ID: 344994
Cookbook: browseurl.jbs
Time: 15:33:52
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

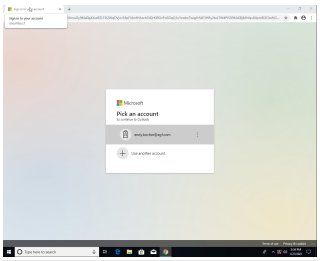
Analysis Report https://ww-agf.primside.ga/YW5keS5rb…

Overview

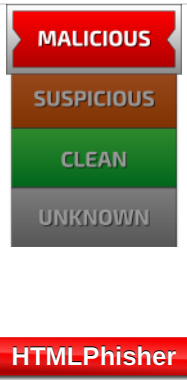
General Information

Sample URL:	http://https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==
Analysis ID:	344994

Most interesting Screenshot:



Detection



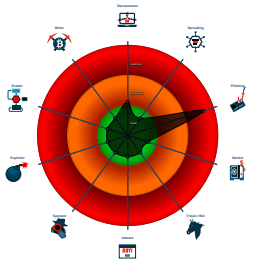
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4524 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6240 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,17962765629472374647,17200529593153591552,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1832 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

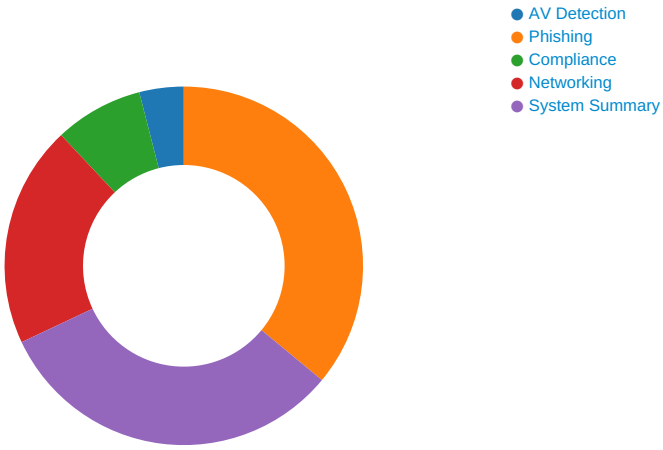
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

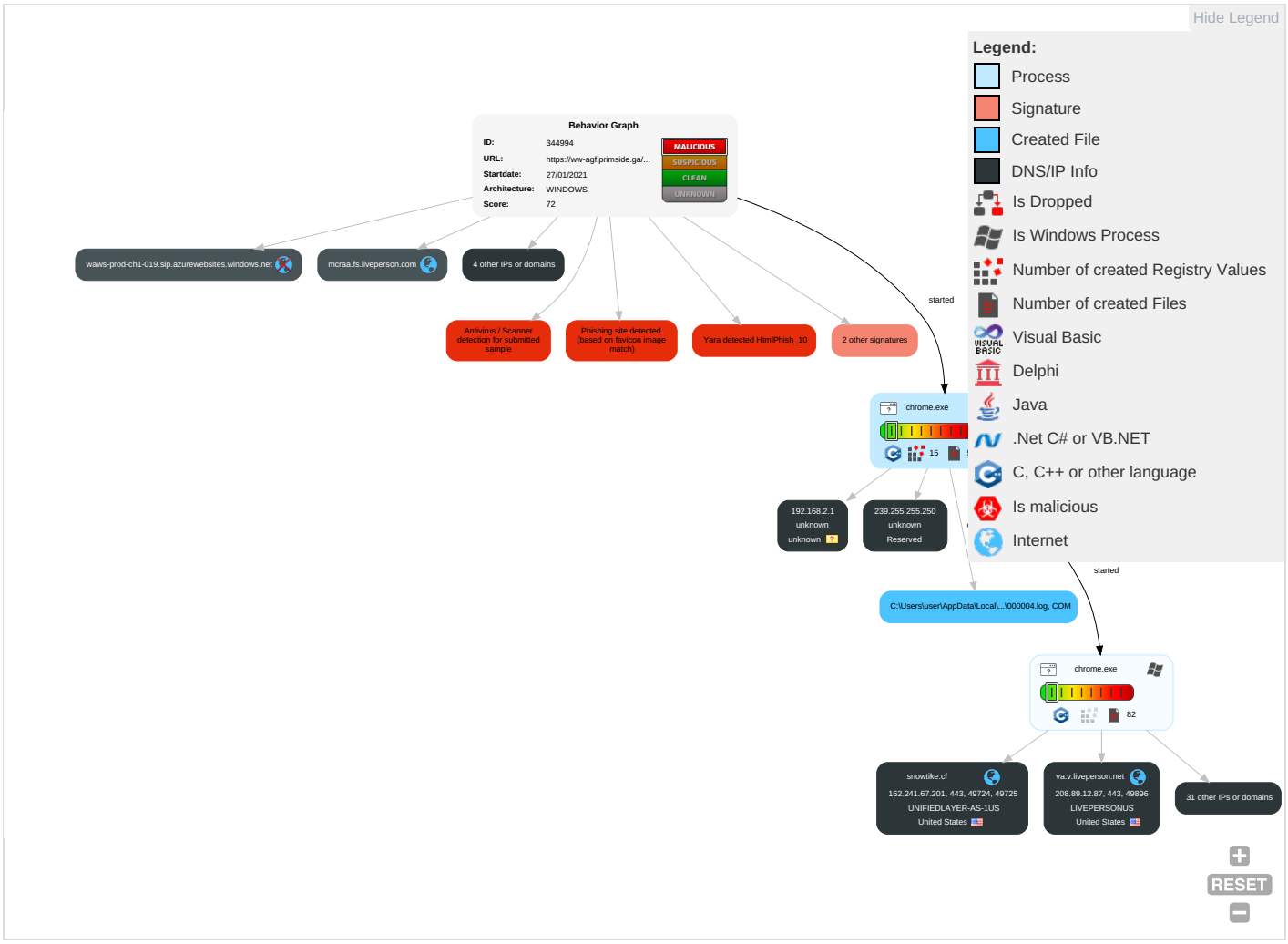
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

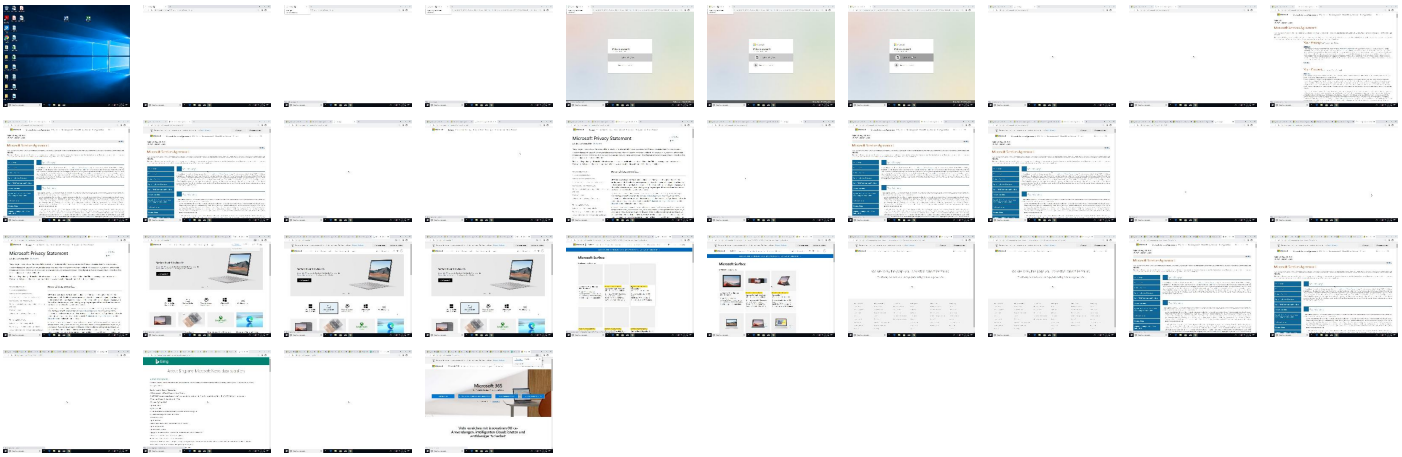
Behavior Graph

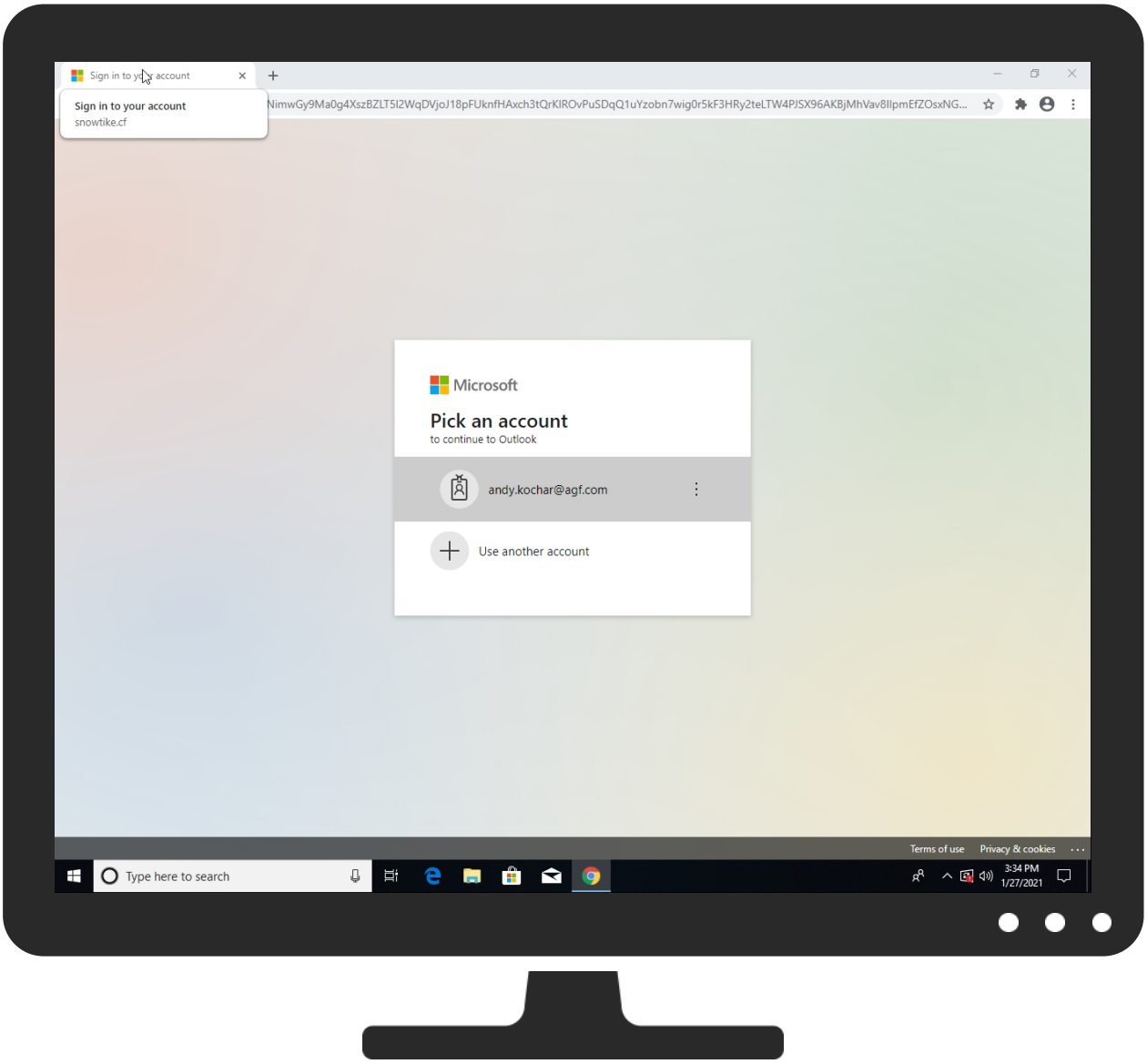


Screenshots

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://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==	0%	Avira URL Cloud	safe	
http://https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.clipart.email	0%	Virustotal		Browse
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://assets.onestore.ms/	0%	Avira URL Cloud	safe	
http://https://lpcdn.lpsnmedia.net(_https://lpcdn.lpsnmedia.net	0%	Avira URL Cloud	safe	
http://https://snowtike.cf/7b6eYENimwGy9Ma0g4XszBZLT5l2WqDVjoJ18pFUknfHAxch3tQrKIROvPuSDqQ1uYzobn7wig0r5kF3	0%	Avira URL Cloud	safe	
http://https://consentreceiverfd-prod.azurefd.net/v1	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=Surface&market=de-ch&uhf=1	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.jsaD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.jsaD	0%	Avira URL Cloud	safe	
http://https://cdn.clipart.email/de08a54070b0e35e96d77ab05a6eea4a_microsoft-logo-transparent-png-picture-75	0%	Avira URL Cloud	safe	
http://https://redux.js.org/api-reference/store#subscribe(listener)	0%	Avira URL Cloud	safe	
http://https://snowtike.cf	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.jsaD	0%	Avira URL Cloud	safe	
http://https://snowtike.cf/andy.kochar	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://cdn.clipart.email	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://controls.account.microsoft-dev.com:44308/me/profile-image?partner=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.clipart.email	104.26.5.196	true	false	• 0%, Virustotal, Browse	unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
microsoftwindows.112.2o7.net	35.181.18.61	true	false		high
ww-agf.primside.ga	162.241.67.201	true	false		unknown
dh1y47vf5ttia.cloudfront.net	143.204.11.96	true	false		high
va.v.liveperson.net	208.89.12.87	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
mcraa.fs.liveperson.com	3.218.234.129	true	false		high
snowtike.cf	162.241.67.201	true	false		unknown
liveperson.map.fastly.net	151.101.1.192	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.22.225	true	false		high
logincdn.msauth.net	unknown	unknown	false		unknown
lpcdn.lpsnmedia.net	unknown	unknown	false		high
accdn.lpsnmedia.net	unknown	unknown	false		high
statics-eas.onestore.ms	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
static-assets.fs.liveperson.com	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
bingexplore.azurewebsites.net	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
statics-neu.onestore.ms	unknown	unknown	false		unknown
statics-wcus.onestore.ms	unknown	unknown	false		unknown
statics-eus.onestore.ms	unknown	unknown	false		unknown
publisher.liveperson.net	unknown	unknown	false		high
amp.azure.net	unknown	unknown	false		high
lptag.liveperson.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://publisher.liveperson.net/iframe-le-tag/iframe.html?lpsite=60270350&lpsection=store-sales-de-ch&buttons=lpChatService,lpChatSales	false		high
http://https://snowtike.cf/7b6eYENimwGy9Ma0g4XszBZLT5l2WqDVjoJ18pFUknfHAxch3tQrKIROvPuSDqQ1uYzobn7wig0r5kF3HRy2teLTW4PJSX96AKBjMhVav8IlpmEfZOsxNGCUlD4pvWYF8xZb51qiGfLjKsnz7gIUTOJ6h2wyHAEeQStRu90oamrk3PCcMXBVylpIMhzXU2iS1AGETa09oZcDBf8bY5jgHOQkesK7CF6w3L4NxtmqVPvnWuJR/2MogmySibBcJaLQGZ4IN8UACq7l1V5THpfzE0hjKxktrFu9RYPeWXvnwO36D.php	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.onestore.ms/	Network Action Predictor-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb105	42bd799063a0846f_0.0.dr	false		high
http://https://lpcdn.lpsnmedia.net(_https://lpcdn.lpsnmedia.net	000003.log6.0.dr	false	• Avira URL Cloud: safe	low
http://https://liveperson.net/hF	mojo.4524.6164.171464390995534 45664.0.dr	false		high
http://https://liveperson.net/yER	5db4ad138a5b020e_0.0.dr	false		high
http://https://publisher.liveperson.net/	000003.log0.0.dr	false		high
http://https://liveperson.net/)	72090e93af2b3d0c_0.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.9.1.min.js	b180e6523891105c_0.0.dr	false		high
http://https://snowtike.cf/7b6eYENimwGy9Ma0g4XszBZLT5l2WqDVjoJ18pFUknfHAxch3tQrKIROvPuSDqQ1uYzobn7wig0r5kF3	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://consentreceiverfd-prod.azurefd.net/v1	2fc23221b4b80782_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.jsaD	4897c6f9e2ff1f8b_0.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js	0f33a3f4bd9b4e23_0.0.dr, f46ad 1d2652b0b43_0.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb695	4fa8d4ec20662298_0.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/zones?fields=id&fields=z	72090e93af2b3d0c_0.0.dr	false		high
http://https://lpcdn.lpsnmedia.net/	000003.log0.0.dr	false		high
http://https://liveperson.net/7	5db4ad138a5b020e_0.0.dr	false		high
http://https://live.com/	5a0d44391b90ff78_0.0.dr	false		high
http://https://publisher.liveperson.net/iframe-le-tag/iframe.html?lpsite=60270350&lpsection=store-sales-de-	Current Session.0.dr	false		high
http://https://lpcdn.lpsnmedia.net/le_secure_storage/3.12.0.0-release_5037/storage.secure.min.html?loc=http	Current Session.0.dr	false		high
http://https://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/UISuite.js?_v=3.43.0.1-release_5028	50030ae951750ff1_0.0.dr	false		high
http://https://publisher.liveperson.net	000003.log6.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.js	de5c13cb0b3aac41_0.0.dr, 73b12 b162f1cf8a7_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=qqZibvSk5NPpeVskPih5brHhq86%2FDi59RVJPmWdEE7bFo3xlwOzMxQ5%2B6T	Reporting and NEL.2.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/campaigns/1644274130/eng	e4b92c98510f85ab_0.0.dr	false		high
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	e4b9b26cef092fbf_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb887	18841ffaedbdc9b3_0.0.dr	false		high
http://https://liveperson.net/Z	3b99dc3d3bc104fb_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lpcdn.lpsnmedia.net/le_secure_storage/3.12.0.0-release_5037/storage.secure.min.js?loc=https%	5db4ad138a5b020e_0.0.dr	false		high
http://https://dns.google	e5ece1d7-752d-4f2d-9d57-ecb70cd32a31.tmp.2.dr, b77204b7-b0f9-4e12-aa3e-b9d791ceb5e0.tmp.2.dr, d83355af-bc8e-4bdc-8100-3c9e2de178d0.tmp.2.dr, 2b9f8560-d962-4d75-b6ec-34695c1acf5c.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.js	5a0d44391b90ff78_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lpcdn.lpsnmedia.net	000003.log6.0.dr	false		high
http://https://liveperson.net/Q	4fa8d4ec20662298_0.0.dr	false		high
http://https://liveperson.net/	22fb0e1969c285c1_0.0.dr, 42bd799063a0846f_0.0.dr	false		high
http://https://mem.gfx.ms/meversion?partner=Surface&market=de-ch&uhf=1	5884bcf8588200e3_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://accdn.lpsnmedia.net/api/account/60270350/configuration/engagement-window/window-confs/164451	8548771546cff460_0.0.dr	false		high
http://https://liveperson.net/V	43fb384703621b6c_0.0.dr	false		high
http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1	4ac2f448771ab57b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.jsaD	5a0d44391b90ff78_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	4897c6f9e2ff1f8b_0.0.dr, 094e2d6bf2abec98_0.0.dr	false		high
http://https://storage.live.com/Users/0x	de5c13cb0b3aac41_0.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.jsaD	28ed6ffa51f53762_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.clipart.email/de08a54070b0e35e96d77ab05a6eea4a_microsoft-logo-transparent-png-picture-75	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.jsaD	0f33a3f4bd9b4e23_0.0.dr	false		high
http://https://redux.js.org/api-reference/store#subscribe(listener)	de5c13cb0b3aac41_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://snowtike.cf	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/overlay.js?_v=3.43.0.1-release_5028	309184ad59030aa2_0.0.dr	false		high
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://amp.azure.net/libs/amp/1.8.0/azuremediaplayer.min.js	166ee82c52b87e97_0.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.jsaD	de5c13cb0b3aac41_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://snowtike.cf/andy.kochar	Current Session.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net	e5ece1d7-752d-4f2d-9d57-ecb70cd32a31.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.clipart.email	e5ece1d7-752d-4f2d-9d57-ecb70cd32a31.tmp.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	e5ece1d7-752d-4f2d-9d57-ecb70cd32a31.tmp.2.dr, b77204b7-b0f9-4e12-aa3e-b9d791ceb5e0.tmp.2.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.js	00add0752dc81105_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.microsoftonline.com/common/oauth2/authorize?response_type=id_token&client_id=	de5c13cb0b3aac41_0.0.dr	false		high
http://https://static-assets.fs.liveperson.com/microsoft/lp_ada_enhancements-prod.js	3b99dc3d3bc104fb_0.0.dr	false		high
http://https://aadcdn.msauth.net	e5ece1d7-752d-4f2d-9d57-ecb70cd32a31.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://controls.account.microsoft-dev.com:44308/me/profile-image?partner=	de5c13cb0b3aac41_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lptag.liveperson.net/lptag/api/account/60270350/configuration/applications/taglets/.jsonp?v=	43fb384703621b6c_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lptag.liveperson.net/tag/tag.js?site=60270350	22fb0e1969c285c1_0.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
208.89.12.87	unknown	United States		11054	LIVEPERSONUS	false
151.101.1.192	unknown	United States		54113	FASTLYUS	false
162.241.67.201	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
104.26.5.196	unknown	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
35.181.18.61	unknown	United States		16509	AMAZON-02US	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
143.204.11.96	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344994
Start date:	27.01.2021
Start time:	15:33:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ==
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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@51/298@27/13
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.microsoft.com/en-US/servicesagreement/ • Browse: https://privacy.microsoft.com/en-US/privacystatement • Browse: https://www.microsoft.com/en-US/servicesagreement/ • Browse: https://go.microsoft.com/fwlink/?LinkId=521839 • Browse: https://www.microsoft.com/ • Browse: https://www.microsoft.com/en-us/servicesagreement • Browse: https://www.microsoft.com/en-us/servicesagreement/faq.aspx • Browse: https://www.microsoft.com/en-us/servicesagreement/default.aspx • Browse: https://go.microsoft.com/fwlink/?LinkId=716894 • Browse: https://www.microsoft.com/microsoft-365
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 172.217.23.35, 172.217.23.78, 172.217.20.237, 216.58.207.174, 74.125.104.87, 104.43.193.48, 173.194.188.234, 13.107.246.13, 23.211.5.92, 95.101.22.202, 95.101.22.235, 23.210.249.93, 152.199.19.160, 95.101.22.224, 95.101.22.216, 173.194.187.106, 172.217.23.10, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 216.58.207.170, 172.217.20.234, 95.101.22.225, 95.101.22.193, 104.108.38.107, 104.108.39.131, 95.101.27.142, 95.101.27.163, 51.11.168.160, 51.103.5.186, 23.50.99.143, 65.55.44.109, 178.249.101.23, 8.253.204.121, 8.248.117.254, 67.26.81.254, 67.27.157.254, 67.27.159.126, 40.126.31.137, 20.190.159.138, 40.126.31.135, 40.126.31.139, 40.126.31.141, 20.190.159.136, 40.126.31.4, 40.126.31.1, 178.249.97.99, 178.249.97.98, 95.101.22.201, 95.101.22.208, 52.169.188.255, 172.217.23.67, 104.103.92.90, 23.210.248.208, 204.79.197.200, 13.107.21.200, 23.96.187.5, 95.101.22.233, 52.155.217.156, 23.210.248.85, 173.194.188.38, 20.54.26.129, 173.194.151.103 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, publisher.livepersonk.akadns.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, ev.support.microsoft.com.edgekey.net, a1945.g2.akamai.net, clients2.google.com, e3843.g.akamaiedge.net, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, au-bg-

shim.trafficmanager.net, www.bing.com, dual-a-0001.a-msedge.net,
global.vortex.data.trafficmanager.net, ris-prod.trafficmanager.net,
lgincdnvzeuno.ec.azureedge.net,
assets.onestore.ms.akadns.net,
statics.onestore.ms.edgekey.net,
skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, r1---sn-4g5ednle.gvt1.com, lgincdn.trafficmanager.net, r1---sn-4g5e6ne6.gvt1.com,
cdn.account.microsoft.com.akadns.net,
translate.googleapis.com, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, r1---sn-4g5ednse.gvt1.com, a1985.g2.akamai.net,
support.microsoft.com, statics-storeexp-neu-ms-com.akamaized.net, i.s-microsoft.com, r5---sn-4g5e6nsr.gvt1.com,
db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, prod-video-cms-rt-microsoft-com.akamaized.net, r1.sn-4g5ednle.gvt1.com,
auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net,
160c1.wpc.azureedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net,
accounts.google.com, cs22.wpc.v0cdn.net,
mem.gfx.ms.edgekey.net,
accdn.lpsnmedia.livepersonk.akadns.net,
a767.dscg3.akamai.net, star-azureedge-prod.trafficmanager.net, login.msa.msidentity.com,
lptag.liveperson.cotcdb.net.livepersonk.akadns.net,
c.s-microsoft.com, go.microsoft.com.edgekey.net,
e8819.g.akamaiedge.net,
az725175.vo.msecnd.net,
e13678.dspb.akamaiedge.net,
wcpstatic.microsoft.com, arc.msn.com.nsatc.net,
e13678.dscb.akamaiedge.net,
www.tm.lg.prod.aadmsa.akadns.net,
e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com,
audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net,
update.googleapis.com, a287.g2.akamai.net,
inv.mp.microsoft.com,
watson.telemetry.microsoft.com, www.gstatic.com,
a1778.g2.akamai.net,
e10583.dspg.akamaiedge.net, fs.microsoft.com,
content-autofill.googleapis.com,
aadcdnoriginwus2.azureedge.net,
displaycatalog.md.mp.microsoft.com.akadns.net,
aadcdnoriginneu.azureedge.net,
skypedataprdcolcus17.cloudapp.net, statics-marketingsites-wcus-ms-com.akamaized.net,
www.googleapis.com,
web.vortex.data.trafficmanager.net, r5---sn-4g5ednsk.gvt1.com, e10583.g.akamaiedge.net, t-0003.t-msedge.net, e55.dspb.akamaiedge.net,
blobcollector.events.data.trafficmanager.net,
aadcdnoriginwus2.afd.azureedge.net,
privacy.microsoft.com.edgekey.net,
par02p.wns.notify.trafficmanager.net,
dub2.next.a.prd.aadg.trafficmanager.net,
au.download.windowsupdate.com.edgesuite.net,
a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net,
mscomajax.vo.msecnd.net, redirector.gvt1.com,
emea1.notify.windows.com.akadns.net, r1.sn-4g5e6ne6.gvt1.com,
windows.microsoft.com.edgekey.net,
displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r1.sn-4g5ednse.gvt1.com, windows.microsoft.com,
waws-prod-ch1-019.cloudapp.net, r5.sn-4g5ednsk.gvt1.com, client.wns.windows.com,
db5.inv.mp.microsoft.com,
ctldl.windowsupdate.com,
e1723.g.akamaiedge.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net,
aadcdnoriginneu.ec.azureedge.net,
web.vortex.data.microsoft.com,
lgincdnvzeuno.azureedge.net, a-0001.a-afdentry.net.trafficmanager.net,
privacy.microsoft.com,
lpcdn.lpsnmedia.livepersonk.akadns.net, oc-inventory-prod.trafficmanager.net,
e13678.dscg.akamaiedge.net, r5.sn-4g5e6nsr.gvt1.com,
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 NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:35:36	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.l6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0847546854849544
Encrypted:	false
SSDEEP:	6:kKtZmbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:1Zv3kPlE99SNxAhUeo+aKt
MD5:	A05846FF90E82DCAE0BCCE94BC3CAF34
SHA1:	D87FB90BCCC6ED90E18B5EA2ED5BB2963E0D9793
SHA-256:	08351420414121D23B03E869B5AD7EFD10F1435C5680A949BCB9F3D1897F23D7
SHA-512:	D476D65C0EDECF3CA00E7B789AE8F896BBDB1851A1007C718EB6A4D72D9A2C50E848E13CA0FDE99A07BC3A420ECC0EC54294740D35177A11F0650890789B1EED
Malicious:	false
Reputation:	low
Preview:	p..... .....(@.....(..... .....&.....h.t.t.p.:.//./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\41b99a6c-b341-4617-9c22-b106eaabd80f.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):	366659
Entropy (8bit):	6.050195436060262
Encrypted:	false
SSDEEP:	6144:71lAumJe8UEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinw:7LAumJgEGNPUZ+w7wJHyEtAW9
MD5:	95E335FD1C1702D986E3518AD24EAE00
SHA1:	68CDF05B2C315CACADDEC892D1A28ECA76740D4A
SHA-256:	293AD3D8D7F9F208077EF48F59448B3EAB7009066A9B37A8A62536C2571971D2
SHA-512:	C4F20CFBE7D0DFD892E0065EE58B10761C59DFD805C3FFC31919B4E2232CA144110D6B1BA2AE6689BD1BF0105E17907ABB79683ED0928F69CEF217484844236
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\41b99a6c-b341-4617-9c22-b106eaabd80f.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611790490352083e+12,"network":1.611758091e+12,"ticks":160297850.0,"uncertainty":2859861.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\48d816ac-1017-4c2a-99d5-f9320e5108eb.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):	366660
Entropy (8bit):	6.050195512755131
Encrypted:	false
SSDEEP:	6144:Q1lAumJe8UEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinw:QLAumJgEGNPUZ+w7wJHyEtAW9
MD5:	B6D574F5D14B7D1142C0A139740E4980
SHA1:	8CE86BCC0DE5FE5A4E16A4765E2B4F7B8B293A71
SHA-256:	AB6C90283E3D4290681AEAFB0EB153EF07E799DFB84FFC5D753E3EFD928168C7
SHA-512:	38E4D160361B548E622C05F0B2989147AB98B335867A87BECF09970192D4E42C6C5589E364FD68A38B7AE4E08EF51D422C04684DE9529A40DD230C036FD09BB9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611790490352083e+12,"network":1.611758091e+12,"ticks":160297850.0,"uncertainty":2859861.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488217886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\591bd74d-2d35-401d-a9ca-7f57ac9221f0.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):	358188
Entropy (8bit):	6.028672537537657
Encrypted:	false
SSDEEP:	6144:/1lAumJe8UEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinw:/LAumJgEGNPUZ+w7wJHyEtAW9
MD5:	06D58C9585A68BC21B41DDCA050889E5
SHA1:	ABA186C8C878E1E725FE006E1D33E7C6A4F3FD25
SHA-256:	8CC05A0D6D012558847A3FDB69DB0CDD1D2A560B339E404604869582A157F83F
SHA-512:	D627A38377A56DA41B3E7B4F5EAFD89278CAEB7681F4BDCA15E501F253546415818E01499B8DA5D70AE3D64DB8D65C41EF931476887BF017A4C1CECEDB4AE4E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611790490352083e+12,"network":1.611758091e+12,"ticks":160297850.0,"uncertainty":2859861.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488217886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c79b71f-656c-4447-a969-314fbcb86d7a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.752101241313275
Encrypted:	false
SSDEEP:	384:ofe1Bf42fgjLVkq54NZryvdn3mpDiHzaGq9rlbRpxWLvTurshmc/43Jph2OHfJNU:2+2BNWvW+keXhrrIfTinKB3d27
MD5:	D7D196F4552D233073169C61CC10F39C
SHA1:	7550B70CB75614B4ABCCD218033207B30051CA08
SHA-256:	D5C5D9EF9AEC27610B6EC5A246B9A97FE6405115285B9DD8401BECE408284328
SHA-512:	053C38652D346E777BD83747C7ADDD5D7005725E35C977E20B4E2707DB8834DFA10ED956ACF49923CE25F246221F9D4377990C343D31B5B32F9DE91FA360F651
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c79b71f-656c-4447-a969-314fbcb86d7a.tmp	
Preview:	`o.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..../8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\61f65fc9-facc-4478-a4da-fed7695bab76.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	358190
Entropy (8bit):	6.028672615400712
Encrypted:	false
SSDEEP:	6144:O1lAumJe8UEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinw:OLAumJgEGNPUZ+w7wJHyEtAW9
MD5:	6E51ABEEA9B17196DA4F6A52FF0D109D
SHA1:	B556405E3DFCFF7E99050E276F8FCE05FA961DEF
SHA-256:	43AA16D91B19F0BB080D44268FC7D1C6C319F4DB4B1E795E32D6A72EDF2EBD6E
SHA-512:	E48DF60655612836677A3CA3D277B46D2388E5B35996B8FF3BB48CFC02C00FB8C63FA19CB49FEA4EE6877F7A1C0B3428226878F1C9DA1A7DC904015F40DA39B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611790490352083e+12,"network":1.611758091e+12,"ticks":160297850.0,"uncertainty":2859861.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488217886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\72a2b33e-aee2-4f8f-a217-309756c36aa6.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):	366660
Entropy (8bit):	6.050195198184401
Encrypted:	false
SSDEEP:	6144:j1lAumJe8UEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinw:jLAumJgEGNPUZ+w7wJHyEtAW9
MD5:	3E1280DB04DBFFF80CC59FEB38839544
SHA1:	3CB619E358D313563EFEE62A94302199C9A15F6D
SHA-256:	8227946961707388990 51CC7BD2625593E97396E9C9B18ECB95216B6D8345039
SHA-512:	C16DCAC82D47099C9BB8F068B1EACB51DBBDAB0356144F13999BFC13A5B98B5BA67CC97973FAC830C4B70F3D11FCB59CD5DAF23C321C85938065E0D008D30B2
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611790490352083e+12,"network":1.611758091e+12,"ticks":160297850.0,"uncertainty":2859861.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488217886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\022788f8-f157-450e-b39f-0bb4e705c93f.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):	22614
Entropy (8bit):	5.535968854816611
Encrypted:	false
SSDEEP:	384:7uWtFLlv1XS1kXqKf/pUZNCgVLH2HfDRrUdHGsnTO4dC4c:FLlpS1kXqKf/pUZNCgVLH2HftrUBGsne
MD5:	7BA20528870ADAE22E5DA84FF6A32EA8
SHA1:	6B165F8BC921F0FC2169E0EEB3A6E125227E5FA7
SHA-256:	039E39E01D55A8012B2F59A44FE31B42005056CC77FA921423BCEBCF316879CB
SHA-512:	F781B9B1CD9728CE6DB1F43B928419D477803751BEEF87C6564106916F6F55D62F19F41279E9537D23186586B6992B89CEB80CCB80C6EC196E9939A9AD547BFB
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":"13256264087995632","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0ac2aa7e-5dae-41ce-b7cc-020ce941a73c.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):	16763
Entropy (8bit):	5.578507193018851
Encrypted:	false
SSDEEP:	384:7uWtoLlv1XS1kXqKf/pUZNCgVLH2HfDRrUl45C4v:oLlpS1kXqKf/pUZNCgVLH2HftrUYCY
MD5:	198AE6C0362DED920F44CB4B29186371
SHA1:	D73109E65BF75A97DA5BBABBF5D92BA3F2DDDEC9
SHA-256:	03A088BA42FB9A0CA9E838822AE5A4B1A6D83F8137980A84CF45A2651EA23F07
SHA-512:	481CA457DD3E9492ADD9E3B50F1B91A45F6D4447D6D8CACA34E1681D12B75E27E56D19875D39247FA2A5B928AEC39449E662A5A48E516ADF7D3A0621AC48BD3
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":"13256264087995632","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14a09176-bff7-4496-9980-236988310fad.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\2903a80a-1590-4505-9a07-3bbd48700194.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2903a80a-1590-4505-9a07-3bbd48700194.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1711
Entropy (8bit):	5.576670093386399
Encrypted:	false
SSDEEP:	48:YBU9k6UUhcSU99eUo3OU98KUeUUoDaUeP9wU9ahUew:AU9dUUaSU99eUoeU98KUDUoDaUtU94UD
MD5:	F17F0CBAAB0D5CECB7E6637C65CFFFA4
SHA1:	3607E657A1F84E98DB3FEB3625FFBB7C3A36903A
SHA-256:	239A26391A06DFA3ABFE07339C4F7DA7F23ED60DB70277A0818C6F3F92E9F703
SHA-512:	3217B783A71C8FF6DDA0FD8AF29F80EB21C048B63EF6B5468A9AE4BCFB3583B64FA027529B780A49D8048B50A41E1FBB7A2135EF211CB16BF2906D117D9E807C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643326580.610564,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790580.610568},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1643326572.699503,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790572.699507},{"expiry":1643326531.039919,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611790531.039923},{"expiry":1643326532.506522,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790532.506526},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2935fafe-ae78-4e6d-9ac9-7de7b12c1197.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):	5967
Entropy (8bit):	5.186215406794772
Encrypted:	false
SSDEEP:	96:nuVZF0GC7s41Y1u66veaAVrBGPxk0JCqRWL8okY1fcHbOTctVuwn:nuVZis4HG9C4qYDkYBcjb
MD5:	4FDF94E62D49EAFA122A33C8FB0C81FA
SHA1:	ABEA8CA2F6A89045A9A44D057BB9F9AA76564668
SHA-256:	9B16E7043F067572F9AC91F71CCD3621426A97C9CFB32510D85DA53858D26633
SHA-512:	343E2C0F00EBD7BF4324315017CFC1F85C074EED65EA2A2801CF854DED105CC9C0522924A97DA93A84321299654598F299A73B5FC6BFE045027E12AC4982988F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256264088328849","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2e24b595-f004-4ec2-b9cc-19e7cb000570.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):	5859
Entropy (8bit):	5.1852863687249835
Encrypted:	false
SSDEEP:	96:nuVtFcC7s41Y1u66veaAVrBGJxk0JCqRWL8okY1fibOTQVuwn:nuVtps4HG9q4qYDkYBY
MD5:	670E029230624B4D1B09A3ABAEDCAC3B
SHA1:	366BF08F66E3869E2B2DE5221FED55DBABA88EE8
SHA-256:	73BE753CD430968F71AB4407E005CB35D0167EB3F491F7B2289E76493C54846F
SHA-512:	E6599FAE8675E25582A53867583674D0FA2105269F21F05140B0F71557E18F4655F77A39124430AE48DB7EF4AF63E8FFEF0C0057B7A81EC0B7452E2012124009
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256264088328849","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\32823cb3-9dad-4f30-8304-86274c2ec992.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\32823cb3-9dad-4f30-8304-86274c2ec992.tmp	
Size (bytes):	22613
Entropy (8bit):	5.536041762456514
Encrypted:	false
SSDEEP:	384:7uWtFLlv1XS1kXqKf/pUZNCgVLH2HfDRrUdHGPnTO4cC4I:FLlpS1kXqKf/pUZNCgVLH2HftrUBGPnp
MD5:	AFB5A10CBF183A167E70DD3DEAA85819
SHA1:	1E4F01C3D9574DF80FCA377E7FFD900E382AA7EA
SHA-256:	69934FE24024E9F38526E5F3C11D19376A6DA590D378AB0199F96093F72C8F12
SHA-512:	A5F58EB102A964AC6F05824866988AAACB71722F2E55243D77F7B23111172B636DBA86FFCCDFC80B8587D318F2692C2DC3B593316DD47F43567E53D57634157D
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":"13256264087995632","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\363b47ad-fd55-4697-ad02-bec9e4ce3f8b.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):	1710
Entropy (8bit):	5.577207260869758
Encrypted:	false
SSDEEP:	48:YY4uvU9SD6UUhcx9U9yaeUo3OU98KUeiUUoeaUeP9wU9ahUew:CyU9SWUUax9U9yaeUoeU98KUvUUoeaUC
MD5:	595AA43D219DFF1E3D9F58DFEF7CCFA8
SHA1:	2E19576CCC01EF659F7AF2E2E0AAF954150D9B12
SHA-256:	3187A6962FCF7BB7FB3C7C0FAB23D147E208E2A98D64E1D0E280C5828A475F29
SHA-512:	E4F899F6F18373DEC6F3B3BB50A983B7112EF92C8C8312FFF34069E247DDC68DCA419683280A8BBD163BDF1EAC991059CFF5DC65C2B7B0DB83F762EDA1E1BD57
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643326566.907739,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790566.907743},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1643326567.95711,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790567.957113},{"expiry":1643326531.039919,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611790531.039923},{"expiry":1643326532.506522,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611790532.506526},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\49141f8a-31f0-4b9c-acdb-d94ea6770e0f.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):	22613
Entropy (8bit):	5.536016791789913
Encrypted:	false
SSDEEP:	384:7uWtFLlv1XS1kXqKf/pUZNCgVLH2HfDRrU2HGinTO4GC4h:FLlpS1kXqKf/pUZNCgVLH2HftrUWGine
MD5:	09A50F14C27E1AC6648392BC0962E8A3
SHA1:	5FDF73A748727AFD9C1AC9373B052D9678922E5D
SHA-256:	7DD9F5DB7E2C1C01F977114376728DA9B6AEC689FA9F27368E587446B4D450EE
SHA-512:	10F09D0C86F5F35B6D5A689AB7A744F8696520D6ED1634662FD2D73C92F460CBD3C2BBAE67B33D2933638BD2212D9D946C9B68249589671087014 7E9D66FA040
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":"13256264087995632","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\7e73bdf1-0408-44e5-9d3e-54aad430f79b.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):	5226

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e73bdf1-0408-44e5-9d3e-54aad430f79b.tmp	
Entropy (8bit):	4.983901735431879
Encrypted:	false
SSDEEP:	96:nuVDF8qm4paAVrBGLxk0JCqRWL8okY1fibOTQVuwn:nuVD5m4p9K4qYDkYBY
MD5:	1B3C9653E74AB3041CDF4E7AE8DC1567
SHA1:	FEB2F40EED50299692D560093BE2AE4A74EEBDB3
SHA-256:	40A814F5440F6C24EDF49C1C83A63071A690D7DD16C2FA15ED994A478F1A5431
SHA-512:	50F5165EF796EB6E08F98F9E867E73B5981216058593D153ADE7856A0A1F111C781629B9659B7A271F7D14A95AD51AB34BB2EC5FB48C67DE531EC47C7358994F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256264088328849","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8bf49b0f-b41d-4263-a21b-f7323be312a6.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):	5858
Entropy (8bit):	5.185312656908949
Encrypted:	false
SSDEEP:	96:nuV5FcC7s41Y1u66veaAVrBGTxk0JCqRWL8okY1fibOTQVuwn:nuV5ps4HG9A4qYDkYBY
MD5:	F5BC5223D7084148D8619FAC71117B11
SHA1:	126443E99F352E4C3C89B6EA5B9520F7798FAA36
SHA-256:	942B65B8BBB9BD224C8D82AA3CA67131C7D22BDB8BC6BF69AA01B1E043DF10A8
SHA-512:	3A2481E0C24F40618AB0184059AD839125B0BBEC45E105EF40FB01F0432B8C4BBA1B3C1C0F62E39A832903A3C36205214D7CF319CDC060E892C0F7B72D1BA53
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256264088328849","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.227547642515617
Encrypted:	false
SSDEEP:	6:mb4EI+q2PN723iKKdK9RXXTZIFUtpI9FVmWZmwPI9FVNVkwON723iKKdK9RXX5LJ:tEI+vVa5Kk7XT2FUtpm/PiV5Oa5Kk7XH
MD5:	A11D04383D9986B1473D6B1F5C59C3E3
SHA1:	5FD33285BAF86E74776AFE03D7B023F839ADBEF0
SHA-256:	7F4F0988FF02A247116D2A1003A9A24BDFB8198582D84863484061F3B7C534DE
SHA-512:	90C6AADA3B6D8B975B9E2A4C32C700ED5BFAFC118C41E9DCC32B01811F7E349EA407C24430C96061454899D0E995C242FCCF2CFE1CF433F3B93DE4735E25B3 7
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:59.878 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/27-15:34:59.880 180c Recovering log #3.2021/01/27-15:34:59.880 180c 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):	324
Entropy (8bit):	5.238480313758349
Encrypted:	false
SSDEEP:	6:mbGEkN+q2PN723iKKdKyDZIFUtpIlAWZmwPIs8iVkwON723iKKdKyJLJ:P+vVa5Kk02FUtpcX/P58iV5Oa5KkWJ
MD5:	6D8FAD48AB68BEF17A55BC8E690C63EE
SHA1:	154BE36E55BCE9298FFD27A86F676A98D845B02D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
SHA-256:	B68885792D51EC7EBB27EDF9E52E26DB88AF927EE9597ED19E163EA2A993C685
SHA-512:	A5E859D656F7F8DBFB88FA685B265ECAB58DC2C5EC437E85214C212AA874581741900E3124202727D8DEB84AA2E5A4F116DE480E53A47806F44EAF8949BB5F9
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:59.872 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-15:34:59.873 180c Recovering log #3.2021/01/27-15:34:59.874 180c 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\00add0752dc81105_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	362
Entropy (8bit):	5.8942657551956215
Encrypted:	false
SSDEEP:	6:mOsi/lXYL8vc7Z6cVLx1Dob/g4Wt4vgCm45l/bK6tziVcTaVjfe6S7j0qqS+gCm4:3siti0c7Z6cRDobPWrCmDNF2iajfe6SN
MD5:	FEA8EB55D1B858364D80416CF6B88355
SHA1:	430FA1D72856A7428068535FC99974E625FE31B0
SHA-256:	7448FD85246AE11A3935EFB40F14CC3F8C890E167669454561DA536B77D3072E
SHA-512:	AA1D26D9D3EBE54B4515433C4CAB6DCA7CADEEDA89FEA26AE23D0109FF060E7933A83F332C5EB1C4A4BF25459D61907AD071073F2BF3A5A6AAF76D90DDA064EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...?@Is...._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meCore.min.js .https://microsoft.com/...../.....(.....a..^...PxDE|H.k)...xN..A..Eo.....8.x.....A..Eo...../.X...A990740961AA5E046889B2A6F26AE3B3D1158B4320B68B77CAD1FA9969519E22.....a..^...PxDE|H.k)...xN..A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.574900562347547
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKIf8QPKxWStHWFvDFYtRsUcu/lHCynltlrl58tyGdDmq0Q/J:m3VYyK08fNH1DsUBgyXvyL6ohK6t
MD5:	CD7524BEA511D54725DC4DEFBF0D148C
SHA1:	22134706C739B58E579258E02F27C76AA4C78859
SHA-256:	C5AB2EB82B666EF715C8FDB255F73F17B0AB728E8E13E3EF05C53DCCDC41CCCE
SHA-512:	7C388C47288EEBE52F5C4062F5606F282677928F64B219031E5987E0FED5CA3581784100CBC55881656B1AA5758A9AF298D42C111682DC569CE0489032898729
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/.T..../.....B.....=.z-.7.K]..~..=..9.....8...A..Eo.....P/.!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f33a3f4bd9b4e23_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94840
Entropy (8bit):	5.78744381851882
Encrypted:	false
SSDEEP:	1536:S2PXzXmzNvZfSiDGZDimcbZg/URPGwsrQiEdFdaKWhMHSHzzHy+:hmvcBpciMBGcjd6KaXD
MD5:	8777BB855489A558274C31CEC7940AE0
SHA1:	95D02BF441FBCFB6795B7A153784B704A770F783
SHA-256:	85FEEF9D85693642BEE374C76598DC2E557C3E3EAF16B194F0A10DA5C72AF438
SHA-512:	B939EAA69633717136285595739342l4F444B8E7A59F1DB6C85E7511F7F8D1CA397831AC16CCF84CCD78FBA01A2FEDBEBA8528C39FF208144C401901036A39A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....}.....6FDF1C6A87D1FDFC265E86DCE44407847F06B05FC6A88A9B8D93317E57319A3E.....'.wr....O''... q.....@.....(S.4..`$....L`.....(S.....`:.....L`.....Rc.....O....M...Qb..2u....cy....Qb^.T.....cu....Qbb..u....ct....Qb...K....cs....Qb...v....cr....Qbr&Y.....ci....Qb.....ch....Qb.-.....cb....Qbn.....ca....Qb..p.....b_....Qb...g....b$....Qb...U....bZ....Qb~.u.....bB....Qb...1....bo....Qb.....bn....Qbj`.....bm....Qb..y^....bl....QbVJ.....bk....QbF.....bj....Qb26.....bi....Qb.....U.....Qbn\<J....T.....Qb.....S.....Qb*..(....K.....Qb...}....J.....Qbf..|....n.....Qb.1.....m.....Qb:.....l.....Qb.5q.....h.....Qb.....c.....Qb.x.....d.....Qb.P.D....f.....S...Qb..`!....j.....QbbZ.I....k.....Qb...%....o.....Qb.....p.....Qb..m.....q.....Qb.x.....r.....Qb..T'....s.....Qb6..`....t.....R....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\145375f6fd9456d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	406
Entropy (8bit):	5.514027906498634
Encrypted:	false
SSDEEP:	12:czDFbKQvuLesKlITsMqTeq1rKDyKFdkkA5lT:czhHEesthqTH1rK2f
MD5:	47649205DAB3C77F02CF658907E7DD7A
SHA1:	909095B9D478C7909B313D56F72428FD797EC3E7
SHA-256:	09792BABDCBB6034C32B7AFCCC971E28A7227A2793992D8A8D4D31B40FEFE447
SHA-512:	826FDD50E8A14CAF7CE1327B686DA713FDF17227DE1EC97044F35949882F5A992D0B2B96A916278397645BA3C0C5925B120233BB912951AB464487B598796ADD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://www.microsoft.com/mwf/js/MWF_20201028_28422223/alert/autosuggest/contentplacement/contentplacementitem/flipper/flyout/glyph/heading/hero/heroitem/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain/social?apiVersion=1.0 .https://microsoft.com/.v.../....."".....(.I/.....M....1..Q....A..Eo.....@~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\166ee82c52b87e97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.444190435479306
Encrypted:	false
SSDEEP:	3:m+lkLI6v8RzYmfksCVbKEfQXtkMEOZuFvDFYtRFFi//lHCgl/5yZ9aPjGWTh/z4s:mY6EYmcRR3/wZdD/i/ggni96VrBhK6t
MD5:	A4950E7773CDAE40FDF146D05A092F99
SHA1:	42A0C445688BADD3F38FEA8D55B516652DAC4A90
SHA-256:	48975AD99B7326769DE8D2F5ED59D60D2635EF920D98441AAD1D43ACA6A2F485
SHA-512:	40AC3B6569EAF55ECEFFE5B24F5AE7F1C2736A9B697E7DC9E86749695B175415C7CCC6E0AE90FF1F567782AFCE214F2CE5E4631AED69027EB094A1AEC7B60A3E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...\n....._keyhttps://amp.azure.net/libs/amp/1.8.0/azuremediaplayer.min.js .https://microsoft.com/.. .../.....Y.....(..A=Z....F...1/.k....s6...A..Eo.....Nil.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18841ffaedbdc9b3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	268
Entropy (8bit):	5.581912592216073
Encrypted:	false
SSDEEP:	6:mv/VYcBB8LjFke/BDWDQICW0ZSVC6cMHvWd/gDAv6pUgrrDK6t:TnN/hWDxCxqC3MHvhAcF
MD5:	EB3430D58A4258F15EA0AA6660F61DF3
SHA1:	BCDBA9908CCCD0485758D001B93221E744E73C3E
SHA-256:	41713022D4665699D483DF2F6DCA258FD4EC1CBDF274E304392B39DC6081470E
SHA-512:	AF4BA05B35C8A83AC3732C83CF1CF17A38F4118FE72790F6131DAD30A5BAEEEF24651585125770595BC2244ABDACAC4802CF517A4013311FF645B7BEC663F70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4....._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb8879x87778 .https://liveperson.net/.d_.../.....cS.....*....B.M{b.U4f..5.f".K(.A..Eo.....iF.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22fb0e1969c285c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.448569302065496
Encrypted:	false
SSDEEP:	6:mCVCVYv0iffhQ3fvlgBXCx/pK4qhK6tWCVCVYv0iffhQ3fvJ1l/gwhx/pK4bK6t:VVuAavyn7XVuAavJPX
MD5:	986E66C433B9B2CBA0B712CF59F0C895
SHA1:	BC2F9E14DC91F2D78B79549B6CEB39C2EEA5585A
SHA-256:	7B6EC4FA46706E68C2D128B9E668DE23B856A39F601EE69D0297C13D42385E6A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22fb0e1969c285c1_0	
SHA-512:	E82762C906E7BB551AA3BD47EE2A65BB50A5ACDEA68C28D3C0EE123BCAE8AEEC36D7F37724F2BDB6B30018C6CEE331ACABAD3F217B6839F1DA5AF65D6AFD48FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....p.3...._keyhttps://lptag.liveperson.net/tag/tag.js?site=60270350 .https://liveperson.net/..../.....'.....5+.o....D.o.p..3lm...\....x.A..Eo.....v.....A..Eo.....0\r..m.....R....p.3...._keyhttps://lptag.liveperson.net/tag/tag.js?site=60270350 .https://liveperson.net/...../.....<.....5+.o....D.o.p..3lm...\....x.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24d8148eb4e4c27a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	67544
Entropy (8bit):	5.694283036903534
Encrypted:	false
SSDEEP:	768:M3cjvMPZ4IoHmPcmQ4di2UIlCqRYnN5ivGt3qxnC5Doo/noj/HmgjEhVx:M3cjShQ4dnUIUZ5ibS/ns/H4
MD5:	8EEE619C53586069F40CE02D081F0280
SHA1:	B056D05F3A440C4A8735A82CBD16A77A97BA77E5
SHA-256:	FBB9232A3E7B4044942B5CED3A02250133F1F9CF7752EBAEFF4C7628957C7F02
SHA-512:	0973B2073902D7C6575549905D6959279358DD1C4B19AD4D4F7463D2136582B113691A8CD809AA3C1C610F210E42A47CC1A76A996C4B0C5467C2588C3348541E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....k;.....402147C9A77D20F8F02E7C4A82A4D6900B12765B6A51102422AC7229B4C3E8DD.....'.....O.....kj.....(...P.....x.....t.....(S...Q...`\ .....A.L`.....(L`.....(S.....Ia.....Qe:*.....getQueryValue...E.@.-.....P.....https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\28ed6ffa51f53762_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	73216
Entropy (8bit):	5.691188939597882
Encrypted:	false
SSDEEP:	1536:ZzatwcqOfIheFoceBkUq6L0z4KjPJXzzZImtNAzLwRwJpkP5xYi1rMQtcDtdsYqM:Z7O/iT
MD5:	03F7E1BBA45DAF96B8200F487CC05FB8
SHA1:	C2C1E6F96DAE548A3922D9707E54D8E5CC8A8EE0
SHA-256:	477E7585E09F4A9548C6695587BD9529C186C9455D53FE29CBA34C04E8038404
SHA-512:	8B3A05FA634837703505D2831BD4EF0E0936AC1E938B32AE764D94879DA6D7BC14A5D39A94EBA7F1B34115B53A98FC22691896B7D5D5E4178FBEB171EEB5FC00
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...-..+....A990740961AA5E046889B2A6F26AE3B3D1158B4320B68B77CAD1FA9969519E22.....'.....O.....h.....l.....(S.H..`L.....L`.....Q.`2..t....MeControlDefine...Qc..X....meCore.....`.....M`.....Qcb..0....exports..$Qg"6.....@mecontrol/web-inline.... Qf..P]....@mecontrol/web-boot..(S.....`&....}.L`:.....Rc.....Qb..8....h.....QbR..N....f.....Qb..m.....r.....QbN:.....d.....Qb.5.....s.....S...R....QbR.4.....l.....Qb.t.....v.....Qb..S.....k.....Qb:7.^....p.....Qb..S(....n.....Qb.....o.....M...Qb.....c.....Qb.IC.....S.....Qb..o.....A.....Qb.?q.....P.....Qb.vO.....m.....Qb>..K....y.....Qb.....T.....Qb..^.....E.....QbfuS.....L.....Qbb.....O.....Qb.V.m....F.....Qb.S|l....N.....QbFUNm....U.....O...Qbn.8.....I.....Qb&.....D.....Qb.m.....C.....Qb..z.....M.....Qb.:.....H.....Qb.....B.....Qb.k.....w.....Qb..,.....,.....Qb.....x.....Qbb..O....R.....Qb.<.....W.....Qb..>.....z.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fc23221b4b80782_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	276760
Entropy (8bit):	5.581140846551918
Encrypted:	false
SSDEEP:	3072:/LGlixZKW6RII7Oe36t6yICsanyEE/cE1jTJBwwbR02Ukt+LQpP3AjcT6VApco47:/LBEnSpt6kW0bkt+LgPAwg
MD5:	E5F8233DC4756DB0F8AE622C32D97C95
SHA1:	704998D2AFCFAB4112A170BF9C33487E407DA82C
SHA-256:	F065BEFA5017980F94EEF5CE8291E2BF2BC2F3D344342DA0CEB26928E9341727
SHA-512:	280F12E82FD75BAED3E5D3190BD48F0B72A4BB05E6A388EEB9669EE723510C7C1240BDB23B5028379C0050F77A54A9478395D2BA65B0E420B8F459E8D101A279
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fc23221b4b80782_0	
Preview:	0\r..m.....@.....4B9DAFE5A7B03A95CA8C8B468B7725467B7841978F4424269367E2E99E9C9AEB.....'.tT....OP....7....{H.....\....%.....(.....4.....H...,.....H.....d.....|.....L...L.....$.....$..`..,... ..|.....|.....$.....p.....p.....P.....(.....$.....|...8...|..(S.`..`|....$L`.....L`.....Qd..e}....WcpConsent...(S...`.....LL`'....@Rc.....Qb..d.....e.....M....S.b$.....I`.....a....F....(S...`.....L`.....Qc.....exports..$..a.....C..Qb:.....I...H..!....a.....Qb..A.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da\...T.....e..... P.....@....@.-....HP.....:...https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js..a.....D`....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\309184ad59030aa2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.543138526974484
Encrypted:	false
SSDEEP:	6:mORUYbLjFCsWLqLUqxYy6cUqmvJv/g0rNllZK6t:Zbn3WOAvr1
MD5:	7C52D50BFD980B6BF744CFF0B32D8329
SHA1:	BEEADB028A3AD7161F8F74CF19BFEDB4049F6F9D
SHA-256:	9780733A42B4A9D813BFBF58776DE4D3FE74417E0DFA2CA134F12AE5CEDF5234
SHA-512:	9BE504CFB9518BC67495C7D8752F061082744B6C4E2ECD6535EE5CC651880C4758E315C8E05CB74B184C2E4C7521FDCF6FCBAED634D1852D770B47DA9118BC1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}.....4....._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/overlay.js?_v=3.43.0.1-release_5028 .https://liveperson.net/..\.../.....R.....E.J2'.+..... %..(.....h6G.qx..A..Eo.....S..i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b99dc3d3bc104fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.463015824827973
Encrypted:	false
SSDEEP:	6:moinYkhcV5lT6Rsbm59LPWNves/VabjPnFK6t:EEpRs0uNvJdcj3
MD5:	16577AAE943F2F39A43C7BF5CFC67EAD
SHA1:	981B3850D62B60516E77702D0F771B04F6A88338
SHA-256:	61BB8975F2A0521D960201252B9D101306466509FC12C3508A67709345CEDB6F
SHA-512:	93FED17E79FAAB03A45F949748EEE10CEEFCF9442F117F4A8F31E661078CBED74710F6EC61B8EDDD208417C6026E973B518B42153D60573A6AE32BCE26C2DC3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...~.F...._keyhttps://static-assets.fs.liveperson.com/microsoft/lp_ada_enhancements-prod.js .https://liveperson.net/Z..../.....Q2.....j\.!.&.....I....B..m..(..w.G!..A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\428111ef80473512_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96472
Entropy (8bit):	5.827966356599375
Encrypted:	false
SSDEEP:	1536:2t6+VXHfHkg1AEyQ/SugDQ9//c3sC0Xyjs8kFnw5O46:iEYywSug5cC0X+MFnw5O3
MD5:	6A2FD9630BAB0EDC5A7747A52E958033
SHA1:	0972759F8BA67848294D242B0391CF87C0B00C99
SHA-256:	938570C404050E8B2180133995FD847444BD622544E28DF1EDEE184AD32C40A1
SHA-512:	70B377D9F38F094B7B72FE45C6BDF49122FB99B3BF28CA175E1ADF5FE5765373FD9435061968EB5C27C19762ADEB1D9D2E78A97137B7CF99E648A3E4442881F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.../.7Z....37DFF8F4DD16843074A538BE0BF515B9ABC80D808546594A0BA15EE6AEC07545.....'..S....O!....w.....H#.....,.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb..]v....t...`....I`....Da....I.....Q.@.....module....QcBO.....exports...Qcz{.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa....0...I.....@.-.....P.1.....https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.jsa.....D`....D`....D`.....Y....`....&...&..!.&....&.(S...I#..`FF.....L`.....Rct.....2....Qb:.6k....e.....Qb^..M....r.....S...Qb".f....o.....M...Qbz.HK....s.....R....QbR.....I.....Qb.....c.....QbREC.....f.....Qb.E.....p.....Qb.b.....d.....Qbv+N.....h.....Qb>\.....y.....Qb.f.!...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42bd799063a0846f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42bd799063a0846f_0	
File Type:	data
Category:	dropped
Size (bytes):	269
Entropy (8bit):	5.628443842758664
Encrypted:	false
SSDEEP:	6:mKryEYcBB8LjFke/BDWDQICW0ZSVCRRhVfv6+/gnqaYwDK6t:HyjnN/hWDxCxqCHvdg
MD5:	E0CB5139003DCC3B0EF60F36634F23BC
SHA1:	83485C8D9543994B3D35691FB4027A6227287551
SHA-256:	DB9BBB292CA95F75DCF11EF3F721AF9622006FA5BC4C03BDB98828A158680706
SHA-512:	685324502926E5BB0E0BAC0F76BC92636EAB75893237E91EB90B623AAC36267025AA6C3B52F62E731CFAE0248F55D4C74F64C1DA66D360AABB65EE422ECE8F4 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Su...._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb10531x26350 .https://liveperson.net/\r..../.. .....D?.....+..Dg.....@q~.{..O.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\431ab35fa84a13dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.562561069945225
Encrypted:	false
SSDEEP:	12:H/pDQLf+5KWFhhBoKRtCOXXc8HNC1Ngw9jMuwLmzlKDk2D0Wl:fpj5FhHhtCOXXc8tCrMu0mzQA2J
MD5:	17341E50528CF86FBCE336FD7FB2CC39
SHA1:	7C5965986500C24D13DDFAD8066D68434E2E620F
SHA-256:	FFF487BF0B49E8467052827C30EA82D7CB6E216B13BA3578E198D0852B0C22AD
SHA-512:	117BA7A732BC7BEBC3A8C34A5B8596FCA4F3089A7F6A19A526FF99247A2C6684D9E87BA45230FA9E19A9F4A6282BF4A4DC9623E423FB57B10BD54605F240B61
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/2f-63ce8f/2d-7a9063/dc-7e9864/4f- 5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92- 10345d/f8-73a5f2/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/50-f1e180/e3-082b89?ver=2.0 .https://microsoft.com/N...../.....!.K .R..{S*^...5._b.nY|o.....A..Eo.....}N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43fb384703621b6c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.590549127191572
Encrypted:	false
SSDEEP:	12:Uiu/hWDxCEbBx0RrvntxRvepQNmiu/hWDxCEbBx0Rrv5iBRvepTJ7:Uiu/hWcSudtxRmSmiu/hWcSudWRmtp
MD5:	4F9C1BBA93E169F9EAD793005DC79611
SHA1:	DD45A93CD662EAC3EA04B44941B18BE50F2E3476
SHA-256:	EED52AB81C379D98613953E722B545AE229B15D7D399114F5B141D54D715153A
SHA-512:	80A3446BCBE1439B6F381F7D870EF8800D31B3CAC3C578D7410A658043793BE2D2D3DB831F4011CFC3A882F22A516532A2908792A4F06F5483B49D14BAC74CF2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H^.?...._keyhttps://lptag.liveperson.net/lptag/api/account/60270350/configuration/applications/taglets/.jsonp?v=2.0&df=0&s=store-sales-de-ch&b=1 .https:// liveperson.net/.h..../.....+.....6W.....\Oy.se...Ml.1@;....A..Eo.....A..Eo.....0\r..m.....H^.?...._keyhttps://lptag.liveperson.net/lptag/api/account/6027035 0/configuration/applications/taglets/.jsonp?v=2.0&df=0&s=store-sales-de-ch&b=1 .https://liveperson.net/V...../.....2>.....6W.....\Oy.se...Ml.1@;....A..Eo.....b.bM..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4897c6f9e2ff1f8b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	104456
Entropy (8bit):	5.793263367051172
Encrypted:	false
SSDEEP:	1536:3Mq8ufpWmnTL1cK+C5sJMpV9r/3Z0p+glGP345/dNsfOSj+qkqU:cYj19+tJMpV9NI+tP3YVNULj+DR
MD5:	1F79AC23CEB67C715887D9B12331CF64
SHA1:	A451E8A1E3C092028D18A50AB0A15BFC984E8A9C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4897c6f9e2ff1f8b_0	
SHA-256:	2795DF99711F4F11E874A810DB8433D76E2AAD2AC937E06D4DE0637BB40B50C3
SHA-512:	8ED01015FB4E42ACBD59DD9ED2BD5DE8F0FAF18CFC36E47FB0ACF10B4678D190FA20A910760025A4DBE5F13E1835B2EB8F3FA7581323B2535186B6425340221
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...>.....9CB476A01AEA3707EAC2340BA275CBD69E424FEF563DA089779990F822F35BC9.....'..v....O#.....f.....d....&.....`..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....N.....Q.@z.:.....module....Qc...a....exports...Q c.k.v....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa....!...I.....@.-....HP.....;...https://ajax.aspnetcdn.com/ajax/jQuery/jquery- 1.11.2.min.js.a.....D`....D`....D`....]....`....&...&..!.&....&.(S....&..`8M.....L`@.....Rc.....8.....M...Qbf.....c.....Qb.l:.....d.....Qb..p.....e.....Qb:I."....f.....Qb:.....h..... S...QbNb.....j.....Qb:.....k.....Qb.PV.....m.....Qb.:\.....n.....Qb.La$....o.....Qb&.....p.....Qb>.....q.....Qb..9i....r.....Qb~.....t.....R....Qbf.!U....v.....Qb.#.....w.....Qb.n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ac2f448771ab57b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.52505116443036
Encrypted:	false
SSDEEP:	6:mCVYL8uCKxwVOdD2DOMv/gGmXu5df/CxJWom4vlZK6t:irbwVgD2DtvgXgfyWHyT
MD5:	3B64C2A0CE5D9C2B74E798F7BD337E06
SHA1:	2E6460F3397E7390FCD5F1BEF3F04FEC715360C0
SHA-256:	41CBD79942449BDF9D85A6219B6704BDD488A41A917812C878F7361ABA06DBFB
SHA-512:	7CAE112F3F625CAE97740DE9794FD1F4C4857BC797793CC97D00E0D1B155454E8ECA7B1AD062DBC283BB4E2728E008DCA6C9F3537B20EB7310A83E2D24AB9E 01
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....f.;...._keyhttps://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1 .https://microsoft.com/.O..../.....*d..,.....cP..Tl.*...A ..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fa8d4ec20662298_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	269
Entropy (8bit):	5.647571155129393
Encrypted:	false
SSDEEP:	6:mK+6EYcBB8LjFke/BDWDQICW0ZSVCszg9vev/gye8qbWPBK6t:dnN/hWDxCxqCsUveviqz
MD5:	73FBB050393E9E19BDEE5E63D5C30465
SHA1:	351422BCF0B1D36F62DCA313FBCB097A1B85C45F
SHA-256:	45220A0224C1A0FE9C163611AFD48387D0EB2BE11FCB8B86B1308682BFEBAEDD
SHA-512:	C22E17C70911B4F6F06CBFAF1A623200396AE36F65F6F371211025C5B145CD3A080EAD242A3004FA40D49D323C147BB8E8E8A0465ACF7B2EF97021A7E4B5AC7(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....)d...._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/setting/accountproperties/?cb=lpCb69539x21797 .https://liveperson.net/Q..../... .....%2.....[..j..5x.8..+..>....S..=...6..A..Eo.....,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\50030ae951750ff1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.627790758918637
Encrypted:	false
SSDEEP:	6:mOWVYbLjFCsWLqLUqxzZUqmvl+/gJbc25fhm4mK6t:e0n3WOGvlPI2Vkf
MD5:	8207A522E707BE8C5CED5A3F7320864A
SHA1:	274266C7F75160C27214A93E357D9BAA6C609BF8
SHA-256:	56CE822E85AA08E3F76809CB8A21E08D804B9D3B32AD740832A384B34212A823
SHA-512:	758D08CA9FEB39F31926451392B951E9B2C21420617A1F1707DB8C8BB1D3393ABA9CACFD39EA6DFB2C2595D6C6DB6E7ECDABE3D967AFBA6C7A852CD3C1964 3D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....~....._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/UISuite.js?_v=3.43.0.1-release_5028 .https://liveperson.net/.~]..../.....R.....\P. .yV..L....8I.0%.U.1..T.....y.A..Eo...../.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\547db41b413d52f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.598536382979707
Encrypted:	false
SSDEEP:	6:mXYGLTDQyKfZ+OsFRzh+UXVZOfzKDi+HgsOZV+kqK962Sm4Q/ZK6t:yDQLsFhh+UF+KDiyOZV+k596jmnT
MD5:	AA02D1D922ED0E423434850B4C466075
SHA1:	24AB037AE0E449D00913303BA0494725AC23E0FA
SHA-256:	396D22DB69418EB34E4979DB914487FE00705934DFB5C9036ECD9BEB67A886B5
SHA-512:	63AC57E4F0BAF2684CA59689C5EF9C8FA87C05B8B19171D116196BB6FF74C9CC23CBD82FF682F68CFD45F08F81CCFE65D62DD01607D5942F9B0C9A210D54DF C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/78-6f121b/94-3cd1e0?ver=2.0 .https://microsoft.com/.).../....."......!.$|p6.g..OG."A....-.o.d.3).....A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\560eb50eaa655bc7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19410
Entropy (8bit):	5.993114566088203
Encrypted:	false
SSDEEP:	384:CMhMRk8lZ6HVcbJvL8KlOTppI4x8qKva1n:3pkTpHlKcn
MD5:	B0E39C443929D21519140A98C8886E89
SHA1:	E75D05EA8C96C80762FCE214C214546D484EF7C0
SHA-256:	4F06933F3253753B43DF99890A63468AFD9F7C00B7D06E369C04FC444B5CF157
SHA-512:	89C005786D1E1883AD0A8E97D6BC960A6A030E2F0242E327D452BE43A8BB411E53E9C68224A3925FA4B63F512AEAED150C479AB681C227B50203C7BB963C930
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1 .https://microsoft.com/^...../.....#g,b.v.U..c`.^...h.....A..Eo.....>.m.....A..Eo.....'.....O.....H.....i.....(.....(S.0..`.....L`.....(S...`.....L`.....LRc".....Qd..-[....requirejs.....Qc...2....require...Q.@...Z....define....Q.P.( .....__extends...d.....I`....Da.....(S...`.....L`>.....Rcf.....*.....Qb.:\.....n.....Qb..9i....r.....Qb.hR.....s..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5775d7ea69d43f30_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.674945240572063
Encrypted:	false
SSDEEP:	6:mE9YGLTDQyKfZ+OsFRzh9FNTHKDplHg9COhmZDG9kAMDK6t:nxDQLsFhh9FNTHKDplYnh++kf
MD5:	1040303F0A71A3277FAB44B32CBE5B4B
SHA1:	DE6EDF2FFB859447A856EDB02D332BCD45672D62
SHA-256:	059EECE96BF184C228ED29C223BC397C5A57CD84FF304964F31AAC7FB97D013E
SHA-512:	33A7B503A6906910A0B8C0EE1F78AD7EE0565BA622B95EDE19922C25F8CA06E6B8115862891A54BDDB3B56922AAF5CEFE9E5DC1ABCB5C71390925D3286727B C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;.M...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/b7-5b4bf5/a4-539297?ver=2.0 .https://microsoft.com/.(.../....."....."....6,.#.w..s.....BF...h...A..Eo.....*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5884bcf8588200e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.458599997032534
Encrypted:	false
SSDEEP:	3:m+lwOHv8RzYLLI2P8EfsAIsUVDFYtRL//lHC2/kLPxEmor4TeGoMm7lpK5kt:mXOkYL8YuD2DL/g2/k19Ve/XK6t
MD5:	FC88D55A4ACCC4A6C4C44DEA3CC0264A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5884bcf8588200e3_0	
SHA1:	49FF9EDF6A60779C0CA03C7B23A9A4FC648E8319
SHA-256:	908EFB081075F6D07F2E7108C1A4881EAA59995C7C53A978B7AEC2BC153E2299
SHA-512:	E2EF5B51D349714A102051DD38066268AF51C5DCF7FD130A67A0EEA2853A6F8C69D5D48669F6057A823E788235E533631DB5DA9F64879DD303D38A898F4B229C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...[k.k...._keyhttps://mem.gfx.ms/meversion?partner=Surface&market=de-ch&uhf=1 .https://microsoft.com/o...../.....H<.....H.hO.h...J.+..Z.....5...!.....J..A..Eo.....&.O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59c8294b97fbf34c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.371368366439327
Encrypted:	false
SSDEEP:	12:BA3aFhVKiKACt6goOvHOXIUX3NC1Ngw9jMuw81vcDY4jIv/mV:B6Ch/Ck/O/OXJdCrMup1vcp8va
MD5:	19E7865A28C445DB359388E1EF1D14B0
SHA1:	49C57976E644016B84E47E818C68A078C3DCBAE6
SHA-256:	E6D678E5531334C0CEBDD09CEE65200382777E44322803F289E0E84F014E6DF9
SHA-512:	5D0C496304AB87B452ACA1B0AE12FCEFFB12C3F2673A5EC07260A2DC798B30BEA2E757FA86FAFA498EC71D252B2467777343FFFE247F3F38B9F48AEBD7081ED3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3.V....._keyhttps://statics-storeexp-neu-ms-com.akamaized.net/store/_scrf/js/themes=store-web-default/42-ea0369/2f-63ce8f/12-f9cbf0/2d-7a9063/8b-b7e929/69-f75c22/ff-8418b5/8f-165e61/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/e1-c35781/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/b2-7087f0/ab-30f5b9/91-97a04f/1f-100dea/33-abe4df/fe-a5cf09/e3-082b89/85-7f00e9/4d-d4cd89/1c-e1eb2b/7f-25cd1c?ver=2.0&_cf=11242019_3231 .https://microsoft.com/...../.....<.....y..{qm`....k.b..|...Q.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a0d44391b90ff78_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17753
Entropy (8bit):	5.6380939658171885
Encrypted:	false
SSDEEP:	384:LfvVszKqbg0AXutnKiwm/1Cgo8oTl6AJ7Zwc3lWP:beBmutnKiT/rodl8cv
MD5:	7C7A5D61C94E4DDDC659E3C8281E3BEC
SHA1:	A509F139C72C2BFA3B4041FF19F7FD614052D5DF
SHA-256:	FE2D03D3D5C66B1A08D3766BDF6A46E6B407D2373DEE1E73FAAD15E61DFE2665
SHA-512:	9EA0ED7680F9EDEDCA447F76E72105DBF16E463AA3981084C5094593A4213059AF45F543345F3D3375697202AE6ED6C0BEAE5D58FA1BE21BCAE6643ED4E0016
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i...)2F,...._keyhttps://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.js .https://live.com/.!.../.....3.....i~....F.-d.....xN..^.. ....A..Eo.....A..Eo.....'..C....O.....C....\.....(S.....`.....L`.....L`F....(S.<.`2.....L`....I..K`....Di.....%.....g.....g.....g.....(Rc.....Qb....._iY.`....Da....h.....b.....B...@.-....`P.q.....R...https://logincdn.msauth.net/16.000/content/js/MeControl_cfDm2fEwfL1YuSiw8j6tzA2.js..a.....D`....D`....D`.....)....`....&...&..A,&.(S.....Ia@...X.....Qb....._Du.E..A/d.....&.(S...Iad.....Qb~:....._Bd.E.d.....&.(S...Ia.....QbN..1...._BD.E.d.....&.(S...Ia.. .....Qb*.....E..E.d.....&.(S...Ia.....Qb.U....._BE.E.d.....&...(S...Ia!...9.....Qd&?Y....strOrDefaultE.d.....&.(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ce38a7727ba7508_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.462426323058121
Encrypted:	false
SSDEEP:	12:PjDQLsFhhBoK7uCOXXc8HNC1Ngw9jMuwLmzlKDnY9xD:L/hHKCOXXc8tCrMu0mzQDY7D
MD5:	F5752ACA13DAC504F2FE063BA827C971
SHA1:	321A48002A32258A14B98FEDC3CBFC67A6713D95
SHA-256:	763DCC4EFF8F7E4E3352DA848814C393395173A978F8C1DF14AECAAD3C2AD9B0
SHA-512:	D79563811CF644524BE6A516CBFFED4352962CC680A03BA9560FAA142A2CB306AFF3E6B72C9B74E18D0F87941F8CFBB6CDB0B8C415B8EF567D8E8DA3319E32B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ce38a7727ba7508_0	
Preview:	0\r..m.....,..k...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/50-f1e180/e3-082b89?ver=2.0 .https://microsoft.com/...../.....".....&.... .8....=.9.!.H..}r.A...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5db4ad138a5b020e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	686
Entropy (8bit):	5.662413877212545
Encrypted:	false
SSDEEP:	12:oqnfUxPSf/CHMtvS+n+jXldX5qqnfUxPSf/CHMtvT1XNdl7:oiUiS24dX5qiUipXDl7
MD5:	8B1975A007D92AAB631D6F50E9C66109
SHA1:	3923C300F275B1ED2539392FBFDD2B0D869455C4
SHA-256:	38A77DE1C4EAF0F64055730CD25E8C6819E5742045652554915C01DBB5197F72
SHA-512:	A76A3C7E2BEB306F9790BD613B1014F587D20922040640FC4012B8DB610A17F19710C2896A13EE49ECA141DFD4206CC2F8C3CA87DE93F3D50A1CD98FA3CCA2D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{Z....._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.12.0.0-release_5037/storage.secure.min.js?loc=https%3A%2F%2Fpublisher.liveperson.net&site=60270350&force=1&env=prod&isCrossDomain=true .https://liveperson.net/7...../.....e7.....Lju.~.T...h.....O....l.,_k4|B.A..Eo.....A..Eo.....0\r..m.....{Z....._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.12.0.0-release_5037/storage.secure.min.js?loc=https%3A%2F%2Fpublisher.liveperson.net&site=60270350&force=1&env=prod&isCrossDomain=true .https://liveperson.net/yER.../.....P.....Lju.~.T...h.....O....l.,_k4|B.A..Eo.....I..#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67ff2080fc2646fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	454
Entropy (8bit):	5.390530329850831
Encrypted:	false
SSDEEP:	6:mKIqYGLTDFbDH2QshaBokqPSuwykNWXeFODOtyIgoGV17vKDc9/gXW8ovP49bK6t:CCDFbKQLEPjTxTjoc1rKDEGVoHQN
MD5:	89036DDFF3AFB4ABF4DF81970A78BA02
SHA1:	EEA33CAEC3315AEB9EA6D15109E948B32139491F
SHA-256:	5C821FD5C57A4221FAD34A97CD0AB2471C866739E1F7315E56075A269E6B622C
SHA-512:	EADD4EC50E1C2579E76F0D9955F20D18B585B80394ECCAF3E4B5A86EC3643F076DEB01F3F190D009AF40A063B0B66245086AD49B3BF2C4BE556265F634A0D2E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....u.q...._keyhttps://www.microsoft.com/mwf/js/MWF_20201028_28422223/alert/ambientvideo/autosuggest/button/calltoaction/dialog/divider/feature/glyph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/logo/mosaic/mosaicplacement/multislidecarousel/pagebehaviors/rating/skiptomain/social?apiVersion=1.0 .https://microsoft.com/.d..../.....\..Wp....9.ad..q...fJ.....A..Eo.....yDq.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6913b319d60c7157_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	396
Entropy (8bit):	5.4960805035459765
Encrypted:	false
SSDEEP:	6:mGYGLTDFsnuq+oK5gBoPsdbGnddnN5QHXsCAHfetwxvKDB/g+Nlf3y3o3BK47thD:bDF2uqf9jlnPHQHsHfHKDBhII/t7
MD5:	61DDF8F2622E6AE5E32FC2C86017EC57
SHA1:	FD421A4F74E3D9E6484C24E7BA361B684A8DF945
SHA-256:	ABA4BCFDAEADBC03E4B9686ED05244312C2AFE836D430A3D3AD18BD898BC355F
SHA-512:	3E80E112FAD9327B948B1E2E426817C4074119236699722998E796949D15589CF9962FA5796D644ED5E218FECE8BA0DBF642DD640FD24345FA0FC10BA7E0CEAE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C9y...._keyhttps://www.microsoft.com/mwf/js/MWF_20200416_22921869/actiontoggle/alert/autosuggest/channelplacement/channelplacementitem/dialog/flyout/glyph/heading/image/list/navigationmenu/pagebar/pagebehaviors/pagination/skiptomain?apiVersion=1.0 .https://microsoft.com/U...../.....<.....l...alk..x.....:.F/..I.7k~. n..A..Eo.....Q*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6aa8f657d25858ac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6aa8f657d25858ac_0	
Category:	dropped
Size (bytes):	19401
Entropy (8bit):	5.996400202431514
Encrypted:	false
SSDEEP:	192:cM2x+1M3MlduPVey76JM2roacbJvie80nZ4ODzF1JIO/h9pJyCoIISY8qO/MKzrS:cM26M3kw76HVcbJvL8Klh+Cy8qKva1f
MD5:	80118725F9809E51236D9DC111C62B85
SHA1:	81A96A139A2ECB1A12D4D65F2CBD18127D967875
SHA-256:	CDE1A1D06B9ABACF8831A12694B9C2FEEE30288059C34020C8E42B0C42717906
SHA-512:	13C90FDEA710F4CEB9923748E87D8B021E30B2EF056179FE205661DE756AB8F2D500CF9C6ECC0BA6D1CCD3BD7E955E0D4A4DC76DDFE58D4B0ADE7AA0861C6B8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1 .https://microsoft.com/O..../.....?.....YP].4.=...K.....;.=p...<..A..Eo.....!.....A..Eo.....'.....O.....H.....(.....(S.0..`.....L`.....(S...`.....L`.....LRc".....Qd.{.(....requirejs.....Qc...)....require...Q.@Fbw.....define....Q.P.5....__extends...d.....I`....Da.....(S...`.....L`>.....Rcf.....*.....Qbf..|....n.....Qb.x.....r.....Qb..T'....s...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b848a87f40dd230_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.563003488810547
Encrypted:	false
SSDEEP:	12:yW7RPAvKelGh6AqLoW7RPAvgAYh6Aqv0T:yWVqK6Gh7qLoWVqgAYh7qvY
MD5:	78291F5AAF82775FCAB97B5694DF66CF
SHA1:	157CDDB8F24C151994844C1C0F2BEFFC7838E311
SHA-256:	2619778D95BD6D65E211C1A450501BB2B3B8DB18BCFA9E398F30E75C425F2E2B
SHA-512:	2A5756E7828DCCC7CE354BA03492E6AAE0339030A69AF26226451732439FE9C75501F7F7B9B31608A8BED1FD623DD3FEF50DFB85EB4C6762ECE995E1E683B1BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....ZcW...._keyhttps://az725175.vo.msecnd.net/scripts/jsll-4.js .https://liveperson.net/...../.....v$.....:....XJ.2.x.b....K .ZQ...Cj..T...A..Eo.....A..Eo.....0\r..m.....M....ZcW...._keyhttps://az725175.vo.msecnd.net/scripts/jsll-4.js .https://liveperson.net/...../.....<.....:....XJ.2.x.b....K .ZQ...Cj..T...A..Eo.....7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71f52630121e1252_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	295
Entropy (8bit):	5.544249614403217
Encrypted:	false
SSDEEP:	6:mDYkEX3LEE3RFGFRzVKqYhgLBORFz8DSn+v/gi0l4bilbK6t:iA3aFhVKBcDSn+Yz
MD5:	33BCFD15B931697518BD5C8521413120
SHA1:	3A90AE354B4A428B2BE070694FFBBDD92496005C
SHA-256:	7B1CB45ED2B2883ECFC7CB8B28BE16B18205179BF0A96AE4A4F63D939849003C
SHA-512:	A58BD45341360E1DD49BFF8129DE5A6989D952779C80276D25DE50F50B63B20DB111D4F867F20FE64E23461522B8B4C37714B30DFF44978F744C43ABB9C7FB6C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4S.j...._keyhttps://statics-storeexp-neu-ms-com.akamaized.net/store/_scrf/js/themes=store-web-default/e2-ed7413/1e-fd610f?ver=2.0&_cf=11242019_3231 .https://microsoft.com/7...../.....<.....k9.4.:..2e....}..n5.fo.Y..-...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\72090e93af2b3d0c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.66371103328985
Encrypted:	false
SSDEEP:	12:ICnN/hWDxC8mxHvvU7KZCCnN/hWDxC8mxHvMa/1:zN/hWc/vBZN/hWc/Ms1
MD5:	B4BC266BC309A6EA543DFCE49F60C8EC
SHA1:	B7174F21B2C3EF76148EA80F08B0DB032275BF05

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\72090e93af2b3d0c_0	
SHA-256:	1EC4E838130F87E84D498B489EB9F525FCA336E8D5E2CE5298A58CDE55E6A34D
SHA-512:	85E54C594EBAE545CE8D2B1A2C3F252EDB286250B71D18246BFDC2AE2F2C801B32FFFACC7DDA85CF4728DD6C4DA5D88FCD2732671459AD57CD113F9DE69C BA6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....".C....._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZonesStaticCB .https://liveperson.net/.j.../.....2.....@...u.RV.%.b...k..,V..... ..A..Eo.....A..Eo.....0\r..m.....".C....._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZonesStaticCB .https://liveperson.net/).....?.....@...u.RV.%.b...k..,V..... ..A..Eo...../.....A ..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73b12b162f1cf8a7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	362
Entropy (8bit):	5.876624178069644
Encrypted:	false
SSDEEP:	6:m9YL8vc7Z6ckVDJgH8PpeentbK6t0vs9kUZScEyCOIpeeM:X0c7Z6cKD488SrKs22v37RB
MD5:	6A170E2A63EFC157BB8E0F4A3CADE028
SHA1:	02503A9A70F47E8EF929C65B92A6D427F8DB5493
SHA-256:	78AC335CC2A9883C9381B8065E451DA480F2FE966D9819D183EA1199C9F436AA
SHA-512:	1AFA5F36DEC5427305B4082149DEF54C9DB55D468A4DA3FA00D36D5E131FE5A7074CC7B8D8C9C53801F3831CA978E444A40BF67F022B64AD147E7163281F29B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.20321.2/de-DE/meBoot.min.js .https://microsoft.com/{}.../.....$.....^.i8.....C>.fk..;.%.M";.`y..L. .A..Eo.....z.....A..Eo.....{}.../..o..012386C4CF09BDABF73404E0F2F6C8BF481CF5749798F7F3F06E48E86D17EF01..^.i8.....C>.fk..;.%.M";.`y..L..A..Eo.....A. $L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\781980b07f1bb38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8256
Entropy (8bit):	5.479127074173347
Encrypted:	false
SSDEEP:	192:YxZnQeH6AekifXZBrE6Vay2Xg4KPYET4XQ:YxdHuF8p/QdPz0XQ
MD5:	31175C9DF9808A4EB00270C581F71B96
SHA1:	8A5B9988FD1D96D2B89A4C00A58C46697EDFD18D
SHA-256:	D07506E67D5D790F6A4CB5B48302A31B92E1B3CDE37ABDBEFA399B0D765CA40A
SHA-512:	DC337949840B4DCA1BEB248E862340684450A7B6F2982CB0F1BB146EFAC195FD4E8521E21D5B9E1C4A55D5E096A493751A85716B4E9952AAA337C3CD2EF5869
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...0.v....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/Q...../.....K.....5...a... ..S...s5.O..8O....F$.\|3F.A..Eo.....A..Eo.....'.....O.....\.....(S....`x....dL`.....L`.....(S.....Ia&...m....,QiV.KX....ShowSele ctedComponentKeyPress...E.@.-....hP.....\...https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4a.....D`....D`....D`..... .`>...&...&....&.(S...Ia.....Qe.....ShowHighLight...E..A.d.....&.(S...Ia....(....,QibS.8 ...SetRightSideNavigationMenuHeightE.d....).....&.(S...Ial...M....$QgB n^Y....SetRightSideHeaderHeightE.d....!.....&.(S.....Iak..... ..f.....u....$Qg.....ShowSelectedComponent...E.d.....D&.(S...Ia....9.....d..... .....e.....-....-.....Qd.-.o...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8548771546cff460_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	284
Entropy (8bit):	5.687262203526755
Encrypted:	false
SSDEEP:	6:mIPEEYcBB8LjFke/BDWDQICACJe15SZlSNvH+/g8o26B8H4VrK6t:ejnN/hWDxCACkeZSvCo26B8I
MD5:	BE43EC4A7E57C55705EFAD17319186BC
SHA1:	7E86996EB5532226847341F1AD90FC54902842E2
SHA-256:	F7EDA61D37E419C177FA42A06207C2D3C6F2A00A68FBD236F1936F08240CFF1B
SHA-512:	4C02D48C83809AB814FBAEEC7956B36BB27687B0F325C19A73F5DAEA5AA32AFD816EDB52E73239B610053F0CBFF8CFA7C8F3FCC52479ECFB7ECD2021010E6 66
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8548771546cff460_0	
Preview:	0\r..m.....l...._keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/engagement-window/window-confs/1644511330?cb=lpCb73511x47724 .https://liveperson.net/.)b.../.....T.....k..`.'n.e.0.D....$..~X.k.A..Eo.....@`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.825634307380487
Encrypted:	false
SSDEEP:	6:mXYI4McTDsJegDmAovtga1TrlEflgK6t7KPIliLUoP2VTrlEX:e+TDsYgDmvp13txqi0UoPC30
MD5:	F54EB1A229F2F80C109095D845BC68CB
SHA1:	773C90FCC0009E35A7311C981A201617CB9E8E98
SHA-256:	13362C6D47558C539E2F339AE16627FC790503D352588F4275C2A7D3D04BD060
SHA-512:	B9E6B000931955A0CDFBEB1120AB86EC56BFC64FD08A83AEBC91BF0FCF43697BBD39F8C8ACF2BAFCEB26EE9FB0A8E8B6D5C6EFFED199B98AB27C2066E66FD1A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/...../.....<.S....l....*.W.U\..E?`..r.A..Eo.....+.@o.....A..Eo...../.p8..4B9DAFE5A7B03A95CA8C8B468B7725467B7841978F4424269367E2E99E9C9AEB....<.S....l....\*.W.U\..E?`..r.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9299ed2c4c7a3963_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	5.747369407839822
Encrypted:	false
SSDEEP:	6:mttVYGLTDQyKfZ+OfojOW7kXWFRzhGP4BOfzKDB+/gyJF1+dahQ/hK6t:AjDQLf+5KWFhh8KD0F7+daqT
MD5:	4C3023DA55E8B47E319EA646A2762D06
SHA1:	7DA1E4DFF9AC8A85DC530D04AF020E62B1746A7D
SHA-256:	F3E6B816186CB451E29EE8ACAD2C2F97B09B39FF85E745C458DABB02A270309E
SHA-512:	0B295B6A729772882F894F4314D3E585441748FDD3524D611736803C06B9B677679A58E7B0AA02C181B8C30837ECBCBDB480053ADE562767AEA7FA47AA23811E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.Hz...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-bcc229/94-3cd1e0?ver=2.0 .https://microsoft.com/T...../.....'....3.hi!.....QF.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9a5575bef7c495dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.897507140787921
Encrypted:	false
SSDEEP:	6:m0iYGLTDQyKfZ+ONNKM3IGRWm8SIyD+ogEDU0Jf3797K6tonTM6jwVs2xYggTR08:D6DQLjl4mxIyD+wwM3n56jwcJGUM3+
MD5:	0004BC4D59EB7DF0A4EDD0015DB4D35D
SHA1:	A52C66C801B48E033E1C65ACE68071B1383661E7
SHA-256:	D595D225350F601D528ED5223BE111660B026DD033A96F1B5B28EB3C1911E4D8
SHA-512:	0425512D9E5A40E0D20E736D00E1BED9C6A3A304545851B405E5C4D831221988508173D1876DE86C4296EEB89CEFAD1D55BFCBF2BF1E7391024D14D1E02921E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k@...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.js .https://microsoft.com/h(.../.....".....'|.....C..j.,c%X.i.Y-....F...N.A..Eo.....8.b.....A..Eo.....h(.../.0x..37DFF8F4DD16843074A538BE0BF515B9ABC80D808546594A0BA15EE6AEC07545.'|.....C..j.,c%X.i.Y-....F...N.A..Eo.....d.;L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b180e6523891105c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.489960387263397
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b180e6523891105c_0	
SSDEEP:	6:mc/gEYyK08f2yDrv/gKUeR3vY934hDK6t:/vKjf2yDr7UO3vM8
MD5:	BB2C5E97154A49049CD5B9A09710B6ED
SHA1:	1E5230C2A9F4C32FC233A6F39D496D20178CC862
SHA-256:	619113C3E84CBDCE8FEEBF0C88AFAD2A7F15B20FDA34699497CC816BFC552FF6
SHA-512:	751412912160D12083EE703292932CEC75FCC84754EC2CD80340B63275D41EC43B3392806555C1451DC0C6C39D64826D9253B9D6C43729DAC938ACFEE9914703
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....2...._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.9.1.min.js .https://microsoft.com/.:.../.....sJ.....~."1...W.9.w.....C.oe.7.GS^.%7..A..Eo.....0^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7b12560f839e230_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.580554523637064
Encrypted:	false
SSDEEP:	6:mr/VYkEX3LEEkM3IGRWm8SIyDwd/gZY165F4IbK6t:8lAkMl4mxIyDVYUFJN
MD5:	885FB4FF7F3F94DCE68F70DA7761E841
SHA1:	A8A63EDD06DB10331A7EA1F941B62BDF7B36FE4A
SHA-256:	E941A2C6A65422DD553205DE4777FACA7FD4D46C848489EE4B4E888706AD669A
SHA-512:	5B47A87C0AB9776BFDAEA2036158D6CDA52595AD640B085519AB72E4820061AE4060644E732695713180479D04E5B61F4A2B767A0F173AD9B5A46E9D61669281
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://statics-storeexp-neu-ms-com.akamaized.net/_h/46c44584/coreui.statics/externalscripts/jquery/jquery-3.3.1.min.js .https://microsoft.com/...../.....<<.....\.R.....x.4.N.>.%..WZ.)...A..Eo.....CQ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de5c13cb0b3aac41_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	159680
Entropy (8bit):	6.353500205983787
Encrypted:	false
SSDEEP:	1536:M8n71tx6MFUoXYQ22GFYWt4OafB6DeM5xY3Wu0sFCzF4v8a3vc/3QFyHMzjwhsWy:M8nhT6MhYcGFX4mCR3Wu1Ff3Ogy8tj
MD5:	CB015A4C82E972F73D5E4F18E3AD9131
SHA1:	4B72BEAE864FB0A5024B0E2DB380F455B484F4B3
SHA-256:	B7B34DF1503D594F5BC8779C516B370A83E2E877320A2A7A20161FA91BFB45BE
SHA-512:	148CD44AA84E8E4E8644182B93D55CFCFC66E7D68581330B5119748FCFFB788954D02B864DF137C977A30C2615353E1FEF85C059CD379677A7B9416279915B31
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....V.....012386C4CF09BDABF73404E0F2F6C8BF481CF5749798F7F3F06E48E86D17EF01.....'.;[....O)...Hn...{^1.....8.....<.....<.....d.....h.....(S.H..`L.....L`.....Q.`2..t....MeControlDefine...Qc.....meBoot.....`.....M`.....Qcb..0....exports..$Qg"6.....@mecontrol/web-inline....(S.....`.8.....L`.....!.Rc.....Qb..o.....A.....Qb.5.....s.....S...R....Qb:7.^....p.....Qb.k.....w.....Qb.....T.....QbN:.....d.....QbZ.>.....e.....QbR.4.....!.....Qb..S(....n.....M...Qb..m.....r.....QbFUNm....U.....O...Qb..,.....,.....QbR..N....f.....Qb..8....h.....Qb.V.m....F.....Qb.?q.....P.....Qb.vO.....m.....Qb.m.....C.....Qbb..O....R.....Qb.S|l....N.....Qb&.....D.....Qb.....o.....Qb.....c.....Qb.....x.....Qb>..K....y.....Qb..z.....M.....QbfuS.....L.....Qb..S.....k.....Qb.t.....v.....Qbn.8.....I.....Qb.IC.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4b92c98510f85ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.646155932922844
Encrypted:	false
SSDEEP:	6:m0+6EYcBB8LjFke/BDWDQIC8mKVmLPVQTw7VNvKZ/gUy3gxWap/SK6t:J+CnN/hWDxC8mTxVNvgy3gUapM
MD5:	6C443A249529A6DF452AE95F16AE8D95
SHA1:	4F12410C2593F84D4D072432D778B4774ADF5B21
SHA-256:	E32D2C298CAE5FC2A1C63C01358C64BE3CC07C37B98EBA1D237C4BE07C7846A8
SHA-512:	457C78D8834E298BDE5227DD354AE443C4726D9965A8B567FA3CE5E8CB83CC23899C341DCB4239F1FEFE0A7C98581527DDB162B3128A82252B7EE7651149B56
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....keyhttps://accdn.lpsnmedia.net/api/account/60270350/configuration/le-campaigns/campaigns/1644274130/engagements/1644512430/revision/15604?v=3.0&cb=lp1644512430&flavor=dependency .https://liveperson.net/..^.../...../S.....J.Q!?"..Ek.;g.X.....|...z..n.A..Eo.....].c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4b9b26cef092fbf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.607397725861536
Encrypted:	false
SSDEEP:	3:m+lbGRa8RzYLLI2P8kIRgEe0sAIsUVDFYtRjvt/lHCZltkAVUI6tY6GfGkRmLtlJ:mcGRXYL8UdD2DjFgKA96dGfGhLRK6t
MD5:	224E20F97A49E59D5AEA80A6EBD9C33E
SHA1:	031426D887555C480DAB231BAB9F1C7F4B0CF174
SHA-256:	ABEEE57D11B16EAB80160B62BD2C321A491B2B864AFD778CE04107D40181BB8B
SHA-512:	4CF8D2B25A718C3BB514393DF4774B01FC8939C74D5DD9A5F7B6ADB51E5BA8C3731600C83452DBB0E22FB69BC597940E16EC1C9E9288DD71065F4F5FA9938FE A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1 .https://microsoft.com/...../....."........t..-...}~I.1..?D.=.#.&.6d..A..Eo. .....9{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.515884627879926
Encrypted:	false
SSDEEP:	3:m+lSxla8RzYJb9yKIf8QPKxQBHWFvDFYtRLKF/lHCSN/Xyq5EzDHz4msVW/tpK5M:mfYyK08fUH1DuFgC/iq5Efzr0QK6t
MD5:	652C1A7E407B1EF065242B70686681E1
SHA1:	67A1699FE78144631DAD78FF8707EB9F189C3E63
SHA-256:	FDAA0C8C354DCA3C15F9060AD3C36BC3CEF244790D44A5A00AE1BA1D45B184A2
SHA-512:	C1F3BF18ACC86A397ED328F8288B30F295721A2E9DE2E088B1E4E00946D7C2FE6ABE6600DACA49C5E21D6390BD6B80DC42CA994115D7B4F80FB6C81956246A 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...T....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://microsoft.com/Z#..../.....f....cB..cWhT..6..(..$....G..A..A..Eo..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f50f7e3b3653a201_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.740160488749379
Encrypted:	false
SSDEEP:	6:mUXYGLTDQyKfZ+OfojOW7kXWFRzhoHIQFYUHA+CTyJyS/y6jKDO+/gLtn3mKRK6t:VzDQLf+5KWFhhoH3FiTTyJN/HKDPY
MD5:	C2080A7A1DA08CB558E54775A9AFC0CE
SHA1:	088431371A5E32B8E06C971468512C9288EEA3AB
SHA-256:	3AEA873408780610B488983EEAE5F41661D8F416C8D0BD8CDEEB480493F25C73
SHA-512:	C979DB0A711C7A2F67F00B21EB2B9ED17DA4AF6372A47FBF06A56307E6F8832B93B8D3078F2C14D56B37A8000E0396842B0931DC3601C585C4220C9E12A86BFE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'^Y....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-6ade99/ff-dc7b13/2b-b6ab60/8a- 91655a/28-8f59e1/71-4da314/58-f3fc85/d6-6e76d0/e6-9d6ac7/1a-3fe6fe/a3-aff1e9/cd-8ce651/f5-7e27a5/7a-3277aa?ver=2.0 .https://microsoft.com/._..../..... y.&{....K...y.(....^.|.\.A..Eo.....B.C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fbfb01c217345625_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5992
Entropy (8bit):	5.806919461511644
Encrypted:	false
SSDEEP:	96:LS7V1slfdQMiEpGMyr7CBAOB/xm5+44gHZFzXLU/4Y8PPR/yfAtvMw7:gsl1QjGGbBOB/x+FHZFz7U/4Y8PPRKfo
MD5:	E54BCE757526EB5109118A52F5DE58EF
SHA1:	9305C0E2CD9FFB9BC84E30054AB5949CBFC452E2
SHA-256:	1D031FA66AF9BF9D40A3414F96B7E5B4E6E4438631069396DF11A6D7D61472DC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fbfb01c217345625_0

SHA-512:	D302EA7BEA1AF20A576DA7C29EB5E9DD6F939E51E95AC90A38F2B14FC85BCCE63BFC963BDE36515650C39B7F9698F22BCA9D0309EFCF73302B2743B505FC1A 63
Malicious:	false
Reputation:	low
Preview:	0\r..m......x..........._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c27a4b8-356f-dd50-ddb2-9e2c834bf9c4 .https://microsoft.com/.m..../.............B..........D#[.. ..?.`.......c.M4#..@..A..Eo........-'.........A..Eo................................'.*v....O.........C4......................................(S.y...`......L`\......L`.....(S.....Ia&...m....,Qi:g......ShowSelect edComponentKeyPress...E.@.-....hP.......\...https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c27a4b8-356f-dd50-ddb2-9e2c834bf9c4a........D`....D`....D`.....Q....` ....&...&....&.(S...Ia.........,Qi..6 ...SetRightSideNavigationMenuHeightE..q.d....)..............&.(S...Ia.........$QgN.......ShowSelectedComponent...E.d...................&.(S.....Ia......... (..f.................-............d................4......d...........-...........d.........!.!..........Qd..}....ShowToolTip.E.d....................D&.(S...Ia....>......e.........-.-............. Qf.u.`....AssignToolTipToH ref.E.d.......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff3254c380ce1732_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1235
Entropy (8bit):	5.1940462129873
Encrypted:	false
SSDEEP:	24:MjXJaGN4zXk16FHPtJ8dtUUuzi19EJkuLUkI5E/9RLFePp7dSW2WzSV:M9aGQXi6OdCzLJk+UkeE1nePpBK
MD5:	35DB85A289ADAFC5DF5BCF4C2CC264FF
SHA1:	D705907F5A8B0D1F659F20EFF1B6411EC9172946
SHA-256:	C9F39F0E3DB19E01412E1350072BA7EF4D0671F996CBA4D2C0D4DDA307C80278
SHA-512:	03991DF6113E7A402B6F93C2A87DB47D5DD7FB6CE0DC57B577DE13CDE1DAC3070B87E2E6B658B40EFF44FCBC9A64216DC0421D26637216005F4D10250179F3
Malicious:	false
Reputation:	low
Preview:	0\r..m..........'......_keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742 bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19 ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645- b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1- fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9- e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0- 4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8 .https://microsoft.com/ez...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.9253656736561031
Encrypted:	false
SSDEEP:	96:dNw1NHM/alzLl1NwpJAiin3/HIRotkdsQ7QK2cNHM/allAioRfPckslP:duSaFLfuR2vNmO3K2ZaBJl
MD5:	37055C3E9EADCCBE2707F55515AF0DB7
SHA1:	8F864381C2863E3C7978E35433AC8CBD8F150455
SHA-256:	3FF633773B5F6DC218B81862254B61511CF9ADA0119C19ECD4B08B5352F89E1E
SHA-512:	51D0FD193AF07F8E725687391C7453A9633E7FDD9268418F6E148E35C5BB06D0144B6FC616C83443D7BE7300CE5EE34477643DC57901ADD41C016F4E09A16F14
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:	modified
Size (bytes):	25672
Entropy (8bit):	1.0340008479053016
Encrypted:	false
SSDEEP:	48:8pIvZXC/aFq5LLOpEO5J/Kn7UvxLluNHDpIOXC/aAqekLLOpEO5J/Kn7UJ8:C/aFcNwNLluNHM/aAMNw+
MD5:	E7D015A6EF962050B540CCD717F65815
SHA1:	C46C68DE78E75BF564787EEC51CA6EFF25559CCC
SHA-256:	48CF0EA918960BEBA75989DC3C4051F43655FF69FB6E8B2365FA8608B76B3EE6
SHA-512:	4384B2B98DAD1BB831B4E1EECA03C113961CF517AFE77A4E437A918A7DC1E259985798DB1405BFDA91D8096EF54526C6D723869131F8F98D7034834101E3CB9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	.....vPM..... ....

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):	25647
Entropy (8bit):	3.4121680256662668
Encrypted:	false
SSDEEP:	192:3DxiAlQTtN4DEX0fc6SyOxR6LADCqU5SpDC9NGMUC:T5lUvyhchpSUMF
MD5:	5DCFFD773D4EAC31C9DDC718142D3340
SHA1:	FC7143EE5AD3C0497F522C3257E6281789EDAD6D
SHA-256:	CBA5DEA41587788BA892BFAF87C487BE78C5C2FD23919B025A738D266B9D4F6B
SHA-512:	D96BD262DFBC4FB760ED421C5C0D4B9DF867B5FF062A9F3D25A79CF9F88F4FF13A01C4A7B311D07E718D04DE4071869F1BF749BC37181D8E76AE22A0FD262F0
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...c550eae4_f8e5_4883_8e9f_5bf504a94764...../.m..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....1.,.....E...https://snowtike.cf/7b6eYEN imwGy9Ma0g4XszBZLT5l2WqDVjoJ18pFUknfHAxch3tQrKIROvPuSDqQ1uYzobn7wig0r5kF3HRy2teLTW4PJSX96AKBjMhVav8llpmEfZOsxNGCUlD4pvWYF8xZb51qiG fLjKsnz7gIUTOJ6h2wyHAEeQStRu90oamrk3PCcMXBVylpIMhzXU2iS1AGETa09oZcDBf8bY5jgHOQkesK7CF6w3L4NxtmqVPvnWuJR/2MogmySibBcJaLQG Z4IN8UACq7l1V5THpfzE0hjKxktrFu9RYPeWXvnwO36D.php.....S.i.g.n. .i.n. .t.o. .y.o.u.r. .a.c.c.o.u.n.t.....h.....`.....`.....h..... .....`.....7.....7.....X.....E...h.t.t.p.s.:./.s.n.o.w.t.i.k.e...c.f./.7.b.6.e.Y.E

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Entropy (8bit):	5.235748149020235
Encrypted:	false
SSDEEP:	6:mbwMgOq2PN723iKKdK8aPrqIFUtpIwFZmwPIwiFBkwON723iKKdK8amLJ:LavVa5KkL3FUtpbF/PbmB5Oa5KkQJ
MD5:	8E2954D5BF4007D03765FF1E2D49EDAA
SHA1:	A6D3439F2D12BC349A70915BEF8474CCBBF1B7DF
SHA-256:	AE781F515DE283E6A525F31AB6490080FCB1F6C217F094C59AAD193B5F182306
SHA-512:	F37F7972FEE7BD78E65EBCBAF577CCA5A623CC65DC0FFA08FD5D72225A3949B910216C960E8C423C18E57A114C3ECF33D3AA923C9EF8F539F1321F64723D9E B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:48.391 1894 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-15:34:48.393 1894 Recovering log #3.2021/01/27-15:34:48.396 1894 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Reputation:	low
Preview:	.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):	326
Entropy (8bit):	5.186674127146289
Encrypted:	false
SSDEEP:	6:mbg6q2PN723iKKdK8NIFUtpIShZmwPIS7kwON723iKKdK8+eLJ:ovVa5KkpFUtpJh/PJ75Oa5KkqJ
MD5:	C640C3C80B711CF4943216A429F9D483
SHA1:	52D9485A694C031F9A7732DCC616DB8211B30EE9
SHA-256:	003D02FDB7CA99A67E47E096553BC20CDBE328829A8DADC03F4CDEB79B6B2B8D
SHA-512:	969C3E6090294C7C307A96F757F9EB622F643E12127D793C3BFE5FA83FAF0D76BE1B2BF5A084DE6A6AA67F0F02EC9A708C76F6D1A6DABEE1F050207CC1F8735 5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:50.593 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-15:34:50.595 1840 Recovering log #3.2021/01/27-15:34:50.595 1840 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
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/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKlcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9l/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_2_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
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/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKlcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9l/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+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=","hqSRpGQ3USU2bZJsZ+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):	77824
Entropy (8bit):	2.739822978088924

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Encrypted:	false
SSDEEP:	384:2M+a6VKUvyO2a6wC6EcyB6O2a6fRVwALrzyI6dS73j5:F+a600yO2a6h9ck6O2a6f2ddUj5
MD5:	E9C19F57ABDD4402779A4F059FEE4493
SHA1:	B9DD77F5F12B0F4C1A9BD91CC8A7B1AA2D37CF43
SHA-256:	53AD4CF9C7931F46BAD1A0C3806C3197A661C07C10204CF2A0A23E80858FF58A
SHA-512:	6A01A4E7F71598498B07A6305B2E605F2C9BAF46BCBDD22820E73F63B0F7B3CDDC251D81CE9E639C20F09A90013C4198C3CBB3D7403D9FC07AF0FAE9FF27BC3
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):	77160
Entropy (8bit):	1.9216991026320713
Encrypted:	false
SSDEEP:	192:5L8+c+EavSwCAKA2F8u4OA+EavSwsb3ASARrAZGAh3rASxGA3fT413rACmxGAq:5w+aa6Yj26PO2a67cbyF2c3fsqCAq
MD5:	86A7EB17DF97B2B64A36B8AB07F165A1
SHA1:	C5BC2A6DFFEFC8B3D1EADD29E3AC1589A4148B2B
SHA-256:	44D85526BE7E667FF0461743FB2866E4FBBBF14668C710BCE2EAB774E96E1100
SHA-512:	7601737FCCD579C34CE14A812AD5EE1324477C8BB3AB46461A396B1FF1C86A994FB761E27E4FB8440FE2396C366319D080F8B170B6F1D96166B03745B474D08D
Malicious:	false
Reputation:	low
Preview:	.....A..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.270446564329367
Encrypted:	false
SSDEEP:	6:mbUFN+q2PN723iKKdK25+Xqx8chI+IFUtpIfSlWZmwPIfCNVkwON723iKKdK25+M:5FN+vVa5KkTXfchI3FUtpcd/P0CNV5Op
MD5:	D64AFA71ECC622549D64FB059E9076E1
SHA1:	988D16E248471D132F1470B75FF7B6FF761AED55
SHA-256:	1470D991523ACEFCA12887D902A6862C68EBB6CFE237BC29B3A9AC7DCF8466ED
SHA-512:	2B7CDA8D715B867766FDDA2A97E8EEFFCC04282B4F72E277FBFA4A48B1E9C4D0D53CCA5D1F70BF3597DE4A1BD1C0E4462ECB53BBE4D05C64444F1059EDD2CDC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/01/27-15:34:59.845 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/27-15:34:59.846 180c Recovering log #3.2021/01/27-15:34:59.847 180c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.220300793252204
Encrypted:	false
SSDEEP:	6:mbvSN+q2PN723iKKdK25+XuoIFUtpIbWZmwPIFiVkwON723iKKdK25+XuxWLJ:Yi+vVa5KkTXYFUtpn/PyiV5Oa5KkTXHJ
MD5:	86081059429535136C96A6AA0D275104
SHA1:	67A88FF40D287970817B25C4D4C46B6AD0044015
SHA-256:	B8FE4BC1702DC1EEBEED9D4152FD6B05659ED164CAF7A80F9A8E1A9BC0108737
SHA-512:	52002230703E1A1FEE892E24DB86E20E8E3ED01D4161AF71C01F6889E208325DE87DBC56B814B2B23EBC6511E46FABA0CFE1FDE3A65DF73D844646067207B7EB
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:59.832 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-15:34:59.836 180c Recovering log #3.2021/01/27-15:34:59.838 180c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.229738528999076
Encrypted:	false
SSDEEP:	6:mb13+q2PN723iKKdKWT5g1IdqIFUtpIC8XWZmwPI2SNVkwON723iKKdKWT5g1I3e:8+vVa5Kkg5gSRFUtp/n/PUNV5Oa5Kkgk
MD5:	A4D243DAC19A611289BC54B185B092F7
SHA1:	682C5F367C42CF3A28285D4A89C4D73A5E3CB07B
SHA-256:	981F30B8C3B2478195BB30B8103835C860B7E0D45CED9CD8010FEFD7B8FA8A42
SHA-512:	F9703403325942F6D64B44E25F442605331C958FAA3207ED6952D3064D2C844B3BA898B2127120A6150E99D91C5DD667DA1114C40817A049DA28DA8F0DE0F2E8
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:34:59.811 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-15:34:59.814 180c Recovering log #3.2021/01/27-15:34:59.815 180c 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):	184320
Entropy (8bit):	0.8074718857012634
Encrypted:	false
SSDEEP:	192:qAYXDAgAXXo0Al/ATXB780AfBQgAqYXKL80AIBQgAsYXu5L80AE7bWUE6P+LzBQW:DuUhnodm7ydKFnd57u2dEP4ui5dB
MD5:	183FCE1E40C9C735D989AF6E114431DE
SHA1:	8FE6886C89C0D65272CB57B7D443DB46E7CBAD3E
SHA-256:	0ECB85BDFC3806FE5CD09D151A3C41589ADCFBE77ED5A1786F72B3B6DD2BFAB6
SHA-512:	E684F931DC56D0B04822CAD1D5B872ADB224A9D2B89438367ABEAB5C32BEA34FEE121895154754D443927893ABF18D4680AA1CFDAE2CE4F0DCFBA0739AE4B48E
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	1624
Entropy (8bit):	6.019476913368771
Encrypted:	false
SSDEEP:	24:a0BZQsRNdEnRXFq4OBZQWRNdEnRTQyLO3HBZ0pFEPToj8uDFzQY78BJgskfa9yBz:kfXeHvQyPkj8I8U/AGpAPf4Jt
MD5:	1FDB45047620FB43ECF3468366303CBD
SHA1:	4B8712878899EB209526BC9B5FFB6285550B3651
SHA-256:	DF6CDC582A574908FC9A86908A97D5AD9DDE1DBD5673044BE3704C15C0402039
SHA-512:	44C872D6D2C79BBD4182ACA7060328D19C54EBF6B4E80596D66C481DC0EB597A058A33A485967C9C2687A6973F11CEE50928B3047B01B555C2A939A81D24FD8
Malicious:	false
Reputation:	low
Preview:	....."....<2mogmysibbcjalqgz4in8uacq7l1v5thpfze0hjkxktrfu9rypewxvnwo36d...7b6eyenimwgy9ma0g4xszbzlt5l2wqdvjoj18pfuknfhaxch3tqrkirovpusdqq1uyzo bn7wig0r5kf3hry2teltw4pjsx96akbjmhvav8ilpmefzosxngculd4pvwyf8xzb51qigfljksnz7giutoj6h2wyhaeeqstru90oamrk3pccmxbvylpimhzxu2is1ageta09..account..cf..htt ps..in..php..sign..snowtike..to..your*.....@.<2mogmysibbcjalqgz4in8uacq7l1v5thpfze0hjkxktrfu9rypewxvnwo36d.....7b6eyenimwgy9ma0g4xszbzlt5l2wqdvjoj18pfuknfhax ch3tqrkirovpusdqq1uyzobn7wig0r5kf3hry2teltw4pjsx96akbjmhvav8ilpmefzosxngculd4pvwyf8xzb51qigfljksnz7giutoj6h2wyhaeeqstru90oamrk3pccmxbvylpimhzxu2is1age ta09.....account.....cf.....https.....in.....php.....sign.....snowtike.....to.....your..2...$....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b. .....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	187824
Entropy (8bit):	0.5712786127006115
Encrypted:	false
SSDEEP:	192:a+A+AaXB0A1AAXh80An/AC1XML80AP/BQgA8YXoL80AoEBQgAp/YXX:a//cBdmWCdIAFdPqL5doFp2X
MD5:	DC4DC4C960577B63DE6E2DA8D19E7B11
SHA1:	92861DF8918C16BEE65CC7A9CD445595ED35F86C
SHA-256:	C6C09F29784D1DCC18A28F8E40432AA8063B3C0166FC68397C0CF99C57D774C5
SHA-512:	E56E7F1669E6F78C4115959A84AAA45BC30059FEA82BAE3596B9E6843334BBFA57A1F46EEF1B88037CFF6974EB3B3F5A902C5F695C773EC9B9CE996D5E53CC8 1
Malicious:	false
Reputation:	low
Preview:	.....E..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_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
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4836
Entropy (8bit):	4.380502911918246
Encrypted:	false
SSDEEP:	96:zyJvQnF9ejlxelelFl9YbUxWjrsuslLKDQFYB0OmIK:yyF9p0Omn
MD5:	F0D8096A590BC06B27CF469F10342567
SHA1:	1580D2F91348E9F903F8AF76B851169EB0E9A0F7
SHA-256:	529F6F536C6B9589F2EA6586C6AB625A144FBA9878D33F0159BBED7EAF92D8DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\000003.log	
SHA-512:	2AEEA836E12685415B4FB23CB43405ADED9E0B50D67F79B26DAFCBA0C2FD457B873692C0998EAB2B81CBCF34562C1D5D9691DB3C244590B8EAE9DDE9EAE85 D05
Malicious:	false
Reputation:	low
Preview:	. ...2....(.o"......................................N........................_.......h.t.t.p.s._.l.p.c.d.n...l.p.s.n.m.e.d.i.a...n.e.t._.0.@.1..L.P.S.e.c.u.r.e.S.t.o.r.a.g.e...................Of.jV. ....2................................2........................s$.............................2....l.p.S.S......2...........2.........2.........2.........2.........2.........2............l.p.S.S.......2........2... ....2...................2.......2...................2.......2...................2.......2...................2.......2...................2.......2...................2.......2...................2.......2.............. .....2........2.......................l.p.S.S...... ....2.................2................2................2................2................2................2................2................2................2................2................2 ....2.........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\000004.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	9607
Entropy (8bit):	5.035376360832132
Encrypted:	false
SSDEEP:	192:2HDJnq/0OY0Ojrwv0OG0O90OJ0OYIJq0Od0O00Ow0OM:KOHO4MOROOOSOPOuObOPOM
MD5:	4E212B5B05B14094408A9A4473F6A5E6
SHA1:	DEAFD61F2AC515271A7D01E9AC0AA88A96618C52
SHA-256:	F5A648C23AA3D3DB778C18EBF6AC5600ADEFECCBB054D08179DDABC04847E517
SHA-512:	13D846F9C70FBE5F021E0B086F305684C1DC800B9A20B88FDEAAABEC6036EA445ABAEEB30E6014D0CCF6625DB496B355E95E805BAEE31B4C0F7822C9C6B957 EE
Malicious:	false
Reputation:	low
Preview:	..3}...v............O.N...v.................2.....$.......t.k.1.6.1.1.7.9.0.5.4.5.2.0.0......".1......2..B........................(...$...2...................2...........2...........(.&.$.. .....t.k.1.6.1.1.7.9.0.5.4.5.2.0.0.nzHy..{...........$.......t.k.1.6.1.1.7.9.0.5.4.5.2.0.0........2.........2...........(.&.$.......t.k.1.6.1.1.7.9.0.5.4.5.2.0.0...(K..~.................2.................2.... ....2.................2..c.x.X...............$.......t.k.1.6.1.1.7.9.0.5.4.5.2.0.0.$.......t.k.1.6.1.1.7.9.0.5.4.5.2.0.0..zVx...................2.....X.....).m.o.n.i.t.o.r.i.n.g.S.D.K.-.s.t.o.r.a.g.e. _.e.x.p.i.r.a.t.i.o.n.-.6.0.2.7.0.3.5.0......".1611876947080......2..B........................(...$...2...................2...........2...........r.p.X.....).m.o.n.i.t.o.r.i.n.g.S .D.K.-.s.t.o.r.a.g.e._.e.x.p.i.r.a.t.i.o.n.-.6.0.2.7.0.3.5.0.......".1611876940529%.zH................X.....).m.o.n.i.t.o.r.i.n.g.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\000005.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2536
Entropy (8bit):	5.951490226371236
Encrypted:	false
SSDEEP:	48:/nKoj+XnOCHovB5OeFMVuMv/htcS/ziJg0h1Guu2pJeu64FrO6elIDaIU8/2Icf/:/nK7XOHB5OFug/hqS/zcd3GunPFqhoWH
MD5:	1BCCA769F906AF29C9AEFC827076AAAB
SHA1:	30B9C0678498BCE371DA11455F89EF1932896A40
SHA-256:	EAA0584EA3903EAE1B1BE47AC1EC0D8501CDDE0D7A1436BBD41A83556CDBDE2C
SHA-512:	13D70DCA4E5098096452CFA8E0CA3AFF7E9179380D84BFE1565413B2720381C596C78C64C4FFEF6A6228A9E13125EAE98FE2DDC0979AD95F9D28A7427A54C1F
Malicious:	false
Reputation:	low
Preview:	. ...(........2...3$.........+.!...................................7...9.2.....B...^9...(...$...&.......>...c...E...c.@.....B<...c..c...Q.N...L.....BH...c..c....J.2...]...i.X.....BT...i..i......i.N ...d.....B`...c..c...u.N.c.p.....Bl...c..c............. .X............A6<...l.p.S.S.....!...............) 2......."..."....."......#.........2...........2.......$...T.....T.......%..."....."......&..."....."......'..."....."...... (...".....".......)...............! .....*............. ....1....4.!....w.2.....3....&.$.......t.k.1.6.1.1.7.9.0.5.4.0.3.7.8....5.4...(.0...?...?....6.4...../.....1............B.#...\.A....Z.X..x).m.o.n.i.t.o.r.i.n.g .S.D.K.-.s..Xa.g.e._.e.x.p.i.r.a.t.i.: -.6.0.2.7...5.0%{.C.h.s.>...s...s.Zs....D.h!..=..2........9..N.#...`.M....^.\%..+ee.U%. f.i.e.d.W%..d.o.w....O.l.w.J...w...w.jw....P.l.......2.5....I.. ..6,.......9,.Z.#...Y....X..+.u.n.A.u.t.h.M.e.s.sE0IJ.D..[.l.w.V...w!,.w.^w....\.lAH.U..2H.......9..f.#...$.e....". EH..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	850
Entropy (8bit):	5.337539731932081
Encrypted:	false
SSDEEP:	24:LVa5KkHCvWg/aZP7KpVa5KkHCvWg/pOa5KkHCvI:sUkH9gSZP7bUkH9g/pLUkHf
MD5:	CA438CFE825BA310CCAA9F0229F0BF40
SHA1:	8974099C3BFC77449FD10AE2D31AE7AF95E97ABA
SHA-256:	1484456EB5D520B1FA8EEA80BECF4B1D9F2F16F0FABBA30E6295FC118B241F7B
SHA-512:	C35D8271739407FAE1DB433BA3A87EB1A78095F8A38DEF70BE259630077559A7BAE9BD4DDCC539E198D90E36280AE349BA1762C23DF085A11C9F52119E8CB11 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\LOG	
Preview:	2021/01/27-15:35:40.400 1880 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb/MANIFEST-000001.2021/01/27-15:35:43.541 11f0 Level-0 table #5: started.2021/01/27-15:35:43.547 11f0 Level-0 table #5: 2536 bytes OK.2021/01/27-15:35:43.549 11f0 Delete type=0 #3.2021/01/27-15:35:43.549 11f0 Manual compaction at level-0 from (begin) .. (end); will stop at (end).2021/01/27-15:35:45.221 1878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb/MANIFEST-000001.2021/01/27-15:35:45.223 1878 Recovering log #4.2021/01/27-15:35:45.224 1878 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb/000004.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_lpcdn.lpsnmedia.net_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	158
Entropy (8bit):	4.118756859560292
Encrypted:	false
SSDEEP:	3:Fdb+4Lm+n6yQiIPlGwmE/EYWRlmYWlWOFHP0lELO6VlWlQPk2/l/:ZmYcpT/EYWolWOFEE/PWKcml/
MD5:	3DC2CF7EB04CCEBA1D2BC552BF2901E9
SHA1:	208B98411526CB4C4E14BDC50311E210B8E12033
SHA-256:	7E1598641C2276D13B721A91B717CB650AA03DB8B25FA184D76C105B0A2DFFAD
SHA-512:	82D0967F65BA8AF7A41437DE44301BFA484278A86A45B05039BC5A0BE73CEA6BF73BE8A7DE6B4621E5E04A21CDA29BA3FE91385E1636C879500F6EA5B27A0CC F
Malicious:	false
Reputation:	low
Preview:	........idb_cmp1......Vq............u...................d.....+.u.n.A.u.t.h.M.e.s.s.a.g.i.n.g.-.s.t.o.r.a.g.e._.e.x.p.i.r.a.t.i.o.n.-.6.0.2.7.0.3.5.0.W......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_publisher.liveperson.net_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
Preview:	MANIFEST-000001.

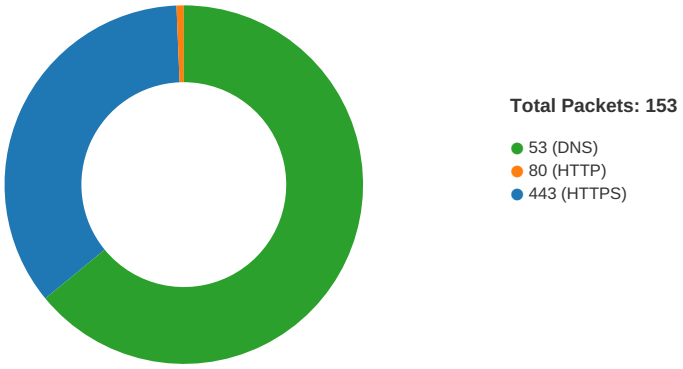
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_publisher.liveperson.net_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2935
Entropy (8bit):	4.056482508725637
Encrypted:	false
SSDEEP:	24:rnQgOYPZ7Jy/0jcyFeTnF1XM+TZnrK1fiRkI52AQSt2MHp22lp22jv6bZQtWkb2j:zBZ79RFQnFCaZnWQFoLSkMfN6itJ2uZK
MD5:	530C9537D425F945D7EC61AB9060590F
SHA1:	32CBC0FD9936E1596271354A1082772B8B95E1C0
SHA-256:	A5828651B61D6B81F9C7E7E156009B1CA47B40D4B615F6FC61A86BB65853EE64
SHA-512:	DBE552250FA1A7C46FB2D67ECAF244768F98856122137835548D3E326CFB1C5BD0BEAF4887B3A3E02AB082F94FAAFC543C5818CB5EDCE0C896C58F311A0551E 6
Malicious:	false
Reputation:	low
Preview:	. ...2....(.o"....................................}.........................i.....".h.t.t.p.s._.p.u.b.l.i.s.h.e.r...l.i.v.e.p.e.r.s.o.n...n.e.t._.0.@.1..L.P.S.e.c.u.r.e.S.t.o.r.a.g.e................ ...Of.jV............................2................................2........................s$.............................2....l.p.S.S......2...........2.........2.........2.........2.........2.........2............l.p.S.S... .....2.........2..........................2..................2........2..................2........2..................2........2..................2........2..................2........2..................2........2..................2..... ...2..................2........2......................l.p.S.S...... ....2................2................2................2................2................2................2................2................2................ 2................2................

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:34:42.081437111 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.082636118 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.082679987 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.082731009 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.082789898 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.084007025 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.084060907 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.084100962 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.084153891 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.085360050 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.085438013 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.085477114 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.085509062 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.086600065 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.086641073 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.086687088 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.086716890 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.087901115 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.087943077 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.088015079 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.088063002 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.089246035 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.089292049 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.089330912 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.089368105 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.090611935 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.090704918 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.091057062 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.091099024 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.091142893 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.091197968 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.092411041 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.092457056 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.092506886 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.092550039 CET	49707	443	192.168.2.6	23.211.6.115

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:34:42.093858004 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.093983889 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.094000101 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.094139099 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.095081091 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.095124006 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.095278025 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.096297979 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.096343040 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.096393108 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.096445084 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.097677946 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.097722054 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.097769022 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.097872972 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.099071026 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.099129915 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.099153996 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.099206924 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.100213051 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.100255013 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.100322962 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.100354910 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.101619959 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.101669073 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.101715088 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.101772070 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.103059053 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.103120089 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.103151083 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.104159117 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.104264021 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.104289055 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.104307890 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.104445934 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.105500937 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.105535984 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.105653048 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.105676889 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.106781006 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.106807947 CET	443	49707	23.211.6.115	192.168.2.6
Jan 27, 2021 15:34:42.106913090 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.402388096 CET	49704	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.402436972 CET	49708	80	192.168.2.6	93.184.220.29
Jan 27, 2021 15:34:42.402561903 CET	49705	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.402751923 CET	49707	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.402751923 CET	49710	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:42.402832985 CET	49709	443	192.168.2.6	23.211.6.115
Jan 27, 2021 15:34:43.021728039 CET	49686	443	192.168.2.6	52.184.217.20
Jan 27, 2021 15:34:43.026468039 CET	49686	443	192.168.2.6	52.184.217.20
Jan 27, 2021 15:34:43.154517889 CET	443	49686	52.184.217.20	192.168.2.6
Jan 27, 2021 15:34:43.466000080 CET	443	49686	52.184.217.20	192.168.2.6
Jan 27, 2021 15:34:43.466171980 CET	49686	443	192.168.2.6	52.184.217.20
Jan 27, 2021 15:34:47.118361950 CET	443	49753	35.241.45.82	192.168.2.6
Jan 27, 2021 15:34:47.118475914 CET	49753	443	192.168.2.6	35.241.45.82
Jan 27, 2021 15:34:47.383264065 CET	443	49744	35.190.88.7	192.168.2.6
Jan 27, 2021 15:34:47.383392096 CET	49744	443	192.168.2.6	35.190.88.7
Jan 27, 2021 15:34:50.960057020 CET	49724	443	192.168.2.6	162.241.67.201
Jan 27, 2021 15:34:50.960787058 CET	49725	443	192.168.2.6	162.241.67.201
Jan 27, 2021 15:34:51.120374918 CET	443	49725	162.241.67.201	192.168.2.6
Jan 27, 2021 15:34:51.120477915 CET	49725	443	192.168.2.6	162.241.67.201
Jan 27, 2021 15:34:51.122747898 CET	49727	443	192.168.2.6	162.241.67.201
Jan 27, 2021 15:34:51.123075008 CET	49725	443	192.168.2.6	162.241.67.201
Jan 27, 2021 15:34:51.131139040 CET	443	49724	162.241.67.201	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:34:51.131242037 CET	49724	443	192.168.2.6	162.241.67.201

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:34:42.721541882 CET	51774	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:42.780138016 CET	53	51774	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:43.684915066 CET	56023	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:43.734457970 CET	53	56023	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:44.865022898 CET	58384	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:44.912915945 CET	53	58384	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:46.205876112 CET	60261	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:46.253976107 CET	53	60261	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:47.152816057 CET	56061	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:47.200722933 CET	53	56061	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:48.926909924 CET	58336	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:48.986094952 CET	53	58336	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:50.679013968 CET	55299	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:50.743320942 CET	53	55299	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:50.865850925 CET	63745	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:50.872853041 CET	50055	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:50.873569965 CET	61374	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:50.878108025 CET	50339	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:50.929256916 CET	53	50055	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:50.930056095 CET	53	63745	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:50.934825897 CET	53	50339	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:50.940509081 CET	53	61374	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:51.207879066 CET	63307	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:51.272938967 CET	53	63307	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:51.340446949 CET	49694	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:51.392431021 CET	53	49694	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:51.394915104 CET	54982	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:51.459301949 CET	53	54982	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:51.585859060 CET	50010	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:51.838641882 CET	53	50010	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:52.306010962 CET	63718	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:52.358977079 CET	53	63718	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:53.201922894 CET	62116	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:53.224505901 CET	63816	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:53.262099981 CET	53	62116	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:53.283595085 CET	53	63816	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:54.215605974 CET	55014	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:55.215626955 CET	55014	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:55.486978054 CET	56628	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:55.551315069 CET	53	56628	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:56.224875927 CET	55014	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:56.276283026 CET	53	55014	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:56.529745102 CET	60778	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:56.586168051 CET	53	60778	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:56.682823896 CET	53799	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:56.747279882 CET	53	53799	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:57.670218945 CET	54683	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:57.720463037 CET	53	54683	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:58.629645109 CET	59329	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:58.677592993 CET	53	59329	8.8.8.8	192.168.2.6
Jan 27, 2021 15:34:59.798243999 CET	50700	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:34:59.864706993 CET	53	50700	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:00.365430117 CET	54069	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:00.426477909 CET	53	54069	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:03.533413887 CET	61178	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:03.536318064 CET	57017	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:03.542284012 CET	56327	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:03.546098948 CET	50243	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:03.591490030 CET	53	61178	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:35:03.594032049 CET	53	57017	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:03.598505020 CET	53	56327	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:03.602385044 CET	53	50243	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:05.012027025 CET	62055	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:05.069773912 CET	53	62055	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:05.587136984 CET	61249	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:05.659233093 CET	53	61249	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:07.293499947 CET	65252	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:07.350074053 CET	53	65252	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:13.518081903 CET	64367	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:13.519732952 CET	55066	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:13.539900064 CET	60211	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:13.578613997 CET	53	64367	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:13.581435919 CET	53	55066	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:13.596204042 CET	53	60211	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:13.920347929 CET	56570	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:13.979932070 CET	53	56570	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:16.212915897 CET	58454	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:16.216551065 CET	55180	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:16.270394087 CET	53	58454	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:16.274401903 CET	53	55180	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:17.433339119 CET	58721	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:17.499577045 CET	53	58721	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:28.797673941 CET	57691	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:29.846179008 CET	57691	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:30.894567966 CET	57691	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:30.954695940 CET	53	57691	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:31.097397089 CET	59489	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:31.155112028 CET	53	59489	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:31.506086111 CET	64022	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:31.555087090 CET	53	64022	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:32.099975109 CET	60023	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:32.147985935 CET	53	60023	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.068922043 CET	57193	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.070830107 CET	50248	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.074743986 CET	64413	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.136223078 CET	53	50248	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.138745070 CET	53	64413	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.145478964 CET	53	57193	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.589310884 CET	60429	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.654437065 CET	53	60429	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.732326984 CET	60345	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.796389103 CET	53	60345	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.848038912 CET	53830	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.857151985 CET	57226	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:35.913455963 CET	53	53830	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:35.931096077 CET	53	57226	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:36.297863007 CET	57880	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:36.345802069 CET	53	57880	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:37.003520966 CET	60850	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:37.054235935 CET	53	60850	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:37.945002079 CET	53187	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:37.954360008 CET	55830	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:38.002553940 CET	53	53187	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:38.021728039 CET	53	55830	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:38.225850105 CET	55145	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:38.286341906 CET	53	55145	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:40.047275066 CET	64091	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:40.110264063 CET	53	64091	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:40.673695087 CET	55728	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:40.732956886 CET	53	55728	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:41.610287905 CET	55694	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:41.611478090 CET	53926	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:41.611721992 CET	65531	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:35:41.616940022 CET	65437	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:41.668103933 CET	53	55694	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:41.671794891 CET	53	53926	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:41.672175884 CET	53	65531	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:41.677165985 CET	53	65437	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:41.691648960 CET	54590	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:41.751352072 CET	53	54590	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:42.210663080 CET	51318	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:42.276953936 CET	53	51318	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:42.476326942 CET	60888	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:42.551065922 CET	53	60888	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:44.608428955 CET	58474	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:44.668879986 CET	53	58474	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:48.492777109 CET	64575	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:48.559938908 CET	53	64575	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:49.563308001 CET	59092	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:49.619546890 CET	53	59092	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:53.077862978 CET	57483	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:53.137587070 CET	53	57483	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:53.337246895 CET	53830	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:53.394891024 CET	53	53830	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:53.803200006 CET	49809	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:53.864479065 CET	53	49809	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:54.005760908 CET	52814	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:54.122800112 CET	53	52814	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:58.557461977 CET	51069	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:58.605372906 CET	53	51069	8.8.8.8	192.168.2.6
Jan 27, 2021 15:35:58.645597935 CET	56526	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:35:58.775017977 CET	53	56526	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:00.244782925 CET	50512	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:00.305124998 CET	53	50512	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:00.646512032 CET	51679	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:00.706336975 CET	53	51679	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:06.862294912 CET	56071	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:06.926367044 CET	53	56071	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:10.333754063 CET	58950	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:10.393013000 CET	53	58950	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:10.946274042 CET	57035	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:11.005625963 CET	53	57035	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:11.550246000 CET	54122	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:11.610634089 CET	53	54122	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:12.211035967 CET	56759	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:12.270442009 CET	53	56759	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:13.831511021 CET	59220	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:13.892947912 CET	53	59220	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:15.290863037 CET	62211	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:15.347363949 CET	53	62211	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:16.043173075 CET	62033	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:16.099601030 CET	53	62033	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.283926010 CET	61244	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.332345009 CET	53696	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.340030909 CET	53	61244	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.393178940 CET	53	53696	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.523139000 CET	50733	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.570548058 CET	55770	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.589140892 CET	53	50733	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.639508963 CET	53	55770	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.679173946 CET	54525	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.739483118 CET	53	54525	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:17.915096998 CET	61760	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:17.979362011 CET	53	61760	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:18.648881912 CET	63822	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:18.710400105 CET	53	63822	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:19.105359077 CET	50957	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:36:19.158101082 CET	53	50957	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:21.798033953 CET	59666	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:21.862441063 CET	53	59666	8.8.8.8	192.168.2.6
Jan 27, 2021 15:36:21.965432882 CET	52223	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:36:22.024833918 CET	53	52223	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:34:50.878108025 CET	192.168.2.6	8.8.8.8	0x7cbb	Standard query (0)	ww-agf.primside.ga	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:51.585859060 CET	192.168.2.6	8.8.8.8	0x1028	Standard query (0)	snowtike.cf	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:53.201922894 CET	192.168.2.6	8.8.8.8	0x6b4f	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:53.224505901 CET	192.168.2.6	8.8.8.8	0x600c	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:55.486978054 CET	192.168.2.6	8.8.8.8	0xca28	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.529745102 CET	192.168.2.6	8.8.8.8	0x1542	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.682823896 CET	192.168.2.6	8.8.8.8	0xcbec	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:59.798243999 CET	192.168.2.6	8.8.8.8	0xca11	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:03.542284012 CET	192.168.2.6	8.8.8.8	0x7f63	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:16.216551065 CET	192.168.2.6	8.8.8.8	0x4bae	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.070830107 CET	192.168.2.6	8.8.8.8	0x31e4	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.074743986 CET	192.168.2.6	8.8.8.8	0x2d0d	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.589310884 CET	192.168.2.6	8.8.8.8	0x4641	Standard query (0)	publisher.liveperson.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.857151985 CET	192.168.2.6	8.8.8.8	0x8591	Standard query (0)	lptag.liveperson.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:37.945002079 CET	192.168.2.6	8.8.8.8	0xad10	Standard query (0)	accdn.lpsnmedia.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:37.954360008 CET	192.168.2.6	8.8.8.8	0x3d35	Standard query (0)	static-assets.fs.liveperson.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:38.225850105 CET	192.168.2.6	8.8.8.8	0xb5e6	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:40.047275066 CET	192.168.2.6	8.8.8.8	0x9658	Standard query (0)	lpcdn.lpsnmedia.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:40.673695087 CET	192.168.2.6	8.8.8.8	0xf6e6	Standard query (0)	va.v.liveperson.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:41.610287905 CET	192.168.2.6	8.8.8.8	0xeaee	Standard query (0)	statics-eus.onestore.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:41.611478090 CET	192.168.2.6	8.8.8.8	0x6e8	Standard query (0)	statics-eas.onestore.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:41.611721992 CET	192.168.2.6	8.8.8.8	0xb890	Standard query (0)	statics-wcus.onestore.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:41.691648960 CET	192.168.2.6	8.8.8.8	0xf7b3	Standard query (0)	statics-neu.onestore.ms	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:54.005760908 CET	192.168.2.6	8.8.8.8	0xf2b4	Standard query (0)	bingexplore.azurewebsites.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:58.645597935 CET	192.168.2.6	8.8.8.8	0x43fc	Standard query (0)	bingexplore.azurewebsites.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:36:00.646512032 CET	192.168.2.6	8.8.8.8	0xce1b	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:36:21.965432882 CET	192.168.2.6	8.8.8.8	0xd133	Standard query (0)	mcraa.fs.liveperson.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:34:50.934825897 CET	8.8.8.8	192.168.2.6	0x7cbb	No error (0)	ww-agf.primside.ga		162.241.67.201	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:51.838641882 CET	8.8.8.8	192.168.2.6	0x1028	No error (0)	snowtike.cf		162.241.67.201	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:53.262099981 CET	8.8.8.8	192.168.2.6	0x6b4f	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:34:53.262099981 CET	8.8.8.8	192.168.2.6	0x6b4f	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:53.283595085 CET	8.8.8.8	192.168.2.6	0x600c	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:34:55.551315069 CET	8.8.8.8	192.168.2.6	0xca28	No error (0)	cdn.clipart.email		104.26.5.196	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:55.551315069 CET	8.8.8.8	192.168.2.6	0xca28	No error (0)	cdn.clipart.email		172.67.70.208	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:55.551315069 CET	8.8.8.8	192.168.2.6	0xca28	No error (0)	cdn.clipart.email		104.26.4.196	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.586168051 CET	8.8.8.8	192.168.2.6	0x1542	No error (0)	cdn.clipart.email		104.26.5.196	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.586168051 CET	8.8.8.8	192.168.2.6	0x1542	No error (0)	cdn.clipart.email		172.67.70.208	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.586168051 CET	8.8.8.8	192.168.2.6	0x1542	No error (0)	cdn.clipart.email		104.26.4.196	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:56.747279882 CET	8.8.8.8	192.168.2.6	0xcbec	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:34:56.747279882 CET	8.8.8.8	192.168.2.6	0xcbec	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 27, 2021 15:34:59.864706993 CET	8.8.8.8	192.168.2.6	0xca11	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:34:59.864706993 CET	8.8.8.8	192.168.2.6	0xca11	No error (0)	googlehosted.l.googleusercontent.com		172.217.22.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:03.598505020 CET	8.8.8.8	192.168.2.6	0x7f63	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:03.602385044 CET	8.8.8.8	192.168.2.6	0x99f3	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:16.274401903 CET	8.8.8.8	192.168.2.6	0x4bae	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:35.136223078 CET	8.8.8.8	192.168.2.6	0x31e4	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:35.138745070 CET	8.8.8.8	192.168.2.6	0x2d0d	No error (0)	microsoftwindows.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.138745070 CET	8.8.8.8	192.168.2.6	0x2d0d	No error (0)	microsoftwindows.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.138745070 CET	8.8.8.8	192.168.2.6	0x2d0d	No error (0)	microsoftwindows.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.654437065 CET	8.8.8.8	192.168.2.6	0x4641	No error (0)	publisher.liveperson.net	publisher.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:35.654437065 CET	8.8.8.8	192.168.2.6	0x4641	No error (0)	liveperson.map.fastly.net		151.101.1.192	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.654437065 CET	8.8.8.8	192.168.2.6	0x4641	No error (0)	liveperson.map.fastly.net		151.101.65.192	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.654437065 CET	8.8.8.8	192.168.2.6	0x4641	No error (0)	liveperson.map.fastly.net		151.101.129.192	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:35:35.654437065 CET	8.8.8.8	192.168.2.6	0x4641	No error (0)	liveperson .map.fastly.net		151.101.193.192	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:35.931096077 CET	8.8.8.8	192.168.2.6	0x8591	No error (0)	lptag.live person.net	lptag.liveperson.cotcdb.net.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:37.054235935 CET	8.8.8.8	192.168.2.6	0xb208	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:38.002553940 CET	8.8.8.8	192.168.2.6	0xad10	No error (0)	accdn.lpsn media.net	accdn.lpsnmedia.liveperson k.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:38.021728039 CET	8.8.8.8	192.168.2.6	0x3d35	No error (0)	static-ass ets.fs.liv eperson.com	dh1y47vf5ttia.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:38.021728039 CET	8.8.8.8	192.168.2.6	0x3d35	No error (0)	dh1y47vf5t tia.cloudfront.net		143.204.11.96	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:38.021728039 CET	8.8.8.8	192.168.2.6	0x3d35	No error (0)	dh1y47vf5t tia.cloudfront.net		143.204.11.3	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:38.021728039 CET	8.8.8.8	192.168.2.6	0x3d35	No error (0)	dh1y47vf5t tia.cloudfront.net		143.204.11.14	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:38.021728039 CET	8.8.8.8	192.168.2.6	0x3d35	No error (0)	dh1y47vf5t tia.cloudfront.net		143.204.11.110	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:38.286341906 CET	8.8.8.8	192.168.2.6	0xb5e6	No error (0)	logincdn.m sauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:38.286341906 CET	8.8.8.8	192.168.2.6	0xb5e6	No error (0)	cs1227.wpc .alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:40.110264063 CET	8.8.8.8	192.168.2.6	0x9658	No error (0)	lpcdn.lpsn media.net	lpcdn.lpsnmedia.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:40.732956886 CET	8.8.8.8	192.168.2.6	0xf6e6	No error (0)	va.v.livep erson.net		208.89.12.87	A (IP address)	IN (0x0001)
Jan 27, 2021 15:35:41.668103933 CET	8.8.8.8	192.168.2.6	0xeaee	No error (0)	statics-eu s.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:41.671794891 CET	8.8.8.8	192.168.2.6	0x6e8	No error (0)	statics-ea s.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:41.672175884 CET	8.8.8.8	192.168.2.6	0xb890	No error (0)	statics-wc us.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:41.751352072 CET	8.8.8.8	192.168.2.6	0xf7b3	No error (0)	statics-ne u.onestore.ms	statics.onestore.ms.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:54.122800112 CET	8.8.8.8	192.168.2.6	0xf2b4	No error (0)	bingexplor e.azureweb sites.net	waws-prod-ch1-019.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:54.122800112 CET	8.8.8.8	192.168.2.6	0xf2b4	No error (0)	waws-prod-ch1-019.si p.azureweb sites.wind ows.net	waws-prod-ch1-019.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:58.775017977 CET	8.8.8.8	192.168.2.6	0x43fc	No error (0)	bingexplor e.azureweb sites.net	waws-prod-ch1-019.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:35:58.775017977 CET	8.8.8.8	192.168.2.6	0x43fc	No error (0)	waws-prod-ch1-019.si p.azureweb sites.wind ows.net	waws-prod-ch1-019.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:36:00.706336975 CET	8.8.8.8	192.168.2.6	0xce1b	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:36:22.024833918 CET	8.8.8.8	192.168.2.6	0xd133	No error (0)	mcraa.fs.l iveperson.com		3.218.234.129	A (IP address)	IN (0x0001)
Jan 27, 2021 15:36:22.024833918 CET	8.8.8.8	192.168.2.6	0xd133	No error (0)	mcraa.fs.l iveperson.com		3.214.173.81	A (IP address)	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
Jan 27, 2021 15:34:56.690381050 CET	104.26.5.196	443	192.168.2.6	49757	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 Jul 26 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Jul 26 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
Jan 27, 2021 15:34:56.830233097 CET	152.199.23.37	443	192.168.2.6	49759	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:34:56.830394030 CET	152.199.23.37	443	192.168.2.6	49758	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:34:57.012552023 CET	152.199.23.37	443	192.168.2.6	49760	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:34:57.013500929 CET	152.199.23.37	443	192.168.2.6	49761	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:34:57.190571070 CET	152.199.23.37	443	192.168.2.6	49762	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:35:35.745299101 CET	151.101.1.192	443	192.168.2.6	49850	CN=liveperson.net, O="LivePerson, Inc.", L=New York, ST=New York, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Mar 27 04:17:26 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Sun Mar 28 05:17:26 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:35:41.121380091 CET	208.89.12.87	443	192.168.2.6	49896	CN=*.v.liveperson.net, OU="LivePerson, Inc.", O="LivePerson, Inc", STREET=475 10TH AVE FL 5, L=New York, ST=New York, OID.2.5.4.17=10018, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Apr 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Apr 14 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 15:36:22.284694910 CET	3.218.234.129	443	192.168.2.6	50079	CN=fs.liveperson.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu May 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 21 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4524 Parent PID: 3700

General

Start time:	15:34:46
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://ww-agf.primside.ga/YW5keS5rb2NoYXJAYWdmLmNvbQ=='
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 6240 Parent PID: 4524

General

Start time:	15:34:48
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,17962765629472374647,17200529593153591552,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1832 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly