ID: 321415
Cookbook: browseurl.jbs
Time: 19:54:11
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

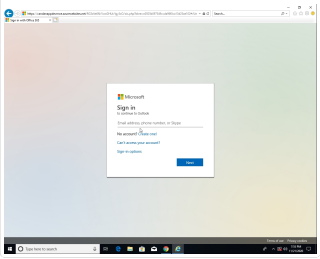
Analysis Report https://www.canva.com/design/DAEOE…

Overview

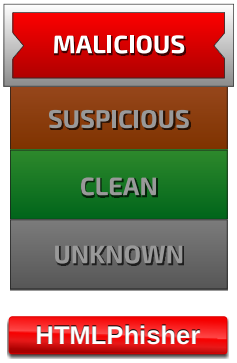
General Information

Sample URL:	https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_co...DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton
Analysis ID:	321415

Most interesting Screenshot:



Detection

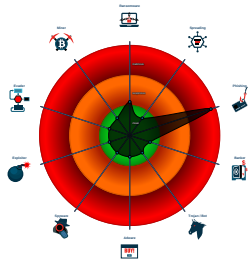


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6732 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: 6960 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,11732546741858598205,15005368519812649130,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- dllhost.exe (PID: 1364 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- iexplore.exe (PID: 8120 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5052 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:8120 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

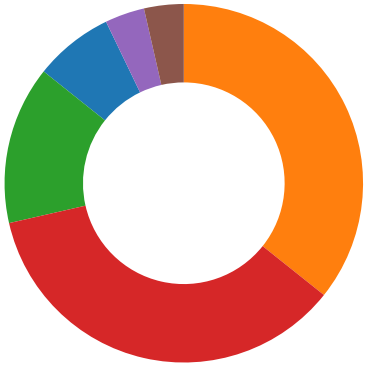
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ois[1].htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ois[1].htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Networking
- System Summary
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

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

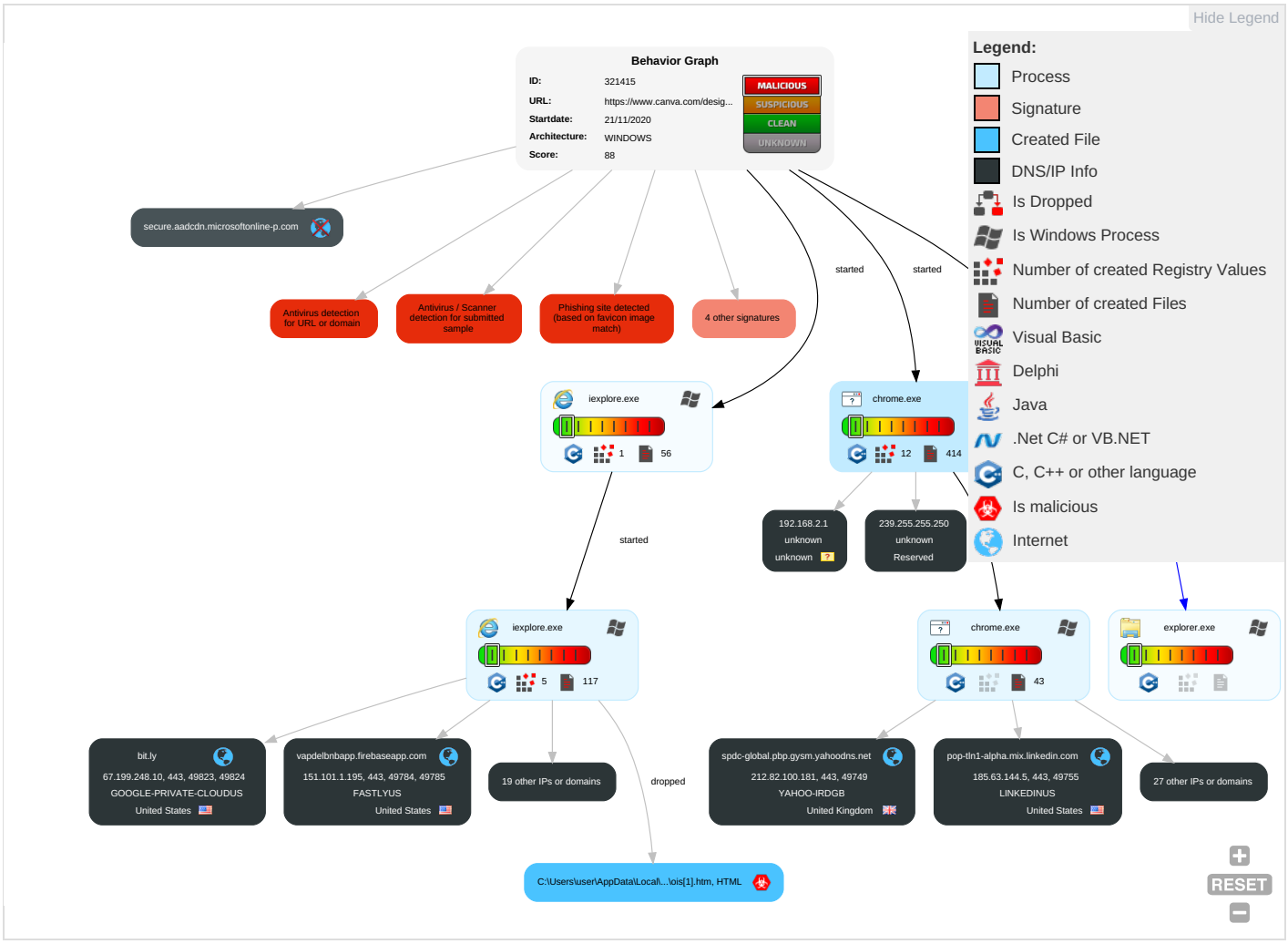
Phishing site detected (based on image similarity)

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 1	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

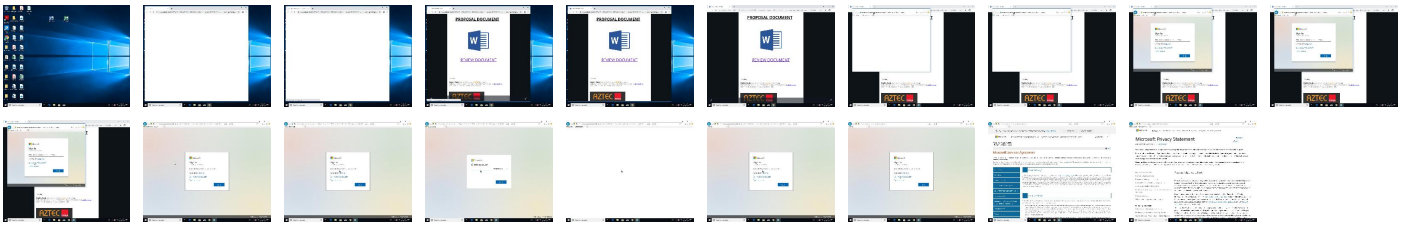
Behavior Graph

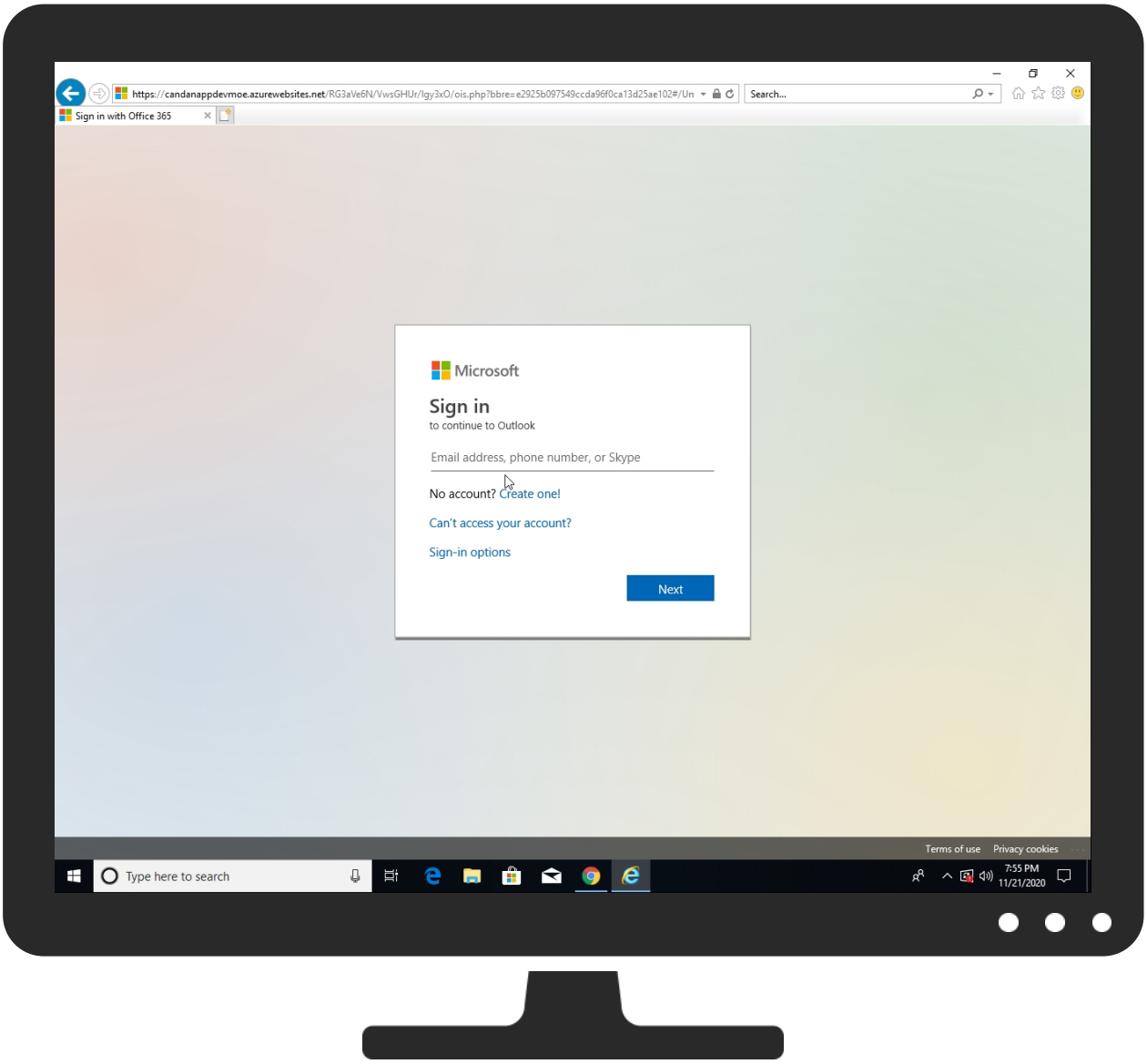


Screenshots

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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#/Umolh1n7Zre4LrFlHAzNANn4EAJkljplAJQJ2a9-@&!nMo7W9B6y82fXLE3mVQIAZOb5sgkq@!&4Z1UuNv62qmRrls3xtfOVy5pbFc&@!-PenYufW5GJ10TL4CWplkVPjQPYhRRPu3UpBfORylr9rgqo1afqTdA8dbrthM595yl030V7c0y7J45Qhsl7jmrmZB008iRII-8tEiLm1CEIozXYyPvoAMQUjyEoOBKIybdzgJF6a2YehPPRNl9jogm8OQcHXhcmC6lqkTIdwTnA/D1710RZrrztcKgkEZ4JFqlWIPWV5jXvcqcQGJBtbA7iNk0YKz7LRuiS5wa888sf8gq	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#/riY01eQv887WU97FVLJpUH3nwahsbJVSKWGfN1S-@&!nMo7W9B6y82fXLE3mVQIAZOb5sgkq@!&4Z1UuNv62qmRrls3xtfOVy5pbFc&@!-ALxhpotzQX4Kno3EABjId9bKhZXdr81TPrNibSp5cetprWbvSr2wotx6wTV7UbQxXWoy8oxtr8Y75ffZCVcXCY5SHEkNm5u-5CSfWsT50XMXwKBmzDTgjftO5FWYMCKrYujcOUMofd7ZpHVGMlp5vUkBW2pkno7bpIMMZCmgbw/1LczHYZ0J6EiKvr07cnkHnbiTXBH4kslNTBLXfkemVwqzryLlzmwn1Swku1zFAFj9p	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://adservice.google.co.uk/ddm/fls/i/dc_pre=CPXhifynlO0CFQbhuwgdo-gHww;src=9812343;type=retar0;c	0%	Avira URL Cloud	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://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	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/SPS	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://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	

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		unknown
cl.canva.com	104.18.216.67	true	false		high
vapdelbnbapp.firebaseapp.com	151.101.1.195	true	false		unknown
www.canva.com	104.18.215.67	true	false		high
spdc-global.pbp.gysm.yahoodns.net	212.82.100.181	true	false		unknown
pop-tln1-alpha.mix.linkedin.com	185.63.144.5	true	false		high
cnd11.smsmail.net	172.67.185.66	true	false		unknown
static.canva.com	104.18.216.67	true	false		high
pagead.l.doubleclick.net	216.58.205.226	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	67.199.248.10	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	104.16.124.175	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
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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#/Umolh1n7Zre4LrFlHAzNANn4EAJkljpIAJQJ2a9-@&!nMo7W9B6y82fXLE3mVQIAZOb5sgkq@!&4Z1UuNv62qmRrls3xtfOVy5pbFc&@!-PenYufW5GJ10TL4CWplkVPjQPYhRRPu3UpBfORylr9rgqo1afqTdA8dbrthM595yI030V7c0y7J45Qhsl7jmrmZB008iRII-8tEiLm1CEIozXYyPvoAMQUjyEoOBKIybdzgJF6a2YehPPRNl9jogm8OQcHXhcmC6lqkTIdwTnA/D1710RZrztcKgkEZ4JFqIWIPWV5jXvcqcQGJBtbA7iNk0YKz7LRuiS5wa888sf8gq	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0ca13d25ae102#/riY01eQv887WU97FVLJpUH3nwahsbJVSKWGfN1S-@&!nMo7W9B6y82fXLE3mVQIAZOb5sgkq@!&4Z1UuNv62qmRrls3xtfOVy5pbFc&@!-ALxhpotzQX4Kno3EABjId9bKhZXdr81TPrNibSp5cetprWbvSr2wotx6wTV7UbQxXWoy8oxtr8Y75ffZCVcXCY5SHEkNm5u-5CSfWsT50XMXwKBmzDTgjftO5FWYMCKrYujcOUMofd7ZpHVGMlp5vUkBW2pkno7bpIMMZCmgbw/1LczHYZ0J6EiKvr07cnkHnbiTXBH4kslNTBLXfkemVwqzryLlzmwn1Swku1zFAFj9p	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

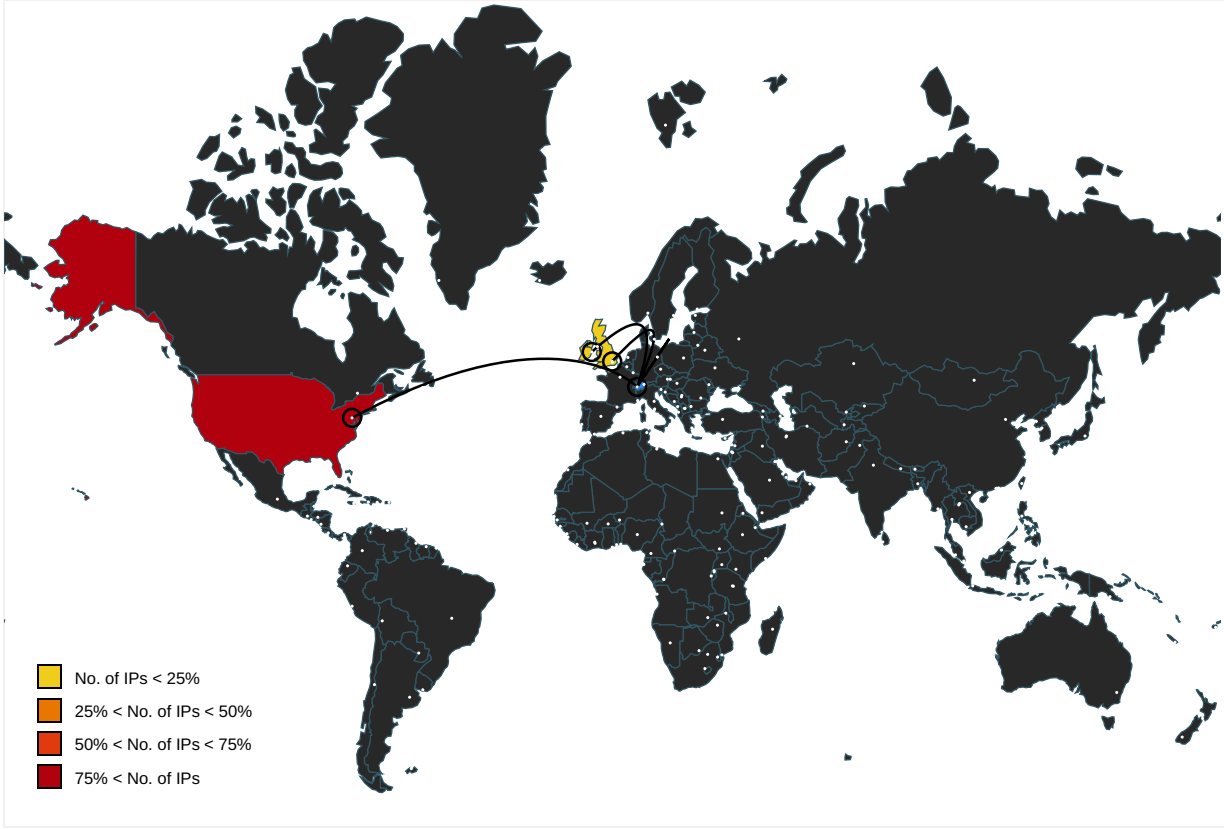
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.9.dr	false		high
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/	~DF9D51126FF4AB1D0F.TMP.8.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://www.acuityads.com/opt-out/	PrivacyStatement[1].htm.9.dr	false		high
http://https://a.nel.cloudflare.com/report?s=aW2xMiZ3RDaz89WO4lC7JHnHmA8KwPbvn2lgToL2UL%2BuOFrik%2FuuuxVGKh	Reporting and NEL.1.dr	false		high
http://https://www.youradchoices.ca/fr	PrivacyStatement[1].htm.9.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.9.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.9.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct)	servicesagreement[1].htm.9.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	PrivacyStatement[1].htm.9.dr	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.669306015.000000000B976000.00000002.00000001.sdmp	false		high
http://https://a.nel.cloudflare.com/report?s=v4prBolerkKeiP8s3KyQOMPHSF%2FOV8X4ERoqkDtraXTfrNWH0AcLl114zcoG	Reporting and NEL.1.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.9.dr	false		high
http://opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.9.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_X1BYS2jZMbi7hfUj8VuqFA2[1].js.9.dr	false		high
http://www.sajatypeworks.com	explorer.exe, 00000003.00000000.669306015.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.00000000.669306015.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/taxservice	servicesagreement[1].htm.9.dr	false		high
http://https://skype.com/go/myaccount	servicesagreement[1].htm.9.dr	false		high
http://https://adservice.google.co.uk/ddm/fls/i/dc_pre=CPXhifynlO0CFQbhuwgdo-gHww;src=9812343;type=retar0;c	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.canva.com/web/b144f4025476bd90a66e5378b1d15df650125aed.strings.js	4cbfe86bb692371e_0.0.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.9.dr	false		high
http://https://www.appnexus.com/	PrivacyStatement[1].htm.9.dr	false		high
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	signup[1].htm.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/ois.php?bbre=e2925b097549ccda96f0c	{18055A4C-2C2B-11EB-90EB-ECF4BBEA1588}.dat.8.dr	true	• Avira URL Cloud: safe	unknown
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, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.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.9.dr	false		high
http://https://canva.com/$2	4cbfe86bb692371e_0.0.dr	false		high
http://https://www.youronlinechoices.com/	PrivacyStatement[1].htm.9.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.9.dr	false		high
http://https://dns.google	2a4dce63-53c8-42f1-bd1f-a68a480ec17f.tmp.1.dr, 13f18794-7164-4700-be87-b9da15fd8ee6.tmp.1.dr, e8d153f1-2252-49dc-be36-ebde0e5a28b9.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.adjust.com/opt-out/	PrivacyStatement[1].htm.9.dr	false		high
http://https://www.xbox.com/managedatacollection	PrivacyStatement[1].htm.9.dr	false		high
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	signup[1].htm.9.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=yKTF3Tw3WsroBgCs9Rxj4V5KpFLD3NThcAIBlXbYHHfXWpC34FRp1AxKnv18dg	Reporting and NEL.1.dr	false		high
http://www.mpegla.com).	servicesagreement[1].htm.9.dr	false	• Avira URL Cloud: safe	low
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	signup[1].htm.9.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://9812343.fls.doubleclick.net/activityi;dc_pre=CPXhifynlO0CFQbhuwgdo-gHww;src=9812343;type=ret	Current Session.0.dr	false		high
http://https://www.skype.com).	servicesagreement[1].htm.9.dr	false	• Avira URL Cloud: safe	low
http://https://www.xbox.com	PrivacyStatement[1].htm.9.dr	false		high
http://https://acctcdn.msauth.net/lightweightsignuppackage_oZIcfFtGMdm_yHyDEji_8w2.js?v=1	signup[1].htm.9.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.9.dr	false		high
http://https://github.com/douglascrockford/JSON-js	signup[1].htm.9.dr	false		high
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	imagestore.dat.9.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, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.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.9.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfU j8VuqFA2[1].js.9.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.9.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=RrI6%2F6uhRf8Bamd0EHaUo7aah9x8n8AF%2BnzkNA10dqLmwzpodG9QtLqKsz	Reporting and NEL.1.dr	false		high
http://https://a.nel.cloudflare.com/report?s=j58cTkLrSxTm%2BifGB25qLfcJ949J3J7RS44PQ%2Ft0qiSIgYwA30jMx5yas%	Reporting and NEL.1.dr	false		high
http:// https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html	PrivacyStatement[1].htm.9.dr	false		high
http://https://www.skype.com/go/legal	servicesagreement[1].htm.9.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.9.dr	false		high
http://https://www.microsoft.	{18055A4C-2C2B-11EB-90EB-ECF4BBEA1588}.dat.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://canva.com/p	c3d256598d5af694_0.0.dr	false		high
http:// https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/$HTTP	~DF9D51126FF4AB1D0F.TMP.8.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/legal/privacy-policy	PrivacyStatement[1].htm.9.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.9.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	PrivacyStatement[1].htm.9.dr	false		high
http:// https://candanappdevmoe.azurewebsites.net/RG3aVe6N/VwsGHUr/lgy3xO/SPS	~DF9D51126FF4AB1D0F.TMP.8.dr	true	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.9.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	PrivacyStatement[1].htm.9.dr	false		high
http://https://login.skype.com/login	PrivacyStatement[1].htm.9.dr	false		high
http://https://npms.io/search?q=ponyfill.	lodash.min[1].js.9.dr	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://www.skype.com/go/ustax	servicesagreement[1].htm.9.dr	false		high
http://jquery.org/license	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.9.dr	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://canva.com/h	e4115b2c93fca474_0.0.dr	false		high
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://acctcdn.msauth.net	signup[1].htm.9.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.optimizely.com/legal/opt-out/	PrivacyStatement[1].htm.9.dr	false		high
http://sizzlejs.com/	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.9.dr	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://signup.live.com/error.aspx?errcode=1045&mkt=en-US	signup[1].htm.9.dr	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://canva.com/q3	56a246e5228caa4a_0.0.dr	false		high
http://https://9812343.fls.doubleclick.net	Current Session.0.dr	false		high
http://www.typography.netD	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.669306015.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.privacyshield.gov/welcome	PrivacyStatement[1].htm.9.dr	false		high
http://https://ondemand.webtrends.com/support/optout.asp	PrivacyStatement[1].htm.9.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.9.dr	false		high
http:// https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMO YoF6OWlu9bVg/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.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://snap.licdn.com/li.lms-analytics/insight.beta.min.js	5e83b9cfa3f81ad1_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
216.58.205.226	unknown	United States		15169	GOOGLEUS	false
172.217.22.66	unknown	United States		15169	GOOGLEUS	false
104.16.124.175	unknown	United States		13335	CLOUDFLARENETUS	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.199.248.10	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
104.22.9.79	unknown	United States		13335	CLOUDFLARENETUS	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:	321415
Start date:	21.11.2020
Start time:	19:54:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
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:	16
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@36/273@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?bbre=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, svchost.exe, wuapihost.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, 216.58.212.163, 172.217.16.142, 172.217.18.13, 216.58.206.14, 173.194.182.74, 172.217.16.138, 216.58.205.227, 172.217.23.104, 151.101.1.208, 151.101.65.208, 151.101.129.208, 151.101.193.208, 2.18.69.168, 204.79.197.200, 13.107.21.200, 172.217.23.174, 216.58.208.36, 13.107.42.14, 104.42.151.234, 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, 172.217.21.227, 52.147.198.201, 51.132.208.181, 104.108.39.131, 13.71.170.130, 104.43.139.144, 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, 52.155.217.156, 20.190.137.64, 20.190.137.1, 40.126.9.98, 20.190.137.78, 52.170.57.27, 2.20.142.209, 2.20.142.210, 20.54.26.129, 92.122.145.53, 92.122.213.200, 92.122.213.219, 2.18.70.63, 152.199.19.160, 92.122.213.247, 92.122.213.194, 152.199.19.161, 92.122.213.240, 104.108.38.107, 172.217.16.131, 172.217.18.99, 173.194.182.233 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, assets.onestore.ms.edgekey.net, clientservices.googleapis.com, i.s-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, au-bg-shim.trafficmanager.net, acctcdnvzeuno.ec.azureedge.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, t-0001.t-msedge.net, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, 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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, skypedataprdcoleus14.cloudapp.net, go.microsoft.com, ams2.b.f.prd.aadg.trafficmanager.net, www.googletagmanager.com, e13761.dscg.akamaiedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, fonts.gstatic.com, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, 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, audownload.windowsupdate.nsatc.net, 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, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus16.cloudapp.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, aadcdnoriginwus2.afd.azureedge.net, privacy.microsoft.com.edgekey.net, r5---sn-4g5e6ns7.gvt1.com, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, d2.shared.global.fastly.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, displaycatalog.mp.microsoft.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, ctldl.windowsupdate.com, Edge-Prod-FRAr3.ctrl.t-0001.t-msedge.net, r5.sn-4g5e6ns7.gvt1.com, account.msa.trafficmanager.net, 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 exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many 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
19:55:00	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:\Users\user\AppData\Local\Google\Chrome\User Data\4007a6f6-7c08-484e-a2c4-b5fa92c8e8c7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.75127385414108
Encrypted:	false
SSDEEP:	384:nrXk0WZT+mhAjNMr9vIU330CDHejGTmrxGUGxX6SKVrBcmViV2kAIzO2KAN510di:d6FJ6K330efiYi0HvewKG4gRz
MD5:	0755F3FA2F669F2B4CAA424C278DC5B0
SHA1:	BEAAC1DCEE0090F8C08E5D49AC2FD55F0F40521F
SHA-256:	0BCC57F62E431D695191DCC4C62A53B044A5456905B1FDEE2F09565C376F3F0E
SHA-512:	26B4B8DDD0533DBD303315C41AF7780755E795A174CD353C909AD6674C73458CCE12316EAC4E8844F7D8120E847267EA6DA83DBE2B42028202B416E5902B03E
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)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\984134fe-e9b9-4fb6-98a5-206eeb4dc9fe.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):	162578
Entropy (8bit):	6.082966773571222
Encrypted:	false
SSDEEP:	3072:89wA2NNCxQM9b0q+szv+tnMI1FcbXafIB0u1GOJmA3iuRO:ywrExQM9b7fD+ZMcaqfIlUOoSiuRO
MD5:	FD4A810071A015549E0549A77F1753F3
SHA1:	D67922F7A44933E1FD753142DCFF19EC0DB27B06
SHA-256:	32756CDF3A4D24F0E2717E43DAF474CABB268F4A4652A6C6D4EE1FEB12577818
SHA-512:	D4095A4EC5B3CAB30AB6B2643D19D8D337F1DE1B47BC43A377D0BB303B4AC0AD303D6776F0CAEB60C1220F399FEA8F99A1D83FCAAE4CD433B07A0AF70D1C4 819
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605984898154947e+12,"network":1.605984898e+12,"ticks":300544607.0,"uncertainty":2447193.0}},"os_crypt":{"encrypted_key": "RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiL GeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwR gUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715349536"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\00a53aa8-48ec-40ab-be40-fb1bac72e355.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):	5414
Entropy (8bit):	5.17235674583412
Encrypted:	false
SSDEEP:	96:nSCLEXiN1uJ+7Xx9IVGKHk0JCKL8EvkI1HXbOElVuHn:nSCLPN1++7h9I7P4KhvkI5c
MD5:	91F256FDCC91B481CBC510FAECCCEEE7
SHA1:	866F7A1E02D12CEC509C55E2A995B8D06CB0E533
SHA-256:	1CE2EEC89F53304297309887136016A5CDCC5898AE9EDF4D3F847E5494FC729F
SHA-512:	902EA3B0129666178EF13C5B504DC4997B6B256BFEB2B3294BC43841CEDF5E0B57D90C2A3C8A13D813A3DADA36D9CB153FD88502CCA3CBC29DA0287EFAF3089
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250458496586823","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\13f18794-7164-4700-be87-b9da15fd8ee6.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7451052b-e8bd-46fd-b306-473b9332d20b.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):	5402
Entropy (8bit):	5.170765700947694
Encrypted:	false
SSDEEP:	96:nSCLbdiN1uJ+7Xx9IVGKHk0JCKL8EvkI1HXbOElVuHn:nSCLIN1++7h9I7P4KhvkI5c
MD5:	3653465877ED98D67E2A45F2EE7C81F6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7451052b-e8bd-46fd-b306-473b9332d20b.tmp	
SHA1:	C50A171839057A153E736B0EF93DE7C8867CDD2C
SHA-256:	0F4A76F398018D5AE94B179162BBEB10A108B84060B5A317FC4D17A303C41DD6
SHA-512:	0330EC1AF8975F741867BF5C1EB69E1F8D246C4BDB43E4A648C4462EB424102CBB71FD4C89DA590D85D6393B0C6B36E2B1E41F9D3400E9CA81650F8161E5169
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250458496586823","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"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}},"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","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9e7b714b-9213-4edb-837c-bff706fa3709.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):	21282
Entropy (8bit):	5.552951464505231
Encrypted:	false
SSDEEP:	384:f9iVtO8LlGgp0Xrb1kXqKf/pUZNCgVLH2HfDTyrUBa1HGugknZ4sqG0+4F:fQ+8LlGqmrb1kXqKf/pUZNCgVLH2Hfvn
MD5:	B600B746AB0AEFFA16F543F31A6AE9C6
SHA1:	BA2690BBAC745AE8436BC41096D73271F52E9778
SHA-256:	F5A0313571276DFB3BAE3D424A8742D59A982D10336073998E200C2E6DDD5D1D
SHA-512:	F9368939A7B35273DAA4296D35F01EF8BBC04D94ADFD65F7E96078CCE9AC6CBDA4970C3CBD8DAFC6B5817E0DD6D4F85A652E63BE62D2375323933E2332844E E2
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":"13250458496324826","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.171309731270786
Encrypted:	false
SSDEEP:	6:WL+q2Pwkn23iKKdK9RXXTZIFUtwzoZmwyzZiVkwOwkn23iKKdK9RXX5LJ:Y+vYf5Kk7XT2FUtwc/yYV5Jf5Kk7XVJ
MD5:	E032E12A864E7B0B57F3536DC7A4CFFD
SHA1:	C35E2F8FDE71796BA4AD44BF772BB1B85EF50D64
SHA-256:	53892D135379A09F39EFDF216265E307C99EA74A4A84BC93B636D46F7C915710
SHA-512:	33D3606B60725F896BD7754CB188DA597AE886300217BDC68D9A06A37B354A35C7F12972980CFFE4AEB2153527BB709FD63FDFA8048761250D17319FED218A99
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:05.034 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/21-19:55:05.035 1adc Recovering log #3.2020/11/21-19:55:05.040 1adc 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):	5.158000463094086
Encrypted:	false
SSDEEP:	6:lF+q2Pwkn23iKKdKyDZIFUtwzRXZmwyzBDiVkwOwkn23iKKdKyJLJ:7+vYf5Kk02FUtw9X/y9GV5Jf5KkWJ
MD5:	7B258E6B2DC5AFA19762E48A1AE52205
SHA1:	8947857411269F03F0F14FFE8CAFA3B14F251F69
SHA-256:	67C3E3FB85BA7121C2F98C672132D1175EEA6F0A01EBBDD24A6445ED14F2456F
SHA-512:	D2F39BAC61259072D9E86ECC2B884807BF1C6E7EE83D9577A480A1F3D96E3360A549634692A50CD70A68CC68FE85D6D492B317EB4671D9704C4CCBD71943ED A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:04.993 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/21-19:55:05.003 1adc Recovering log #3.2020/11/21-19:55:05.004 1adc 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):	5.459785335804086
Encrypted:	false
SSDEEP:	6:ms7lPYGLAAmrDXdLTArRCVNvgvwN0qCm4ZK6t:Bh4tnArRCPvB0q9A
MD5:	F7FD1F0A163E69AA4AFBE628457ACDEE
SHA1:	E2C09CAFFF600BF17C0F38277C9AF5A9D6F779C8
SHA-256:	A48D2856ECCD180436D97FA566A1E2FF45993371A70E091A35CCE71B2E335F22
SHA-512:	D5898286AF3E833E9DA1E0D03B42C2F9C902B867C31C9C18F34CEC21957B348B0AEF9620D756A221FF99C6C26D9350A52BB2E6E0DA2F418B9E806569C32E140
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...6....._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://canva.com/M...8./....._8...Z...b.N[.9.n._.g..R_..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4cbfe86bb692371e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.656928047697876
Encrypted:	false
SSDEEP:	6:mO6Yk+TymRL9ZxGIHCg8Ge8MkH4IthK6t:/G+TymZ9ZxGeCVGenG
MD5:	27560E195C931469EED19C1FBAFDBA84
SHA1:	03035534C3C4746C08012A660945AF094143850E
SHA-256:	F3E86335D871EFCA6C6A7FD6FC6F841A69AD6D64D462D3EA2F9D98C84D2355F8
SHA-512:	D3BFAA0017A5205D58D3B54C1F035D20700FCAA72A0B7921268010EE0566BF768FEDC823415B1C2778CBE07194084AC069C084765F6675B8F409D9BC485B37F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....e....._keyhttps://static.canva.com/web/b144f4025476bd90a66e5378b1d15df650125aed.strings.js .https://canva.com/$2..8./.....H.....g..qi...-I-.....7.vD!.]....._..A..Eo.....l.S.....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):	5.48514269966848
Encrypted:	false
SSDEEP:	6:mekYk+TZEaoUGpr6HidXgUxscVhP44K6t:70+TCpr6CdXrFVT
MD5:	DFB99F2C2564B6D96B57BC7588CDB8E0
SHA1:	3D5DCEBC4ADC8C67DA7165B2774CE06269512F74
SHA-256:	9BC74742D4F9071D39A8D114BBA7ABCA436F79254F01462D6A31449059FEB898
SHA-512:	24E13BBFACCD9C2CA3D0E439A8CB4CBB352F94FA7A90D8E128A928AB226344A2223CA95A2B00BE5604A3BC3A93FF693A99AA35BA699F43BB5B8301F363BF6815
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...."/v...._keyhttps://static.canva.com/web/169aab431c6d134d2e5b.2.js .https://canva.com/q3..8./.....YO....etn..._.. .9.....&)...A..Eo.....M.6.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e83b9cfa3f81ad1_0	
Entropy (8bit):	5.4799237504642475
Encrypted:	false
SSDEEP:	6:msRXXY+PW/ULMdaN1myvFlHgsCVothNhK6t:BhArU8yvFlHDF7
MD5:	EC823936C1F05EBE8213DD562D9E3CF6
SHA1:	2940E77E492A09BB1AF3A577076AB4DA865E8B06
SHA-256:	170E2D6F6B7A5D05D8529EBC59D1AB093FD91E4F584A58BF0A44495570375347
SHA-512:	2E6B68B52DFA7EB6D22A637234299BB959886AFCEF9B0BF14A9F90D027171DC0E460ADAB133345DA709456CECEEF2D76AE02981CDD1F03434FE6C36C946793 7
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/.1..8./.....\C*...2hK.....>..I.B.....g....A..Eo.....M.n.....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):	5.470238351323452
Encrypted:	false
SSDEEP:	3:m+lwRXa8RzYrSLLiMZJXMLHbJRCLTEmFMH/lHCwl8iVXHRh0IGZmup1lpK5kt:m3hXYGL+MHMBNmF8gwl8iVXDh8K6t
MD5:	8AF361D3B25AD7F0778BF5B203CEA729
SHA1:	8F72C3080839942B3D82C52DF37AF152B9D56DE7
SHA-256:	50AB8CDBA7E3209C17E3BA4B2D1E457752269754D7DBA74D116DBFA9B895FCB0
SHA-512:	A08FD72C6B48B40A9208BCE6C79EF3205D6ACA6D27B0165DF94014286F76389BB3E0C8983B3272F8E0AE3CA07C5A588089CA7517C96338E47D780237A58FBCD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....1.,...._keyhttps://www.google-analytics.com/plugins/ua/ec.js .https://canva.com/1...8./.....H5.0..~.E..z`.@...{Q.~....q/.N..A..Eo.....X.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f6bd7aed19fc99b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	743
Entropy (8bit):	5.922303433014594
Encrypted:	false
SSDEEP:	12:jB4tnAAdLoKsht3plHux2pHgyyN31ABurf1IpdpbI8mWNjSNfbQiEsaR8idniZ7q:uSAdLoKsht3plHuyAyyNloYy/5H8ZEs8
MD5:	3DF5764DA4E003F927FE3DE0D39A4590
SHA1:	D3E8D72898EE8BCE60C3095EB69847E968738227
SHA-256:	81458BF973A68153EB0B1050398B21A6D8EE0D94C4E1279A5F2493F2ABD0BCED
SHA-512:	3DEDFDEBB3AE996FC8C309B0AAF1612275D75E784B5B4CB084FEFFD1E645524F2043F7DF04B747F791B23D0A9A88413F2A63BE95602B536005DC196CA2A5F9D F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....*.-...._keyhttps://www.googleadservices.com/pagead/conversion/804757079/?random=1605984900626&cv=9&fst=1605984900626&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=60&u_java=f alse&u_nplug=3&u_nmime=4&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.canva.com%2Fdesign%2FDAEOEcu9Gnc%2FC6LvqPRfMOYoF6OWlu 9bVg%2Fview%3Futm_content%3DDAEOEcu9Gnc%26utm_campaign%3Ddesignshare%26utm_medium%3Dlink%26utm_source%3Dsharebutton&tiba=AZTEC%20E NGINEERING&hn=www.googleadservices.com&bttype=purchase&async=1&rfmt=3&fmt=4 .https://canva.com/.'..8./.....4.....AF.p.&...5.d.}..C.5..V.E*.s.G..A..Eo..... .....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):	5.580719662221967
Encrypted:	false
SSDEEP:	3:m+lKkqOA8RzYkwLTLTi5tTBYHGhD5djLoCLTEzNt/lHCR/lBcQzBgFFoYrBzWgl/:m+nYk+TTU7ebg7qQS3oYtagWnnhK6t
MD5:	C914B12730F4B925B5B2A9DF66D556A5
SHA1:	F1C9C61A89E3CFBB47D87138D14F0E4BB701D351
SHA-256:	495CC9F649B3DDA6D7F93C2F5EF87F917CBAFCD579300CCADC2278D931D4B22E
SHA-512:	23E0996C3C3ADBEECCB08F9B7FA28C2EF161E20AAD2049FE059E74D9F9C68A79C3D5FA8157822D4EC00A8CEBE23F756D95C8EA94D331EB7BB2D8C471BFEE F28

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b21148925dccb19e_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....7...._keyhttps://static.canva.com/web/36db7dd680be1e933b01f9539cc51480.2.js .https://canva.com/.+..8./.....A.....,....8..E.$.M.....h.|AQ....A..Eo. .....6.!.....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):	5.573110573983996
Encrypted:	false
SSDEEP:	6:mvYk+Tndfcs2WWoSNLXgAllll4Az4gZK6t:G+T1cs2WWoSNrtbPv
MD5:	EC71016FCD7624627B737B7355AB2823
SHA1:	F20182C2121405E3367607DFB2E5A984DA913EF6
SHA-256:	DCD56D38B24ED396476662E52C05AB51645F63702EF3A68D584A4B8ACF6E3534
SHA-512:	3B833E1B99EACDFCDF59B963667C133AE2D8BCA3FD72A1C2E7985A561BC58401D06D3463BEFF714DF327A500F94832FA7A39241A1B536AE3C8FBECA0995C09 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...X.0...._keyhttps://static.canva.com/web/3ad8884d65b676ef0625a45577e2cc20.2.js .https://canva.com/U_..8./.....n...n...QF...0..:.`x.ZQ....A..Eo..... .$3b.....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):	5.568419148720404
Encrypted:	false
SSDEEP:	6:m9Yk+TU0b3W7CPsgva/EiMFXaPkAtZK6t:Y+Tj+CPsz/IyHT
MD5:	A2A29E89DBE83FBB95FB5253AC1FBCFF
SHA1:	63AC49F63FBB0E4C30C321429B5FBFF9CBBE65FA
SHA-256:	08FDD3AFD505732151A1BFDBAE97DB3A823A38EC57D3C06FB0CC345886AFA8AB
SHA-512:	BA337F0B70C87E6458B448F13B6A826AF88EB13F03384D79062DDFD24FD17EC7EDCB02F0CB5CA39546FAA8D05E56B5113771A9306CD80BB281D1283F25382DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...._i...._keyhttps://static.canva.com/web/a8284a82e57c7d67d5e3.2.js .https://canva.com/.0..8./.....z.V!.,@..j..R.....P.... O....A..Eo.....,}Y.....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):	5.319924942128468
Encrypted:	false
SSDEEP:	3:m+lLX+/la8RzYW147CVRCLTEpiH/lHCL/xf15EuKax04mK47l//pK5kt:mvXYW+wNsgLb5ka6K4JhK6t
MD5:	3C2D3E96EF5D150E865ED51D33DA871C
SHA1:	E4124C20326416696EC91D8B3B0BABA414CC4DDF
SHA-256:	50D8ED7A67F4C1D1837A0C195FD56AFF40405E074215620D75DE6434D199610A
SHA-512:	6F43A1BE88FD5B9CA22F7EF19C0270E36E48380561A764384D646A9A3F004B83DC3BB055D36886904E246EC7AA828FE2936036C6C5FFB9E2214E1CAE099E6CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3...x.5/...._keyhttps://bat.bing.com/bat.js .https://canva.com/>&..8./.....m.....T.F..6Q..'s:....m6.7.M.... .o...A..Eo.....0.....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):	5.378393248661601
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3d256598d5af694_0	
SSDEEP:	6:mCllVYGL+MIwJJ8sngd6gUNn/M+425/ZK6t:flwv8cdgwM+9T
MD5:	470A2B19FF83D1EF45DDE9ABD0CA7A00
SHA1:	090448F658F9ED276295A15BB99963149A766804
SHA-256:	98F5DB774F16FB9B2171124BFDDED6E579E9B4DC793A7652FA772AB748896E87
SHA-512:	8BEEC47A4649D38D34386EC5E6BBF859B5F90B27230A0EC1EC23B2603F2F68388650B0FAA4CD7725D40C675899DA4A31CCA5CEECC8A33C34A248816EE929043
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...].t....._keyhttps://www.google-analytics.com/analytics.js .https://canva.com/p...8./.....(.....-.B.....l,e..c....A..Eo.....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):	5.460172799063119
Encrypted:	false
SSDEEP:	3:m+lQNwlA8RzYkwLTLTikBGKE4xcKQVL/uFvDCLTE0MKt/lHCeh/HqpzG1P1yNm2X:mQXYk+TFs4BqC0Rgeh/KdG1NvQK6t
MD5:	BAE81DF2B0A366F9A98A4E772CDA1719
SHA1:	C9B59BCF7E1D0895256F1662E1CE4C00CF13D4B4
SHA-256:	E445DF83232460664FB2F9AF16F062E427D535EEF2C08BA03FE29FE551E760F9
SHA-512:	BEF6B47AA877ACF39B70AC09315386A1E8F71F169D27D9F521831FA567F98C24EA218610204539120E976836EFE1F1907304E1C93836C24582F85ABF4D0D1E21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....\....._keyhttps://static.canva.com/static/lib/sentry/5.15.4.min.js .https://canva.com/....8./.....Q^.....Q.....;.....]XN.J.X.A..Eo.....1.z.....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):	5.421215460804133
Encrypted:	false
SSDEEP:	6:mGGYk+TFs+x8lv8gxlilKFccGYfC5//hK6t:4+Tu++Q8xlKFclF/7
MD5:	FF05183400CFE4634AB3035ECACB903E
SHA1:	F159004A85E0B01434071D1DCE70086E0B138A76
SHA-256:	FCFA2A97CB3EA34EF0F8E1CA9B28C457732CAA25DF4CA7FE96487020EE99CCA0
SHA-512:	4141C2B81C743F20B2D94A91B591FFE10916248E4B8C90247A5FD950B24145FBDCAD011E95BEA31227FAC7D600FB63F8727ADDA0706A3507F338DF4F011C6A0
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/.?..8./.....8m...Ul.....)p...{.w.....A..Eo.....Sg.....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):	5.584669879657908
Encrypted:	false
SSDEEP:	3:m+lejlA8RzYkwLTLTi5lDuBmxm0LXSRCLTEwOt/lHCj/rAEf2rtt9q8TARmwh5vB:mdYk+TjExRXewagjMzt28TAAwK6t
MD5:	B41EBADDD8BF35F607C9A237096B8D86
SHA1:	9E6D1DE903B52300DA997C2D60ABD427A8B74F05
SHA-256:	BAC82A244EFCB51DB91C635E180152013FED1B5E38B08F595E7ABBFBA1E9A0A0
SHA-512:	78AE52973C2D22CBBAF887E8D103B1C4E2FC3EE8654EC06D46236F46B03C4E1B85BCCC56815F16904C5B4672C61D5C10687BDAFD6D8DBABE5A9D3ED40161C0A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...Z....._keyhttps://static.canva.com/web/cb08f5718bdf9fb49247.2.js .https://canva.com/'v..8./.....-._...U.<i..N..=P...-{...[pY6.52.A..Eo.....Cs.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3511df7a5a5c326_0	
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.5430585968219965
Encrypted:	false
SSDEEP:	6:m5Yk+TRK2/aes7WNSJ+HgHaw70NJaZK6t:c+TRK2/al6SJu+a/PaT
MD5:	8118C15B781521D6EFF410A174FC8686
SHA1:	B6B628EEDFDBF40B91E900F9542CDF5E418E01AD
SHA-256:	881BF4B050EE7F1ADB4E045B081ACA2B23ABCF61FFB10686432B07178F942A30
SHA-512:	B9004F9F2A80DC02F402710966CA7F36AB18A6C46A5EBB7425706E5BAC27C2DE7E462028D7F27CD80AC16CD4487C822C001E0036B48DACD5FC60B14A62D50B B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...u.%...._keyhttps://static.canva.com/web/292bbecde0fce6ffe18847a12c9a6dc6.2.runtime.js .https://canva.com/.w..8./.....L.....z....f..t..O.....ly..m kK.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:	3:m+l+iz/a8RzYGEndKIJAL4r0IMHWFvDCLTE1T+1t/lHClll1P71OtNcSRxhm5mRH:m5irXYLIiNrQ64tgvxcNjDk4RDK6t
MD5:	EF6E187FEE0B4627D5C9C4930C960CA3
SHA1:	9A17057DEB87F47C161350534C78C81815C5BEBA
SHA-256:	39DC3495F2BD56759903B2D96EFAD58D2E643956EBAFD75C89397307D778049C
SHA-512:	2C141AF501337512378E9CA3B087398B1652B0C1B53A6C3FAE326FBCF83EDD67F633DCF764B0909E23169F5C5710DC84D91E8E5BF6B092403C679FD4BE04553
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/h...8./.....P.p..._.P..K.HG..(.0M..7..).q...A..Eo.....f.....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):	5.647840711217252
Encrypted:	false
SSDEEP:	6:msB/XYGLSmXZCLRlZpEP9dX1tgyJlihLLWGK6t:DIZpEP/XHLYP
MD5:	5D98312764C5799178E8FBE38D97DFEA
SHA1:	98FD35D1C44D2CE45A1D1F36D825DE4E399FC6B9
SHA-256:	E43080FA5C2ECA2126D977D82AC33915A6D9E600B55D17694CA20B0452BDDA1D
SHA-512:	8638921F8BB6926B8B0A402AFC8F5CDAABC54748880E2C65DB6E6D99C071A285C03D014FBF0A1BBE27B631812DEF4C0BF3DD7CB117F6539837AF9CF2152AA0 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...&..}...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-TZPTKRR&l=dataLayer .https://canva.com/....8./.....m.:.....z)....T....*r4.....A..Eo.. ....?.....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):	5.085545492451736
Encrypted:	false
SSDEEP:	6:utrSvEnzlihZFuHu0FlU11lE0B98ZpoqVqSm8Ptfc2+8FSzcTxzPawAfyDnq9n:0SG5HtlU11r8FPPRcn85ZXUys
MD5:	8F855F3E422DC98AA834A4345A0E0F1E
SHA1:	2A964D99D500A5CA72EFEA554D2ADA88B76377DD
SHA-256:	C4433738976D9E0E1ECE21A885AEA3B6B998A01CD56B77E86ECDA22418C35699
SHA-512:	569D770B7BE813EAF047121CB903B87B7073B36D83F8F57DDA9C7CA40174B20B22540D3E50A5E81EC803481480963CC2DCFA52AEE813EEC55AA459D42E352BE 5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Malicious:	false
Reputation:	low
Preview:	......2Doy retne.....2.....k.....8./.....o..-.&g....8./.....^....8./.....Z.YV.....8./.....R..'....8./.....,..V.....8./.....cb..H.....8./.....t...,[.....8./.....@q ..U.i.....8./.....].H.....8./.....J..".F.V....8./.....1[.>.....8./.....G.....8./.....jKs.F.....8./.....&....Q....8./.....7..k.L....8./.....h.....8./.....^}.Np....4&../... .....-..0..x..4&../.....3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....8./.

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):	3.3439693878468786
Encrypted:	false
SSDEEP:	192:zuroSvVv9Mu16BAgAeLAtmfMIL56hPKJLy2+LDBSDN83e1:cHdm+6BAgAuAIL5YPKJLy2+LdhO1
MD5:	E430AE175EFE80BA6E1DAD51C1D3B741
SHA1:	F00BD2D0A370AE3A878BDD7641DA182EE428AF0F
SHA-256:	47B533AA632F5DAD196A460C38267970732CDC637D858E3CF5B776009741FC63
SHA-512:	1E9FE5326D009E993182FABE34355E2A15F5D93222DC7672B8A28D1094F2344AD0335ED74480305FCBAA8C8A3068846BB1CE25C730748B987FBBD3CB167A6293
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):	0.9727537247575553
Encrypted:	false
SSDEEP:	24:he9H6pf1H1oNjqLbJLbXaFpEO5bNmISHn06UwK8:hbfvoNjq5LLOpEO5J/Kn7U18
MD5:	4FA06C5A1E42DE88E78D19E570485A55
SHA1:	FC00125BE4C52BB01BBA46DC65EA7A57D4D6BBF2
SHA-256:	0561E2FE1FC1F0410B66C6616E5B5FC2D17EF7FD0BE845F3B013E1D80757AA53
SHA-512:	34B48F8E029B7E9B61905B7B587F76C5CB98B7F036CFE829B7990AB6DA959A544A1D8EFB4063847493F55E623F0F4A350A5A4DF2B3E80BEBE58A8B37E2BB5456
Malicious:	false
Reputation:	low
Preview:	.....Y..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8543
Entropy (8bit):	3.78754557069839
Encrypted:	false
SSDEEP:	96:34j+Yws6HxSxvQQHhsxJhsx2yfvQQHhsxJhsxzvQQHhsxJhsxMahvQQHhsxJhsxt:3cveS52Yhn2YD2YM62YDn2YN+y
MD5:	6315498C76D66A35EECA5A3F2C8892F4
SHA1:	3963C268D401DDF3503D5D8775A03485A14580BF
SHA-256:	7BB5A41E9DBA1C347547701CFC6F1067BBB786081503B8F4E474D77DA8545BDF
SHA-512:	72E6CD90D82F4505C90D0FDC0964B472A25CD115BAEE3F46A980B8C8601EEA80C22B210B3ECDD0B7F9EA4C260F76C35C4735BF113289A54B43AFF8A3952E828
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...19ac6058_7953_472c_ab0a_329ed75e6b61.....5..0.....&... {730C75E3-B87A-4292-818B-DC8F984D08AE}.....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..... ..`.....4k.....4k.....@.....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):	320
Entropy (8bit):	5.143214240145558
Encrypted:	false
SSDEEP:	6:U0Aq2Pwkn23iKKdK8aPrqIFUtwxeZmwyxSFjkwOwkn23iKKdK8amLJ:U0AvYf5KkL3FUtwxe/yxSFj5Jf5KkQJ
MD5:	A6F19D87A9FECD74BECD85527B2AA15A
SHA1:	B2558F22DB4B9B72C8DF48C1D964FDCBCE624DD2
SHA-256:	F8A38B6E1F0BA9244F8BB75AB29A0EE899A5DEDFC846C33F35C3E3A1A0ADFF65
SHA-512:	51A48E52E6213D36F80BD3E429DE168725706A4F8352D6F17E0BE08A978D2B738482F8B7B89D11109D2590ED88C4F517A2A1C7FDBC86B870B184DB204404EE85
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:05.227 1b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/21-19:55:05.229 1b50 Recovering log #3.2020/11/21-19:55:05.230 1b50 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	C92EABB217D45C77F8D52725AD3758F0
SHA1:	43B422AC002BB445E2E9B2C27D74C27CD70C9975
SHA-256:	388C5C95F0F54F32B499C03A37AABFA5E0A31030EC70D0956A239942544B0EEA
SHA-512:	DFD5D1C614F0EBFF97F354DFC23266655C336B9B7112781D7579057814B4503D4B63AB1263258BDA3358E5EE9457429C1A2451B22261A1F1E2D8657F31240D3C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.231082936424725
Encrypted:	false
SSDEEP:	6:Qft6Vq2Pwkn23iKKdK8NIFUtwffhgZmwyffraIkwOwkn23iKKdK8+eLJ:KwVvYf5KkpFUtw3hg/y3raI5Jf5KkqJ
MD5:	65C30C27720A26DBA28D3112F13505B6
SHA1:	41DA63D4B6111631327539477FF9A67C1A99CA34
SHA-256:	9032CB7A84AD1B776329E4E5FEE8A6F3B2BBADC05B6304C8B04962FA5FD0822C
SHA-512:	DBC01E28FAB4ABD3E090831D94D733010D133D4813713DB37F534A0141B38B84208F7DD4F5C05A1C2DCEC788A347E608EC0764787EB738CE3B3CCBBD3FEF5E 1
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:58.626 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/21-1 9:54:58.627 1b00 Recovering log #3.2020/11/21-19:54:58.628 1b00 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:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49 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:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	22528
Entropy (8bit):	2.0413358500835925
Encrypted:	false
SSDEEP:	48:XBmw6fUfB18vw/1Z8o8wBj1wdrlRCOCoN0hRdslhWntdwLXKvkj7T9:XBCIByvw/XdZjGGBhiktdwwkfT9
MD5:	7944315521DF9A96E8F5B64E1F33F4DA
SHA1:	4439C37F332B686E97BAC25B389D409668637B25
SHA-256:	1A1674291274E85E76153A5D012464B558BD561D8F13853A2BA89D9CABB7F76E
SHA-512:	8D27504286AC383C13F115990EB2762E39C2E1E475F084C70BF94046257BF265553C113092400AFB0399CEDA28A3200EBD693E67EA253CEA057A0A75E4C7A2DF
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):	19028
Entropy (8bit):	0.7389446558611819
Encrypted:	false
SSDEEP:	24:77xlldyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwQCP5QE52:JdCBmw6fUSh2
MD5:	AB7DF371E565C59F5D7D22EFC7E400F5
SHA1:	AEA1494CBD916BACA47A32809314EE1FEAAA8FEE
SHA-256:	3AE26FD7DE82C4059AA76C456913A93B8B3F78F32E1C3831DD65215D1BE02CB8
SHA-512:	93B6005430DE47795E03204EC1EFA3519956A16E5E8C23727B060FB17FD32BB776A7F1824EF39B69037D4ECA0BDD178931222CF9A0421AED007E48A5A9DD681D
Malicious:	false
Reputation:	low
Preview:	.....\tp..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.268435071513805
Encrypted:	false
SSDEEP:	6:lMo+q2Pwkn23iKKdK25+Xqx8chI+IFUtwkWcZmwykAG3VkwOwkn23iKKdK25+Xqp:ao+vYf5KkTXfchI3FUtwU/yO3V5Jf5KN
MD5:	D92B59A1A462AA733DD785538834BE93
SHA1:	51F635E88D7077EFDCACB9041335D3909B4B6995
SHA-256:	85B447D8C030C613584D27A9AE6F252820CCBA5976B896BD1B52452B49A5677E
SHA-512:	4395FE69053A847E409CB0E92E2D81CCCD921FA2101568BD37F7FC0D904F639566D2C1B4EB1DF6D160AF48498B0A4CD7C06B34C5DF995FE176DC831955EE3B4
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:04.878 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/21-19:55:04.885 1adc Recovering log #3.2020/11/21-19:55:04.887 1adc 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):	5.229870819917153
Encrypted:	false
SSDEEP:	6:laG3+q2Pwkn23iKKdK25+XuoIFUtwk8Zmwyk7EcVkwOwkn23iKKdK25+XuxWLJ:v+vYf5KkTXYFUtw9/ydcV5Jf5KkTXHJ
MD5:	D1F99F2BB33043816DD7135ABC10B67B
SHA1:	D3EA8AEE8DEE92CFC01879DDB5E79EF39AADBCD6
SHA-256:	7AE516F18621A9F48111FD58D3F9244B3A322DEFB11A3114C5FB3FA29D41A0E6
SHA-512:	EAF33C11D7FB19B97645820E725D2B860F4A2ED3BF48049EB957755BDC7A68C1E88B1390754809EFEFD2DC9FC403C2EF4221D70C5E61B91D751B0488905D91C
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:04.845 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/21-19:55:04.846 1adc Recovering log #3.2020/11/21-19:55:04.847 1adc 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):	5.226210103241379
Encrypted:	false
SSDEEP:	6:lE+q2Pwkn23iKKdKWT5g1IdqIFUtwkYYZmwykYoVkwOwkn23iKKdKWT5g1l3ULJ:a+vYf5Kkg5gSRFUtwbY/yboV5Jf5Kkgk
MD5:	C247C4E74A7AE9FE49644972E4BCFC88
SHA1:	E23E3C42665529FE4C94C38D2482DB610C335E63
SHA-256:	DEAAFAC52D69D09C52F54CD8CC9B129EE90313F3CAB8D48C74AD66CD9610AFD3
SHA-512:	81B389C28AD1CAACDC06CAAC6F64A58F8D8F1A32050FFA8B42EF4472334C93661592F669BF803B4FD3E5CFFC126D938EF954FA5828A456926C68A6980F05665
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:04.828 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/21-19:55:04.830 1adc Recovering log #3.2020/11/21-19:55:04.830 1adc 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):	0.19748670680235086
Encrypted:	false
SSDEEP:	12:TL+A/WMfY9XWkmtNYy9s7M/C1joNuQ6dxWGI/BCbNVd9XWkmtNYy9sL:TLxWT9mHuOs7M/Wjsuhdx9bND9mHuOsL
MD5:	90D579147BA560FDEBF489214663F8E9
SHA1:	08FFA0B0D30C02A79C99AA82FB44F485742E71C3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA-256:	4B69F05CE6624EB05AB713C3ACF65423C496D246A2FC957A06F77C293744686A
SHA-512:	75A4E0FE98C7C92CC50BAB66A1EFAB957E1C5CC4BABC0766279D0A44FCFE22582851CAEFFC7DECF5E6515E444B78A3F492205104F29463571B9C87546EAB1C92
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1171
Entropy (8bit):	5.597298810729724
Encrypted:	false
SSDEEP:	24:Kx5H8NFTseyxvDLxNeSsVs3aPrr7WXU1SNoX1DY78BJgskfa9yBDOxo7nQBrxzG2:KP7rxvDLp3aPrroNmU8JFGf1nHz4L
MD5:	6B8039B8C980DA2265F7D0442B61ED4B
SHA1:	A66737FBEFD42ED053CE240ACDB0F76E32C8D257
SHA-256:	80EF0401D1B18F9301B51243B47ABCF140D0D4CC2DDD1C858135ADADF370EB67
SHA-512:	D608A2EE2E93EB8704AA57CE0B9DAE68E5C4B213873151CEBC2ED6182BD93799CF447C257C7D916010F90B4D5D12D30D321EA49FD3591800FA6DBEB548FB1D38
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):	0.11636997099821819
Encrypted:	false
SSDEEP:	12:LsaTkBDTwRfJmRqLBj/p3l84nMWQASjG9LjZBQZ8fOP:JMqLBp37f1NjZTfK
MD5:	3FD7571F20C29E41D4DB6D852F0D4843
SHA1:	C84E77D6D87E3A3E0FEBC7714BB3F4F4CDCFE8F1
SHA-256:	06A4CC2347A464BA5B8E1C1591EC72660E750422DFA1FF013B8447F5C9714007
SHA-512:	7F853EC2274733EFFAC5CCE654F6080449494C9338D351DB68A8AE74FAA0F4230648FCD5EBD69D2B0687B75A4168D64270B86DAB86DF03E26D8DCFE49BA547A4
Malicious:	false
Reputation:	low
Preview:	.....;uC..... ....

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
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb\000001.dbtmp	
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):	4.06381637451596
Encrypted:	false
SSDEEP:	96:zlTv4TcpX6zFE405PNUaxAfaKWpN1dO4RpJ2O:ZTCCUQAfdWpFRpQO
MD5:	14164B3B685D4DC67E14CA65C053C01B
SHA1:	0831FF6B4229220F941EDAFAB17BEC3B4E0A56C4
SHA-256:	430A632362A99BCD3C5E5558CF79F0DFBB1FED4FBF04E24C39F09B82B2581D83
SHA-512:	C6EFB0964B0D54F639E7FD63E62A963ED6C020D0FD04A6557B7C0747237B64FECC9CD17BCB70107A10DC8D954727C67071108D65BFE789E1079AB3DAAF9EF2A
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. .I.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. ....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):	173
Entropy (8bit):	5.353814790038526
Encrypted:	false
SSDEEP:	3:tVP9Fd3idevwDKKqFkPt+kiE2J5iKKKc64E/x14kfSbTihO/IrscWIV//Uv:h+dVq2Pwkn23iKKdKEqSZVIFUv
MD5:	5CADD316C96DED0EE2BFD00B31C2A475
SHA1:	9512FACBB8108E5A7F44155FBAC829BC5BE7E98A
SHA-256:	F19D8BB35E09913CEEF972291D0BD36D014D7AE446CBF047F5B91823048B070F
SHA-512:	9326E14E91A4B96FEF2251A6F3DB503C769F4DB1BB11B7A60C9F9E008E8714BFB0883AFD767E9A1A40BEEDD2874D615287F099A0C9DAF124F8DB3381F2D500F5
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:00.384 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.canva.com_0.indexeddb.leveldb/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
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):	32220
Entropy (8bit):	4.068082203765116
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
SSDEEP:	384:CF/CtEKyrfYigUgvjWyjX10kUEQ/F51QHyajbij:BtEKyreWyjX10kUlQbHI
MD5:	0D3139BF6DCF7E74CDC599D9464DDF68
SHA1:	F6715D2610ACDB04F5348B79E4313F8293961316
SHA-256:	77AB8035BD5C49E8A0D42E376F3C36056008E04A3F99B2D2687988854D4BA033
SHA-512:	345D3E18726003602A0B35F4F4B3F268E0AC5742063F05F325F3809A24241626E832B7ADA3D287BE844544C3925DE4DA3AE2E73CAC67C6F67D4F66E5216B5F56
Malicious:	false
Reputation:	low
Preview:	.!T|.l.*.....META:https://www.canva.com....._https://www.canva.com.._uetsid!.0ea5b5602c2b11ebb164fd0a9cd0fd05.#_https://www.canva.com.._uetsid_exp..Sun, 22 Nov 2020 18:55:00 GMT.._https://www.canva.com.._uetvid!.0ea6ad802c2b11ebae6bad0465c7ceb1.#_https://www.canva.com.._uetvid_exp..Tue, 08 Dec 2020 00:55:00 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-gb","time_zone":"Europe/Berlin","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://www.canv

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.227825184767781
Encrypted:	false
SSDEEP:	6:QfYR39+q2Pwkn23iKKdK8a2jMGIFUtwffSNJZmwyffHV39VkwOwkn23iKKdK8a23:KYyvYf5Kk8EFUtw3S/y31z5Jf5Kk8bJ
MD5:	75B31E4C74806C90B72CCD39F2F140F2
SHA1:	93D4C01F261F34ACA5E70F4976F3C0D56D0EBACB
SHA-256:	D60BA620D62DB3A06E70A689848C5D9C80753DE28037E42021E18676EC7BDBB3
SHA-512:	881F4B47F10B6961F9F1DBFDBD68536879072D185FB605F087FFCC73E4721752AA468CEA0FBE4EEAD1CB0490602CC1994F1259D7AD7D70686B8B7EC0C04401C
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.352 1ad8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:54:56.354 1ad8 Recovering log #3.2020/11/21-19:54:56.357 1ad8 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):	334
Entropy (8bit):	5.206112817362495
Encrypted:	false
SSDEEP:	6:QficVq2Pwkn23iKKdKgXz4rRIFUtwffiNgZmwyffieIkwOwkn23iKKdKgXz4q8LJ:KicVvYf5KkgXiuFUtw3iNg/y3ieI5JfR
MD5:	8DDD44CBC99FA154F3774238003F0368
SHA1:	DE842022EADC865A74C173478FC9ED5FFC8036F6
SHA-256:	0D0737F8F61756EA36BEA8EA258BEC95ABEBA8708302D0FB38089EC2B8CBF81E
SHA-512:	F64ADAAC433120462225B2A872567C4BB9F21679AC9A514F5FD40924936AC7389DFA89DD3623AD89D1EF8B3035BDA6D46E6757A049BF35680CEA2A1DAED97BB
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.650 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2020/11/21-19:54:56.651 1b00 Recovering log #3.2020/11/21-19:54:56.652 1b00 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):	0.4792709645536453
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4pZV:a96EJTv4sXK96EJTv4PV
MD5:	AF331B37541997223B8A5380506D5144
SHA1:	3EF0D7D747EB456235FDB417D7D8F19FCE70F82C
SHA-256:	E9C37BD386EFBA2225C3945CA10F8D80F6CA69F864392EFBC81128C5A573026F
SHA-512:	5CA02541F14308721695126F1F56087331E12F7E08B8CA91D3A1C4477EECA09FC405060155BC3220122508AA5D532AB1CF0FFDFD7D0DF6DFDAA6846BE5A76D4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
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):	0.6551707283962162
Encrypted:	false
SSDEEP:	48:NMko/QqzLbCIG+6bDdsDaKgJgKtHIm50I9a+UW5:NC/QsCIG+6bDdsDaBJvtHIm50I4K
MD5:	A670D0DBDE9B402E76F364B621809417
SHA1:	9278711985B4531434476636E85910FAC7ECCF8C
SHA-256:	17E5E95D6DF932064978FC5C77876738F307900DDD81C58C5F134B2F6DB765DC
SHA-512:	41271EF5A98A7AB92A825A70BB87729A6D01BB49E18DD974EFC3C0138A862C66B42940712673B09966BBB05E509B37A1CFCE495D80E5206A690468C0F99769A0
Malicious:	false
Reputation:	low
Preview:	.....\..... .....c.....z

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):	1.6524930467877832
Encrypted:	false
SSDEEP:	96:wIElwQF8mpcSAuciHCEaoI4nAaoImX85Q:wIElwQF8mpcSAucIxanyAanmXKQ
MD5:	D457C32BBCEB3F869D2A6F5C61050BCB
SHA1:	F32CF74BA7040AFF882795A89EE5B549BFA77B7F
SHA-256:	36961E9A53B1E53D98897323ABBECF8B1A80715C81BC8A7E97090EEE0F3FA35E
SHA-512:	045DC49B93CB6AB67D70D4C04819E1C6DFAC63958513D2A9F831629E3195BEAF8122051E725E6077A2C7B3AD1571630D7275B379204E7A9DB41D0E32E7EB50D
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):	0.6278969138196809
Encrypted:	false
SSDEEP:	48:ZsqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUW4:ZshIElwQF8mpcS9
MD5:	772FF81058A8B3632A663E6807A8A14F
SHA1:	8CFFB28B0511EB3A6D9ED4600C71D5A33BF7B22A
SHA-256:	E9C43080C8F13CD5E90322C03A0B628814CBB831F30DD3D0A71655972B8ADA44
SHA-512:	365FEA972719F7A91CF1F6A19258EEBB50EE12E1E4006D5B2B0655AFDBE5D5BA9A106C9A3D8671331EDD78A163D41CAF0450512D478F154FF0BA3BC24299AD7 8
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:5ljljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.208201114245301
Encrypted:	false
SSDEEP:	6:QfZN9+q2Pwkn23iKKdKrQMxIFUtwffy9JZmwyff1AN9VkwOwkn23iKKdKrQMFLJ:KZOvYf5KkCFUtw36/y31s5Jf5KktJ
MD5:	70598DE7ADFAF5006A0419927658EF0F
SHA1:	7CD291C5C4AA41110FD82DBD8BF2AC73B5000E3B
SHA-256:	D5C1C676F1A24CAF754B780D9D9BD6BDC3DFD9C3AE1EA88AA4B81319E6C3DE4B
SHA-512:	26522B74C78B3FCCBAB523AFC49C093629FB2CA1570F5E29E813FEDCEAA29CD690B859B4B91B6615E9A1B5358FBC4EF32CC63545B0D193EFB74CF05DF9B0AE 15
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.538 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2020/11/21-1 9:54:56.539 1b08 Recovering log #3.2020/11/21-19:54:56.540 1b08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.181523537628372
Encrypted:	false
SSDEEP:	6:Qfu39+q2Pwkn23iKKdK7Uh2ghZIFUtwffNdJZmwyffoF39VkwOwkn23iKKdK7Uh9:KnvYf5KkIhHh2FUtw3Nn/y3oF5Jf5Kks
MD5:	0C7D8B27321D1E9399C63724822D5F12
SHA1:	2F7904945F28EAB51508F2B82E125DFB4F40A7A1
SHA-256:	EA28C4C6069BA72F8F55C2A4FA4127343456603B34FB6483623DD29143A0A098
SHA-512:	2F715027D0196E57214E421166365D6BDCB1DB29BD1B2DDDBE09EADE37F6AC94374823F5E96E30F1CE7D2A1E19E596EFAC33964094D6E6EFD50057A153C1773 4
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.310 1ad8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2020/11/21-19:54:56.311 1ad8 Recovering log #3.2020/11/21-19:54:56.312 1ad8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.289877843460079
Encrypted:	false
SSDEEP:	6:QfzAN9+q2Pwkn23iKKdKusNpV/2jMGIFUtwffxJZmwyffx9VkwOwkn23iKKdKusO:KkOvYf5KkFFUtw3b/y3x5Jf5KkOJ
MD5:	0ED0911ABAF451FE633B4D12F58D4EC4
SHA1:	39AE670B2C184072A6B8C4DFC82A7DA841587402
SHA-256:	37C8E2AFEE70C3D9B3826162F54016A51FDD48EFB17B761722D226EFB2F0E7B7
SHA-512:	04400DB35E50A6D9E62E46A2C0F96CE808427732465F46EF134FEE46CA4C438A70266DD21145916D3A28AA75D7455A31E60ADFB3859277B22CDB446A7B89ED2
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.546 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:54:56.547 1b08 Recovering log #3.2020/11/21-19:54:56.547 1b08 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.282435384855127
Encrypted:	false
SSDEEP:	12:KiyVvYf5KkmiuFUtw3iB6g/y3iB6l5Jf5Kkm2J:KlYf5KkSggf3oJf5Kkr
MD5:	B5E912D2149B579352C271C29B59C5B4
SHA1:	43BC2C1470BC48FE3B9A3FF7B2D25E5D2DCBCCAA
SHA-256:	49349375CF801F1FBBB144E78F4DDF06866D8EDA0D35679367834CC87BFCEFC5
SHA-512:	AEC1D9396B4AFEA4EA0305C89F0368564209C4ACD2BA1D5675C2E176579EA0DCE8D1BC3CCF51D7D697E51A0068360778EF4C37C1635E5F30E5CB338D3B55BE 24
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.667 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2020/11/21-19:54:56.669 1b00 Recovering log #3.2020/11/21-19:54:56.669 1b00 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Size (bytes):	418
Entropy (8bit):	5.216401763167752
Encrypted:	false
SSDEEP:	6:dSVq2Pwkn23iKKdKusNpZQMxIFUtwAU6gZmwyKHaIkwOwkn23iKKdKusNpZQMFLJ:QVvYf5KkMFUtwAU6g/ycaI5Jf5KkTJ
MD5:	9969DC19A055F0DA5A06A22CCD0BEC64
SHA1:	542CA82EBB32209A0C5E154AA2D70EA321D00AD2
SHA-256:	3CAFAC79703AD82E3A57E0CD7174F975A8C63FFD83B684265B636406925F5FE8
SHA-512:	D6A051EB00C8EC38F39ECCA986D70C98AD5B3248302CBC97C1914EE9323DB87EE2E394935793ED01F75E4F3BA0C27F64AF35FCA828A552F1F4AB5FAE271425(8
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:12.860 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2020/11/21-19:55:12.861 1b00 Recovering log #3.2020/11/21-19:55:12.862 1b00 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\e8d153f1-2252-49dc-be36-ebde0e5a28b9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isol ation":[],"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\2a4dce63-53c8-42f1-bd1f-a68a480ec17f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2 F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isol ation":[],"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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.186569329892306
Encrypted:	false
SSDEEP:	12:UXvYf5KkkGHArBFUtwxSFK/yxr5Jf5KkkGHAryJ:0Yf5KkkGgPgfN/Jf5KkkGga
MD5:	6E524D0A040E60B7D9DE497E003776D6
SHA1:	CEF699CCE43DD387BFDA451679A64A45CEC6F993
SHA-256:	D5AD76E2E9EE7A5C1F20EAA44778207B786609BCFAAEBD2FCF3A01662ECC240F
SHA-512:	04272E34DED0BDA54208977033474C3ABC46577AD6B172A4A584F62D5BF130448C26A2F20D4415CF12F45648E17CDB90F699B651F04E25E3351534E60588D268
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:05.228 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2020/11/21-19:55:05.230 1b40 Recovering log #3.2020/11/21-19:55:05.232 1b40 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.182828892015308
Encrypted:	false
SSDEEP:	12:ru6VvYf5KkkGHArqiuFUtwwg/yhI5Jf5KkkGHArq2J:rlYf5KkkGgCgR8Jf5KkkGg7
MD5:	B8795C48BB8B0F7ADDABA45127E1A7F3
SHA1:	DB04A80D869E1A31165759D3EEA12E8093D80031
SHA-256:	2CD14C1CBF119445051E6154820433D08B51A20056C84E120DF57C1B8A074731
SHA-512:	DFA8A40B7D8295C04C1090A75D1F3B516A7D3743399C10D57A6F3142507B12669ECFB1BB50F21B7AB71CE3C39564494BF3F07DDDF3D591FA87F672BEA307AB4C
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:05.409 1b00 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2020/11/21-19:55:05.410 1b00 Recovering log #3.2020/11/21-19:55:05.411 1b00 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):	418

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.199479393727897
Encrypted:	false
SSDEEP:	12:b7ovYf5KkkGHArAFUtwGz/yGp5Jf5KkkGHArfJ:beYf5KkkGgkg1GG7Jf5KkkGgV
MD5:	E3D8B5354A3F5ABCCB86585FADD4AC25
SHA1:	5A19F69E5ADBFAB55AD874BB84D67327854027A1
SHA-256:	6878786076323C91009273636215A3B257A52760E8CCB9F68AF2932DCF8B4CFC
SHA-512:	1AF0F17528D55A3DF50D379B5B786F4FCF3E90F5B711CD7358BE19314FD4A4CB7F2BCCB23BA2915FE570FC67DA6FD9023669D8E624223E976272CE4DBC6CFB A
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:20.535 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2020/11/21-19:55:20.537 1b08 Recovering log #3.2020/11/21-19:55:20.537 1b08 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.279747798112741
Encrypted:	false
SSDEEP:	6:QfRd9+q2Pwkn23iKKdKpIFUtwffVV3JZmwyffOBN9VkwOwkn23iKKdKa/WLJ:KRevYf5KkmFUtw3VVZ/y345Jf5KkaUJ
MD5:	B83533B6EEDC5B54BEA1A7C2D67E7F7F
SHA1:	E6A73A45CB3C06645E92953320C7555E88610280
SHA-256:	DBDE04043E88F86E35ABA96314FC988C49D4D4C71C9C2A28D5B829B9F1FE7DEF
SHA-512:	45E215EFE081433D21C2708A3745D07B1DE9C902ED298FD474321A9A90953BCCE2806FB7063FEB683B7AE70C2CC4BD5AD53176B215309E9FAABD6E5B5860F70 A
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:54:56.333 1ad8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2020/11/21- 19:54:56.337 1ad8 Recovering log #3.2020/11/21-19:54:56.338 1ad8 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):	402
Entropy (8bit):	5.282729010381734
Encrypted:	false
SSDEEP:	12:n8vYf5KkkOrsFUtwmi/ymO5Jf5KkkOrzJ:nGYf5Kk+gpvmYJf5Kkn
MD5:	80A247FDBE81D4E965CBF1C732C19A19
SHA1:	F084E8B54C3BB716ADADD283130D829DFD0EB8D2
SHA-256:	8FA13C258E139292BB263749548E1544B88305F371E4008E06170BC6DD66B3F2
SHA-512:	63C041ED65B22687B1C71BC8485A91F65A4A81335D21C2A21473C318EE0ECC4FF635F0C5F3AC03AEB1EEC84E823B3082CB2798E5523EB5F89BAE514807FDF3E 8
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Reputation:	low
Preview:	2020/11/21-19:55:06.174 1b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2020/11/21-19:55:06.175 1b50 Recovering log #3.2020/11/21-19:55:06.175 1b50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	2.9182958340544896
Encrypted:	false
SSDEEP:	3:wQOcBg:ccW
MD5:	F6F565AB482950A0DDEC2E59AEE08FF0
SHA1:	59B64E6D5CD466EE93CB513D1E05F5A2BBC4E257
SHA-256:	42ED4CA450D693D8020981F801399B9CA770179CE873FC1BC80BF9C244826E9C
SHA-512:	521D7AF2DD4473EFC8A9D6489961B5BF642B611ACF861B2F46E81BB5E91FFE2EF8A3AA1D5F059C4D7B6188F0F44D29CE79D48AF24D204069EEA6B7D6EBD0E3E8
Malicious:	false
Reputation:	low
Preview:	.....uJs....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c53c27a6-cdb1-47f5-a1aa-c44562c2649d.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):	5047
Entropy (8bit):	5.604487385755322
Encrypted:	false
SSDEEP:	96:2fwj1KXs/yqYq+Umf+URlU4+ieUZieUQUUoUR3U7UBUWUT+KUeFU6PeU3U2UsUjt:2Yj1KXs/yqYq+UJURlU4+ieUnUQUUoUd
MD5:	75C3125B26E7539A6A17060D68D4A3B2
SHA1:	D7F99D0C7436E954E2EC298199CB6FBB9FEA9C7E
SHA-256:	EE64D25DD001ACC0806AC95BEE4A87143A75A25CE0F9E4A92A0B2EBA01BAAB56
SHA-512:	07AC71211916F57E3247A3752129723C75612B813409A8EB3A8EE152E977F6503E800F25C564C85364F6B163C79B5F9D0537770D6BF026DC3C326B269AA6AE5B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1608576900.679521,"expect_ct_observed":1605984900.679521,"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":1606589700.335584,"expect_ct_observed":1605984900.335584,"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":1606589701.529092,"expect_ct_observed":1605984901.529092,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"HIplQqWMs6ZxBLdnO3HzMXf8AYhhbIad/Qg77wu6W6Q=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606589700.275678,"expect_ct_observed":1605984900.275678,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"ThT+U8nQYq+ZrB7qkByu3lLYgUKH+P

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c620d02a-bb2b-4a86-97db-32acab4519b5.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):	21284
Entropy (8bit):	5.5528613644174705
Encrypted:	false
SSDEEP:	384:f9iVtZ8LlGgp0Xrb1kXqKf/pUZNCgVLH2HfDTyrUBa1HG/gknZ4sqNf+4Lz:fQp8LlGqmrb1kXqKf/pUZNCgVLH2HfvE
MD5:	72271E6BBE6C348EF1331F995F6968DA
SHA1:	500CD684C6E873A51E33851E15029DCA9A84DCB3
SHA-256:	BD8E9351279125EE9A4D1EB643B3F8D97FE09B838BC05866384FBF8C8A2B0C9E
SHA-512:	1D0429A879E56B24EF0E7839820922E96BBA425745A03F78C221DF293A34648690C71DC7AE1DB8F55BFA3E9C4F13928644BF490DF9C543123BF65FB83A01FD79
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":"13250458496324826","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cc4c80bb-8921-4ef6-91ae-17d42d6b7a64.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.628707872451545
Encrypted:	false
SSDEEP:	3:tVP9FdzQEa1ZmwvKAFdzZozSV8nAFdzMbkSWGv:lQLZmwykWSVSkCkStv
MD5:	4B8C4B9DA93834F8913D2950C8564FDF
SHA1:	0B8E5AF7289DEBBB1C9E2184414B4A7E806BCFE4
SHA-256:	CBAE456A9E83BC5EF915CE37AC0B72081D78CFE0D816208734E46045B32C7C3F
SHA-512:	3099A31A100B6C43C2A237DE92EDD311F57BACA64E405C150EB7FAD4BEAB82D91BAD45C14F1AFE3810F1A237582130C27F324FB48615FF045A775BEF65A261CB
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:04.567 1adc Recovering log #3.2020/11/21-19:55:04.614 1adc Delete type=0 #3.2020/11/21-19:55:04.637 1adc 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
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
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:Y/lFllxFEG2l/n:6+/l/n
MD5:	4B7F9A03AB53F3EA38FAF15B65A2FA4C
SHA1:	D2C12F21754B9345FA4412F4F6DD5E7322728DD9
SHA-256:	10D9EB164FEE816CA898BF8C36E4CC5848757517276CE51822A414B05F8D6223
SHA-512:	6EB223A114B4E96A55299F7BD38708B19DEB557EAC5C0379AA0E3ED9D99EF98BB2C6EE31EE6541F6203A7952B52B5F5E846CAFFC0FBA89120DEB7ACD901DBFC3
Malicious:	false
Reputation:	low
Preview:	.....Z..... ..... .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):	338
Entropy (8bit):	5.169944922138832
Encrypted:	false
SSDEEP:	6:Fq2Pwkn23iKKdKfrzAdIFUtwJKZmwyJ2kwOwkn23iKKdKfrzILJ:FvYf5Kk9FUtwJK/yJ25Jf5Kk2J
MD5:	ABEBA8008F04C091E67BB3A6CEBC5A0F
SHA1:	556919EE2AB8592A47B0832083397DFFEE35583A
SHA-256:	88495DF4CE3ADAE83CE2C13AA9E87791993FFD71E85BF2D4B4D2B24F79FD4AC7
SHA-512:	A6BE3E0C33C83B2D48B511AB65B046EFC7F5D0FC92DAA048F7CA3939FAC7523DFB4945A906B03C0847F6450E6F27B2BBAFEE9A1246AB1F17176DD2206988609 1
Malicious:	false
Reputation:	low
Preview:	2020/11/21-19:55:05.144 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 0/11/21-19:55:05.145 1b40 Recovering log #3.2020/11/21-19:55:05.145 1b40 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\c073a44b-4e22-4b24-b824-6603e06d2713.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):	162578
Entropy (8bit):	6.082966096642649
Encrypted:	false
SSDEEP:	3072:+9wA2NNCxQM9b0q+szv+tnMI1FcbXafIB0u1GOJmA3iuRO:4wrExQM9b7fD+ZMcaqfIlUOoSiuRO
MD5:	4B13AE3C0D2FE110CF0A01704A4019E6
SHA1:	D8D939469A65F2A270ACD0B62CDAACA9EC5F624A
SHA-256:	72D1B54D598A4CE8C4C0F82699078678E40991E8FEE1CBD0EEB70C57123D2B9F
SHA-512:	F6107CEA8EC6C8F6D7FD5A9B7B1EE1E3E6D2D9E7E45063987C4F0503E8C498957AD9078A1F48CBB2EDA3BF76AB9101D1444C2DB1AE29DDDE6E12F49002FC7C70
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605984898154947e+12,"network":1.605984898e+12,"ticks":300544607.0,"uncertainty":2447193.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\daf0b36f-ca66-4a83-8f93-d06681184404.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751779123235707
Encrypted:	false
SSDEEP:	384:RrXk0WZTC9mAVRjAjNMr9vIU330CDHejGTmrxGUGxX6SKVrBcmViV2kAIzO2KANz:du6FJ6K330efiYi0HvewKG4gRn
MD5:	8B73D5CA5A8C2FB10E3BDD412E68F3FA
SHA1:	35D79D8E3F507DCDA20389E0981A2EE1F1629C5B
SHA-256:	434360C950E7B73E4B400022B4C79B703BF96B2C9DB38A22264FBF8A7381E4E8

C:\Users\user\AppData\Local\Google\Chrome\User Data\daf0b36f-ca66-4a83-8f93-d06681184404.tmp	
SHA-512:	956C0169B3E5F58881EFF373C88A97BA1ED13B0F309AC886C92764558C6ACC035CAF7E952192A9354C43C3D8B1F863CC87925B7BDEAFC0C4CA3434216C9391A
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)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\f43de022-f4d8-4e35-bf84-2d423e4a1f62.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):	162578
Entropy (8bit):	6.082966096642649
Encrypted:	false
SSDEEP:	3072:+9wA2NNCxQM9b0q+szv+tnMI1FcbXafIB0u1GOJmA3iuRO:4wrExQM9b7fD+ZMcaqfIlUOoSiuRO
MD5:	4B13AE3C0D2FE110CF0A01704A4019E6
SHA1:	D8D939469A65F2A270ACD0B62CDAACA9EC5F624A
SHA-256:	72D1B54D598A4CE8C4C0F82699078678E40991E8FEE1CBD0EEB70C57123D2B9F
SHA-512:	F6107CEA8EC6C8F6D7FD5A9B7B1EE1E3E6D2D9E7E45063987C4F0503E8C498957AD9078A1F48CBB2EDA3BF76AB9101D1444C2DB1AE29DDDE6E12F49002FC7 C70
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605984898154947e+12,"network":1.605984898e+12,"ticks":300544607.0,"uncertainty":2447193.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\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):	11371
Entropy (8bit):	4.916578591652501
Encrypted:	false
SSDEEP:	96:E4+KMja+KMjfpAda+KMxfpAda+KM5fpAma+KMd4fpAta+KMRfpAGa+KMRfpAGa+e:H
MD5:	E87B2B46C93D8C830E9B8A83BF4FA37D
SHA1:	C8EFBB2CAD70523C5AD194140CE894EB376D9610
SHA-256:	5BD853D672B09DF5F3280F5499D78DF2B37B2884984ED69A3751654F98D23763
SHA-512:	57A4008E5BADB645AE92E1197788ABAC650A46E92B6F9F93DE3519D3AD8B6E600DD46A41D0A05C179BC535E0EB9612AFD0961A6A2392A0D416108637D55BEC 6
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="nbrteststt" value="" ltime="3702557408" htime="30851127" /></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="3723447408" htime="30851127" /></root><root><item name="userkey" value="{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}" ltime="3723447408" htime="30851127" /><item name="browserkey" value="{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":""}}" ltime="3723487408" htime="30851127" /></root><root><item

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{18055A4A-2C2B-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.852158696987364
Encrypted:	false
SSDEEP:	192:r7ZvZn2O9W/t9uifqfhzMqZBGTDQisfQ1LfMjX:rNR2OUl9fXAYQxQ1k
MD5:	AD601FA911C83F326895128831D6C4B0
SHA1:	316B1E9B021DC4953FFC2221C6FD89127DEEE7B3
SHA-256:	A593F59513A050A47350AA3241A27461B00511163D6030FAAD737203DC21FD8F
SHA-512:	8B48F78E0510723580CCE0D51A03616086251B0B4E1A80E92E7D33ECF654DB0B6EF71562B83D5DB29E4EE28C40263DF18066C42C634C736FF35337CE40A42DD

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{18055A4A-2C2B-11EB-90EB-ECF4BBEA1588}.dat	
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\{18055A4C-2C2B-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	162200
Entropy (8bit):	2.950852624682376
Encrypted:	false
SSDEEP:	384:rb+8WXhuQ/OXiQux+NoS0QoZ4a5vzT4a5vdbwnWP3PoHgSs7okl9iNN65BgW9uVA:4mIjvZf5vnf5v66qCSCW+rhyJkewZSa
MD5:	B94FA344128338CA47B26FD9C9660627
SHA1:	6CF6B90DE0B4CC6CD8FA4F5AEB7AB060984C530C
SHA-256:	CBFBDF470688FA2549DFA7194554B30F28C9A7C9BF23C90049BCB5DDDF6E8770
SHA-512:	C6248D6A65751B8D4BC3D662C71663FA67AE0E6AE7361DF92CE5A5807F3C337D8D6A4551654A0071896507D4943BF6995570D775CDDC37D505A4CF81F09265B
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\{1F0C296B-2C2B-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5644495079894611
Encrypted:	false
SSDEEP:	48:IwsZGcpruGwpaNZG4pQUGrapbSgrGQpK2G7HpRgTsTGIpG:rs/ZGQN76iBSgFAhTgT4A
MD5:	D4C51D135BE62BCA9A45FA7A0CF9F9F6
SHA1:	2453A8B53F725497452F788DA2594643509DD40C
SHA-256:	02BD1590AEF7CA3625F5BD6B452F2EF7C236625B9DBA5DAF7D80296E7FD2855F
SHA-512:	522F181EFFAD5878635D6055BBA5C78715C6AD6D66C837574C70FE70A5BD81551B4A9B1FE5736EDB3692A89707267F38F98CD6E6E8F3273F922CB16955269955
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	72296
Entropy (8bit):	3.075289071804108
Encrypted:	false
SSDEEP:	96:njUjLjDjUjLjmQQQQQ0QQQQQwQQQQQsQQQQQZ:f
MD5:	6AA26C283438205FE0BE69D30E329651
SHA1:	8955427DFFAF9C632A4DFEC038434F5FCEC8CDA2
SHA-256:	0DDF8F9FCA62CBC992B77839800B39C59B40C29998A507955FE6147FB2787468
SHA-512:	C4796799CA3DE13600CF02BAC588E82255FD5F1286EEC897EFEA2E30ECFFD91F013F76F1821F9CF31C33FEC2B3766D7B153AEC1E576484F4D5159AD0B75AA0 0
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..... ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...33333333333333333333333333333333 ...333333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\39oebGZ[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	175
Entropy (8bit):	5.094603337082556
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDy5P6nJMdKsOVzx5DwWmEIqsK0EIkVHbQFSXbKFvNGb:qFzLIeco3XLx925PSJMdKjrSosxEIkVr
MD5:	F87CF707CD5DE27A2DC45E8937B5B279
SHA1:	D41FEC89494938DF928E0F24ADB01CA39DBC46E8
SHA-256:	FDD2F5C270688B4A112324C8A4A879B0B846BE1A4A3187369D80A6E9C8E24506
SHA-512:	A55CB09FA5F8F1370140D42E00ABB0D41A30019ED923C5A7BC538B85415F287F26153EEC6C59ACC8E60279C2992CE68C4B71D539AF87EF74679722012BC4B79
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\7d-3b8b80[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	168619
Entropy (8bit):	5.044040083782762
Encrypted:	false
SSDEEP:	3072:OzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCx8:clZAXLkeeds
MD5:	7A091EA3F595695C19CED8B52228FF48
SHA1:	587B8C1FFF5C84755C8BE6C2029FC0B46C0F76B3
SHA-256:	C55B3700FA0698B9F057F40512CFD3B9D6AED620598BACE734338F4F6DAF7A86
SHA-512:	522DC920EDA85D8C7F6FA56E959552C477133E1C5C39939331962A221E5C5AEAEC0643FE8F6AFF4384125B4B58E3930751A21CEB7C60C309AD037ED12865AF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/4a-f2fa13/d2-97697e/15-b02cf6/8d-8de298/30-e5ac82/cd-1bda0a/e7-838d86/7d-3b8b80?ver=2.0
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\axios.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\axios.min[1].js	
Category:	downloaded
Size (bytes):	34714
Entropy (8bit):	5.415836929747288
Encrypted:	false
SSDEEP:	768:ReNLXgwUCeDTo9LtrCv6wnr3iWavo+3r4zfduDs/hasZhn9zn9hLh8EuC9eW:CBAToBiyWO4phtJzZH
MD5:	B371B4971205183230CC6C734C09BD7C
SHA1:	4AD94B8585F7F4F8F642FCF43BDF0D40F8EF1BD5
SHA-256:	6B2114A050AED49F4A24237D4D1F437B75CA10C6FC8623EAE23C0558C53A7E21
SHA-512:	D7AD8B26A40183B17EF0D5C6885BA4CF1D9450B194CA721F432BB6CC09A8CD73B3DB4364099174AD6959F1C0C1A428720FAE9CADC8AB5562F3F9C771550732E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unpkg.com/axios@0.16.1/dist/axios.min.js
Preview:	/* axios v0.16.1 | (c) 2017 by Matt Zabriskie */!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&& define.amd?define([],e):"object"==typeof exports?exports.axios=e():t.axios=e()}(this,function(){return function(t){function e(n){if(r[n])return r[n].exports;var o=r[n]={exports:{}, id:n,loaded:!1};return t[n].call(o.exports,o,o.exports,e),o.loaded=!0,o.exports}var r={};return e.m=t,e.c=r,e.p="",e(0)}([function(t,e,r){t.exports=r(1)},function(t,e,r){"use strict";function n(t){var e=new s(t),r=i(s.prototype.request,e);return o.extend(r,s.prototype,e),o.extend(r,e),r}var o=r(2),i=r(7),s=r(8),u=r(9),f=n(u);f.Axios=s,f.create=function(t){return n(o.merge(u,t))},f.Cancel=r(26),f.CancelToken=r(27),f.isCancel=r(23),f.all=function(t){return Promise.all(t)},f.spread=r(28),t.exports=f,t.exports.default=f},function(t,e,r){(function(e){"use strict";function n(t){return"[object Array]"===_.call(t)}function o(t){return"undefined"!=typeof e&&e.i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\converged_ux_v2_RfnRCrmapm3W_OFn994CMA2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95459
Entropy (8bit):	5.292153801820765
Encrypted:	false
SSDEEP:	1536:QpHDIqBBw+T6azA/PWrF7qvEAFiQcpmKboBdiyMUWC8ErpH/TVTDrwCGNJZ3yU0P:IBFNyUM
MD5:	45F9D10AB99AA66DD6FCE167F7DE0230
SHA1:	D443993E7ADB3108167BCD94E5D3126A2E3EE7EE
SHA-256:	D72952FC8950D26C08C6BAD73D389C35D0EAF164CB73503183A2966DEFAAD991
SHA-512:	0DBCCCB37A3A249C7DBB948AC756FD332298DD8A742E92DF6A767FD565C925768058C05AF182106F8DA29979C0D23BD3E9ECE9E41C1EA931F4F198CBDCE8B3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .//---------- ----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any perso

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 169

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:58.449170113 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.449896097 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.465579987 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.465764046 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.466362953 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.466850042 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.467900991 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.469058990 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.484498978 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.485347986 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.486027956 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.486063004 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.486217022 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.488565922 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.488605976 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.488729954 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.677824974 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.678656101 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.678910017 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.679251909 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.679795027 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.694199085 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.694443941 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.694675922 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.694916964 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.695616007 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.696057081 CET	443	49729	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.696119070 CET	49729	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.696234941 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.697921991 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.738687038 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.751477003 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.870841026 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.870897055 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.870934963 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.870961905 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871001959 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871046066 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871079922 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871083975 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871119022 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871139050 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871145010 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871154070 CET	443	49730	104.18.215.67	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:58.871181965 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871206999 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871221066 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871234894 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871260881 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871280909 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871304035 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871337891 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871356964 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871364117 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871392012 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.871412039 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.871484041 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.965415001 CET	49736	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.965831995 CET	49737	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.966303110 CET	49738	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.966706038 CET	49739	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.967117071 CET	49740	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.967662096 CET	49741	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.968700886 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.968811035 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.968907118 CET	49730	443	192.168.2.4	104.18.215.67
Nov 21, 2020 19:54:58.981895924 CET	443	49736	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.982039928 CET	49736	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.982142925 CET	443	49737	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.982238054 CET	49737	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.982382059 CET	49736	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.982757092 CET	49737	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.982769966 CET	443	49738	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.982933044 CET	443	49739	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.982930899 CET	49738	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983031988 CET	49739	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983232975 CET	49738	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983344078 CET	443	49740	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.983433008 CET	49740	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983681917 CET	49739	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983941078 CET	49740	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.983968019 CET	443	49741	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.984049082 CET	49741	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.984298944 CET	49741	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:58.985017061 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.985127926 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.985199928 CET	443	49730	104.18.215.67	192.168.2.4
Nov 21, 2020 19:54:58.998692036 CET	443	49736	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.998931885 CET	443	49737	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.999598026 CET	443	49738	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:58.999886990 CET	443	49739	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.000160933 CET	443	49740	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.000600100 CET	443	49741	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.001364946 CET	443	49739	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.001452923 CET	443	49739	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.001518965 CET	49739	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:59.002230883 CET	443	49737	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.002263069 CET	443	49737	104.18.216.67	192.168.2.4
Nov 21, 2020 19:54:59.002319098 CET	49737	443	192.168.2.4	104.18.216.67
Nov 21, 2020 19:54:59.002708912 CET	443	49736	104.18.216.67	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:52.305254936 CET	49714	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:52.332334995 CET	53	49714	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:53.278882980 CET	58028	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:53.306013107 CET	53	58028	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:54:54.611046076 CET	53097	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:54.638128996 CET	53	53097	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.415560961 CET	55854	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.416763067 CET	64549	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.421098948 CET	63153	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.421952963 CET	52991	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.443717957 CET	53	64549	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.451342106 CET	53	55854	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.456878901 CET	53	63153	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.457498074 CET	53	52991	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.779618025 CET	53700	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.815156937 CET	53	53700	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.866080046 CET	51726	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.901637077 CET	53	51726	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.931282043 CET	56794	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.935286045 CET	56534	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:58.958282948 CET	53	56794	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:58.979412079 CET	53	56534	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:59.089412928 CET	56627	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:59.124893904 CET	53	56627	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:59.391707897 CET	56621	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:59.398111105 CET	63116	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:54:59.427376032 CET	53	56621	8.8.8.8	192.168.2.4
Nov 21, 2020 19:54:59.433726072 CET	53	63116	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.028892994 CET	64078	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.065092087 CET	53	64078	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.073333025 CET	64801	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.073960066 CET	61721	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.100493908 CET	53	64801	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.100860119 CET	53	61721	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.313949108 CET	51255	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.326953888 CET	61522	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.329091072 CET	52337	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.353543043 CET	53	51255	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.358627081 CET	55046	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.360234022 CET	49612	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.364232063 CET	53	61522	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.364469051 CET	53	52337	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.366148949 CET	49285	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.371567965 CET	50601	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.376214981 CET	60875	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.398437023 CET	56448	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.398575068 CET	53	50601	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.409907103 CET	53	49285	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.413866043 CET	53	60875	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.415350914 CET	53	55046	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.416527033 CET	53	49612	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.425745964 CET	53	56448	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.535382032 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:00.538383007 CET	59172	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.559439898 CET	443	56450	172.217.18.102	192.168.2.4
Nov 21, 2020 19:55:00.559494019 CET	443	56450	172.217.18.102	192.168.2.4
Nov 21, 2020 19:55:00.561907053 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:00.562412024 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:00.574210882 CET	62420	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.575953960 CET	53	59172	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.577044010 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.592865944 CET	443	56450	172.217.18.102	192.168.2.4
Nov 21, 2020 19:55:00.593517065 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:00.600692987 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.600737095 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.602124929 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.604156971 CET	443	56450	172.217.18.102	192.168.2.4
Nov 21, 2020 19:55:00.604305029 CET	443	56450	172.217.18.102	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:55:00.604723930 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:00.609906912 CET	53	62420	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.626431942 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.626949072 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.643425941 CET	60579	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.657310009 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.657735109 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.667061090 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.667109966 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.667315006 CET	443	62421	172.217.23.98	192.168.2.4
Nov 21, 2020 19:55:00.667398930 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.679274082 CET	53	60579	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.681611061 CET	50183	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.692859888 CET	62421	443	192.168.2.4	172.217.23.98
Nov 21, 2020 19:55:00.719407082 CET	53	50183	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.778455019 CET	61531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.797175884 CET	49228	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.814315081 CET	53	61531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.840684891 CET	53	49228	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.911633968 CET	59794	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:00.938721895 CET	53	59794	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:00.977962971 CET	55916	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:01.013884068 CET	53	55916	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:02.090147018 CET	52752	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:02.117448092 CET	53	52752	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:03.093986988 CET	60542	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:03.129749060 CET	53	60542	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:04.120573044 CET	57525	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:04.147818089 CET	53	57525	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:04.612677097 CET	53814	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:04.658819914 CET	53	53814	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:05.865763903 CET	53418	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:05.901587963 CET	53	53418	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:06.296479940 CET	62833	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:06.323740959 CET	53	62833	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:06.356069088 CET	59260	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:06.400084019 CET	53	59260	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:09.573498964 CET	51275	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:09.600640059 CET	53	51275	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:13.770406961 CET	63492	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:13.797714949 CET	53	63492	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:14.556548119 CET	58945	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:14.592350006 CET	53	58945	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:15.566292048 CET	56450	443	192.168.2.4	172.217.18.102
Nov 21, 2020 19:55:15.608675003 CET	443	56450	172.217.18.102	192.168.2.4
Nov 21, 2020 19:55:15.819519997 CET	60779	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:15.857460976 CET	53	60779	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:16.559012890 CET	64014	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:16.586123943 CET	53	64014	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:17.149624109 CET	57091	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:17.176800013 CET	53	57091	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:17.350298882 CET	55904	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:17.392167091 CET	53	55904	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:17.661531925 CET	52109	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:17.688553095 CET	53	52109	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:18.556700945 CET	54450	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:18.636883020 CET	53	54450	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:18.854604959 CET	49374	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:18.881742954 CET	53	49374	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:19.327658892 CET	50436	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:19.365626097 CET	53	50436	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:19.550518036 CET	62605	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:19.586273909 CET	53	62605	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:19.820928097 CET	54256	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:55:19.864953041 CET	53	54256	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:20.404047966 CET	52189	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:20.431183100 CET	53	52189	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:20.889204025 CET	56131	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:20.916402102 CET	53	56131	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:21.267322063 CET	62992	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:21.304341078 CET	53	62992	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:21.378319025 CET	54432	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:21.405978918 CET	53	54432	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:21.584997892 CET	57227	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:21.629545927 CET	53	57227	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:22.926868916 CET	58383	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:22.954147100 CET	53	58383	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:23.554860115 CET	63136	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:23.581883907 CET	53	63136	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:23.600641012 CET	50911	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:23.638427973 CET	53	50911	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:23.849716902 CET	63409	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:23.876873970 CET	53	63409	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:35.534991026 CET	59185	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:35.572357893 CET	53	59185	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:37.186909914 CET	64236	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:37.222752094 CET	53	64236	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:37.544651031 CET	56157	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:37.580539942 CET	53	56157	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:39.038996935 CET	55601	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:39.095701933 CET	53	55601	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:39.136528015 CET	52984	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:39.197056055 CET	53	52984	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:39.559030056 CET	51141	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:39.618598938 CET	53	51141	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:40.618248940 CET	53610	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:40.654087067 CET	53	53610	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:40.689491987 CET	61247	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:40.705799103 CET	65165	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:40.725541115 CET	53	61247	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:40.733115911 CET	53	65165	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:41.279854059 CET	52076	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:41.315845966 CET	53	52076	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:41.612822056 CET	54903	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:41.652292967 CET	53	54903	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:42.628973007 CET	55045	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:42.664999008 CET	53	55045	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:43.078960896 CET	54464	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:43.114710093 CET	53	54464	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:43.685628891 CET	50970	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:43.712954044 CET	53	50970	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:43.810323954 CET	55261	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:43.860775948 CET	53	55261	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:44.120760918 CET	59809	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:44.148020983 CET	53	59809	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:44.296025991 CET	51278	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:44.331904888 CET	53	51278	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:44.575284958 CET	51932	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:44.614861965 CET	53	51932	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:44.895946026 CET	59494	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:44.933082104 CET	53	59494	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:45.136858940 CET	55915	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:45.174843073 CET	53	55915	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:45.711035013 CET	49779	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:45.748281002 CET	53	49779	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:45.757584095 CET	49458	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:45.796130896 CET	53	49458	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:45.926772118 CET	57164	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 19:55:45.927516937 CET	49840	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:45.954621077 CET	53	49840	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:45.962181091 CET	53	57164	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:47.320807934 CET	57174	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:47.357928991 CET	53	57174	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:47.648597956 CET	58531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:47.684361935 CET	53	58531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:48.027924061 CET	49608	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:48.050354958 CET	55682	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:48.065583944 CET	53	49608	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:48.088222027 CET	53	55682	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:48.652822018 CET	58531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:48.688800097 CET	53	58531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:49.088040113 CET	55682	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:49.115178108 CET	53	55682	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:49.690341949 CET	58531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:49.726185083 CET	53	58531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:50.089132071 CET	55682	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:50.124876022 CET	53	55682	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:51.619921923 CET	62436	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:51.657179117 CET	53	62436	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:51.691298962 CET	58531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:51.727049112 CET	53	58531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:52.090245962 CET	55682	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:52.117274046 CET	53	55682	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:52.169516087 CET	61230	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:52.172230959 CET	64730	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:52.206650972 CET	53	61230	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:52.210566044 CET	53	64730	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:52.428376913 CET	60624	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:52.465797901 CET	53	60624	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:55.692770004 CET	58531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:55.719907045 CET	53	58531	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:56.091542959 CET	55682	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:56.127362013 CET	53	55682	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:56.514761925 CET	62600	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:56.560683966 CET	53	62600	8.8.8.8	192.168.2.4
Nov 21, 2020 19:55:57.404012918 CET	61034	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:55:57.439759016 CET	53	61034	8.8.8.8	192.168.2.4
Nov 21, 2020 19:56:00.111776114 CET	57687	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:56:00.148915052 CET	53	57687	8.8.8.8	192.168.2.4
Nov 21, 2020 19:56:00.901180029 CET	49839	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:56:00.944948912 CET	53	49839	8.8.8.8	192.168.2.4
Nov 21, 2020 19:56:00.998908043 CET	57975	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:56:01.043113947 CET	53	57975	8.8.8.8	192.168.2.4
Nov 21, 2020 19:56:01.091021061 CET	57610	53	192.168.2.4	8.8.8.8
Nov 21, 2020 19:56:01.128808022 CET	53	57610	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 19:54:58.416763067 CET	192.168.2.4	8.8.8.8	0x362d	Standard query (0)	www.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.931282043 CET	192.168.2.4	8.8.8.8	0x259	Standard query (0)	static.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:59.391707897 CET	192.168.2.4	8.8.8.8	0x2591	Standard query (0)	font-publi c.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:59.398111105 CET	192.168.2.4	8.8.8.8	0x893b	Standard query (0)	media-priv ate.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.028892994 CET	192.168.2.4	8.8.8.8	0x7818	Standard query (0)	cl.canva.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.073960066 CET	192.168.2.4	8.8.8.8	0xb99f	Standard query (0)	js.appboyc dn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.313949108 CET	192.168.2.4	8.8.8.8	0xc8ef	Standard query (0)	sdk.iad-01 .braze.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 19:55:00.326953888 CET	192.168.2.4	8.8.8.8	0x21e1	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.358627081 CET	192.168.2.4	8.8.8.8	0xec83	Standard query (0)	9812343.fls.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.371567965 CET	192.168.2.4	8.8.8.8	0x82df	Standard query (0)	sp.analytics.yahoo.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.376214981 CET	192.168.2.4	8.8.8.8	0x6350	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.538383007 CET	192.168.2.4	8.8.8.8	0xe4d5	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.574210882 CET	192.168.2.4	8.8.8.8	0x7cf3	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.643425941 CET	192.168.2.4	8.8.8.8	0x5214	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.797175884 CET	192.168.2.4	8.8.8.8	0xda95	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.911633968 CET	192.168.2.4	8.8.8.8	0xc2ee	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.977962971 CET	192.168.2.4	8.8.8.8	0x3624	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:04.612677097 CET	192.168.2.4	8.8.8.8	0x641b	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:18.556700945 CET	192.168.2.4	8.8.8.8	0x8ab	Standard query (0)	candanappdevmoe.azurewebsites.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.327658892 CET	192.168.2.4	8.8.8.8	0xee1b	Standard query (0)	cnd11.smsmail.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.820928097 CET	192.168.2.4	8.8.8.8	0x3432	Standard query (0)	vapdelbnbapp.firebaseapp.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.889204025 CET	192.168.2.4	8.8.8.8	0xa85d	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:21.378319025 CET	192.168.2.4	8.8.8.8	0x51	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:23.554860115 CET	192.168.2.4	8.8.8.8	0x2b5d	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:23.600641012 CET	192.168.2.4	8.8.8.8	0x1b4	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:35.534991026 CET	192.168.2.4	8.8.8.8	0x9d3d	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:37.186909914 CET	192.168.2.4	8.8.8.8	0xd4fd	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:39.136528015 CET	192.168.2.4	8.8.8.8	0x5848	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:40.618248940 CET	192.168.2.4	8.8.8.8	0x2901	Standard query (0)	client.hip.live.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:44.120760918 CET	192.168.2.4	8.8.8.8	0xfe40	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:45.926772118 CET	192.168.2.4	8.8.8.8	0xb8d4	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:52.172230959 CET	192.168.2.4	8.8.8.8	0xbd6c	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 19:54:58.443717957 CET	8.8.8.8	192.168.2.4	0x362d	No error (0)	www.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.443717957 CET	8.8.8.8	192.168.2.4	0x362d	No error (0)	www.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.958282948 CET	8.8.8.8	192.168.2.4	0x259	No error (0)	static.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:58.958282948 CET	8.8.8.8	192.168.2.4	0x259	No error (0)	static.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:59.427376032 CET	8.8.8.8	192.168.2.4	0x2591	No error (0)	font-public.canva.com		104.18.215.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:54:59.427376032 CET	8.8.8.8	192.168.2.4	0x2591	No error (0)	font-public.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:59.433726072 CET	8.8.8.8	192.168.2.4	0x893b	No error (0)	media-private.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:54:59.433726072 CET	8.8.8.8	192.168.2.4	0x893b	No error (0)	media-private.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.065092087 CET	8.8.8.8	192.168.2.4	0x7818	No error (0)	cl.canva.com		104.18.216.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.065092087 CET	8.8.8.8	192.168.2.4	0x7818	No error (0)	cl.canva.com		104.18.215.67	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.100860119 CET	8.8.8.8	192.168.2.4	0xb99f	No error (0)	js.appboycdn.com		104.22.9.79	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.100860119 CET	8.8.8.8	192.168.2.4	0xb99f	No error (0)	js.appboycdn.com		104.22.8.79	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.100860119 CET	8.8.8.8	192.168.2.4	0xb99f	No error (0)	js.appboycdn.com		172.67.7.226	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.353543043 CET	8.8.8.8	192.168.2.4	0xc8ef	No error (0)	sdk.iad-01.braze.com	d2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.364232063 CET	8.8.8.8	192.168.2.4	0x21e1	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.398575068 CET	8.8.8.8	192.168.2.4	0x82df	No error (0)	sp.analytics.yahoo.com	spdc-global.pbp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.398575068 CET	8.8.8.8	192.168.2.4	0x82df	No error (0)	spdc-global.pbp.gysm.yahoodns.net		212.82.100.181	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.409907103 CET	8.8.8.8	192.168.2.4	0x715	No error (0)	pagead.l.doubleclick.net		216.58.205.226	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.413866043 CET	8.8.8.8	192.168.2.4	0x6350	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.413866043 CET	8.8.8.8	192.168.2.4	0x6350	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.415350914 CET	8.8.8.8	192.168.2.4	0xec83	No error (0)	9812343.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.415350914 CET	8.8.8.8	192.168.2.4	0xec83	No error (0)	dart.l.doubleclick.net		172.217.18.102	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.575953960 CET	8.8.8.8	192.168.2.4	0xe4d5	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.575953960 CET	8.8.8.8	192.168.2.4	0xe4d5	No error (0)	pagead46.l.doubleclick.net		172.217.23.98	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.609906912 CET	8.8.8.8	192.168.2.4	0x7cf3	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.609906912 CET	8.8.8.8	192.168.2.4	0x7cf3	No error (0)	mix.linkedin.com	pop-tln1-alpha.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.609906912 CET	8.8.8.8	192.168.2.4	0x7cf3	No error (0)	pop-tln1-alpha.mix.linkedin.com		185.63.144.5	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.679274082 CET	8.8.8.8	192.168.2.4	0x5214	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:00.679274082 CET	8.8.8.8	192.168.2.4	0x5214	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.679274082 CET	8.8.8.8	192.168.2.4	0x5214	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.679274082 CET	8.8.8.8	192.168.2.4	0x5214	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:55:00.679274082 CET	8.8.8.8	192.168.2.4	0x5214	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.719407082 CET	8.8.8.8	192.168.2.4	0x920b	No error (0)	pagead46.l.doubleclick.net		172.217.22.66	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.840684891 CET	8.8.8.8	192.168.2.4	0xda95	No error (0)	www.google.co.uk		172.217.21.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:00.938721895 CET	8.8.8.8	192.168.2.4	0xc2ee	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:01.013884068 CET	8.8.8.8	192.168.2.4	0x3624	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:01.013884068 CET	8.8.8.8	192.168.2.4	0x3624	No error (0)	pagead46.l.doubleclick.net		172.217.16.194	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:04.658819914 CET	8.8.8.8	192.168.2.4	0x641b	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:04.658819914 CET	8.8.8.8	192.168.2.4	0x641b	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:18.636883020 CET	8.8.8.8	192.168.2.4	0x8ab	No error (0)	candanappdevmoe.azurewebsites.net	waws-prod-yt1-019.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:18.636883020 CET	8.8.8.8	192.168.2.4	0x8ab	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 19:55:19.365626097 CET	8.8.8.8	192.168.2.4	0xee1b	No error (0)	cnd11.smsmail.net		172.67.185.66	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.365626097 CET	8.8.8.8	192.168.2.4	0xee1b	No error (0)	cnd11.smsmail.net		104.31.67.162	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.365626097 CET	8.8.8.8	192.168.2.4	0xee1b	No error (0)	cnd11.smsmail.net		104.31.66.162	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.864953041 CET	8.8.8.8	192.168.2.4	0x3432	No error (0)	vapdelbnbapp.firebaseapp.com		151.101.1.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:19.864953041 CET	8.8.8.8	192.168.2.4	0x3432	No error (0)	vapdelbnbapp.firebaseapp.com		151.101.65.195	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.916402102 CET	8.8.8.8	192.168.2.4	0xa85d	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.916402102 CET	8.8.8.8	192.168.2.4	0xa85d	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.916402102 CET	8.8.8.8	192.168.2.4	0xa85d	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.916402102 CET	8.8.8.8	192.168.2.4	0xa85d	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:20.916402102 CET	8.8.8.8	192.168.2.4	0xa85d	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:21.405978918 CET	8.8.8.8	192.168.2.4	0x51	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:21.405978918 CET	8.8.8.8	192.168.2.4	0x51	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:23.581883907 CET	8.8.8.8	192.168.2.4	0x2b5d	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:23.638427973 CET	8.8.8.8	192.168.2.4	0x1b4	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:35.572357893 CET	8.8.8.8	192.168.2.4	0x9d3d	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 19:55:37.222752094 CET	8.8.8.8	192.168.2.4	0xd4fd	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:37.222752094 CET	8.8.8.8	192.168.2.4	0xd4fd	No error (0)	account.msa.msidentity.com	account.msa.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:37.580539942 CET	8.8.8.8	192.168.2.4	0xc50b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:39.197056055 CET	8.8.8.8	192.168.2.4	0x5848	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:39.197056055 CET	8.8.8.8	192.168.2.4	0x5848	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:39.197056055 CET	8.8.8.8	192.168.2.4	0x5848	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:40.654087067 CET	8.8.8.8	192.168.2.4	0x2901	No error (0)	client.hip.live.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:40.654087067 CET	8.8.8.8	192.168.2.4	0x2901	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:40.654087067 CET	8.8.8.8	192.168.2.4	0x2901	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:44.148020983 CET	8.8.8.8	192.168.2.4	0xfe40	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:44.148020983 CET	8.8.8.8	192.168.2.4	0xfe40	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Nov 21, 2020 19:55:45.954621077 CET	8.8.8.8	192.168.2.4	0x42d6	No error (0)	consentdeliveryfd.azurefd.net	t-0001.t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:45.962181091 CET	8.8.8.8	192.168.2.4	0xb8d4	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 19:55:52.210566044 CET	8.8.8.8	192.168.2.4	0xbd6c	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 19:55:00.510628939 CET	212.82.100.181	443	192.168.2.4	49749	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 19:55:00.695741892 CET	185.63.144.5	443	192.168.2.4	49755	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 19:55:19.421974897 CET	172.67.185.66	443	192.168.2.4	49782	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 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 19:55:19.427054882 CET	172.67.185.66	443	192.168.2.4	49781	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 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 19:55:19.908437967 CET	151.101.1.195	443	192.168.2.4	49784	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	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 19:55:19.913999081 CET	151.101.1.195	443	192.168.2.4	49785	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	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 19:55:20.966162920 CET	104.16.124.175	443	192.168.2.4	49788	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 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 19:55:20.970046043 CET	104.16.124.175	443	192.168.2.4	49787	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 19:55:21.443089962 CET	104.16.19.94	443	192.168.2.4	49791	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 19:55:21.455178022 CET	104.16.19.94	443	192.168.2.4	49790	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 19:55:39.331154108 CET	152.199.21.175	443	192.168.2.4	49809	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 19:55:39.331262112 CET	152.199.21.175	443	192.168.2.4	49806	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		

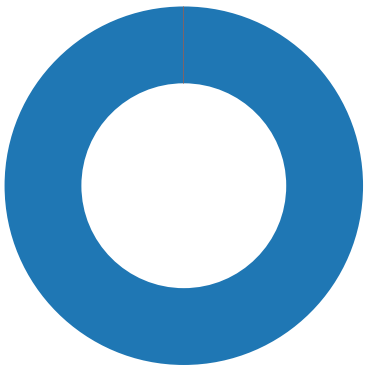
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 21, 2020 19:55:39.331506014 CET	152.199.21.175	443	192.168.2.4	49808	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert 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 19:55:39.331613064 CET	152.199.21.175	443	192.168.2.4	49810	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 19:55:39.331886053 CET	152.199.21.175	443	192.168.2.4	49811	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 19:55:39.332031965 CET	152.199.21.175	443	192.168.2.4	49807	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 19:55:44.207178116 CET	67.199.248.10	443	192.168.2.4	49823	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 19:55:44.207681894 CET	67.199.248.10	443	192.168.2.4	49824	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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6732 Parent PID: 2460

General

Start time:	19:54:55
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:	0x7ff609c80000
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 Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 6960 Parent PID: 6732

General

Start time:	19:54:56
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=1580,11732546741858598205,15005368519812649130,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /prefetch:8
Imagebase:	0x7ff609c80000
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: 1364 Parent PID: 800

General

Start time:	19:55:00

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:	0x7ff714000000
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: 3424 Parent PID: 1364

General

Start time:	19:55:02
Start date:	21/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: 8120 Parent PID: 800

General

Start time:	19:55:17
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:	0x7ff60abd0000
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	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: 5052 Parent PID: 8120

General

Start time:	19:55:17
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:8120 CREDAT:17410 /prefetch:2
Imagebase:	0x180000
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