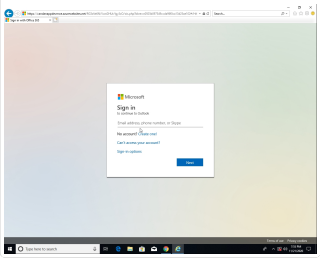
ID: 321414
Cookbook: browseurl.jbs
Time: 19:53:42
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

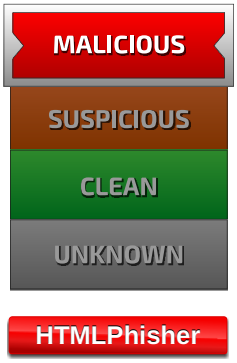
Analysis Report https://www.canva.com/design/DAEOE…

Overview

General Information

Sample URL:	https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_co...DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton
Analysis ID:	321414
Most interesting Screenshot:	

Detection

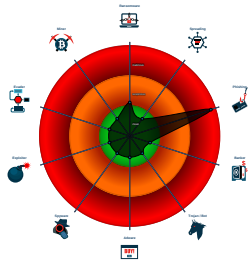


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_20
- Yara detected HtmlPhish_35
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 2412 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --force-renderer-accessibility 'https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3636 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,14482813496842422081,2496366691596550 75,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- dllhost.exe (PID: 6616 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- iexplore.exe (PID: 7072 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6292 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7072 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

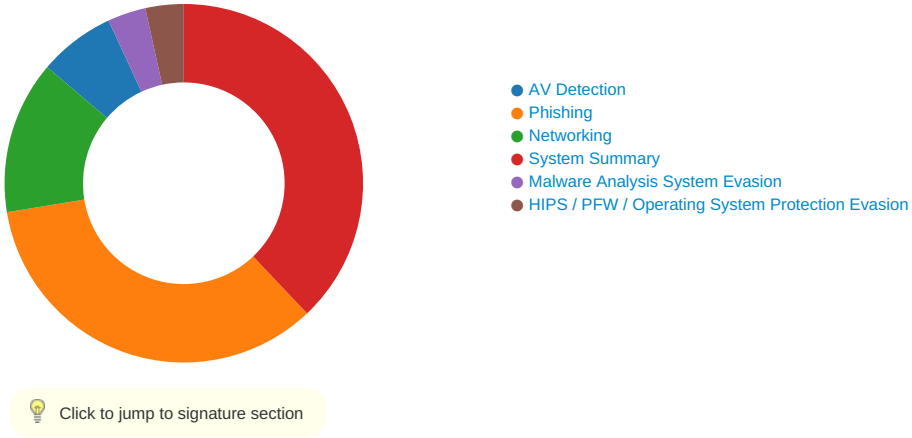
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ois[1].htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ois[1].htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	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

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_20

Yara detected HtmlPhish_35

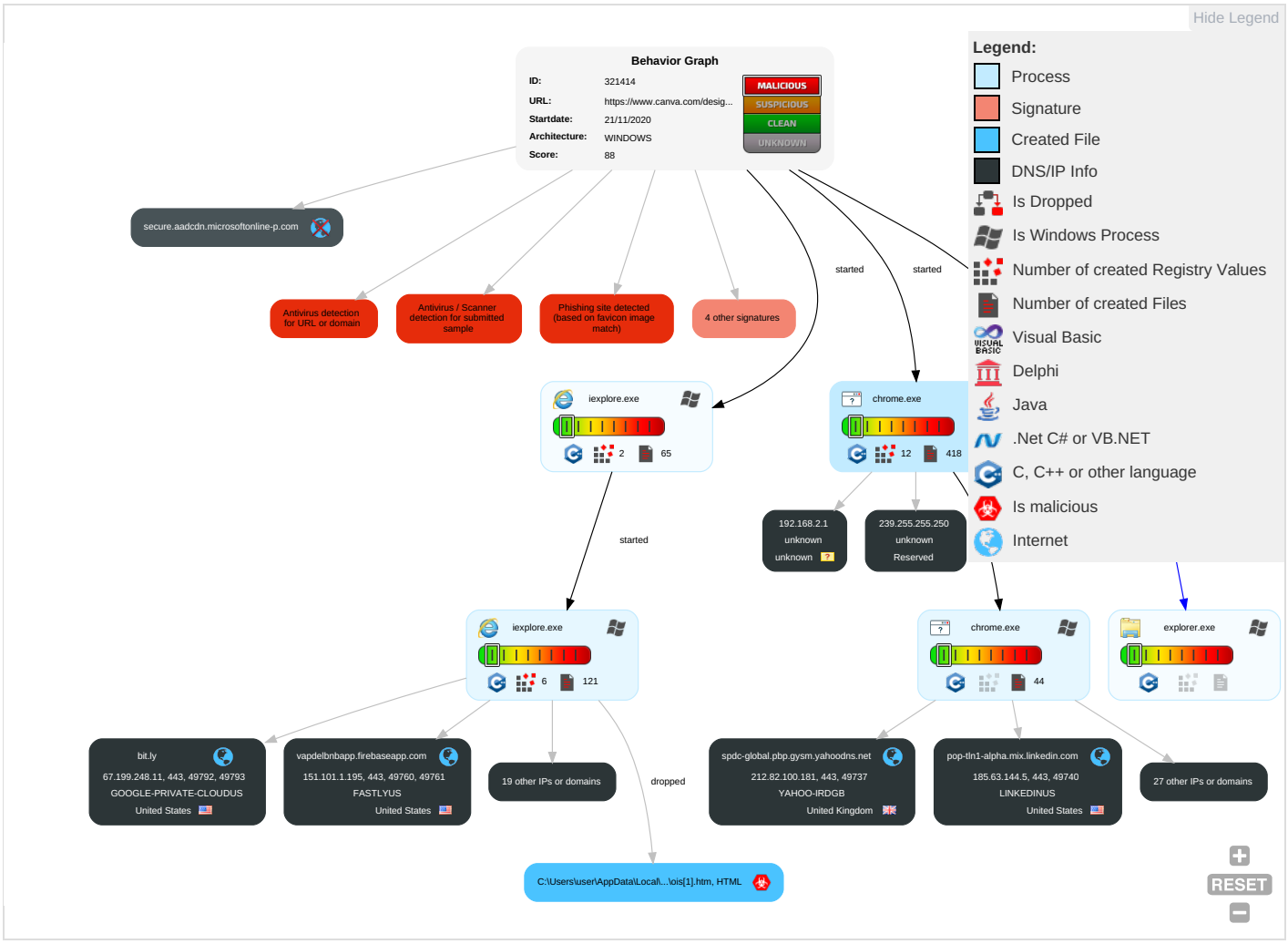
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

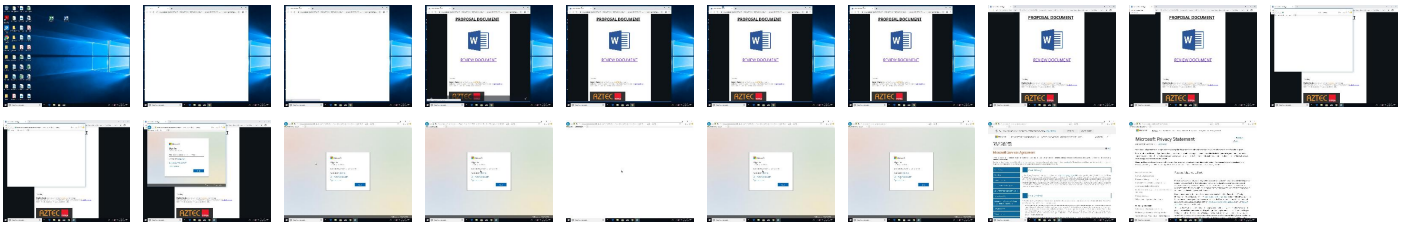
Behavior Graph

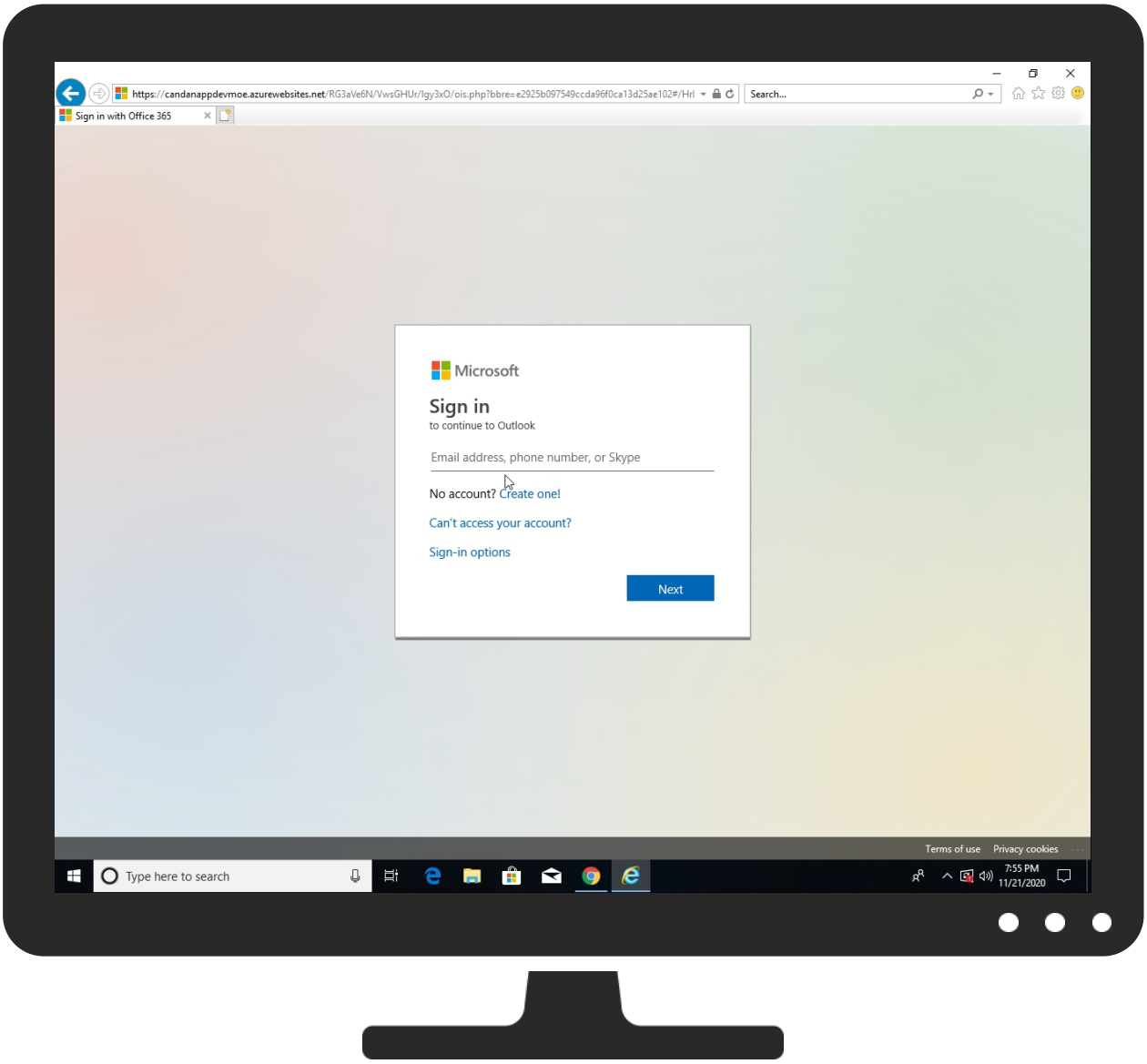


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	0%	Virustotal		Browse
http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	0%	Avira URL Cloud	safe	
http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
vapdelbnbapp.firebaseapp.com	0%	Virustotal		Browse
spdc-global.pbp.gysm.yahoodns.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
cnd11.smsmail.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#	100%	UrlScan	phishing brand: microsoft	Browse
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#/HrL23NdtW72OhsDvgnKTV7Nv5V9Ue8mfvCoKB3G-@&!nMo7W9B6y82fXLE3mVQIAZOb5sgkq@!&4Z1UuNv62qmRrls3xtfOVy5pbFc&@!-hZm2M8cvhno7HhcjvXE5ms0cFIgcPIbydjyxyNy8FsWDItSyEvBo9Tkq7iTwesWYR7C7cpo2eK2TVt7mmLfJugkUSIGpuDY-EoicDWUD9oHAmIGmguDfEbtuTy5PhCbGlyfyBHSrqoE93n7LpTNTF2sZl3II9flnwY0lBZmY2d/xgjRGw3OCMpm9jhxowojcuDfNcvCL860i5ImRV8KAn6eaYYP5slY8DZIE4HIDTBZdr	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0c	0%	Avira URL Cloud	safe	
http://https://js.appboycdn.com/web-sdk/3.0/appboy.core.min.js	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://privacy.m	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	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://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://www.skype.com).	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/lightweightsignuppackage_oZIcfFtGMdm_yHyDEji_8w2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/$HTTP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/ddm/fls/i/dc_pre=CPKCve-nlO0CFcDJuwgdfJIKSg;src=9812343;type=retar0;c	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	Avira URL Cloud	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
dart.l.doubleclick.net	172.217.18.102	true	false		high
pagead46.l.doubleclick.net	172.217.23.98	true	false		high
stats.l.doubleclick.net	108.177.15.154	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
cl.canva.com	104.18.216.67	true	false		high
vapdelbnbapp.firebaseapp.com	151.101.1.195	true	false	• 0%, Virustotal, Browse	unknown
www.canva.com	104.18.215.67	true	false		high
spdc-global.pbp.gysm.yahoodns.net	212.82.100.181	true	false	• 0%, Virustotal, Browse	unknown
pop-tln1-alpha.mix.linkedin.com	185.63.144.5	true	false		high
cnd11.smsmail.net	172.67.185.66	true	false	• 0%, Virustotal, Browse	unknown
static.canva.com	104.18.216.67	true	false		high
pagead.l.doubleclick.net	172.217.16.130	true	false		high
js.appboycdn.com	104.22.9.79	true	false		unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
bit.ly	67.199.248.11	true	false		high
font-public.canva.com	104.18.215.67	true	false		high
www.google.co.uk	172.217.21.195	true	false		unknown
unpkg.com	104.16.122.175	true	false		high
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
media-private.canva.com	104.18.216.67	true	false		high
sp.analytics.yahoo.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sdk.iad-01.braze.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
acctcdn.msauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
client.hip.live.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
www.facebook.com	unknown	unknown	false		high
signup.live.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown
px.ads.linkedin.com	unknown	unknown	false		high
candanappdevmoe.azurewebsites.net	unknown	unknown	false		unknown
googleads.g.doubleclick.net	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
9812343.fls.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

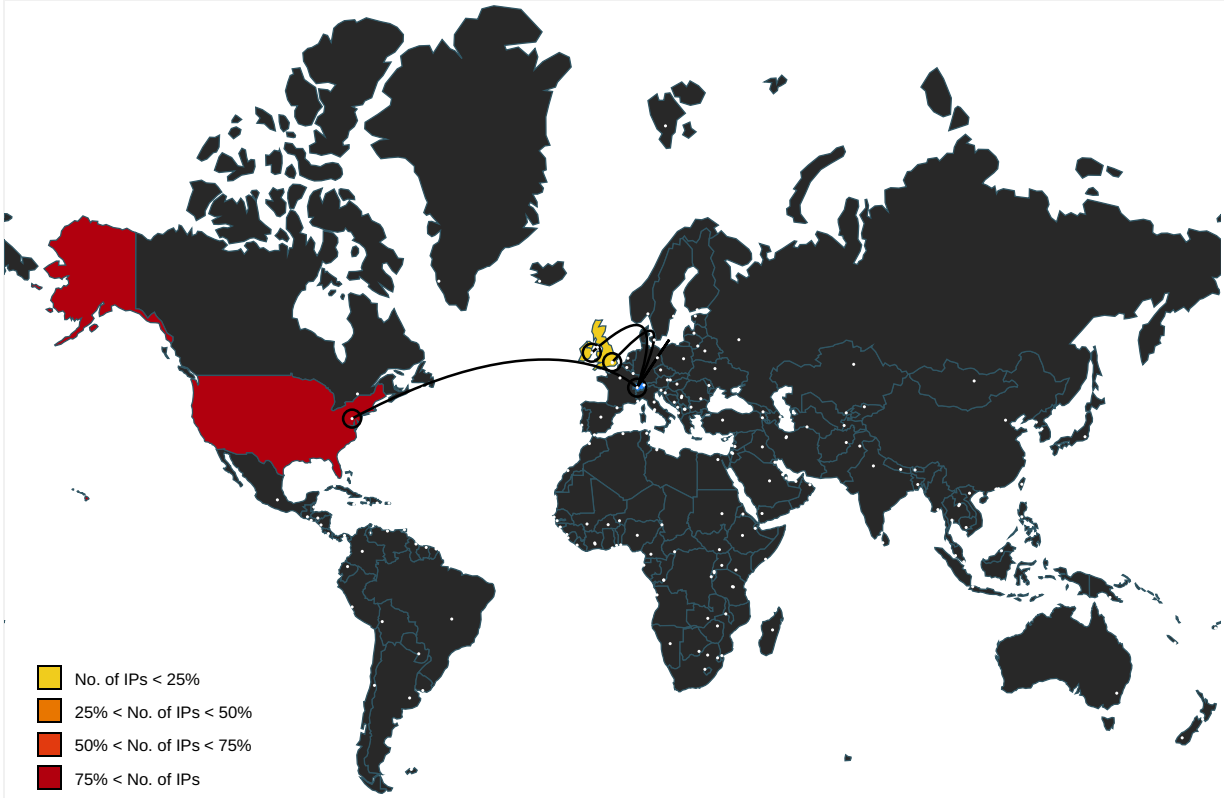
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.8.dr	false		high
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/	~DF6CB4169852C01DFC.TMP.7.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://www.acuityads.com/opt-out/	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.youradchoices.ca/fr	PrivacyStatement[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_pVtahKS9WUIZdNqg1DDhHg2.js?v=1	signup[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.canva.com/	QuotaManager.0.dr	false		high
http://https://www.adr.org	servicesagreement[1].htm.8.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct)	servicesagreement[1].htm.8.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	PrivacyStatement[1].htm.8.dr	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.227759354.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.8.dr	false		high
http://opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfU j8VuqFA2[1].js.8.dr	false		high
http://https://static.canva.com/web/a8284a82e57c7d67d5e3.2.js	be13fec43ec95b31_0.0.dr	false		high
http://www.json.org/json2.js	knockout_3.3.0_X1BYS2jZMbi7hfU j8VuqFA2[1].js.8.dr	false		high
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.227759354.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.227759354.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aka.ms/taxservice	servicesagreement[1].htm.8.dr	false		high
http://https://skype.com/go/myaccount	servicesagreement[1].htm.8.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.8.dr	false		high
http://https://www.appnexus.com/	PrivacyStatement[1].htm.8.dr	false		high
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfU j8VuqFA2.js?v=1	signup[1].htm.8.dr	false	• Avira URL Cloud: safe	unknown
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0c	{78B7B8C5-2C76-11EB-90E4-ECF4B B862DED}.dat.7.dr	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://a.nel.cloudflare.com/report?s=%2FiF37Jdg5v1kkl4zN2xmt40KaHSs2RIhp4VBtMecUDFyqsp8NQOYmTa65bVx	Reporting and NEL.1.dr	false		high
http://https://js.appboycdn.com/web-sdk/3.0/appboy.core.min.js	e4115b2c93fca474_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://privacy.m	{78B7B8C5-2C76-11EB-90E4-ECF4BB862DED}.dat.7.dr	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://priv-policy.imrworldwide.com/priv/browser/us/en/optout.html	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.youronlinechoices.com/	PrivacyStatement[1].htm.8.dr	false		high
http://https://static.canva.com/web/36db7dd680be1e933b01f9539cc51480.2.js	b21148925dccb19e_0.0.dr	false		high
http://https://mixer.com/contact	servicesagreement[1].htm.8.dr	false		high
http://https://a.nel.cloudflare.com/report?s=Q42UNRo%2Fz2ZO04fxuZrsWp6lM1HtqA3LAS8FX0WiaVN62O%2FKlj%2F0O2xX	Reporting and NEL.1.dr	false		high
http://https://dns.google	f12a1474-b215-46cb-a5cf-1ff4f9516ed0.tmp.1.dr, eb720268-0b80-48ff-9de9-f7e2c5524892.tmp.1.dr, bf83cbd0-4553-4aaa-b88b-2db8426c696f.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://9812343.fls.doubleclick.net/activityi;dc_pre=CPKCve-nlO0CFcDJuwgdfJIKSg;src=9812343;type=ret	Current Session.0.dr	false		high
http://https://www.adjust.com/opt-out/	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.xbox.com/managedatacollection	PrivacyStatement[1].htm.8.dr	false		high
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	signup[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mpegla.com).	servicesagreement[1].htm.8.dr	false	• Avira URL Cloud: safe	low
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	signup[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com).	servicesagreement[1].htm.8.dr	false	• Avira URL Cloud: safe	low
http://https://www.xbox.com	PrivacyStatement[1].htm.8.dr	false		high
http://https://acctcdn.msauth.net/lightweightsignuppackage_oZIcfFtGMdm_yHyDEji_8w2.js?v=1	signup[1].htm.8.dr	false	• Avira URL Cloud: safe	unknown
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	PrivacyStatement[1].htm.8.dr	false		high
http://https://github.com/douglascrockford/JSON-js	signup[1].htm.8.dr	false		high
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	imagestore.dat.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.canva.com/static/lib/sentry/5.15.4.min.js	c4950d0815c21f68_0.0.dr	false		high
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.canva.com/web/292bbecde0fce6ffe18847a12c9a6dc6.2.runtime.js	e3511df7a5a5c326_0.0.dr	false		high
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	signup[1].htm.8.dr	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.8.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.skype.com/go/legal	servicesagreement[1].htm.8.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.8.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.microsoft.	{78B7B8C5-2C76-11EB-90E4-ECF4BB862DED}.dat.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/$HTTP	~DF6CB4169852C01DFC.TMP.7.dr	true	• Avira URL Cloud: safe	unknown
http://https://canva.com/r	eba1480a166263c9_0.0.dr	false		high
http://https://www.linkedin.com/legal/privacy-policy	PrivacyStatement[1].htm.8.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://support.xbox.com/help/friends-social-activity/community/use-safety-settings	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	PrivacyStatement[1].htm.8.dr	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false		high
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.8.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	PrivacyStatement[1].htm.8.dr	false		high
http://https://login.skype.com/login	PrivacyStatement[1].htm.8.dr	false		high
http://https://npms.io/search?q=ponyfill.	lodash.min[1].js.8.dr	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false		high
http://https://www.skype.com/go/ustax	servicesagreement[1].htm.8.dr	false		high
http://jquery.org/license	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.8.dr	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://canva.com/g	e3511df7a5a5c326_0.0.dr	false		high
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false		high
http://https://acctcdn.msauth.net	signup[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.optimizely.com/legal/opt-out/	PrivacyStatement[1].htm.8.dr	false		high
http://sizzlejs.com/	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.8.dr	false		high
http://www.tiro.com	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://canva.com/S	be13fec43ec95b31_0.0.dr	false		high
http://https://canva.com/U	f50d7bc85406f58b_0.0.dr	false		high
http://https://signup.live.com/error.aspx?errcode=1045&mkt=en-US	signup[1].htm.8.dr	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://adservice.google.co.uk/ddm/fls/i/dc_pre=CPKCve-nlO0CFcDJuwgdfJIKSg;src=9812343;type=retar0;c	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://9812343.fls.doubleclick.net	Current Session.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=fP6c4NQXT5R6CtiH5v3fb0dwWJNdcVwLQDjTMF3wPbdkFq65nd8VaqX4TE9He0	Reporting and NEL.1.dr	false		high
http://www.typography.netD	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.00000000.227759354.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.privacyshield.gov/welcome	PrivacyStatement[1].htm.8.dr	false		high
http://https://ondemand.webtrends.com/support/optout.asp	PrivacyStatement[1].htm.8.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.8.dr	false		high
http://https://canva.com/D	865fd4c70d31683c_0.0.dr	false		high
http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_cam	History.0.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	imagestore.dat.8.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://snap.licdn.com/li.lms-analytics/insight.beta.min.js	5e83b9cfa3f81ad1_0.0.dr	false		high
http://https://www.canva.com:443	057b19b2-c529-4082-b40c-6b9f75226950.tmp.0.dr	false		high
http://https://www.appsflyer.com/optout	PrivacyStatement[1].htm.8.dr	false		high
http://https://privacy.micros	{78B7B8C5-2C76-11EB-90E4-ECF4BB862DED}.dat.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aka.ms/redeemrewards).	servicesagreement[1].htm.8.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
104.16.122.175	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.22.66	unknown	United States		15169	GOOGLEUS	false
104.18.215.67	unknown	United States		13335	CLOUDFLARENETUS	false
185.63.144.5	unknown	United States		14413	LINKEDINUS	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
172.217.18.102	unknown	United States		15169	GOOGLEUS	false
172.217.21.195	unknown	United States		15169	GOOGLEUS	false
172.217.16.194	unknown	United States		15169	GOOGLEUS	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
212.82.100.181	unknown	United Kingdom		34010	YAHOO-IRDGB	false
104.18.216.67	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.1.195	unknown	United States		54113	FASTLYUS	false
172.217.23.98	unknown	United States		15169	GOOGLEUS	false
67.199.248.11	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
104.22.9.79	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.16.130	unknown	United States		15169	GOOGLEUS	false
172.67.185.66	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321414
Start date:	21.11.2020
Start time:	19:53:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton
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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.phis.win@36/276@32/22
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://signup.live.com/signup?wa=wsignin1.0&rpsnv=13&ct=1526624083&rver=6.7.6640.0&wp=MBI_SSL&wreply=https%3a%2f%2foutlook.live.com%2fowa%2f%3flp%3d1%26RpsCsrfState%3dbcb5f3f6-b97d-ed7b-9df9-8861d8e6ea95&id=292841&CBCXT=out&lw=1&fl=dob%2cflname%2cwld&cobrandid=90015&contextid=982B2F78FD1575EA&bk=1526624084&uiflavor=web&uaid=71693e68d6ab4064b6ac1c2f53d534bb&mkt=EN-US&lc=1033 • Browsing link: https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bre=e2925b097549ccda96f0ca13d25ae102# • Browsing link: https://bit.ly/39oebGZ • Browsing link: https://bit.ly/2Jmn3lA • Browsing link: https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 216.58.206.14,

172.217.18.13, 172.217.16.142, 173.194.187.8, 173.194.182.74, 172.217.16.138, 216.58.205.227, 216.58.212.138, 172.217.23.104, 151.101.1.208, 151.101.65.208, 151.101.129.208, 151.101.193.208, 204.79.197.200, 13.107.21.200, 23.210.249.242, 172.217.23.174, 216.58.212.163, 13.107.42.14, 216.58.208.36, 172.217.21.227, 172.217.18.106, 216.58.212.170, 142.250.74.202, 172.217.21.234, 216.58.205.234, 172.217.23.138, 172.217.21.202, 172.217.18.170, 216.58.207.42, 216.58.207.74, 172.217.22.10, 216.58.208.42, 172.217.23.106, 104.108.39.131, 13.71.170.130, 51.132.208.181, 2.18.68.82, 13.107.246.10, 104.108.36.62, 13.107.42.22, 40.126.1.128, 20.190.129.2, 20.190.129.133, 40.126.1.166, 20.190.129.130, 20.190.129.19, 20.190.129.17, 40.126.1.145, 52.114.77.33, 40.126.9.98, 20.190.137.78, 20.190.137.64, 20.190.137.1, 92.122.145.53, 92.122.213.200, 92.122.213.219, 2.18.70.63, 152.199.19.160, 92.122.213.194, 92.122.213.247, 152.199.19.161, 92.122.213.240, 104.108.38.107, 172.217.16.131, 173.194.182.233, 172.217.18.99

- Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, assets.onestore.ms.edgekey.net, r3---sn-4g5e6ns6.gvt1.com, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, a1945.g2.akamai.net, l-0005.l-msedge.net, clients2.google.com, www.google.com, standard.t-0001.t-msedge.net, statics-marketingsites-eus-ms-com.akamaized.net, acctcdnvzeuno.azureedge.net, skypedataprdcolneu04.cloudapp.net, acctcdnvzeuno.ec.azureedge.net, dual-a-0001.a-msedge.net, t-0001.t-msedge.net, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, www.tm.f.prd.aadg.trafficmanager.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, cs9.wpc.v0cdn.net, afd.t-0001.t-msedge.net, i.s-microsoft.com, adservice.google.com, e9706.dscg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, e13761.dscg.akamaiedge.net, safebrowsing.googleapis.com, prod.fs.microsoft.com.akadns.net, accounts.google.com, fonts.gstatic.com, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, login.msa.msidentity.com, browser.events.data.microsoft.com, c.s-microsoft.com, wildcard.licdn.com.edgekey.net, go.microsoft.com.edgekey.net, l-0013.l-msedge.net, skypedataprdcolwus15.cloudapp.net, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, browser.events.data.trafficmanager.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com, update.googleapis.com, r4.sn-4g5e6nsz.gvt1.com, watson.telemetry.microsoft.com, www.gstatic.com, a1778.g2.akamai.net, www.google-analytics.com, e10583.dspg.akamaiedge.net, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, www.tm.a.prd.aadg.akadns.net, statics-marketingsites-wcus-ms-com.akamaized.net, www.googleapis.com, r4---sn-4g5e6nsz.gvt1.com, blobcollector.events.data.trafficmanager.net, account.msa.akadns6.net, aadcdnoriginwus2.afd.azureedge.net, privacy.microsoft.com.edgekey.net, r5---sn-4g5e6ns7.gvt1.com, r3.sn-4g5e6ns6.gvt1.com, www.googleadservices.com, d2.shared.global.fastly.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, acctcdn.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, bat.bing.com, img-prod-cms-rt-microsoft-com.akamaized.net, www-linkedin-com.l-0005.l-msedge.net, www-google-analytics.l.google.com, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, Edge-Prod-FRAr3.ctrl.t-0001.t-msedge.net, r5.sn-4g5e6ns7.gvt1.com, waws-prod-yt1-019.cloudapp.net, bat-bing-com.a-

	0001.a-msedge.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, www.microsoft.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile 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
19:54:34	API Interceptor	1x Sleep call for process: dllhost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0380481d-6e6d-4286-901e-4e222ba67918.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):	162443
Entropy (8bit):	6.082689798422006
Encrypted:	false
SSDEEP:	3072:Sq3A2NNCxQM9b0q+szv+tnMIsFcbXafIB0u1GOJmA3iuRed:L3rExQM9b7fD+ZMhaqfIlUOoSiuRe
MD5:	018BF125E30AA6FF8903A462C6D5696B
SHA1:	855B2E6ADD86F9EDBAE81DD4E10B92694FEEE3A5
SHA-256:	47176B76A9BDE80B8FAFAD3C615B571A35C89D77D3FE67BEE7B34B3594392976
SHA-512:	DEC8167EA99C6832DD35FB0F9649C11A34D02BACF1610566889E8971F236A8958FF48FFCB0752AD46E63C197B0FB6DE5128A315365DCF62B58A77832CE2DB90
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":1.606017272922974e+12,"network":1.605984874e+12,"ticks":96932932.0,"uncertainty":4340447.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\03d7d4b8-bf47-4e2d-b987-6916b04ceb0b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.752159730526242
Encrypted:	false
SSDEEP:	384:4CsZyrTRuwF6hNV6Q3yN3r0vjJ3EDhwHpAGYXrC9HDx09958rGbmGR+JX3PQOdlU:Hc9eKF9qNA40errdtoHHOZK7pH03
MD5:	8D7D80713807C8841BD2EECC03C6E750
SHA1:	F79F57EB4A91B7AFAE9B011D2AC360120BA1E33D
SHA-256:	B7A197971E17B82C92009A0283F9C4692E9A5AE96A2A9FF907051EFBA931A512
SHA-512:	B3E4625D4A388D557684DA9A1B39513011AA0BBD784A1568D831F0C03CC7A821BC4530ABE5CD7B864BDFBB961BE719ACFA2284E45CCC85732AF6CB33DFBF2C0
Malicious:	false
Reputation:	low
Preview:	`o.....*...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....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\31ad302b-02a6-4233-9239-565cc2cb0a27.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):	162443
Entropy (8bit):	6.082689560512026
Encrypted:	false
SSDEEP:	3072:34XA2NNCxQM9b0q+szv+tnMIsFcbXafIB0u1GOJmA3iuRed:IXrExQM9b7fD+ZMhaqfIlUOoSiuRe
MD5:	AAB69FBE3711F89D6880EC754A7F032C
SHA1:	94B8F5630CC45ECDAD2C795B2BB5B28D4DB3ACFD
SHA-256:	56DD6532D661B692AB5892E0ABB86DC4F1B028020E1313432EE55F51E9581345
SHA-512:	75A465E5E28EFAD701C7BAE86592975D59190ED6343390C95D5C617A52C44C919D56A566B7A214EB836A74524786A71672E0490044282E134C78BE4102AE81C8
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\31ad302b-02a6-4233-9239-565cc2cb0a27.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.606017272922974e+12,"network":1.605984874e+12,"ticks":96932932.0,"uncertainty":4340447.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016249939"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\9dcc89f3-385b-4f05-9c9e-8b575f382a17.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.7514938146288253
Encrypted:	false
SSDEEP:	384:nCsZyrTRuwxh23yN3r0vjJ3EDhwHpAGYXrC9HDx09958rGbmGR+JX3PQOdlfNK1X:Cc2KF9qNA40errdtoHHOZK7pH09
MD5:	45DB23932D1C6FF073D12C9AD1DEAE69
SHA1:	2BF9527C119F2CFC62966F6EC02AB0DD4673BF80
SHA-256:	D7405AB91502C6140232392F717AFB3F5BF7557DD137D4D8496630EE7481526F
SHA-512:	F98AF7653D60C82AC9DEE39BCF05DB7A1FD7E923F4E9EA607933CBCBD9374499680C4DE8BCA42D586A16226954A9819EAC6C37E7C6E62A4EE3C8674572F0D8D
Malicious:	false
Reputation:	low
Preview:	.g.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\037c2da2-f386-4614-bd45-3a13cafd8a19.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):	21278
Entropy (8bit):	5.553097406290666
Encrypted:	false
SSDEEP:	384:fBiCtZHLlGXpZXr31kXqKf/pUZNCgVLH2HfDTqrUBtjHG/8gnT4tBp7y4n:fklHLlG59r31kXqKf/pUZNCgVLH2Hfvl
MD5:	2E15032A8C17C088A01B0C5FB31B0827
SHA1:	632F47F570157B618E8323CC28A60B94D086D306
SHA-256:	DCBDC8D978DF05F787DE263A1ACD9C5CB45ED650E2FF7BA4E1B9B562BC2B5DC6
SHA-512:	0FE413FCB9A8044D7FBCED80DB714C173B8ECDCCD374E10D22C57952F527D583B17E80EDC8F0DA5302B6C328625E8E3DE2FAD26277F6A2445C9F6B64947EEEC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\037c2da2-f386-4614-bd45-3a13cafd8a19.tmp

Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13250490870259270","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\057b19b2-c529-4082-b40c-6b9f75226950.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):	4790
Entropy (8bit):	4.967958818961529
Encrypted:	false
SSDEEP:	96:nSOC5spMpcVSyk0JCKL8Ev4kV182bOEQVuwn:nSOCyapcx4Khv4kVe1
MD5:	57E97F2F7C75F6FEA134BBFE77B045EA
SHA1:	3A9C70CBAA0163E7317CCF8F36A15561EABC0120
SHA-256:	96C3570D2A258CA30ED11586B417A2349CCB6E540A3AF2832C9796F1FEEFDBAE
SHA-512:	184997A77DD9026ECBC0834EAC7ADB96C896EAA551E8121DA6B88B0CEB3B0BFACFB6CB567B289C91DF056290408067C1ACD074404F2E382D09621536D40119 3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250490870560092","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"c ountryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0 ","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ac71887-e8a5-4054-be40-9096647c1069.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cc9e1af-6f77-4fcb-b362-ebbe87246039.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):	5043
Entropy (8bit):	5.604609613455214
Encrypted:	false
SSDEEP:	96:rf8+o/9/CAppUo+UGUkNeUaieUjUUqUzRUE9bdUCUoUxKU5FUiPeU9UE6UkUYUD:r0+o/9/CAppURUGUmeUuUjUUqUzRUE9K
MD5:	F4E95F191D64E7AF9D1D20364D4D7D13
SHA1:	EDC511FEF4EF82F7F51A8263B12BCF95BE850105
SHA-256:	C9FC4BA57263C3A00D782F5DD4B86A041D4D97A12EEFF55BD54F7E8B53021661
SHA-512:	8B39E97227534415A9E0D478A6E0180EB187E883377C50E925DA602FC2EAE90425FB66B12884B4B9C40F3BECD4FFD1CD8FCC493B04ADC4D12F5BAE72139503 A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cc9e1af-6f77-4fcb-b362-ebbe87246039.tmp	
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1608609274.81039,"expect_ct_observed":1606017274.81039,"expect_ct_report_uri":"http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only","host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606622074.141304,"expect_ct_observed":1606017274.141304,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"DEYqY3fY1uk+rWZFaOylMBhnZNdkY4A9bQ0Ct+WSQy0=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606622075.284152,"expect_ct_observed":1606017275.284152,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"HIplQqWMs6ZxBLdnO3HzMXf8AYhhblad/Qg77wu6W6Q=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606622074.092926,"expect_ct_observed":1606017274.092926,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"ThT+U8nQYq+ZrB7qkByu3lLYgUKH+PsG

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6e5f991d-59ff-43cb-b3f8-7faaeff5d978.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):	21277
Entropy (8bit):	5.55287870257681
Encrypted:	false
SSDEEP:	384:fBiCtZHLlGXpZXr31kXqKf/pUZNCgVLH2HfDTqrUBtjHGu8gnT4tB/ry4x:fkIHLlG59r31kXqKf/pUZNCgVLH2Hfvg
MD5:	B56931421C16ACED3D18E03F633CA85A
SHA1:	A46330BE76039F3F8CFE5134CB2CE4AF4A358E16
SHA-256:	8D846BA50298D03196683BE556A7282C4191C70C26AE7FEAE65AFC670E8D631E
SHA-512:	A45ED13AE638E38732FC7442FB65CCBEAC7AAA9EA8BA6057BB61A1FCF370DE7C8CA41B3872717587471103C29C629B754D0A867A8F982BF23F5FF182623405A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13250490870259270","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73d2354f-74b6-435c-b75a-76f4d7a8e861.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):	15427
Entropy (8bit):	5.601314520388077
Encrypted:	false
SSDEEP:	384:fBiCtOHLlGXpZXr31kXqKf/pUZNCgVLH2HfDTqrUwtgYy4K:fkpHLlG59r31kXqKf/pUZNCgVLH2Hfvh
MD5:	56155A6DF29465009661F526F25D1411
SHA1:	34B8ACD3722E48C9F944BE9B7D5393D64D5C6B90
SHA-256:	32A3C15AEF15338D36DB1A25F0014057CF7678D2FE248180DB3DC59730E9D26C
SHA-512:	0458150944343FABB88E4B85FA7B5810F87321C91A04F6F1E4FA30F892E71DF7AD6D2162054B7673A0B9C44EB930FB171CE846D0345BB871C83113FDEE2E5900
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13250490870259270","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.26644656935669
Encrypted:	false
SSDEEP:	6:QfwjMAq2PWXp+N23iKKdK9RXXTZIFUtwffwjOZmwyffwjikwOWXp+N23iKKdK9Rn:KwjIva5Kk7XT2FUtw3wjO/y3wji5f5KU
MD5:	493413B49A5EEBA80F0EAC36A6609970
SHA1:	F7DA659E139E58D09B1B3722263B384F6B84E6B0
SHA-256:	06AD32340B9EDBAEEA80C778AEA67979F54D045A17F02E0E543672B382081000
SHA-512:	5FA418F033231F6FCD2FCE3BF839AAD28E8A7B18AE2D7C43BE1E6B9579CB46E11F18EF20EC588A148B7AB1859EDB6FDFE6A3CA0DF3455426627520CA1523F6A3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2020/11/21-19:54:43.716 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/21-19:54:43.718 14b0 Recovering log #3.2020/11/21-19:54:43.718 14b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.251224892765836
Encrypted:	false
SSDEEP:	6:QfwlBkVq2PWXp+N23iKKdKyDZIFUtwffBSIgZmwyffBSmIRSIkwOWXp+N23iKKdn:Kwzcva5Kk02FUtw3kx/y3kRP5f5KkWJ
MD5:	A693A3ED8B674CD0F358CDD5DD9DE500
SHA1:	5232256A195F303AC335FE28628578CEB000FD56
SHA-256:	F65F07416BC5D1F3E14E6FAF4BBAE8BB15564F6C0086CA523AA5F44B78E0C3B7
SHA-512:	FAFEA233C93CAAD8BC37C620425A2D48BAC50BC2FB7D8FB1E91EFC022DD0D6681B255E59049CFA1932D71456857E02301CA1823239E280A6174172FE6CFF33(E
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.773 1424 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/21-19:54:46.765 1424 Recovering log #3.2020/11/21-19:54:46.770 1424 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\270ae0528ce28f93_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.456274231142861
Encrypted:	false
SSDEEP:	6:ms7lPYGLAAmrDXdLTArRCVNsllgqN0qCm4XK6t:Bh4tnArRCPMH0q9K
MD5:	0C92053E8C849C78C49E0D46F2229FEB
SHA1:	32B714D36F2AC3CA41C40A95EC18B74134FDD75A
SHA-256:	BD7AE56A2B260A982531AA3BE4A2A28754D1C12AB9EDEA582EFC01FDEDA74D20
SHA-512:	C28A5E3C58510E04FF7B2C1398980F001B8CEA52512F687AC0529759076F9BA8B4C815B8D589BF8D5119CB8C15B25F074175CA23F38E735F7DDB617D49F88939
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...6....._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://canva.com/.>.Q@./....._8...Z...b.N[.9.n._.g..R_.A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56a246e5228caa4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.516344401246368
Encrypted:	false
SSDEEP:	6:mekYk+TZEaoUGpr6v+llg91TscVhP4jxK6t:70+TCpr6mwxFVwL
MD5:	9F7BF8CB297A1E59842EBB10C75E6ED4
SHA1:	4DE077967F79F79F135F23B8AC74507041BFAC70
SHA-256:	91BDF5EC42384E8B142D5223790E72B937C966308E26BC0F031F21BEEB126AA1
SHA-512:	DB509A516B41E2AD1B7E152A72A0FFC03491D1F0F67B86EB0C0E3DB11B18E76A30D14F9FC8C4845C31E27336FE03E347D78F6F54E73DEEA4ECECA6F9E618CDE2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...."/v...._keyhttps://static.canva.com/web/169aab431c6d134d2e5b.2.js .https://canva.com/...Q@./.....P{.....YO....etn..._.. .9.....&)...A..Eo.....:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e83b9cfa3f81ad1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.466148431405253

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e83b9cfa3f81ad1_0	
Encrypted:	false
SSDEEP:	6:msRXXY+PW/ULMdaN1moVMellgLutCVothtK6t:BhArU80XJP
MD5:	4A2F417A68CF8912538272E7B6D2A2D9
SHA1:	85FFC7A1E337333CA206C45817583CB7AF68FDAB
SHA-256:	2C215D8420691069B3FB20FC71151DC2F4EA4D8FB9752A7E19E39E1B6DAEEE4D
SHA-512:	0FA720394A48F967980BE5F03799D1B39A498C964193DF7A733F662E6CCC8B10BB1ED49900D4554A4A02808BBD67157E7E65CC1449DF5A1E161250308AEE71FB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...7..k...._keyhttps://snap.licdn.com/li.lms-analytics/insight.beta.min.js .https://canva.com/..Q@./.....\C*...2hK.....>..I.B.....g....A..Eo.....T4.....A ..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6726d42dc28e6fb9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.4182626340939235
Encrypted:	false
SSDEEP:	3:m+lwRXa8RzYrSLLiMZJXMLHbJRCLTEfxvll/lHCrlDVXHRh0IGZmAzc7ll/lpK5M:m3hXYGL+MHMBNfJllgrBVXDhWcnK6t
MD5:	4F48926C0C3AA5C5272C1B0DA8DA8DBA
SHA1:	43EE17CFE4497E57A1632537DA2F57F0A3BC5213
SHA-256:	CBE59CFCE1417D0D62C6CE686F1B22E20683B582B0A57850478FA4026C4D757B
SHA-512:	194C0389F3F354245BF028582A19D869B368BAC26879D209E5D375D29C8EA690009275AD1006AA9FD95D3B919D87775E22CE27069E5156947AF32A212CC5627F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....1.,...._keyhttps://www.google-analytics.com/plugins/ua/ec.js .https://canva.com/.d.Q@./.....H5.0..~.E..z`.@...{Q.~....q/.N..A..Eo.....tY.y.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\865fd4c70d31683c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	745
Entropy (8bit):	5.925712908340997
Encrypted:	false
SSDEEP:	12:ctnAAddGUPnqu6t3plHux2pHgyyyJ31ABurf1IpdpbI8mWNjSNfbQiEsaR8idniK:cSAdDut3plHuyAyyAloYy/5H8ZEsayip
MD5:	98D129AB18AFE9C944F8DA7BB8FC1B51
SHA1:	C9A34BBF7E0514811CD14DC6B43FBA73C3C728C7
SHA-256:	6F7193BE413B8BEEA270972087E48AFC837912D30D94A45FC7D83FF15EAC0340
SHA-512:	6E69F3C4BCBB9E5F9A1136BFBFFE67A06F9DBCEABCBBB6893E83F30CC520528EAFB6ECA9901BE290148C60CE2F253679C6AFBFAC953B8C17EF78B9DB28C9 EAE3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...=.XO...._keyhttps://www.googleadservices.com/pagead/conversion/804757079/?random=1606017274529&cv=9&fst=1606017274529&num=1&rdp=1&valu e=0&label=5VqLCKW6taoBENe83v8C&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java =false&u_nplug=3&u_nmime=4&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.canva.com%2Fdesign%2FDAEOEcu9Gnc%2FC6LvqPRfMOYoF6OW lu9bVg%2Fview%3Futm_content%3DDAEOEcu9Gnc%26utm_campaign%3Ddesignshare%26utm_medium%3Dlink%26utm_source%3Dsharebutton&tiba=AZTEC%2 0ENGINEERING&hn=www.googleadservices.com&bttype=purchase&async=1&rfmt=3&fmt=4 .https://canva.com/D..Q@./.....[.....i..Y.j-o.6.....N...s.j.....A..Eo.....>R .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b21148925dccb19e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.598737680239985
Encrypted:	false
SSDEEP:	6:m+nYk+TTU7e2llg4/qQS3oYtagWnDl/hK6t:X+TRmf/FSYgR01
MD5:	D63E957ED0EA2A4094C1772412D2EB5E
SHA1:	F80D8861ECC2BE4AF7EE1B51B7A79CF6D5270DFC
SHA-256:	17FB4E47073074E2525DEBCD5E3F9E08EEC2A2AED9EBC0D7E9D09AD1DD510568
SHA-512:	DC50F4DADFB07735AFCD1D60925FD7EAB6834C36A32A41D22F57B9CCBFDD8336CC2C6C08535B1CE59A6BE9A4E3707F01C97CC8A0664FAD11365884CFF1DA EF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b21148925dccb19e_0	
Preview:	0\r..m.....Z.....7...._keyhttps://static.canva.com/web/36db7dd680be1e933b01f9539cc51480.2.js .https://canva.com/...Q@./.....|.....,....8..E.$.M.....h.|AQ....A..Eo.....B.y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb69cd55fcfa7140_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.55180852014075
Encrypted:	false
SSDEEP:	6:mvYk+Tndfcs2WWoSNgH+vllgftL4Az42K6t:G+T1cs2WWoSNgH+H8tLPr
MD5:	0B0871D2E4F2281B55241209ADC47446
SHA1:	3895003977CFA31C7B3C759BB81FCF342A6EB986
SHA-256:	3752B8C23CF4011CE6BF210881BB073EE68195520ECDDA7CA13C9C13A93D6868
SHA-512:	ED757B3EAD20FE9092827F68081C57AAC417FED572E1C56914F1F1610C2B866D5BC40EEC1F558B630D79F9D98C8D420D519A2167155E39F9BED3BB91C1A25C7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...X.0...._keyhttps://static.canva.com/web/3ad8884d65b676ef0625a45577e2cc20.2.js .https://canva.com/...Q@./.....n}.....n...n...QF...0..:.`x.ZQ....A..Eo.....p.5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be13fec43ec95b31_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.574348255852959
Encrypted:	false
SSDEEP:	6:m9Yk+TU0b3W7CPg+llggsEiMFXaPkAubK6t:Y+Tj+CPdMIyc
MD5:	6AABE21DAA35FC16EFC5E512B4F25399
SHA1:	CC184280761C1A4656BD56843A08BCDA29CD3D13
SHA-256:	550A8B5D8421FDCD055EF7ADF06726FBA342B0B47581176FBAB877784DF47886
SHA-512:	51AEAADB9F8098EFAFE3508D80D8D54F414C404BF28A7A9D33E1B8B81B4F1753307B8841031F43EEE1630DBE98348B06B79FFCEF525F2081EC0C429BDD03870
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...._i...._keyhttps://static.canva.com/web/a8284a82e57c7d67d5e3.2.js .https://canva.com/S..Q@./.....%{.....z.V!.,@..j..R.....P.... O....A..Eo.....7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2189956b60b2ce5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	5.302737799900454
Encrypted:	false
SSDEEP:	3:m+lLX+/la8RzYW147CVRCLTEas+ll/lHCtkb15EuKax04m+1lpK5kt:mvXYW+wNaJllgS5ka6+RK6t
MD5:	2D503B75CB58158302BCF29F58EE9041
SHA1:	9F3D8A37EAA565AFCEE1972961AC458C34E338A8
SHA-256:	6EE1227BBAB49BE7E771895659230D7F552DDDFEEED22EABAAFBF8FEA53C7A12
SHA-512:	0911CAB4ACF95F02DA415EB083AAB86A0945923E38BE2E667C88D9CA1EB53D6E69F4F8C18309AD48F6DB8A0660C6F6C02B61BDC76F57E6F27D6F78F212E0032 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3...x.5/..._keyhttps://bat.bing.com/bat.js .https://canva.com/.E.Q@./.....T.F..6Q..'s:....m6.7.M.... .o...A..Eo.....v4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3d256598d5af694_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.392099156632564
Encrypted:	false
SSDEEP:	6:mCllVYGL+MIwJJ8f/llgU6gUNn/M+4rSK6t:flwv8fXEgwM+yk
MD5:	59A7AD3E489CEBFD1CE7BDEC92F340D2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3d256598d5af694_0	
SHA1:	B071515BBCE2DA535237E963B0BBE434500C400F
SHA-256:	429F38FF15E860481F1B5F02F8C90AB926269CB11C90833E045E7B93C3E2F119
SHA-512:	9C254B8D3467CCFEBAD9BC6458A69FA65A65A07A85102CB4F79800F75069C6123B312E3F1A7E5BB8F5B672A052C9A6CDC65BB3F228BB1A6334361E658AC8516
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...].t...._keyhttps://www.google-analytics.com/analytics.js .https://canva.com/}..Q@./.....(.....-.B.....l,e..c....A..Eo.....0.}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4950d0815c21f68_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.447178046694423
Encrypted:	false
SSDEEP:	6:mQXYk+TFs4BqCQl/llgKsQdG1NvJynK6t:R+TueqCQlXKiGfkp
MD5:	CD2AA73E381524AB165C92CAEB9BE0F0
SHA1:	D5527A0E675047D95856E3DD82F9B22BD0F434F1
SHA-256:	61A6D59858510133EA26B3A20F765A228A31D0561577BAEBC196C0904720F9BF
SHA-512:	2F82671D26849798040EBA4BB4A5058489867ECF031D93D2F06FD698395EC10F090D60D01C7D1852DF341D67760534E893DC94FC2CD58AAA103D6DF6DF6DC09
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....\....._keyhttps://static.canva.com/static/lib/sentry/5.15.4.min.js .https://canva.com/..Q@./.....z.....Q^.....Q.....;....]XN.J.X.A..Eo....._.+W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d0b48746d2734b6a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.447851784820482
Encrypted:	false
SSDEEP:	6:mGGYk+TFs+x8IvEvllg7lKFccGY/LnK6t:4+Tu++QEHwlKFcly
MD5:	7CF52422171CFF4D35887952DFC274C7
SHA1:	278BF2AFB86E9F699B107AAA6CBEB0E546CAAD66
SHA-256:	77BAA20B0ACD6A6D0903D6934E57C5A6287AC2023F93E60BBDC8A632B9442109
SHA-512:	5EF8EF8EE056CFE3EDFE138F0AE03762F330F84B0FEF7C7ECCDAE710B21829ACE016CA02228FD2D14F41AA3FCAC9F970705ED58340EA0C655068821C415FF8D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....^....._keyhttps://static.canva.com/static/lib/cl/cl-0.4.1.min.js .https://canva.com/.2.Q@./.....R~.....8m...Ul.....)p...{.w.....A..Eo.....A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dda81cf9b0b047b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.6031189414718465
Encrypted:	false
SSDEEP:	3:m+lejlA8RzYkwLTLTi5lDuBmxm0LXSRCLTEhq9ll/lHCZ/1f2rtt9q8TARmzl/lX:mdYk+TjExRXehq9llgZ/gt28TAAPK6t
MD5:	BFFCF5A23C76E9E8F796ABAA406C8C45
SHA1:	1124362FD4890374640B36127BF96FC7C6FD7B74
SHA-256:	8AA7E446E4487900440EE914DCC2DC7D4AAECFD2B512735F3057D29E7E38767D
SHA-512:	6D2F47C0DC9AD824A706F884AFC1045442FA402C7D75892D9A1F50F711B4200C8129A9E69C5920A3A5B83D93874D9ACD6A9CE61C785745CB1BC04463A8D5F46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...Z....._keyhttps://static.canva.com/web/cb08f5718bdf9fb49247.2.js .https://canva.com/..Q@./.....{.....-._...U.<i..N..=P...-{...[pY6.52.A..Eo.....|w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3511df7a5a5c326_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3511df7a5a5c326_0	
Size (bytes):	230
Entropy (8bit):	5.569145553343734
Encrypted:	false
SSDEEP:	3:m+lWEv8RzYkwLTLTi5syj2RfqEp6Xeq9LPWRCLTEfr9ll/lHC9pGw7qr679m6m/Z:m5Yk+TRK2/aes7WNxllg9ow70NvhK6t
MD5:	ACA2A66518915B34CD27CA44D408D479
SHA1:	69B0975E5C613D34B222D8605B30F074C5AA4AC0
SHA-256:	F1A76C84150097BA38965F6334B53C5818216DB7C76A2F022306F0E25547F46A
SHA-512:	9B0F3FF0B44D5F7542693C784C50EC3E4F92CBFB09B38830B4B84E4A0F2829A255B773BCA8974900BC093852B73E2D4D7D3AE36B85067D36413664981ADACE3E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...u.%....._keyhttps://static.canva.com/web/292bbecde0fce6ffe18847a12c9a6dc6.2.runtime.js .https://canva.com/g..Q@./.....{.....z....f..t..O.....ly..mkK.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4115b2c93fca474_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.464864724845465
Encrypted:	false
SSDEEP:	6:m5irXYLIiNrQ6mOlvllgIknxcNjDk41v5RK6t:NrgNNmOFn0eowp
MD5:	107EAF0142DFC49E46A8E6C186D2E5C2
SHA1:	7E1F9B5F82A8B2ECB2D9F4FB7C48969F5D0F804B
SHA-256:	D972C0EE4E5C5A43C6454BED53EE6105C194D61A00F023CDF946AE5E718656B0
SHA-512:	6247CF1C4E8AB000E4CBB191936298DE77693F34A720E723A861C3EC0B75A852EF5BCF17FC5A31545325DB8BAE6C70DC2178E11D57AB7074EC279F2E6DD15CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O.....S....._keyhttps://js.appboycdn.com/web-sdk/3.0/appboy.core.min.js .https://canva.com/.T.Q@./.....h.....P.p..._.P..K.HG..(.0M..7..).q...A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eba1480a166263c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.572934447779907
Encrypted:	false
SSDEEP:	6:msB/XYGLSmXZCLRlZpEPallgdCLLWW/lbK6t:DlZpEPqrtN
MD5:	B94D462412D03612104A3F5F2810CF22
SHA1:	23216B80FBE5DAA73CC4391EDA6C2B571C48E23B
SHA-256:	B05379861DA44F4A4CB11ED2F62172677A9ED783D5F01755CC386CA855EA2014
SHA-512:	AA291DE41561FD3D59ED352378D039EBE0B6EDFE80A73E78837040701B24EEFEA11B3F8B9DBCA75A65E1E9A141988E4ED4BD682148337AA57BAB8848C6DC3196
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...&..}...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-TZPTKRR&l=dataLayer .https://canva.com/r..Q@./.....z.....m.:.....z)....T....*r4.....A..Eo.....E.=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f50d7bc85406f58b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.669980231856586
Encrypted:	false
SSDEEP:	6:mKqlPYk+ThNFforIHb/llgoP3J1zerk4bxK6t:BW+Th7QrebXJhegGL
MD5:	B942FEA758A3B4715F35A651C9724F45
SHA1:	9F87F02AF20B24699FCE62787D4D16CBC141DC7A
SHA-256:	D0C5B37F745683D2D96B09A28A1C36CED1A98F9238DF81DE6589C187A7F7FA78
SHA-512:	1AC72143ACC7F43197CB100781D7189B33F77F297DF7643E674639F193F32816199AD542228F7E7B7851C55E078F55AAF73481F8183D233606C6A2BC5E620256
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f50d7bc85406f58b_0	
Preview:	0\r..m.....h....._keyhttps://static.canva.com/web/c016d495185ffe7a19888c458fd053f3ac228bdc.strings.js .https://canva.com/U..Q@./.....{....._.5.._.~n...,...P...]..[#...m.A..Eo.....V.....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):	648
Entropy (8bit):	5.142338315980612
Encrypted:	false
SSDEEP:	12:KbgxNKvjrvqWvpvktlWtvL1rKvbvwo/2SCn2Epf1Mywazyz7V4ht:FyPlB8totMzZk
MD5:	B3268FD4C16A808FF1CEF6FE911FE90D
SHA1:	0E3E7EAC50437E693B2EE04B995F93A1AC0D4A21
SHA-256:	E80F770537A70321F750DE1E4DA68381EBA19E06A23F6138B08A291AB5C317EF
SHA-512:	E551B009784BD13C7F98DED24BC78F305E4B861DBBAB02FB4D947BC664245DB887DF3658C645D038B27807381633F9F92060AB428C6C4C7657894F735B9EB47A
Malicious:	false
Reputation:	low
Preview:	.....9.oy retne.....2.....<h1..._...Q@./.....o..-.&g..Q@./.....R..'..Q@./.....Z.YV...Q@./.....^..Q@./.....,..V....Q@./.....cb..H...Q@./.....t...,[...Q@./.....@q..U.i.@..Q@./.....].H..@..Q@./.....J..".F.V@..Q@./.....1[.>....@..Q@./.....G.....@..Q@./.....jKs.F...@..Q@./.....&....Q.@..Q@./.....T.{..@..Q@./.....h.....@..Q@./.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../.....)k.Q@./.

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):	20480
Entropy (8bit):	3.3435260645919502
Encrypted:	false
SSDEEP:	192:zugoSvVv9MvnUbYUCblhyvdyN7tKR6F9DDatYFBRjOgRL:PHdmvUbvIl8vdyNtKR6HnaoRSS
MD5:	682D89712B21672F5F7B0526F76A875B
SHA1:	05D9847CA22AD03612BB25F09E1423628462AED0
SHA-256:	2EF2A761B643CF1D41D6AEE203957092871297C14D47EA2E599645A37CCDF4E4
SHA-512:	08E147C2A394344F81A1424DE495C343959F343E158805809E87BBB5126143FC74FDCD9D159659822DE763C2FFE35DF9E263B3E14A23B137BA8CF9C2058E1CB4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9683986714789711
Encrypted:	false
SSDEEP:	24:RcLgAZOZD/4qLbJLbXaFpEO5bNmISHn06UwHz8:R8NOZ4q5LLOpEO5J/Kn7UKz8
MD5:	A49EAC1228669AB29837DDB288B21982
SHA1:	17E06E5DECC82395CC58799C52D12F40B262F93D
SHA-256:	FA11638E6FE28AA58698F476414B194A4D05A13AE6787E7DB8AE2F0DA09C2F4D
SHA-512:	5ED5FFAA1920ECA871D4B29060D29875F76C0035B6D98F686DB2DA8496B89CC1D259780F7C09264203BEAA332B07EF2ACBCA188B2ACC6919405E30AD2A4FB1E
Malicious:	false
Reputation:	low
Preview:	.....D>)..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Size (bytes):	8543
Entropy (8bit):	3.7865087875626924
Encrypted:	false
SSDEEP:	96:34PVUoYws6HxX09YIHrjhsxJhsx9HLIHrjhsxJhsxSIHrjhsxJhsxsaIIHrjhsxX:3mUdek9sYdXYmYsSY8XYK+0
MD5:	9B8FAFC0D12B3FA9C52369CA0BE66A8D
SHA1:	31787F21B6C56286E554F5C57A21BFB9DAB960EC
SHA-256:	ABD11E8E7C4AC61F511C94FDEC09FDC9D1870974CB5B770E255D4FB78C3C1CB1
SHA-512:	1D8DBC6197C1B4AD74C4B3C620CF1390DDCD7902C862BC1ACF2F279D54A0C123C44246B3722EEC1123D34493B94687C70458CE535CC273209A0E24EAB20EB0 4
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...9dc95d65_e44e_42bb_abb4_c558213a203b.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton....A.Z.T.E.C. .E.N.G.I.N.E.E.R.I.N.G...<...8.....0.....h.....`.....@.....h.t.t.p.s.:././.w.w.w...c.a.n.v.a...c.o.m./.d.e.s.i.g.n./.D.A.E.O.E.c.u.9.G.n.c./.C.6.L.v.q.P.R.f.M.O.Y.o.F.6.O.W.l.u.9.b.V.g./.v.i.e.w.?.u.t.m._.c.o.n.t.e.n.t.=.D.A.E.O.E.c.u.9.G.n.c.&.u.t.m._.c.a.m.p.a.i.g.n.=.d.e.s.i.g.n.s.h.a.r.e.&.u.t.m._.m.e.d.i.u.m.=.l.i.n.k.&.u.t.m._.s.o.u.r.c.e.=.s.h.a.r.e.b.u.t.t.o.n.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.301330248698428
Encrypted:	false
SSDEEP:	6:QfwU+q2PWXp+N23iKKdK8aPrqIFUtwffwtJZmwyffwPkVkwOWXp+N23iKKdK8amd:Kwpva5KkL3FUtw3wtJ/y3wPk5f5KkQJ
MD5:	83227DC4CA9589255B9C987BB471DADA
SHA1:	5B02CC429893B29AE6A413F7806ABDC4183D7FF4
SHA-256:	8790D98CEB117995FB00415716E9003A585EB2D05318E556D1D403DD371360F9
SHA-512:	632E763A975D84BCA9F8D7253B535A35FFC8BFF48ADAED47612E8DC69BE34948EAAB56E9CE9EA5A1D89ED5E617183D7F043C85BC7703DBE741367604F158F6D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Reputation:	low
Preview:	2020/11/21-19:54:43.857 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/21-19:54:43.861 dc8 Recovering log #3.2020/11/21-19:54:43.862 dc8 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):	513
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	C92EABB217D45C77F8D52725AD3758F0
SHA1:	43B422AC002BB445E2E9B2C27D74C27CD70C9975
SHA-256:	388C5C95F0F54F32B499C03A37AABFA5E0A31030EC70D0956A239942544B0EEA
SHA-512:	DFD5D1C614F0EBFF97F354DFC23266655C336B9B7112781D7579057814B4503D4B63AB1263258BDA3358E5EE9457429C1A2451B22261A1F1E2D8657F31240D3C
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.250404012770937
Encrypted:	false
SSDEEP:	6:Qfe49+q2PWXp+N23iKKdK8NIFUtwffe6C5Zmwyffe6CtVkwOWXp+N23iKKdK8+ed:Kenva5KkpFUtw3e6O/y3e6i5f5KkqJ
MD5:	378102BADE1C27EE26FF32A13F3AA761
SHA1:	DAAC07EAB2238D4B538E636DC00DDA8E915D6300
SHA-256:	1D013FD13201C077CB70111403CB7E6F7BFCC5011B6A09208240F81B42D53471
SHA-512:	79BCE55F3A197B1ADD2A964574FC64719E9DF48741764FB7B385A2908FBE30E084F566D32D62508C92E9E939E5ACB080B545DF9017340CADED8EF69A1F75EA5
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:32.338 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/21-19:54:32.339 dc8 Recovering log #3.2020/11/21-19:54:32.339 dc8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4roIw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/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):	20480
Entropy (8bit):	2.20123543381794
Encrypted:	false
SSDEEP:	48:0Bmw6fULB1oUD/1lHzAA8wBj1wdrlR3CoN0hRdslhWntdwLXKvkj7T9:0BCsB+UD/XcAZjGCBhiktdwwkfT9
MD5:	2E8DE1584AB90C2ABB7CBF8E8CD37D23
SHA1:	A36E3483924AA2395F08C7A65FE2F02DBD71C871
SHA-256:	4CD88C23F04C8A1D19A3FDE9CD385058154245C182B18AA4639ED4A9761C085E
SHA-512:	D2DFF0E51457A43D5FA8F64E8FD23630928D3EB3F7AAF29660E4DCAB5C7916320051CF0322F43777F679510EA24D0770F7D16620D5A965CC3981FDF65830A7CE
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7781086014392157
Encrypted:	false
SSDEEP:	24:SJIyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwNZ3n:MIdBmw6fUEZ3n
MD5:	E6855C822C58B268ED88A7A388C60897
SHA1:	43C24C9BCAB096FCD770B9C5C117D624452CEBB3
SHA-256:	38E4F0F32F0CDE47E45C52EE3D0C471E5FB59A7B3C02DFD2B7B77FDAF5F5D8AC
SHA-512:	C16C41D8E5E48746B6E550C666C132D672D8AE72503B2E8E42A433722350609611AC3F1CABD4A72F24F6B5D098CA5517238881B593C11D1463E2E7C89A221C88
Malicious:	false
Reputation:	low
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.298094867263405
Encrypted:	false
SSDEEP:	6:Qfwrq2PWXp+N23iKKdK25+Xqx8chI+IFUtwffwmBZmwyffweu5kwOWXp+N23iKKN:Kwrva5KkTXfchI3FUtw3wmB/y3we05fk
MD5:	B1AF751EC2821CF683AE1160AFB0B83F
SHA1:	EBBBBD8B534FBAA11E25FA637078977C706FF27B
SHA-256:	92535A43B4EBE9452BF35826B101158BAD6FCDA02192C39149AC87A83014C76E
SHA-512:	BE85EA7C34CC1CB85CDE6F796ECF0FDA369529D70614224A661A83DB32A9A22FF9FAB487E25910D20968F95C3B1C2B268BF48A43BF5FB33B2AC799DA39E951A
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.664 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/21-19:54:43.666 14b0 Recovering log #3.2020/11/21-19:54:43.667 14b0 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):	358
Entropy (8bit):	5.260913423877164
Encrypted:	false
SSDEEP:	6:QfwCAq2PWXp+N23iKKdK25+XuoIFUtwffw6ZmwyffwEbkwOWXp+N23iKKdK25+Xp:KwCAva5KkTXYFUtw3w6/y3wW5f5KkTXp
MD5:	99A3F8B14F2975BB7116A87B43DB0438
SHA1:	1973EB9F41382955DDF577508CFF1F9C10280418
SHA-256:	ADA65014938C0480EF5D591EEA4E4C6A89ACCF6336AF5A53831FA7BE669EFA2E
SHA-512:	C76ABD460E6A7C42F631A3BD4C67B09DC55188596EE0B86EB3560F9262117C1E6FA8EE11B56FB1CFCFADCF27575359C4CF427E6707DCDB90659A1D0631CADD
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.655 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/21-19:54:43.659 14b0 Recovering log #3.2020/11/21-19:54:43.660 14b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.25380366382486
Encrypted:	false
SSDEEP:	6:Qfw/XIRSVq2PWXp+N23iKKdKWT5g1IdqIFUtwffw/Q9gZmwyffw/2IkIkwOWXp+u:Kw/8Ova5Kkg5gSRFUtw3w/N/y3w/2I/x
MD5:	89F0AF8328FCEC391F0F4BFB3BEE3443
SHA1:	7576ABCF09553EF2CC8576BC6C3544DD68CE109A
SHA-256:	2BE679C8ED990F9D528F7F9E51E1827DC7E9847B04EA59265F1551FA4A8DC51C
SHA-512:	108AA41548764A0BCA8E4BF34E13755D1E2CC0653EAF17473DAB825DC5BAA527F524A56FF90C156D4DD33A4886267B04A1433D155283B2FB1E391C01809DFC1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Preview:	2020/11/21-19:54:43.392 1424 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/21-19:54:43.395 1424 Recovering log #3.2020/11/21-19:54:43.397 1424 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.19754085833771517
Encrypted:	false
SSDEEP:	12:TL+A/WMfY9XWkmtNYy9s7M/CXYNuQXqeGI/ElqCbNVd9XWkmtNYy9sL:TLxWT9mHuOs7M/ocu7rbND9mHuOsL
MD5:	69EF74EB550B7F58EAE1876A6341EEBB
SHA1:	668D5B941939AACACE43C3A784E8937171CFD2EA
SHA-256:	C8C50CF1AB0C747BD1EB90DF7441B590DF9299141ADCE83A9526F9CC0361BD5F
SHA-512:	EAF1799B940378FA215C31F8D6ADED5491BDE1CF261D4895F152C6CB59021860A32C333962B2ACFC507F644EE198A2761D874525DC4840744DEFE8B92D37CBC
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	1171
Entropy (8bit):	5.592174984939801
Encrypted:	false
SSDEEP:	24:65H8NFTseyxvDLxNeSsVs3aPrr7WXU1SNoX1DY78BJgskfa9yBDOxo7nQBrxzGSj:s7rxvDLp3aPrroNmU8JFGR1nhz4L
MD5:	D46B054D7B74914FF8FC99CD8B54D397
SHA1:	AE75493BCB6F2F8293EFB3B4BAE02CB5EF624E2A
SHA-256:	1B5DBA1F0A3D7BA290390796C064554EBB88290DB053F5FF2ADAEE2E803F040E
SHA-512:	9005EB03955DCBE9C1947DB87735F95D90F446CFF95D97E59A61EA2AE88C782EDAF5767D6534F3E823766FD46FBD0F14DEF66EA5F677C5A1A37799B5F8D1EC8
Malicious:	false
Reputation:	low
Preview:	....."....aztec..c6lvqprfmoyof6owlu9bvg..campaign..canva..com..content..daeoecu9gnc..design..designshare..engineering..https..link..medium..sharebutton..source..utm..view..www*.....aztec.....c6lvqprfmoyof6owlu9bvg.....campaign.....canva.....com.....content.....daeoecu9gnc.....design.....designshare.....engineering.....https...link.....medium.....sharebutton.....source.....utm.....view.....www..2.....6.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....y.....z...... .....B..... .....*..https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu

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:	modified
Size (bytes):	42076
Entropy (8bit):	0.11696375163368229
Encrypted:	false
SSDEEP:	6:k0lT5/UkI6C5pg9bNFlWCj/lYwA/l3l24/fMt76Y4QZVRtRex99pG/ekqR4EZY4a:RDwHqLBj/S3l24nMWQA9LHjBQZ8fO5
MD5:	5AD5B2E14F6BFA98A83F20D218B622E7
SHA1:	89EAADE0EA203468C330F4D1420E207FA4C73666
SHA-256:	F7294B9A80ABA48604FF3CBC9C577775007FF0617586CE8471FFD39B879A67F0
SHA-512:	218E5CB2A86B94629D7FF766C1E6DD700A46806D88F9454D1D2C6661029BE24E742FEFFC259FB8BD7D2702D983484AA543A65411CC42D1E49C01F54059F882AE
Malicious:	false
Reputation:	low
Preview:	.....z..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\000001.dbtmp	
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5089
Entropy (8bit):	4.064565376752471
Encrypted:	false
SSDEEP:	96:zlTv4TcpX6zFE405PNUaxAfaKWpN1dO4RpAO:ZTCCUQAfdWpFRpAO
MD5:	7E62BF963EF590BBED1B0E16EA76DEE2
SHA1:	E26DCE9A5D5F0E5737B4234F06F011CD9645784E
SHA-256:	38CDA5C9B42DD94D039FB8F083A89BD0A7DE17D0B5B8A2FC2B09A8E7D105C329
SHA-512:	7B5235EFAD9803D041FE3EB39408307C0C0D87F495AA5C1AEC77F4CE50C9040DFB9B227BA952B97613C2DFC85597C206F096CD5C475C0B136FCFACD1357AFE F
Malicious:	false
Reputation:	low
Preview:	. .....2....(.o".....).....m.....h.t.t.p.s._.w.w.w...c.a.n.v.a...c.o.m._.0.@.1..B.r.a.z.e. .l.n.d.e.x.e.d.D.B. .S.u.p.p.o.r.t. .T.e.s.t..... .....G.....s.....h.t.t.p.s._.w.w.w...c.a.n.v.a...c.o.m._.0.@.1..A.p.p.b.o.y.S.e.r.v.i.c.e.W.o.r.k.e.r.A.s.y.n.c.S.t.o.r.a.g.e.....=-.....b.V..... .....2.....2.....y.....2...d.a.t.a.....2.....2.....2.....2.....2.....2.....2.....d.a.t.a.....2..... .....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2. .....d.a.t.aB.A....$.....2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	172
Entropy (8bit):	5.419659328553877
Encrypted:	false
SSDEEP:	3:tVP9FcfMJrLKqFkPWXp5cViE2J5iKKKc64E/x14kfSbTihO/IrscWIV//Uv:QfMJr+q2PWXp+N23iKKdKEqSZVIFUv
MD5:	C4C41E696BB3322487BE56F3CD333E0B
SHA1:	1EE413FEE6805989A95CAFCD36A6AC422B08F181
SHA-256:	C600CCB4FEF1D64AB8A79FAF99F4659AED950DBBBF00A6AE3449A4AE246AB893
SHA-512:	E400F991A9E58CFB6B09DAC2E7A19AA1407BF4F6ECF455A87F32A8BEA711AF8C2C49860AD62DF6E7ECD7FCEF8EBDFAEEFE4C681326E5ADEAC8B63DCAD12 EC27D
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:34.158 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.lev eldb/MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\MANIFEST-000001	
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....

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):	32226
Entropy (8bit):	4.067747884023246
Encrypted:	false
SSDEEP:	384:5SkPEKyrfYigUgvjWyjX10kUEQ/F51QHyYjOcLt:9EKyreWyjX10kUlQJHx
MD5:	33D243A90C894F7025E3DC4801532C4F
SHA1:	FD81EE3003FE600DF7B5E4730855824552662D39
SHA-256:	CB6A25B6A34C30C8CA2081846392793B08D8EAAF5C36DC88A1D5C62545490C59
SHA-512:	C06D9D17A300DCCA2E339CB1F5486E65C4C2E831D9DBEA92D11E28C3F760CEB52E835FA889436382CCFC4A8B992850F99D46AABBB80D3F82D1E71FD0E7AB953
Malicious:	false
Reputation:	low
Preview:	..S..l.*.....META:https://www.canva.com....._https://www.canva.com.._uetsid!.6eecbee02c7611eb97f6bb236532a462.#_https://www.canva.com.._uetsid_exp..Mon, 23 Nov 2020 03:54:34 GMT.._https://www.canva.com.._uetvid!.6eed02202c7611eb927c7bae0cb8c833.#_https://www.canva.com.._uetvid_exp..Tue, 08 Dec 2020 09:54:34 GMT.J_https://www.canva.com..ab.storage.cc.320f7332-8571-45d7-b342-c54192dae547..{"v":[]}.Y_https://www.canva.com..ab.storage.ccLastCardUpdated.320f7332-8571-45d7-b342-c54192dae547..{"v":0}.V_https://www.canva.com..ab.storage.ccLastFullSync.320f7332-8571-45d7-b342-c54192dae547..{"v":0}.N_https://www.canva.com..ab.storage.device.320f7332-8571-45d7-b342-c54192dae547...{"v":{"browser":"Chrome","browser_version":"85.0.4183.121","os_version":"Windows","resolution":"1280x1024","locale":"en-us","time_zone":"America/Los_Angeles","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"}}.P_https://ww

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):	329
Entropy (8bit):	5.190148644600434
Encrypted:	false
SSDEEP:	6:Qf4TFtq2PWXp+N23iKKdK8a2jMGIFUtwff4dF03JZmwyff4SpkwOWXp+N23iKKdD:KGtva5Kk8EFUtw3M23J/y3xp5f5Kk8bJ
MD5:	3258298CAC9F55383C7519E13327129C
SHA1:	991061D0061ABF1BF693AB43C0483A0D94C3979C
SHA-256:	3B928802A05AD8AD9C9D327C30C4FB0429378056F1B105169194CE645D832A44
SHA-512:	215CA83B412D04EB8C96E67B6815DAF1983DC13305AAE549F2D0FB3B16B0444504A217B947070E9E35AFA3A86705C95CA7889C084AD67322E05E7D9A4CDCD06
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.297 d70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:54:30.299 d70 Recovering log #3.2020/11/21-19:54:30.303 d70 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.28560937649892
Encrypted:	false
SSDEEP:	6:Qf4WB+q2PWXp+N23iKKdKgXz4rRIFUtwff4VZmwyff4SVkwOWXp+N23iKKdKgXzW:K7Mva5KkgXiuFUtw3U/y3t5f5KkgX2J
MD5:	D402C361B043CE4522D60AB1E22426C1
SHA1:	1D0A9AD53BF77DF6A31E25919274DF97C1740674
SHA-256:	847E0139744F68DB456E448001FDCF44137D558470BA2B34DF7B5992650AA0B9
SHA-512:	015B17DC8061D6C27A5104A495199721AF8C7A89897CACCEFF9A4AE640F4E40D32008E3FC38AE8F97A8E30CD01514C088492E1A01384444A071C0D0BBB87D81
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.684 968 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2020/11/21-19:54:30.685 968 Recovering log #3.2020/11/21-19:54:30.686 968 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\QuotaManager	
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):	77824
Entropy (8bit):	0.4793850778073382
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4pNtkc:a96EJTv4sXK96EJTv4ZL
MD5:	5B759EFFE4061975BAD4ACCEDDF9C899
SHA1:	3673C8858C235E0B92F53D391B7FD062318F23EF
SHA-256:	A4548CA47A7023C1BC800827753AA4E384565572F8765D4B968815525082F957
SHA-512:	5649FFD395BC7B46654ECA86E9D619A97C99CD2EF334F74B59DA5302F739EE2DE6CD045C0C531A9E49A201A21D0781E378DEC12CCFC341DB26098948A2D3CE A
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....*.W.L.[.....".....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.6524947707533043
Encrypted:	false
SSDEEP:	48:b5MjQqzLbCIG+6bDdsDaKgJgKtHIm50I9a+Up5:96QsCIG+6bDdsDaBJvtHIm50I4l
MD5:	8AB4A09241A4F730E44C37F34E4DABD5
SHA1:	AE4210A47D0D58A2ECAE4A14F51DD911059762CD
SHA-256:	8C6FE8368A5861EF231122DA3442BBB8A9838D87EFF570C34CD58D2B7FCD6347
SHA-512:	D57C56C2CA4E4B63EE607468E43EC218A2331CD7A4EDE26BE1CC4CB1AABA0D96E8455423F4EF742C398AEAE2FC4655455F0BE3ADC0A26ED912CB7FEE5BCE F9DC
Malicious:	false
Reputation:	low
Preview:	..... .c.....jL),.

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:	modified
Size (bytes):	28672
Entropy (8bit):	1.6472882627967502
Encrypted:	false
SSDEEP:	96:wIElwQF8mpcS8Vwn3+3j0+74UCVQwKw3j0+6tBCVbKSav5Q:wIElwQF8mpcS863+zHoKwzuOKvRQ
MD5:	DFDB086F47CD84ACB2213FAE7B1E657B
SHA1:	73A874F229D49D2D1D6B1AC5CEACBDFF726943AE
SHA-256:	1B0C190066785D108EDEA7217033978BE27EF77E85B76062BCD81324CD526984
SHA-512:	3246FD8DA79470A4094EA7B15DADB7CB0A455A68BC22BE426BAF8C700E848F2BF923C27F90C0FA2C90A081701B3CB3D41F92BF833EAFCE0AD26AB51D8F825D 57
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6288607939044842
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
SSDEEP:	48:6dF8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUi+4:6z8hIElwQF8mpcS2p
MD5:	B83F8093E70F7414F1ACC4A35228E19C
SHA1:	A751776ED7A13E714AB603E5CF99D30F7DF50DE4
SHA-256:	EC04792633C48B4C4AA4AF79B67D5861C7E41AA1D060677A33FB9B0296066771
SHA-512:	0829EC0B74BD513C26223EB66440D8DFB92DAAC0543C2A224D828DF7EFEE80ACBF573B3F786AE17A864425611C0E7ED75B3920132C172815CE7F4A773596868
Malicious:	false
Reputation:	low
Preview:	.....|..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.194472872108031
Encrypted:	false
SSDEEP:	6:Qf4x39+q2PWXp+N23iKKdKrQMxIFUtwff4kGXJZmwyff4kGX9VkwOWXp+N23iKKS:Km34va5KkCFUtw3GJ/y3GD5f5KktJ
MD5:	51BA7256807F13695B255F119B71D39C
SHA1:	BF0000A5D95A2C28295F78BD1E10E05639084DF5
SHA-256:	11B64C1E738D2F7655C7434FD3440C65EC29E13B419A24DFF09AF8CE93B43730
SHA-512:	CD7677C7BCD22F3AED0929D7F46460F9B414A9C6F3FCE5564896DA038010F92FF1F914B3256C2B35200C2203AB380D0BAF4BA48728D3C4699E35A444F05F81C3
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.511 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2020/11/21-19 :54:30.513 dc8 Recovering log #3.2020/11/21-19:54:30.513 dc8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.2116961694758634
Encrypted:	false
SSDEEP:	6:Qf4y3N+q2PWXp+N23iKKdK7Uh2ghZIFUtwff4xZmwyff4FVkwOWXp+N23iKKdK7w:Kh3Iva5KkIhHh2FUtw3E/y3k5f5KkIh9
MD5:	D53DAAAC91B3B7C5FEF3EE4177411E9F
SHA1:	9F5A72EAF3BC6D93D7FB46325023FB1D15AC7210
SHA-256:	79B4A37C112DFD902B52B6EF7856E94BE2B29E81693F6A7A2C272AFBE4F89437
SHA-512:	A72D79F1EE2C72C0E0439B4C2670249250E822994AF68371EDBB3A02B288766E913E76BA3DD22DA579AD8506D4FFB8674C7FDE63F1646DA95E5AC6CE00A3D9E 8
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.245 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2020/11/21-19:54:30.246 dd8 Recovering log #3.2020/11/21-19:54:30.246 dd8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.268603230892367
Encrypted:	false
SSDEEP:	6:Qf4p9+q2PWXp+N23iKKdKusNpV/2jMGIFUtwff4b5Zmwyff4btVkwOWXp+N23iK4:KU4va5KkFFUtw3M5/y3MT5f5KkOJ
MD5:	39F495F307E6491492F754EC80FA864D
SHA1:	E013B7B0A2CD412311C2CC9D3884AE439AEDACD9
SHA-256:	4E8C14DED47B9528D03308FDDB1634B0DACDBC6950F72B24A336D7BBB115AA35
SHA-512:	8B9A3D42328EDBAE28D0712CE213450CE7EE38D20F3176CED719EAA2DA675C7BFEB9228D683FE550473423E683FAD3A3B9116AD5D2FAE166A937C4FA9D3350F6
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.533 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:54:30.535 dc8 Recovering log #3.2020/11/21-19:54:30.535 dc8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.32861655312654
Encrypted:	false
SSDEEP:	6:Qf4G7Gt+q2PWXp+N23iKKdKusNpqz4rRIFUtwff4/B6Zmwyff4EKVkwOWXp+N23n:K77Xva5KkmiuFUtw3J/y3g5f5Kkm2J
MD5:	8AD2753A3234E4DB878685F1D69271EA
SHA1:	1802CC250A5E32ECAE132CDB9C954FE3A1670AF9
SHA-256:	9FA4AF29092AD9649820F215193D6B5C228643C2E8946939369F8B9C5C0FCC6A
SHA-512:	04A29A3CE44EED36AC3B2830EB0BD60138E56940C6D63AF9DF29DEA027ABD92CC068C7C8C695116B622C30658DA97C37F243F807407AF713E6396F9255A5B79
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.775 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2020/11/21-19:54:30.776 dc8 Recovering log #3.2020/11/21-19:54:30.777 dc8 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.300786880654546
Encrypted:	false
SSDEEP:	6:QfBK9+q2PWXp+N23iKKdKusNpZQMxIFUtwffBsFEZmwyffBsFkVkwOWXp+N23iKX:Knva5KkMFUtw36O/y36i5f5KkTJ
MD5:	A149318890111FFD53D084F2DF87AEAA
SHA1:	BA0A146809919D6A7572984725B7585C4047B198
SHA-256:	C989CD5FB4D8C07B6757E11982C325080FF9BF5060D282A05B9EF52EF383AE90
SHA-512:	8D037C4F85A3E696E6A642F60157F02B3E667714213DD40B94CDDD95E7C0BED2CDB74954C27CF82C0EEC0B254CFC71C06FC1A8EEF9EED05F4645EE92495570 4
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:46.448 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2020/11/21-19:54:46.449 dc8 Recovering log #3.2020/11/21-19:54:46.449 dc8 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\eb720268-0b80-48ff-9de9-f7e2c5524892.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Size (bytes):	427
Entropy (8bit):	5.270109488970663
Encrypted:	false
SSDEEP:	12:Kw7va5KkkGHArBFUtw3w1/y3wPlz5f5KkkGHAryJ:KWa5KkkGgPggH30lf5KkkGga
MD5:	FA85117341759A31CA2520B7E7A05ED8
SHA1:	42E4BADF69DB13AA41D04C61B3FDE28D8F1F83A9
SHA-256:	2FACDD12494DABB4D23BDE486F2555FF6B2E07F328699BBC9DF3EC2D57C6C30A
SHA-512:	7C244F480DEE804F096DA6317BD62D7E8D3A81CDE5F6500BAD2B07B9C9493235258CCBC9E0139CBB2F53C068B3FB94BEE466710A9414BA46ED140B24BC79841
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.856 738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:54:43.860 738 Recovering log #3.2020/11/21-19:54:43.862 738 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):	429
Entropy (8bit):	5.221144594508089
Encrypted:	false
SSDEEP:	12:K76Eva5KkkGHArqiuFUtw37VX/y370ND5f5KkkGHArq2J:K7ba5KkkGgCgg7Va37Cf5KkkGg7
MD5:	1ADA9AA48E10E1FEBA7A9157AD3759FC
SHA1:	4B03C7D082260C173CDBFDED8DC93AF9FF1E66D5
SHA-256:	CDE7C9BFC8C16A02A3044A1CCA1F3003C9DCFFC22D93E4D2806C57A73D273A3B
SHA-512:	F880ED38C80A93324792BAB0D3AC11062FB532E4720098F7BAC67CD544B117EC86DEDC243F43B3675D9E868F962013765697EF1BDFB0F072E2B50B1BD1C4FC2
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:44.499 dc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2020/11/21-19:54:44.500 dc8 Recovering log #3.2020/11/21-19:54:44.501 dc8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.24456503357341
Encrypted:	false
SSDEEP:	12:KFOva5KkkGHArAFUtw3QX/y3QF5f5KkkGHArfJ:Kia5KkkGgkggQa3QXf5KkkGgV
MD5:	B7458654375A44E724D3BF4D2ECD89A4
SHA1:	D06321F81B66A9368D79FD7EB66C860828A28BF9
SHA-256:	0FA7BE2E8FC36C9F445125245F2877647D13F5316AFB3D3ACFEA4479884F066E
SHA-512:	103F8320ED8EB28F2E3778D2FF83232259E0330E33EBB831391C0217B5CDC0F3B52302CD76B2B77F3E9AB275CBCB406CDC0780FEB8FC490DCBDA7A93D30368E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Preview:	2020/11/21-19:54:59.492 968 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2020/11/21-19:54:59.493 968 Recovering log #3.2020/11/21-19:54:59.493 968 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\f12a1474-b215-46cb-a5cf-1ff4f9516ed0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.253109470595855
Encrypted:	false
SSDEEP:	6:Qf4l+q2PWXp+N23iKKdKpIFUtwff4wrXZmwyff4XFdVkwOWXp+N23iKKdKa/WLJ:Khva5KkmFUtw3JrX/y3Sj5f5KkaUJ
MD5:	B7567C4E25914F1B8D1E7E5527165664
SHA1:	F05A2E32B777112721FF7A2B6CDC66F7620DB542
SHA-256:	C6BBC7137A53E0ED45434766C3251676339F4887131B967BF4A4B9CD6A7BBF71
SHA-512:	40F19F941B640B5F0A683EF34741332C69CC2D9EAA6C89768AF1F1E547B2985A825B397606AD78EA868D1D8321514A1311207DA339521E89A9B3D5553A702CB7
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:30.282 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2020/11/21-19:54:30.290 dd8 Recovering log #3.2020/11/21-19:54:30.293 dd8 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):	399
Entropy (8bit):	5.401229359960563

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Encrypted:	false
SSDEEP:	12:Kkf4va5KkkOrsFUtw3kEl/y3kt5f5KkkOrzJ:KkCa5Kk+ggkEA3k/f5Kkn
MD5:	1A97E6812B6C9CBAA29E3778CA554376
SHA1:	420B76654A790BA40B278561370EC7B0B68C9A61
SHA-256:	D3EF08FA79F089D53E80874F1DBFEC3AB1F9D1E75158567B9C22DCEA312B72B7
SHA-512:	72D1C8FA4E9B93794D5475358B5ACA22E3C7E09A7A5FFEDD37C4783C0A6CE367CB06336168C5979098EBFDA57080CAEF844A08722DE8D96C5D94146C86C281
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:46.717 738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2020/11/21-19:54:46.718 738 Recovering log #3.2020/11/21-19:54:46.719 738 Reusing old log C:\Users\user\AppData\Local\Goog le\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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:7oBn:7oB
MD5:	D67B577A4DBE038FE8837D7CA1ADAEC6
SHA1:	293E8C99E12DCDDA04F4FE3DC14A8E67EF643B2A
SHA-256:	76EC0201DB53FE417272E1876EE00BD61AC4A8D3C247BDCB3CBC8DA28733FD4C
SHA-512:	A3AC0C8EA6DDA4FCD2EAEA897422A93CE9A6DAA2533F5D6F3A27AACE0C5705A7F73EEA2E265D7B5041FE9E59DEDE61C56EC10870EEAB69F5279403B7AA12 256A
Malicious:	false
Reputation:	low
Preview:	.....-L<

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf83cbd0-4553-4aaa-b88b-2db8426c696f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2c523b8-f53d-44a1-8631-7b2b9fb04159.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):	5399
Entropy (8bit):	5.183161317279906
Encrypted:	false
SSDEEP:	96:nSOCCrpi4I68O3VzeacVSyk0JCKL8Ev4kV182bOEQVuwn:nSOCIQ4xBeacx4Khv4kVe1
MD5:	2B802319BCAE38CED34891A94B81CB87
SHA1:	35723E733D44E0357845C5A27BC1D7B4C67720D9
SHA-256:	C2183448E61F87CB7B239BD4ED514544C4457CE0840AB150194E53BBDBFDD435
SHA-512:	060CFE932FF82ADD6B197D26E8F7E2A55A0B3B7B89F7FE1F1E051A37197B24437F1D1CC3E6D32A86F7E810706E83CEA43D40DC9300D2BDE006EFB7027B331CI 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2c523b8-f53d-44a1-8631-7b2b9fb04159.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250490870560092","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.386696087294219
Encrypted:	false
SSDEEP:	3:tVP9Fcfw3zwdTyZmwvKAFcfwf6A7V8nAFcfwf6A7WGv:Qfw3kgZmwyffwf6A7VSffwf6A7tv
MD5:	D52F86C4A349659DDBAA71E0F0A2D97E
SHA1:	B8E2A8B4CF0E76F67FDD0963DE637C83E2210C50
SHA-256:	F5EE4C1B6452F441D3564351FAF5B66442FF3ACD0831BDD1E50832D349B15B80
SHA-512:	D7D749349B4C95E400C9FA2E66F0039214AF45095EA64E46A5ED7F33A88A62154B50A4E0BFBE6A6FFE877737663207A6BE9F3711F7C2A8E7B8D57954242F8E33
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.218 1424 Recovering log #3.2020/11/21-19:54:43.272 1424 Delete type=0 #3.2020/11/21-19:54:43.272 1424 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db	
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):	0.3408437618760242
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db	
SSDEEP:	12:TLiqixnGb0EiDFIlTSFbyrKZb9YwFOqAyl+FxOUwa5qgufTJpbZ75fOSG:TLi2NiD+lZk/Fj+6UwccNp15fBG
MD5:	089C02B21909DD4D739ADC2F093231BF
SHA1:	B33D36CAF38B5B342ACD0EFA9DC0F6F6C37D5F85
SHA-256:	184814D16B8115D3929672ABCFBAD21D2440E3F41257AAC26429764340FA19EA
SHA-512:	55C049C05F9E2A2AFE7BEB4096191D603CBCA209F21F0842F5D13FD4382A0AA103FF183EFE407A76F13EEE4763A1158C7951106E3BE1EDE272DD81FABEB98B0F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....P..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	524
Entropy (8bit):	0.27937671757176796
Encrypted:	false
SSDEEP:	3:MzXIFllxFEG2l/n:MN+/l/n
MD5:	524B486CA8474D8654F693E956122EE0
SHA1:	3C8AEA183D8885F105677819C85F707EC062A65B
SHA-256:	7C618C2A60F9E230EB9D96B3D0E6BEBE2E779CE8CA42F9743D12FE7EB850C1D8
SHA-512:	6C14F04E3AE3581647956A928725A65765C3816695E3310A53511AFA544530D8DDF6291CC57B3AE8AC87CA1254F21D6ECC93E0FC8C36D317905BE50A167589C1
Malicious:	false
Reputation:	low
Preview:	.....' .... .c.....

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):	335
Entropy (8bit):	5.273561124414725
Encrypted:	false
SSDEEP:	6:QfwON9+q2PWXp+N23iKKdKfrzAdIFUtwffwkHZZmwyffwkHNVkwOWXp+N23iKKdn:Kw7va5Kk9FUtw3ww/y3w45f5Kk2J
MD5:	C42C131EB4507918A9DE8C3504ACDA9F
SHA1:	EA097FDA65ECFC466D91484709E169C3DBAB5166
SHA-256:	0726B68DA615C69CAA25A58C48BD0C09057EF84C866ABB9A7BBECF13BD29DF28
SHA-512:	9973DC2892E4FDAF8783C1120C101ECF7C704FFF9E9050A43B28CA2A793B70435617351309C2F9E342FFE8402E867B2C5F7DD5AF1776AAAA84EFCABBC5681A8A
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:43.782 738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2020/11/21-19:54:43.784 738 Recovering log #3.2020/11/21-19:54:43.784 738 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

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
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8d0fe44-fbe0-40b8-97d9-a857f90af973.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):	162443
Entropy (8bit):	6.082689935564378
Encrypted:	false
SSDEEP:	3072:S4XA2NNCxQM9b0q+szv+tnMIsFcbXafIB0u1GOJmA3iuRed:RXrExQM9b7fD+ZMhaqfIlUOoSiuRe
MD5:	80910CA96FBC458E8B033EF0053F1A28
SHA1:	CC4CDAF03B41A7D04E4B89588553BAA59D358E7E
SHA-256:	F75A2033A597B27D41039935E015B724E135D437C43933CB61112FE6969561DA
SHA-512:	D40E33B8048666C07C47A6BE897054FF4A2E2456890B0F1ACF3CC4F11A2FB7B0FC9EBC83ECC5F5CD7166BEF8375A68C134336EA38FA9261E9F904A8926397ED
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":1.606017272922974e+12,"network":1.605984874e+12,"ticks":96932932.0,"uncertainty":4340447.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\FDWKJ0LQ\candanappdevmoe.azurewebsites[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	13456
Entropy (8bit):	4.895000803035704
Encrypted:	false
SSDEEP:	96:f+KMOV+KMAapA0V+KMYapAhV+KMeapAoV+KMeapAoV+KM3apAhV+KM3apAhV+KMk:6
MD5:	A9E2AD0E689BFB3BBB0C134A21022328
SHA1:	998F174D9F670BE7250AA38C713524BE5169F7C9
SHA-256:	E420B6BB7A1F6442630AFD0A169BB6666C34869AD4ACE73FB5216854964941EF
SHA-512:	EC5D8DE98A783680D5E9AC265E885A4D8D16F166676CF417828F7BED288BCD496D4AE0539B5FA1DA4E2D383E1E7117A2D5920272891C4CED08C03C7AC1EF5F1
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="userkey" value="{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}" ltime="1078672912" htime="30851203" /></root><root><item name="userkey" value="{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}" ltime="1078692912" htime="30851203" /><item name="browserkey" value="{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":""}}" ltime="1078702912" htime="30851203" /></root><root><item name="userkey" value="{"user":{"keepLoginLongtime":0,"Auth

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{78B7B8C3-2C76-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{78B7B8C3-2C76-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.859745692102903
Encrypted:	false
SSDEEP:	192:rzZwZd2s9WytkGfhftvMHVlzH3x4fofSfX:r1gUsUKk8ltUHVlzH3xGUSv
MD5:	1B98D94C374683CCAAF6AD5607192BE1
SHA1:	430BDEA36ADC8C2D6E85F50233BAE846D4266000
SHA-256:	2319AB06EEDBF29E5E4A7AB1E2388776907F0FA524875712425BEEC783AD1F02
SHA-512:	CF3E0C22D055FDE809A93D49AC052657F12898B97DF60AB5A0D9ED2AFC9201E66A41FBC5D89AC55D90405DD7C76E3C3F11C4ABCEDC9D4CCDC923A8A02006FF2
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{78B7B8C5-2C76-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	171344
Entropy (8bit):	2.9138696585490718
Encrypted:	false
SSDEEP:	384:ry83Flhh3MkiV7d+5XLS5Fh93exqg/Fh93g79MBZMol1/F+YhjeO3rt3+AclJzam:RCN06ptSQqhL5voN1
MD5:	23D1F42084A6A9E1B4C02E5DF06DF66E
SHA1:	88E194A2BF2F90AECBDE1961E95FF90A426993C7
SHA-256:	E2DF5856D72FCB67B854C8A82AA05B63668FD02D1F1C9E6496B4ED77292C3757
SHA-512:	E80D86FEC9D696C81F58850260CD795E20044B46AEE793693B7C8F041FDA605D27F4933552BE2B5027B589D0A067C9D30E01B78CAA9EAF25669A41EFA6F9500
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{81CA3E4C-2C76-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565340195843725
Encrypted:	false
SSDEEP:	48:IwJZGcprcGwpaSZG4pQEGrapbSNrGQpKHG7HpRhsTGIpG:rJ/ZUQS76SBSNFAmTh4A
MD5:	62A1D0953BD3D054C636A234B7F75277
SHA1:	A918DA62C0E1D24101ECEF11414901CDADB4D238
SHA-256:	5651142C9C2B7EFEC756E18F00095A93F487427837598DD5538773341440B11C
SHA-512:	3F1C8404FC3210F2172E78EC654FB8FE81BF2A5D526BDB1E043DE37D8C134D8F34C87DBFE121B56F10C9F49E3F56BB04EC986A507DC056489053A862816E3D3
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	72296
Entropy (8bit):	3.075290628437421
Encrypted:	false
SSDEEP:	96:nj0jzjLj0jzjmQQQQQIQQQQQUQQQQQEQQQQQh:/
MD5:	6FE52DB3C1D579C9E45DF61C1D32D397

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat

SHA1:	228CAB5861A6B203AAFDB2178F04375E77833AB9
SHA-256:	AE52BDC32878833E8D90C53D5E9102864CA45EBE2B3AA31E2D769ABD6F8E29E1
SHA-512:	A8537A083B15ED4F75E80C464D164AFF74524D3E612DABA345158E4AFE1DFEECCDC365777B4A58913CBC80162C3AA54E1D05044CA61F85609CBCFF4FC31299 8
Malicious:	false
Reputation:	low
Preview:	X.h.t.t.p.s.:././.s.e.c.u.r.e...a.a.d.c.d.n...m.i.c.r.o.s.o.f.t.o.n.l.i.n.e.-.p...c.o.m./.e.s.t.s./.2...1...6.6.6.9...4./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a...i.c.o.~(................h(......(..... ....(......................................"P.."""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333 333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""" """""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333 333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""""" """" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144. 2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\594a1ffedbcead0d014ab6452e6b1bf4nbr1605868747[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1086
Entropy (8bit):	4.943990229770432
Encrypted:	false
SSDEEP:	12:n/3qtdyuzm96olbOw2XmLxhlFfgaVtnHJX5GL4pr7tnk1A1iGc4bDY8zIXmuA:Pyw60ajXKx/FIWpX5GLW9k53iDjgmuA
MD5:	CB372B95DFCAF79CF09DA253AEDEA8B1
SHA1:	08E7999607C2F6B8EBB5E07681B0F22857D88E94
SHA-256:	118F4D0A8C85BFBE5E7DFA3162E04E73C6FCDA9CF1736B28F9472AA7E03BA2AF
SHA-512:	08476963CF8B4A3DAA000ACE639C9E713D37B0879EEA131287051BD6EEB309C2C267DAE6D36DF48EC093DCE6F4C879095FD0C14482B8B6AEF81077F6BFEFE6 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vapdelbnbapp.firebaseapp.com/fguysvcxcd/themes/css/594a1ffedbcead0d014ab6452e6b1bf4nbr1605868747.css
Preview:	#outdated {font-family:"Open Sans","Segoe UI",sans-serif;position:absolute;background-color:#f25648;color:white;display:none;overflow:hidden;left:0;position:fixed;text-al ign:center;text-transform:uppercase;top:0;width:100%;z-index:1500;padding:0 24px 24px 0;}#outdated.fullscreen {height:100%;}#outdated .vertical-center {display:table-cell;text-align:center;vertical-align:middle;}#outdated h6 {font-size:25px;line-height:25px;margin:12px 0;}#outdated p {font-size:12px;line-height:12px;margin:0;}#outdated #buttonUpdateBrowser {border:2px solid white;color:white;cursor:pointer;display:block;margin:30px auto 0;padding:10px 20px;position:relative;text-decoration:none; width:230px;}#outdated #buttonUpdateBrowser:hover {background-color:white;color:#f25648;}#outdated .last {height:20px;position:absolute;right:70px;top:10px;widt h:auto;display:inline-table;}#outdated .last[dir=rtl]{left:25px !important;right:auto !important;}#outdated #buttonCloseUpdateBrowser {color:white;display:block;font-size

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Print[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	476
Entropy (8bit):	7.35124642782842
Encrypted:	false
SSDEEP:	12:6v/78/8QCeKXzjl5V6VQTdwbtsxET1SDQi7N:sNfF6VYd6tf1SdN

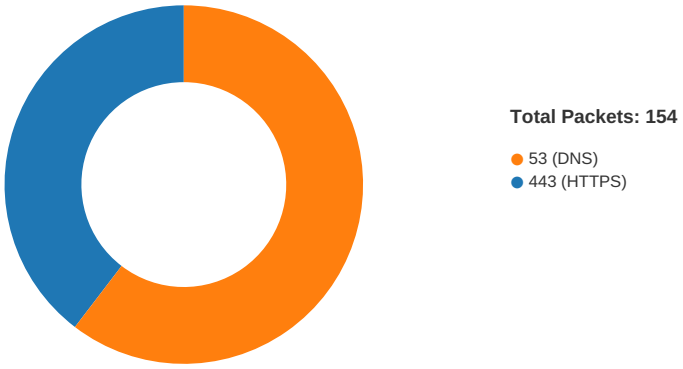
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Print[1].png	
MD5:	B8E8859FCD4E43D51233559C17A3C7BD
SHA1:	F0CA023F26A84761995FA0BF6935DE6A3B8AE6F8
SHA-256:	DC15A37B4015D0DECF639006E4F9002E742DDBFD7C669EC0AE469057F238B78D
SHA-512:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F22005
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....IDAT8O.S;..A.....M6.4....@.47....^I..<."&..W..Y...Y.....m...E.<..$..n...j..kL&.....}.j.....)@.....r..Q....]. .+.w...f3.R)...2^...ddO.^..Ud.BE..*D..h...I.....h..p..t...9.....1.."tD.....y.h.AQ.{."...J.D.U....c.b.i.h.t:..$&q..J..n.+9.r..B..F...e..`<...oS....Z-.H....NG...Jl..D.Z..@!...s<....m.'Ll..vc.?..~..v.n.9.; .m.5..K.A .....z=../>...M....r9..~...*..go.....IEND.B`.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:32.023004055 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.024147034 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.039572954 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.039700031 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.040431976 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.040503979 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.041801929 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.042138100 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.058197975 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.058307886 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.059715033 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.059751034 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.059889078 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.064915895 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.064954042 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.065026999 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.242747068 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.243465900 CET	49712	443	192.168.2.3	104.18.215.67

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:32.243535995 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.243632078 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.244014978 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.259176016 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.259335995 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.259546041 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.259799957 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.259962082 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.259991884 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.260229111 CET	443	49712	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.260288000 CET	49712	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.276102066 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.299799919 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.421665907 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.421694040 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.421722889 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.421760082 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.421916962 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.421978951 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.422080994 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422307014 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422372103 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.422487020 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422702074 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422760010 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.422924042 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422952890 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.422979116 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.423002005 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.423003912 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.423034906 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.423049927 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.423058987 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.423085928 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.423110962 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.462814093 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.519509077 CET	49719	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.519736052 CET	49720	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.520071983 CET	49721	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.520340919 CET	49722	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.520622015 CET	49723	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.520946026 CET	49724	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.522542000 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.522573948 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.522604942 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.535991907 CET	443	49720	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.536071062 CET	49720	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536158085 CET	443	49719	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.536222935 CET	49719	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536278009 CET	49720	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536418915 CET	49719	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536669970 CET	443	49721	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.536748886 CET	49721	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536925077 CET	49721	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.536973953 CET	443	49723	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.537029028 CET	443	49722	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.537040949 CET	49723	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.537085056 CET	49722	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.537201881 CET	49723	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.537265062 CET	443	49724	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.537334919 CET	49724	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.537456989 CET	49722	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.537692070 CET	49724	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.539031029 CET	443	49711	104.18.215.67	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:32.552479029 CET	443	49720	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.552788973 CET	443	49719	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.553350925 CET	443	49721	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.553510904 CET	443	49723	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.553739071 CET	443	49722	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.554131031 CET	443	49724	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.555186033 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.555289984 CET	443	49721	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.555414915 CET	443	49721	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.555478096 CET	49721	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.556056023 CET	443	49723	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.556091070 CET	443	49723	104.18.216.67	192.168.2.3
Nov 21, 2020 19:54:32.556126118 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.556145906 CET	49723	443	192.168.2.3	104.18.216.67
Nov 21, 2020 19:54:32.556160927 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.556190968 CET	443	49711	104.18.215.67	192.168.2.3
Nov 21, 2020 19:54:32.556195974 CET	49711	443	192.168.2.3	104.18.215.67
Nov 21, 2020 19:54:32.556216955 CET	443	49711	104.18.215.67	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:24.515007973 CET	53	58361	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:25.511750937 CET	63492	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:25.547509909 CET	53	63492	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:26.756540060 CET	60831	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:26.783890009 CET	53	60831	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:28.203150034 CET	60100	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:28.230623960 CET	53	60100	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:29.663970947 CET	53195	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:29.691265106 CET	53	53195	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:31.540569067 CET	49563	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:31.567861080 CET	53	49563	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:31.990153074 CET	51352	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:31.990463018 CET	59349	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:31.994901896 CET	57084	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:31.999110937 CET	58823	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.017419100 CET	53	51352	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.033674002 CET	53	59349	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.043188095 CET	53	58823	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.051600933 CET	53	57084	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.266669989 CET	57568	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.327709913 CET	53	57568	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.383701086 CET	50540	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.427541971 CET	53	50540	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.488571882 CET	54366	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.488616943 CET	53034	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.515461922 CET	53	54366	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.515530109 CET	53	53034	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.658099890 CET	55435	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.714838982 CET	53	55435	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.922795057 CET	50713	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.923628092 CET	56132	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.929869890 CET	58987	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:32.950030088 CET	53	50713	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.959065914 CET	53	56132	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:32.965420961 CET	53	58987	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.490806103 CET	60633	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.535000086 CET	53	60633	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.544369936 CET	61292	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.568366051 CET	63619	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.569257975 CET	64938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.579767942 CET	53	61292	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.595432997 CET	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:33.596167088 CET	53	64938	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.795939922 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.834813118 CET	53	61946	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.836817026 CET	64910	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.838721037 CET	52123	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.865668058 CET	53	52123	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.870984077 CET	56130	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.871020079 CET	56338	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.877034903 CET	53	64910	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.909898043 CET	59420	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.914587975 CET	53	56338	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.914618969 CET	53	56130	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.928617954 CET	58784	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.934753895 CET	63978	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:33.953269958 CET	53	59420	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.955568075 CET	53	58784	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.961677074 CET	53	63978	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:33.964423895 CET	62938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.008358002 CET	53	62938	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.041949034 CET	55708	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.061216116 CET	56803	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.081846952 CET	53	55708	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.088495016 CET	53	56803	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.105469942 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:34.128853083 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:34.128894091 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:34.130553007 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:34.130992889 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:34.146435022 CET	57145	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.161076069 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:34.162211895 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:34.172681093 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:34.172848940 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:34.177587986 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:34.189996004 CET	53	57145	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.199426889 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.214301109 CET	55359	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.222826004 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.222872019 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.227010965 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.243556023 CET	58306	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.250490904 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.250730991 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.258198023 CET	53	55359	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.281356096 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.281796932 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.287379980 CET	53	58306	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.291464090 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.291501999 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.291806936 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.292017937 CET	443	57146	172.217.23.98	192.168.2.3
Nov 21, 2020 19:54:34.318012953 CET	57146	443	192.168.2.3	172.217.23.98
Nov 21, 2020 19:54:34.354521036 CET	64124	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.367714882 CET	49361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.368352890 CET	63150	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.381447077 CET	53	64124	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.403429985 CET	53	49361	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.413830996 CET	53	63150	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:34.439745903 CET	53279	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:34.475090027 CET	53	53279	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:35.546881914 CET	56881	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:35.574037075 CET	53	56881	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:36.636668921 CET	53642	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:36.663918972 CET	53	53642	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:37.761015892 CET	49705	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:37.788233995 CET	53	49705	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:38.748706102 CET	61477	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:38.775875092 CET	53	61477	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:39.778623104 CET	61633	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:39.805708885 CET	53	61633	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:40.015793085 CET	49342	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:40.059618950 CET	53	49342	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:42.977767944 CET	55439	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:43.021543980 CET	53	55439	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:45.110114098 CET	57069	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:45.145992994 CET	53	57069	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:49.135467052 CET	56805	443	192.168.2.3	172.217.18.102
Nov 21, 2020 19:54:49.177102089 CET	443	56805	172.217.18.102	192.168.2.3
Nov 21, 2020 19:54:51.594835043 CET	57659	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:51.632180929 CET	53	57659	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:52.777503014 CET	54717	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:52.843632936 CET	53	54717	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:53.825766087 CET	63975	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:53.867655039 CET	53	63975	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:54.493527889 CET	56639	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:54.537364006 CET	53	56639	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:54.986700058 CET	51856	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:55.013906956 CET	53	51856	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:56.911983013 CET	56546	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:56.939256907 CET	53	56546	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:58.559757948 CET	62152	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:58.587045908 CET	53	62152	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:58.718288898 CET	53470	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:58.762640953 CET	53	53470	8.8.8.8	192.168.2.3
Nov 21, 2020 19:54:58.891486883 CET	56446	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:54:58.941345930 CET	53	56446	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:01.279037952 CET	59631	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:01.317080021 CET	53	59631	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:01.324953079 CET	55515	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:01.361999035 CET	53	55515	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:09.049725056 CET	64547	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:09.087121964 CET	53	64547	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:11.054785967 CET	51759	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:11.081964016 CET	53	51759	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:11.306566000 CET	59207	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:11.346303940 CET	53	59207	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:11.924185991 CET	54269	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:11.977423906 CET	53	54269	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:13.882004976 CET	54856	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:13.917880058 CET	53	54856	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:14.154642105 CET	64140	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:14.205842018 CET	53	64140	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:15.850764990 CET	62271	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:15.877813101 CET	53	62271	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:16.252113104 CET	57404	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:16.291651011 CET	53	57404	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:16.617122889 CET	62997	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:16.654344082 CET	53	62997	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:17.366733074 CET	57712	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:17.389451981 CET	60065	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:17.403960943 CET	53	57712	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:17.428900003 CET	53	60065	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:17.476604939 CET	55068	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:17.479435921 CET	64700	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:17.515259027 CET	53	64700	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:17.527961969 CET	53	55068	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:17.785460949 CET	61998	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:17.822402954 CET	53	61998	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:55:21.557188988 CET	53724	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:21.595015049 CET	53	53724	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:22.287286043 CET	52328	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:22.325269938 CET	53	52328	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:22.558027983 CET	53724	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:22.593739986 CET	53	53724	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.022594929 CET	58051	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.059736967 CET	53	58051	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.287872076 CET	52328	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.323818922 CET	53	52328	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.558876991 CET	53724	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.565196991 CET	64130	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.592916012 CET	50491	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.596710920 CET	53	53724	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.605901003 CET	53	64130	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.642940044 CET	53	50491	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:23.914185047 CET	53004	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:23.960052967 CET	53	53004	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:24.289753914 CET	52328	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:24.325520039 CET	53	52328	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:25.694346905 CET	53724	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:25.730271101 CET	53	53724	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:26.291018963 CET	52328	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:26.318291903 CET	53	52328	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:29.694298983 CET	53724	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:29.730123997 CET	53	53724	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.222177982 CET	52529	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.234724998 CET	53656	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.249476910 CET	53	52529	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.291256905 CET	53	53656	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.292285919 CET	52328	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.319410086 CET	53	52328	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.492031097 CET	56059	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.527837038 CET	53	56059	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.576224089 CET	63060	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.619955063 CET	53	63060	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.671252012 CET	51498	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:30.706763983 CET	53	51498	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:30.970029116 CET	59943	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:31.005803108 CET	53	59943	8.8.8.8	192.168.2.3
Nov 21, 2020 19:55:33.101281881 CET	50118	53	192.168.2.3	8.8.8.8
Nov 21, 2020 19:55:33.137161970 CET	53	50118	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 19:54:31.990153074 CET	192.168.2.3	8.8.8.8	0xff07	Standard query (0)	www.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.488571882 CET	192.168.2.3	8.8.8.8	0x7860	Standard query (0)	static.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.923628092 CET	192.168.2.3	8.8.8.8	0x790f	Standard query (0)	font-publi c.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.929869890 CET	192.168.2.3	8.8.8.8	0x3bbc	Standard query (0)	media-priv ate.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.544369936 CET	192.168.2.3	8.8.8.8	0x1de8	Standard query (0)	cl.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.568366051 CET	192.168.2.3	8.8.8.8	0x8b66	Standard query (0)	js.appboyc dn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.795939922 CET	192.168.2.3	8.8.8.8	0xfe46	Standard query (0)	sdk.iad-01 .braze.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.836817026 CET	192.168.2.3	8.8.8.8	0x1185	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.870984077 CET	192.168.2.3	8.8.8.8	0x4280	Standard query (0)	9812343.fl s.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.928617954 CET	192.168.2.3	8.8.8.8	0xf237	Standard query (0)	sp.analyti cs.yahoo.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 19:54:33.934753895 CET	192.168.2.3	8.8.8.8	0x6b7b	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.041949034 CET	192.168.2.3	8.8.8.8	0x7db9	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.146435022 CET	192.168.2.3	8.8.8.8	0xefcb	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.214301109 CET	192.168.2.3	8.8.8.8	0x44f0	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.354521036 CET	192.168.2.3	8.8.8.8	0xba17	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.368352890 CET	192.168.2.3	8.8.8.8	0x2972	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.439745903 CET	192.168.2.3	8.8.8.8	0xada7	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:42.977767944 CET	192.168.2.3	8.8.8.8	0x5a06	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:52.777503014 CET	192.168.2.3	8.8.8.8	0x8a62	Standard query (0)	candanappdevmoe.azurewebsites.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:53.825766087 CET	192.168.2.3	8.8.8.8	0xb47b	Standard query (0)	cnd11.smsmail.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:54.493527889 CET	192.168.2.3	8.8.8.8	0xc8f0	Standard query (0)	vapdelbnbapp.firebaseapp.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.911983013 CET	192.168.2.3	8.8.8.8	0x5b1	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.559757948 CET	192.168.2.3	8.8.8.8	0x5e95	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:01.279037952 CET	192.168.2.3	8.8.8.8	0xe761	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:01.324953079 CET	192.168.2.3	8.8.8.8	0x5b5f	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:09.049725056 CET	192.168.2.3	8.8.8.8	0x5dc3	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:11.054785967 CET	192.168.2.3	8.8.8.8	0x9f24	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:11.924185991 CET	192.168.2.3	8.8.8.8	0x2513	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:14.154642105 CET	192.168.2.3	8.8.8.8	0x2325	Standard query (0)	client.hip.live.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:15.850764990 CET	192.168.2.3	8.8.8.8	0xbf2e	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:17.476604939 CET	192.168.2.3	8.8.8.8	0xdb46	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:23.592916012 CET	192.168.2.3	8.8.8.8	0xed0b	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:54:32.017419100 CET	8.8.8.8	192.168.2.3	0xff07	No error (0)	www.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.017419100 CET	8.8.8.8	192.168.2.3	0xff07	No error (0)	www.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.515461922 CET	8.8.8.8	192.168.2.3	0x7860	No error (0)	static.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.515461922 CET	8.8.8.8	192.168.2.3	0x7860	No error (0)	static.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.959065914 CET	8.8.8.8	192.168.2.3	0x790f	No error (0)	font-public.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.959065914 CET	8.8.8.8	192.168.2.3	0x790f	No error (0)	font-public.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:32.965420961 CET	8.8.8.8	192.168.2.3	0x3bbc	No error (0)	media-private.canva.com		104.18.216.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:54:32.965420961 CET	8.8.8.8	192.168.2.3	0x3bbc	No error (0)	media-private.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.579767942 CET	8.8.8.8	192.168.2.3	0x1de8	No error (0)	cl.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.579767942 CET	8.8.8.8	192.168.2.3	0x1de8	No error (0)	cl.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.595432997 CET	8.8.8.8	192.168.2.3	0x8b66	No error (0)	js.appboycdn.com		104.22.9.79	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.595432997 CET	8.8.8.8	192.168.2.3	0x8b66	No error (0)	js.appboycdn.com		104.22.8.79	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.595432997 CET	8.8.8.8	192.168.2.3	0x8b66	No error (0)	js.appboycdn.com		172.67.7.226	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.834813118 CET	8.8.8.8	192.168.2.3	0xfe46	No error (0)	sdk.iad-01.braze.com	d2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:33.877034903 CET	8.8.8.8	192.168.2.3	0x1185	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:33.914618969 CET	8.8.8.8	192.168.2.3	0x4280	No error (0)	9812343.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:33.914618969 CET	8.8.8.8	192.168.2.3	0x4280	No error (0)	dart.l.doubleclick.net		172.217.18.102	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.953269958 CET	8.8.8.8	192.168.2.3	0xa18c	No error (0)	pagead.l.doubleclick.net		172.217.16.130	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.955568075 CET	8.8.8.8	192.168.2.3	0xf237	No error (0)	sp.analytics.yahoo.com	spdc-global.pbp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:33.955568075 CET	8.8.8.8	192.168.2.3	0xf237	No error (0)	spdc-global.pbp.gysm.yahoodns.net		212.82.100.181	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:33.961677074 CET	8.8.8.8	192.168.2.3	0x6b7b	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:33.961677074 CET	8.8.8.8	192.168.2.3	0x6b7b	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.081846952 CET	8.8.8.8	192.168.2.3	0x7db9	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.081846952 CET	8.8.8.8	192.168.2.3	0x7db9	No error (0)	mix.linkedin.com	pop-tln1-alpha.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.081846952 CET	8.8.8.8	192.168.2.3	0x7db9	No error (0)	pop-tln1-alpha.mix.linkedin.com		185.63.144.5	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.189996004 CET	8.8.8.8	192.168.2.3	0xefcb	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.189996004 CET	8.8.8.8	192.168.2.3	0xefcb	No error (0)	pagead46.l.doubleclick.net		172.217.23.98	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.258198023 CET	8.8.8.8	192.168.2.3	0x44f0	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.258198023 CET	8.8.8.8	192.168.2.3	0x44f0	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.258198023 CET	8.8.8.8	192.168.2.3	0x44f0	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.258198023 CET	8.8.8.8	192.168.2.3	0x44f0	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.258198023 CET	8.8.8.8	192.168.2.3	0x44f0	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.287379980 CET	8.8.8.8	192.168.2.3	0x3c2e	No error (0)	pagead46.l.doubleclick.net		172.217.22.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:54:34.381447077 CET	8.8.8.8	192.168.2.3	0xba17	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.413830996 CET	8.8.8.8	192.168.2.3	0x2972	No error (0)	www.google.co.uk		172.217.21.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:34.475090027 CET	8.8.8.8	192.168.2.3	0xada7	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:34.475090027 CET	8.8.8.8	192.168.2.3	0xada7	No error (0)	pagead46.l.doubleclick.net		172.217.16.194	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:43.021543980 CET	8.8.8.8	192.168.2.3	0x5a06	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:43.021543980 CET	8.8.8.8	192.168.2.3	0x5a06	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:52.843632936 CET	8.8.8.8	192.168.2.3	0x8a62	No error (0)	candanappdevmoe.azurewebsites.net	waws-prod-yt1-019.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:52.843632936 CET	8.8.8.8	192.168.2.3	0x8a62	No error (0)	waws-prod-yt1-019.sip.azurewebsites.windows.net	waws-prod-yt1-019.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:54:53.867655039 CET	8.8.8.8	192.168.2.3	0xb47b	No error (0)	cnd11.smsmail.net		172.67.185.66	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:53.867655039 CET	8.8.8.8	192.168.2.3	0xb47b	No error (0)	cnd11.smsmail.net		104.31.67.162	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:53.867655039 CET	8.8.8.8	192.168.2.3	0xb47b	No error (0)	cnd11.smsmail.net		104.31.66.162	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:54.537364006 CET	8.8.8.8	192.168.2.3	0xc8f0	No error (0)	vapdelbnbapp.firebaseapp.com		151.101.1.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:54.537364006 CET	8.8.8.8	192.168.2.3	0xc8f0	No error (0)	vapdelbnbapp.firebaseapp.com		151.101.65.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.939256907 CET	8.8.8.8	192.168.2.3	0x5b1	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.939256907 CET	8.8.8.8	192.168.2.3	0x5b1	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.939256907 CET	8.8.8.8	192.168.2.3	0x5b1	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.939256907 CET	8.8.8.8	192.168.2.3	0x5b1	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:56.939256907 CET	8.8.8.8	192.168.2.3	0x5b1	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.587045908 CET	8.8.8.8	192.168.2.3	0x5e95	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.587045908 CET	8.8.8.8	192.168.2.3	0x5e95	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:01.317080021 CET	8.8.8.8	192.168.2.3	0xe761	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:01.361999035 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:09.087121964 CET	8.8.8.8	192.168.2.3	0x5dc3	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:11.081964016 CET	8.8.8.8	192.168.2.3	0x9f24	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:11.081964016 CET	8.8.8.8	192.168.2.3	0x9f24	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:55:11.346303940 CET	8.8.8.8	192.168.2.3	0xef2b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:11.977423906 CET	8.8.8.8	192.168.2.3	0x2513	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:11.977423906 CET	8.8.8.8	192.168.2.3	0x2513	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:11.977423906 CET	8.8.8.8	192.168.2.3	0x2513	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:14.205842018 CET	8.8.8.8	192.168.2.3	0x2325	No error (0)	client.hip.live.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:14.205842018 CET	8.8.8.8	192.168.2.3	0x2325	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:14.205842018 CET	8.8.8.8	192.168.2.3	0x2325	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:15.877813101 CET	8.8.8.8	192.168.2.3	0xbf2e	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:15.877813101 CET	8.8.8.8	192.168.2.3	0xbf2e	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:17.515259027 CET	8.8.8.8	192.168.2.3	0xf114	No error (0)	consentdeliveryfd.azurefd.net	t-0001.t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:17.527961969 CET	8.8.8.8	192.168.2.3	0xdb46	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:23.642940044 CET	8.8.8.8	192.168.2.3	0xed0b	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:54:34.065291882 CET	212.82.100.181	443	192.168.2.3	49737	CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Aug 01 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Jan 28 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 21, 2020 19:54:34.143867016 CET	185.63.144.5	443	192.168.2.3	49740	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Feb 05 13:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:54:53.921535969 CET	172.67.185.66	443	192.168.2.3	49759	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Wed Nov 18 01:00:00 CET 2020	Thu Nov 18 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 19:54:53.926249027 CET	172.67.185.66	443	192.168.2.3	49758	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Wed Nov 18 01:00:00 CET 2020	Thu Nov 18 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 19:54:54.579582930 CET	151.101.1.195	443	192.168.2.3	49760	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Wed Oct 21 19:55:39 CEST 2020	Wed Oct 20 19:55:39 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 21, 2020 19:54:54.587806940 CET	151.101.1.195	443	192.168.2.3	49761	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Wed Oct 21 19:55:39 CEST 2020	Wed Oct 20 19:55:39 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 21, 2020 19:54:56.976197004 CET	104.16.122.175	443	192.168.2.3	49767	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	Sun Aug 02 02:00:00 CEST 2020	Mon Aug 02 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:54:56.976771116 CET	104.16.122.175	443	192.168.2.3	49766	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 19:54:58.624902010 CET	104.16.19.94	443	192.168.2.3	49770	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 19:54:58.626650095 CET	104.16.19.94	443	192.168.2.3	49769	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 21, 2020 19:55:12.114929914 CET	152.199.21.175	443	192.168.2.3	49783	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 21, 2020 19:55:12.115078926 CET	152.199.21.175	443	192.168.2.3	49786	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:55:12.115197897 CET	152.199.21.175	443	192.168.2.3	49787	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 21, 2020 19:55:12.115314007 CET	152.199.21.175	443	192.168.2.3	49788	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 21, 2020 19:55:12.115525961 CET	152.199.21.175	443	192.168.2.3	49784	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 21, 2020 19:55:12.115667105 CET	152.199.21.175	443	192.168.2.3	49785	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Tue Oct 05 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Nov 21, 2020 19:55:15.935674906 CET	67.199.248.11	443	192.168.2.3	49792	CN=bit.ly, O="Bitly, Inc.", L=New York, ST=New York, C=US, SERIALNUMBER=4627013, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 05 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Aug 10 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:55:15.936299086 CET	67.199.248.11	443	192.168.2.3	49793	CN=bit.ly, O="Bitly, Inc.", L=New York, ST=New York, C=US, SERIALNUMBER=4627013, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 05 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2412 Parent PID: 4088

General

Start time:	19:54:29
Start date:	21/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --force-renderer-accessibility 'https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes

MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 3636 Parent PID: 2412

General

Start time:	19:54:30
Start date:	21/11/2020
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=1540,14482813496842422081,2496366691596550 75,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: dllhost.exe PID: 6616 Parent PID: 792

General

Start time:	19:54:34
Start date:	21/11/2020
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff7bc440000

File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 3388 Parent PID: 6616

General

Start time:	19:54:35
Start date:	21/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: iexplore.exe PID: 7072 Parent PID: 792

General

Start time:	19:54:51
Start date:	21/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6068a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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: iexplore.exe PID: 6292 Parent PID: 7072

General

Start time:	19:54:52
Start date:	21/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7072 CREDAT:17410 /prefetch:2
Imagebase:	0xd60000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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

Disassembly

Code Analysis