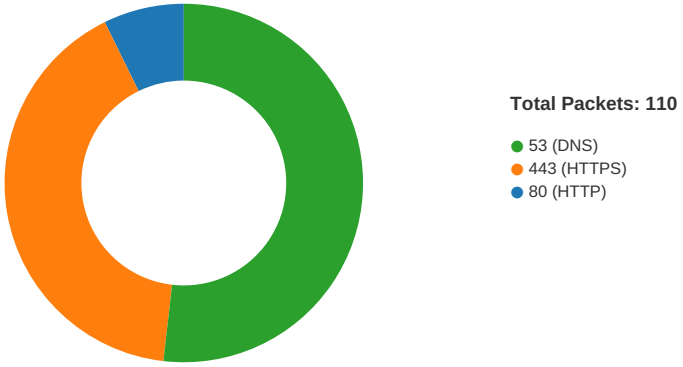
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.1616503116224965
Encrypted:	false
SSDEEP:	12:g4vVa5KkkGHArAFUtpKJ/PKD5Oa5KkkGHArfJ:gKVa5KkkGgkg4cVOa5KkkGgV
MD5:	0C3BA2ABC26028871C24137C49CA4F49
SHA1:	FCAED29C1BFF6C507BFB0D0B5F98FD7EB8806131
SHA-256:	35D3C501C95C4968E6B178B20E98EF334AB5CEB8B633FF1F1A1DF77872267D00
SHA-512:	97FA68F2774482856D1B08BCD4A1FFC4095C611EDC662BF180D634415F063B84F9FB054FABECD9D7612E90803C71CF8CF071C0103ECA895BF5C7C449E2FAD2
Malicious:	false
Reputation:	low
Preview:	2021/01/19-15:19:14.837 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/01/19-15:19:14.839 1820 Recovering log #3.2021/01/19-15:19:14.839 1820 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/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
Jan 19, 2021 15:18:50.607754946 CET	49720	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.608218908 CET	49721	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.765219927 CET	49722	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.812045097 CET	80	49721	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:50.812154055 CET	49721	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.812448978 CET	49721	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.812952995 CET	80	49720	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:50.813033104 CET	49720	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:50.969465017 CET	80	49722	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:50.969641924 CET	49722	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.016355991 CET	80	49721	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.017225981 CET	80	49721	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.031454086 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.057902098 CET	49721	80	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.236320972 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.236562014 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.236857891 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.441975117 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443221092 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443265915 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443305016 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443342924 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443372011 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.443392992 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.443408012 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.483258009 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.483444929 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.483758926 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.688438892 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.688472033 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.688616037 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.688950062 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.710593939 CET	443	49723	54.149.7.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 15:18:51.710630894 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.710788012 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.717593908 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.922595024 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.940857887 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.940884113 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.940896034 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:51.940985918 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:51.981934071 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.015959024 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032217026 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032280922 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032319069 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032397985 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032423973 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032433987 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032532930 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032566071 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032574892 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032602072 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032700062 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032717943 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.032741070 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033591986 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033626080 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033663034 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033689022 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033725977 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033776999 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033826113 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033870935 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.033889055 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224339962 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224391937 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224431038 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224466085 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224468946 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224509001 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224519968 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224549055 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224596977 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224598885 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224641085 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224647999 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224678993 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224705935 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.224725962 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.224797964 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.237174988 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.237242937 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.237509012 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.238406897 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.239263058 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430546045 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430577040 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430593967 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430614948 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430645943 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430660963 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430677891 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430694103 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430696964 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.430711031 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430730104 CET	443	49723	54.149.7.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 15:18:52.430747032 CET	443	49723	54.149.7.8	192.168.2.6
Jan 19, 2021 15:18:52.430764914 CET	49723	443	192.168.2.6	54.149.7.8
Jan 19, 2021 15:18:52.430766106 CET	443	49723	54.149.7.8	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 15:18:45.120186090 CET	61346	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:45.178838968 CET	53	61346	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:46.100409031 CET	51774	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:46.156637907 CET	53	51774	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:50.523495913 CET	60261	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:50.528090000 CET	56061	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:50.529812098 CET	58336	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:50.530298948 CET	53781	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:50.579843998 CET	53	60261	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:50.594902992 CET	53	56061	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:50.594949961 CET	53	53781	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:50.604357958 CET	53	58336	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:50.997013092 CET	54064	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:51.064784050 CET	53	54064	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:51.188529015 CET	52811	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:51.255601883 CET	53	52811	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:52.341064930 CET	63745	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:52.413247108 CET	53	63745	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.074805021 CET	50055	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.134602070 CET	53	50055	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.363372087 CET	61374	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.384694099 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.424655914 CET	53	61374	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.449008942 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.657824039 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.658081055 CET	49694	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.715930939 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.717190027 CET	53	49694	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:53.944129944 CET	54982	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:53.991977930 CET	53	54982	8.8.8.8	192.168.2.6
Jan 19, 2021 15:18:59.222012043 CET	62208	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:18:59.294507980 CET	53	62208	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:00.277501106 CET	57574	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:00.346744061 CET	53	57574	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:04.924196959 CET	56628	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:04.988228083 CET	53	56628	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:06.935475111 CET	60778	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:06.993134022 CET	53	60778	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:10.422394037 CET	53799	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:10.473433018 CET	53	53799	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:11.415056944 CET	54683	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:11.463005066 CET	53	54683	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:19.644046068 CET	59329	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:19.701932907 CET	53	59329	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:23.936288118 CET	64021	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:23.984185934 CET	53	64021	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:24.000423908 CET	56129	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:24.048626900 CET	53	56129	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:24.782113075 CET	58177	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:24.854028940 CET	53	58177	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:25.852689981 CET	50700	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:25.900580883 CET	53	50700	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:30.199570894 CET	54069	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:30.259031057 CET	53	54069	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:35.545481920 CET	57017	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:35.603230953 CET	53	57017	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:46.370151043 CET	56327	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 15:19:46.418111086 CET	53	56327	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:48.427623034 CET	50243	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:48.483961105 CET	53	50243	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:49.349822998 CET	61249	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:49.400623083 CET	53	61249	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:50.600104094 CET	65252	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:50.648164988 CET	53	65252	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:51.750902891 CET	64367	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:51.801675081 CET	53	64367	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:52.500055075 CET	55066	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:52.571793079 CET	53	55066	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:53.266058922 CET	60211	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:53.322585106 CET	53	60211	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:54.261775017 CET	56570	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:54.318098068 CET	53	56570	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:55.116291046 CET	58454	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:55.172832966 CET	53	58454	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:56.261872053 CET	55180	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:56.323420048 CET	53	55180	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:57.543320894 CET	58721	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:57.602691889 CET	53	58721	8.8.8.8	192.168.2.6
Jan 19, 2021 15:19:59.117361069 CET	57691	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:19:59.174688101 CET	53	57691	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:00.556866884 CET	52943	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:00.613239050 CET	53	52943	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:01.378253937 CET	59489	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:01.434278965 CET	53	59489	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:04.682545900 CET	64022	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:04.746798038 CET	53	64022	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:05.019224882 CET	60023	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:05.075725079 CET	53	60023	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:07.972140074 CET	57193	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:08.022849083 CET	53	57193	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:10.842967987 CET	50248	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:10.891036034 CET	53	50248	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:14.784797907 CET	64413	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:14.846200943 CET	53	64413	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:15.742990971 CET	60429	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:15.790961981 CET	53	60429	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:17.388562918 CET	60345	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:17.390896082 CET	58730	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:17.445122957 CET	53	60345	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:17.549531937 CET	53	58730	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:17.566756964 CET	53830	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:17.631253004 CET	53	53830	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:17.893033028 CET	57226	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:17.952214003 CET	53	57226	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:22.947998047 CET	57880	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:23.014420033 CET	53	57880	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:28.679657936 CET	60850	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:28.730480909 CET	53	60850	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:44.793988943 CET	53187	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:44.841954947 CET	53	53187	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:49.392106056 CET	55830	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:49.440058947 CET	53	55830	8.8.8.8	192.168.2.6
Jan 19, 2021 15:20:50.267085075 CET	55145	53	192.168.2.6	8.8.8.8
Jan 19, 2021 15:20:50.325826883 CET	53	55145	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 15:18:50.529812098 CET	192.168.2.6	8.8.8.8	0xb40a	Standard query (0)	www.covid19-siparadigm.com	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:53.074805021 CET	192.168.2.6	8.8.8.8	0xf204	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 15:18:53.657824039 CET	192.168.2.6	8.8.8.8	0x7f18	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:59.222012043 CET	192.168.2.6	8.8.8.8	0xfb98	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 19, 2021 15:19:06.935475111 CET	192.168.2.6	8.8.8.8	0x22ba	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 15:18:50.604357958 CET	8.8.8.8	192.168.2.6	0xb40a	No error (0)	www.covid19-siparadigm.com	neovare-alb-285209131.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 15:18:50.604357958 CET	8.8.8.8	192.168.2.6	0xb40a	No error (0)	neovare-alb-285209131.us-west-2.elb.amazonaws.com		54.149.7.8	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:50.604357958 CET	8.8.8.8	192.168.2.6	0xb40a	No error (0)	neovare-alb-285209131.us-west-2.elb.amazonaws.com		54.186.198.126	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:50.604357958 CET	8.8.8.8	192.168.2.6	0xb40a	No error (0)	neovare-alb-285209131.us-west-2.elb.amazonaws.com		52.37.26.144	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:53.134602070 CET	8.8.8.8	192.168.2.6	0xf204	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 15:18:53.134602070 CET	8.8.8.8	192.168.2.6	0xf204	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:53.715930939 CET	8.8.8.8	192.168.2.6	0x7f18	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 15:18:53.715930939 CET	8.8.8.8	192.168.2.6	0x7f18	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jan 19, 2021 15:18:59.294507980 CET	8.8.8.8	192.168.2.6	0xfb98	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 15:18:59.294507980 CET	8.8.8.8	192.168.2.6	0xfb98	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.161	A (IP address)	IN (0x0001)
Jan 19, 2021 15:19:06.993134022 CET	8.8.8.8	192.168.2.6	0x22ba	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.covid19-siparadigm.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49721	54.149.7.8	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 15:18:50.812448978 CET	40	OUT	GET / HTTP/1.1 Host: www.covid19-siparadigm.com 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

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 15:18:51.017225981 CET	51	IN	HTTP/1.1 301 Moved Permanently Server: awselb/2.0 Date: Tue, 19 Jan 2021 14:18:50 GMT Content-Type: text/html Content-Length: 134 Connection: keep-alive Location: https://www.covid19-siparadigm.com:443/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 15:18:51.443342924 CET	54.149.7.8	443	192.168.2.6	49723	CN=*.siparadigm-covid19.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Dec 07 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Jan 06 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4720 Parent PID: 3572

General

Start time:	15:18:46
Start date:	19/01/2021
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.covid19-siparadigm.com'
Imagebase:	0x7ff7c15e0000
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: 5968 Parent PID: 4720

General

Start time:	15:18:48
Start date:	19/01/2021
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=1592,1923756594479640155,10121834588426309513,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /prefetch:8
Imagebase:	0x7ff7c15e0000
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: 6172 Parent PID: 4720

General

Start time:	15:19:41
Start date:	19/01/2021
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=quarantine.mojom.Quarantine --field-trial-handle=1592,1923756594479640155,10121834588426309513,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3936 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly