ID: 404193
Cookbook: browseurl.jbs
Time: 19:45:41
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

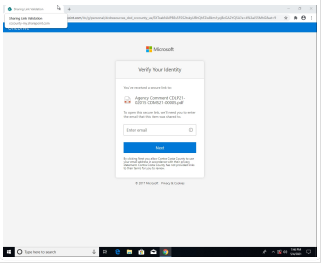
Analysis Report https://cccounty-my.sharepoint.com:44…

Overview

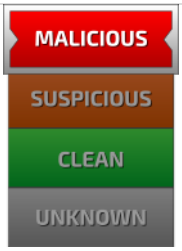
General Information

Sample URL:	https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_ccco...ccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9
Analysis ID:	404193
Infos:	

Most interesting Screenshot:



Detection



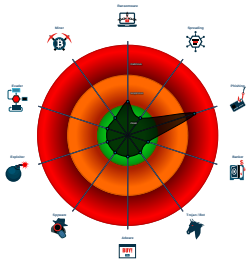
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4440 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4940 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,11341300835914849824,6073494584447434684,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1768 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

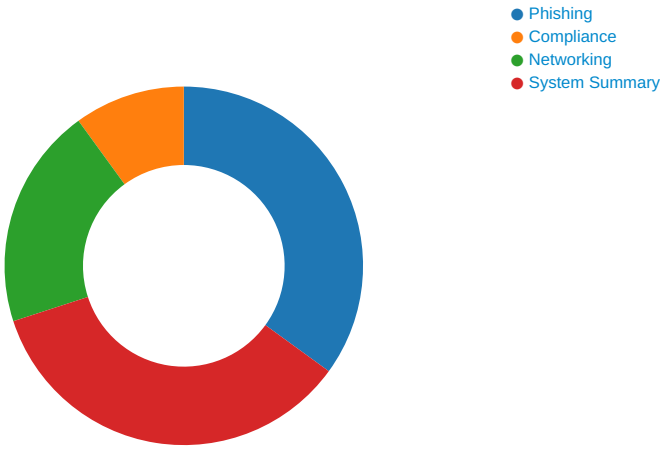
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

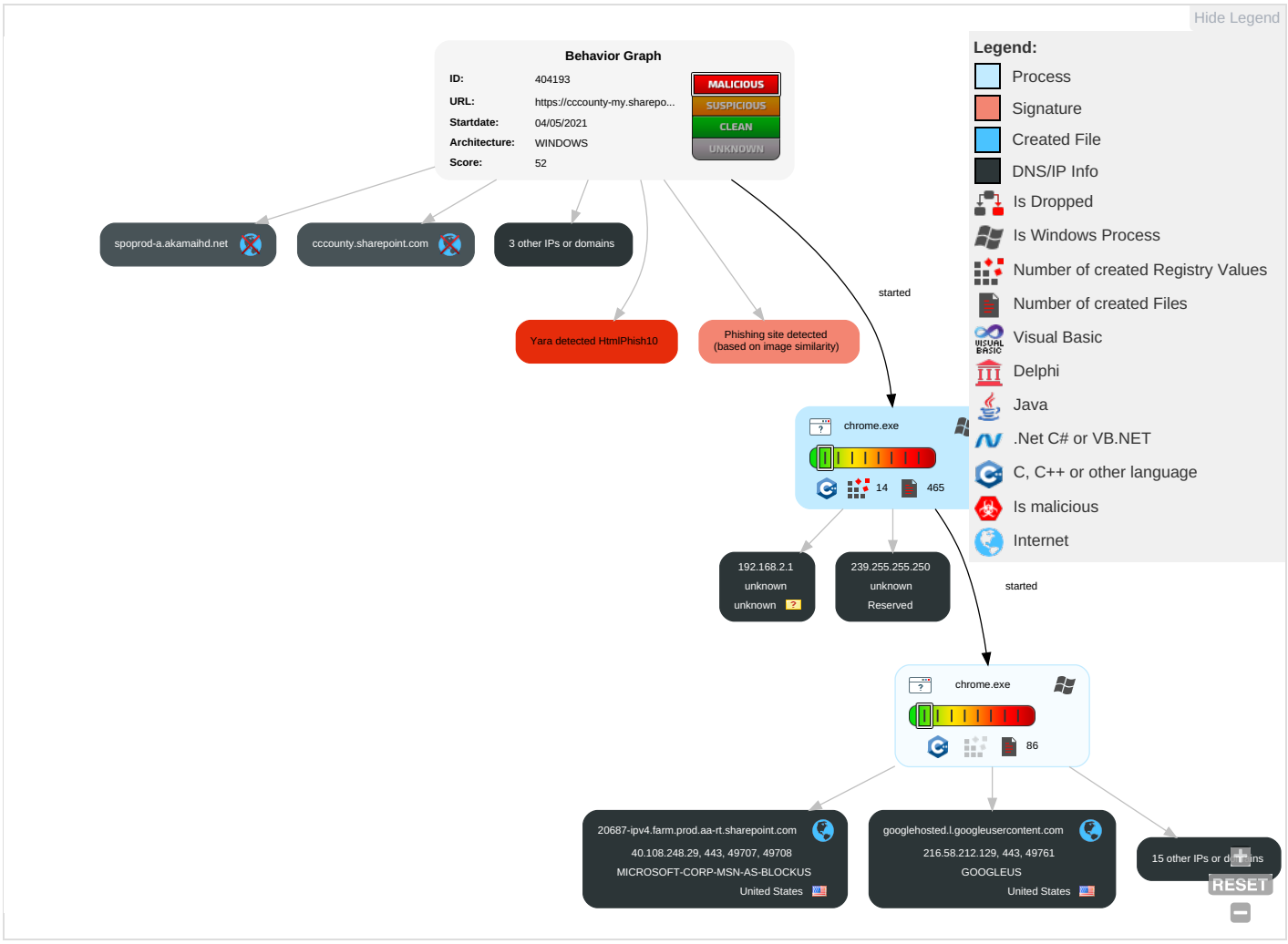
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 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	Modify System Partition
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	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	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	Delete Device Data

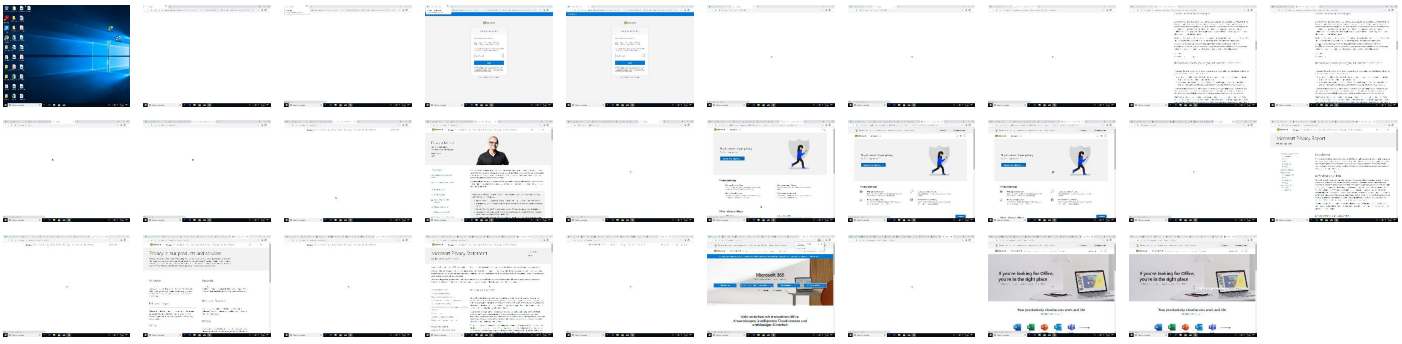
Behavior Graph

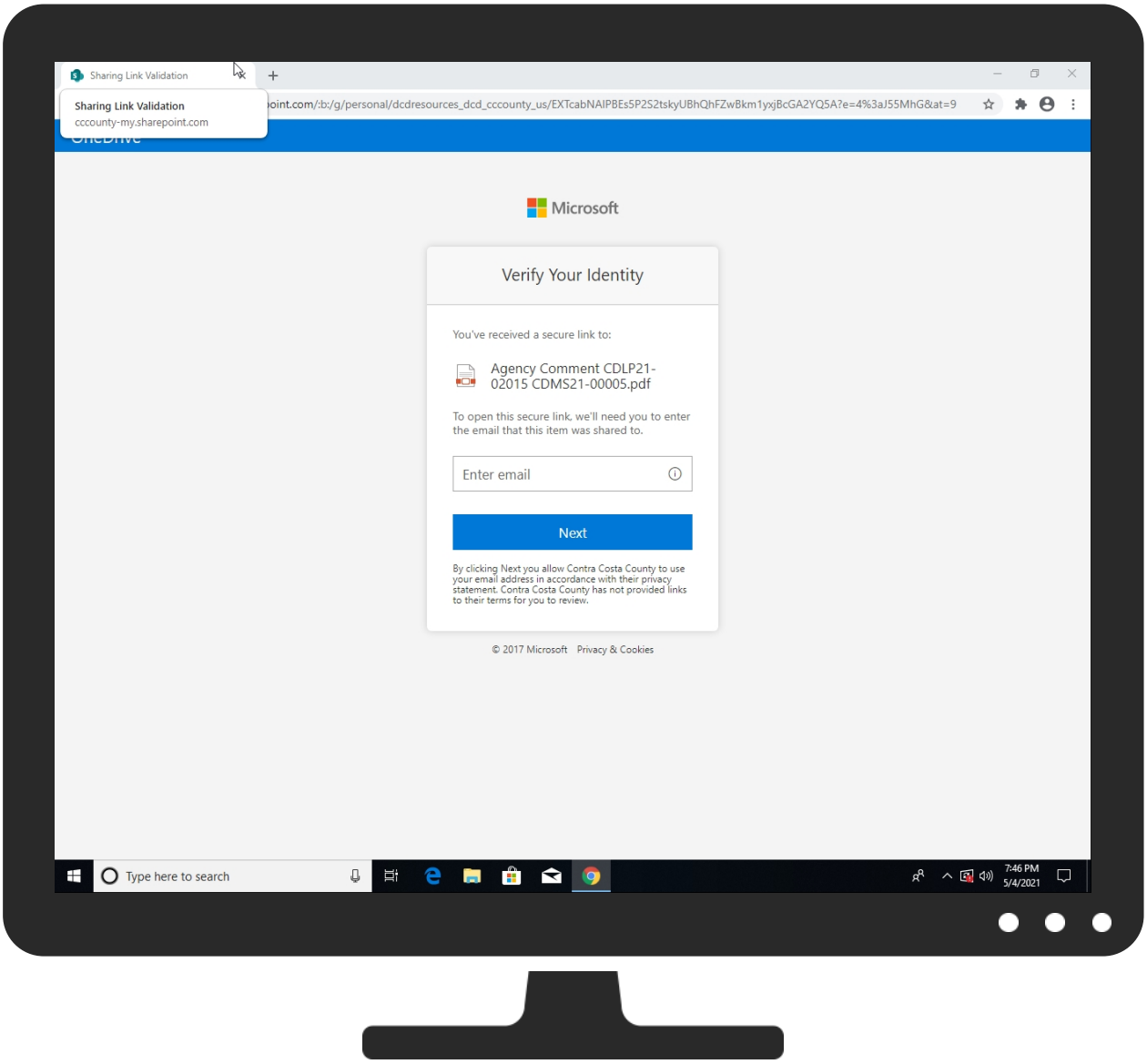


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.js	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.jsaD	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://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meBoot.min.jsaD	0%	Avira URL Cloud	safe	
http://https://sharepoint.com/	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://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meCore.min.jsaD	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tsk	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/10.21035.1/en-US/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=amc&market=en-us&uhf=1	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meBoot.min.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=en-us&uhf=1	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/personal/dcdresources_dcd_cccounty_us/_layouts/15/guestaccess.asp	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meBoot.min.js	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=1fDsP7T8iuixVwu-fVH5iZr4cSvnLTO52_v1doY-7Fhg	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/WebResource.axd?d=M5O6KBnw2Kc30Ye7wKtYeOmA0-ax1yV1j7R_PuQmXE74ijK	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=XLHvvuqUg5InnNgZ7caYxePwb7iO9lfyUqU9z6CieiK1	0%	Avira URL Cloud	safe	
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=XjLkEB_vSvznU474E48kPJA1H9JTKlbxQRrF9mf4oevb	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
aka.ms	95.101.18.109	true	false		high
20687-ipv4.farm.prod.aa-rt.sharepoint.com	40.108.248.29	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
logincdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
amp.azure.net	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
cccounty-my.sharepoint.com	unknown	unknown	false		unknown
mem.gfx.ms	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cccounty-my.sharepoint.com/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.onestore.ms/	Network Action Predictor-journal.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.js	38c7c19d1d0ee3c7_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.jsaD	38c7c19d1d0ee3c7_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	5703ca06-bf7a-46ab-b8b7-8a209145f104.tmp.1.dr, e72addbe-6b1d-45a5-b361-9657049270c6.tmp.1.dr, be4755c6-1d2c-426f-9633-f0817db4ccdd.tmp.1.dr, 7bfb62a6-3a75-44fc-af2c-f79f44843a16.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://live.com/QB	38c7c19d1d0ee3c7_0.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meBoot.min.jsaD	0b6a779b97f6aaad_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sharepoint.com/	a4e37f7fb809c2dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com	be4755c6-1d2c-426f-9633-f0817db4ccdd.tmp.1.dr	false		high
http://https://aka.ms/PrivacyReport5	Current Session.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://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.1.min.js	c94540d4c86c0448_0.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	094e2d6bf2abec98_0.0.dr, 14557f4877e37a1a_0.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meCore.min.jsaD	225853b3d3cc9c98_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cccounty-my.sharepoint.com/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tsk	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://consentreceiverfd-prod.azurefd.net/v1	e80e6e93d4807d92_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.jsaD	14557f4877e37a1a_0.0.dr	false		high
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meCore.min.js	225853b3d3cc9c98_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mem.gfx.ms/meversion?partner=amc&market=en-us&uhf=1	300bb9fb98ab63f0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meBoot.min.js	6686b0c92e7fc912_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=en-us&uhf=1	462d64d34aad30da_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cccounty-my.sharepoint.com/personal/dcdresources_dcd_cccounty_us/_layouts/15/guestaccess.asp	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
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/10.21035.1/en-US/meBoot.min.js	0b6a779b97f6aaad_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cccounty-my.sharepoint.com/	000003.log0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meCore.min.js	0481116f3cd8293f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=1fDsP7T8iuixVwu-fVH5iZr4cSvnLTO52_v1doY-7Fhg	ae966ea7cdbe242d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cccounty-my.sharepoint.com/WebResource.axd?d=M5O6KBnw2Kc30Ye7wKtYeOmA0-ax1yV1j7R_PuQmXE74ijK	a7088b4299cd1633_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/PrivacyReport	Current Session.0.dr	false		high
http://https://cccounty-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	5703ca06-bf7a-46ab-b8b7-8a209145f104.tmp.1.dr, be4755c6-1d2c-426f-9633-f0817db4ccdd.tmp.1.dr	false		high
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=XLHvvuqUg5InnNgZ7caYxePwb7iO9lfyUqU9z6CieiK1	087e843a6a77f2e0_0.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://spoprod-a.akamaihd.net	be4755c6-1d2c-426f-9633-f0817db4ccdd.tmp.1.dr	false		high
http://https://cccounty-my.sharepoint.com/ScriptResource.axd?d=XjLkEB_vSvznU474E48kPJA1H9JTKlbxQRrF9mf4oevb	5563163b962da706_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net	be4755c6-1d2c-426f-9633-f0817db4ccdd.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/PrivacyReportMicrosoft	History-journal.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
40.108.248.29	20687-ipv4.farm.prod.aa-rt.sharepoint.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
95.101.18.109	aka.ms	European Union		16625	AKAMAI-ASUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404193
Start date:	04.05.2021
Start time:	19:45:41

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9
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:	12
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:	mal52.phis.win@41/217@11/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://go.microsoft.com/fwlink/?linkid=845480 • Browse: https://privacy.microsoft.com/ • Browse: https://account.microsoft.com/privacy • Browse: https://aka.ms/PrivacyReport • Browse: https://privacy.microsoft.com/privacy-in-our-products • Browse: https://go.microsoft.com/fwlink/?LinkId=521839 • Browse: https://www.microsoft.com/microsoft-365 • Browse: https://www.microsoft.com/en-us/microsoft-365/microsoft-office
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 93.184.220.29, 104.43.193.48, 20.50.102.62, 168.61.161.212, 92.122.145.220, 13.64.90.137, 142.250.185.110, 216.58.212.173, 142.250.185.206, 95.168.222.146, 95.168.222.141, 23.32.238.138, 23.32.238.153, 23.32.238.115, 23.32.238.128, 172.217.16.138, 92.122.213.216, 92.122.213.248, 142.250.184.195, 52.147.198.201, 88.221.62.148, 92.122.145.53, 92.122.213.219, 92.122.213.200, 152.199.19.160, 23.57.80.253, 84.53.167.109, 92.122.213.247, 92.122.213.194, 23.57.80.111, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 92.122.213.240, 23.50.97.161, 20.190.160.74, 20.190.160.9, 20.190.160.1, 20.190.160.133, 20.190.160.131, 20.190.160.3, 20.190.160.5, 20.190.160.130, 92.122.213.176, 92.122.213.193, 88.221.228.182, 2.17.185.83, 13.107.246.60, 13.107.213.60, 65.55.44.109, 93.184.221.240, 142.250.185.99, 172.217.16.131, 34.104.35.123, 92.122.213.195, 92.122.213.163 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, a1945.g2.akamai.net, clients2.google.com, statics-marketingsites-eus-ms-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, modern.akamai.odsp.cdn.office.net, account.microsoft.com.edgekey.net, compass-ssl.microsoft.com, lgincdnvzeuno.ec.azureedge.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-

s.cms.ms.akadns.net, modern.akamai.odsp.cdn.office.net-c.edgesuite.net.globalredir.akadns.net, edgedl.me.gvt1.com, lgincdn.trafficmanager.net, cdn.account.microsoft.com.akadns.net, translate.googleapis.com, a1531.g2.akamai.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, compass-ssl.microsoft.com.edgekey.net, clients.l.google.com, dual.part-0032.t-0009.t-msedge.net, a1985.g2.akamai.net, e9412.b.akamaiedge.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, compass-ssl.microsoft.com.nsatc.net, i.s-microsoft.com, statica.akamai.odsp.cdn.office.net, e12564.dspb.akamaiedge.net, go.microsoft.com, prod-video-cms-rt-microsoft-com.akamaized.net, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, 160c1.wpc.azureedge.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, cs22.wpc.v0cdn.net, mem.gfx.ms.edgekey.net, wu.ec.azureedge.net, login.msa.msidentity.com, firstparty-azurefd-prod.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, c.s-microsoft.com, go.microsoft.com.edgekey.net, a1963.g2.akamai.net, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com, mwf-service.akamaized.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, www.tm.lg.prod.aadmsa.akadns.net, a1902.dscd.akamai.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, a1778.g2.akamai.net, e10583.dspg.akamaiedge.net, fs.microsoft.com, content-autofill.googleapis.com, part-0032.t-0009.t-msedge.net, skypedataprdcolcus17.cloudapp.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net, statics-marketingsites-wcus-ms-com.akamaized.net, www.googleapis.com, modern.akamai.odsp.cdn.office.net-c.edgesuite.net, web.vortex.data.trafficmanager.net, dual-a-0001.dc-msedge.net, e55.dspb.akamaiedge.net, store-images.s-microsoft.com, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, privacy.microsoft.com.edgekey.net, e2699.dspg.akamaiedge.net, account.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, img-prod-cms-rt-microsoft-com.akamaized.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net.globalredir.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, web.vortex.data.microsoft.com, lgincdnvzeuno.azureedge.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, a-0001.a-afdentry.net.trafficmanager.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, www.microsoft.com, a1813.dscd.akamai.net

- 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a9a0d61-d368-4fa5-bdf1-8a17b1465db0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a9a0d61-d368-4fa5-bdf1-8a17b1465db0.tmp	
Size (bytes):	359275
Entropy (8bit):	6.0154442454166315
Encrypted:	false
SSDEEP:	6144:x84zbfpN0Shrseefa2XJQVR8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/14:x843v0ArPgQVWxzurRDn9nfNxF4ijZV6
MD5:	633474B5E1A41083C8E3B5D861F8B7EC
SHA1:	AB5A6CCAEBA310FC9DFBEAD55AD0493E66396E62
SHA-256:	5C0503D07CB2D4F0E0E7B683F62B7E66AE4FD46A5B4E1610D2B3D3EAB08B319E
SHA-512:	B058A9126A19FFDA7214EC5443A8AAF51E509EEA8B5239C126BE401DC1007AE0C2BD36C7D5F83F4A962C138BA849E83355C2318BB82144E220F3FE347FA26F9
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":1.620182797789722e+12,"network":1.620150399e+12,"ticks":111756009.0,"uncertainty":4486334.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264656394477

C:\Users\user\AppData\Local\Google\Chrome\User Data\3b3a67de-571d-4d50-b611-9a2f58001b13.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):	359276
Entropy (8bit):	6.015444000352894
Encrypted:	false
SSDEEP:	6144:u84zbfpN0Shrseefa2XJQVR8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/14:u843v0ArPgQVWxzurRDn9nfNxF4ijZV6
MD5:	52801ADBA03DAF5F5E9E9A7BE01BA89D
SHA1:	54C44639A87C23CE8F4FA26A73B9901C67B22ABE
SHA-256:	302C4FB0F8BE65BCDECE4EB15A07CE14CA66106765E875A8C61F849588DEBFF7
SHA-512:	C26F8E5350E91A38D79EC0D3CC2DB7B3E3C3C23454B2FA6396EF1634D477217DC3DEE9121360CB3402869105AEE34C8BC7C48BE4732E2504477F3777B681D8E
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":1.620182797789722e+12,"network":1.620150399e+12,"ticks":111756009.0,"uncertainty":4486334.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075593627"},"policy":{"last_statistics_update":"13264656394477

C:\Users\user\AppData\Local\Google\Chrome\User Data\3d8bd7bd-1e0d-433c-937d-3b6fe88ccfb6.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):	362847
Entropy (8bit):	6.028018234046839
Encrypted:	false
SSDEEP:	6144:284zbfpN0Shrseefa2XJQVR8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/14:2843v0ArPgQVWxzurRDn9nfNxF4ijZV6
MD5:	54DA247C9F7ED17DC3F414548FD074A1
SHA1:	1121A2996E3028826B25568BA0F80E2A559B6ED2
SHA-256:	53AE371A4BD23D18F3AA78AE0B3359B75133912F7D42B4978E3D836A72144531
SHA-512:	E1633B0A80FDCB5055047A1B18DE44DA7210D89D3324AD5A8912B6B59C1058A26B5E77C6378EFCF8D4C81A236BD12F7D24D9C905D40B44FDE5E508FA631492
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":1.620182797789722e+12,"network":1.620150399e+12,"ticks":111756009.0,"uncertainty":4486334.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075593627"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\80b92f5e-1af5-47b8-8a52-1d9f2821fd4f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428

C:\Users\user\AppData\Local\Google\Chrome\User Data\80b92f5e-1af5-47b8-8a52-1d9f2821fd4f.tmp	
Entropy (8bit):	3.7491800969622524
Encrypted:	false
SSDEEP:	384:h7/8MeR7KluIVJ7Y7NkrVvAs3v8K7HGbGburpucOx/i6yNrJ0m9xT9e84A7OeCYy:NeKVpKSg/0e/aQKUH/eoKuQIBY
MD5:	904DA576518D007414230A5CBFDFC131
SHA1:	42E06F94F584E202922D0D572642DAB3D28B1E6C
SHA-256:	AEB722C67EB736DCC8EE2C766A95AD3F18C3F0E5940E9B560D3AEADF3CBCBDF2
SHA-512:	287128E118BAB1E25F49D88121DD05EB0F524C67E514D1652CB5A3C24ACD34CAF10794FEFCC4E7F12BD639F65AB9A6909F6AC0B82190F169C857721C9DC6C3
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\82f7701b-8e6a-4d5d-9731-c24499eab8f2.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):	359275
Entropy (8bit):	6.015443804851085
Encrypted:	false
SSDEEP:	6144:484zbfpN0Shrseefa2XJQVR8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/14:4843v0ArPgQVWxzurRDn9nfNxF4ijZV6
MD5:	CFF59A7511E13F9B2AE9F0AFCFBBD070
SHA1:	A8A6C727DFDBACF12712AB40B55308CB33D669C8
SHA-256:	7EBEEFC965B76500959C3A4DEE7EB7779B77C9D29F58F9CA2BFB05B40BEBF9C7
SHA-512:	3460B155CE6754C55BCA862D61DAEBAE90D8884A12A27C8BF98B74CE843E4DC3E6C63AFC186FB68B92D89A024D3F80F8259EBA67B6F433018B52AC61B2C7891
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":1.620182797789722e+12,"network":1.620150399e+12,"ticks":111756009.0,"uncertainty":4486334.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264656394477

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:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\02f10b20-624c-4574-bca9-222400ff88ab.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):	1544
Entropy (8bit):	5.544619160012365
Encrypted:	false
SSDEEP:	48:YBU0A6UUhGxeU+nU0dDKUe78aOUPUeC4wUbUeh:UU0pUUgxeUQU0dDKUo8aOUPUHdUbUc
MD5:	29584BD24391FBBC02956511C41B101B
SHA1:	775B97892145C5537CE0E354B5DC95C1CF501B12
SHA-256:	C4EBED06BBEDC2F591E7BD01F7E6B89CAB6C85A70C623EE566DD1A99228A1861

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\02f10b20-624c-4574-bca9-222400ff88ab.tmp	
SHA-512:	D5BD507D0DE2CABF3BCF919182C5C6BC47434277FAA2E683D829241D0F8197CECEF8FA85B80AFAA24D346F71059A5D33087DD1218AA07099F3405380712B475
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651718813.851016,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182813.851022},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651718807.160284,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620182807.160291},{"expiry":1651718813.026159,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182813.026166},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1651718798.025817,"host":"2fyp6Zj7wfyniJVJxhIrUTsXM1PZeyziOe2tmKst6To=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\07737f85-48a4-4268-a7b1-6fc14a7a82c7.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):	1880
Entropy (8bit):	5.562863890598289
Encrypted:	false
SSDEEP:	48:Y4KUu+6UUh3UUCxeUjVUNDKUe2UYp28aOUPUeC4wUbUeh:iUeUUpUUCxeUxUNDKUbUYw8aOUPUHdUj
MD5:	8305DBF02E7AF33F69C5979A2D39AAF5
SHA1:	8D8282E5A53A10869E3492E39105719EB8B7F8E9
SHA-256:	D01DFC564109AA5593BD4D5D58DD0959F35CA53B58DAD568C7098D6ED0BE8BC3
SHA-512:	20E6AB23C2FF6DA460B3780BF1D2BEC6406AE8441E85F49C6EE18E7F9609932EA8C42D1220A419DA5EEA41206807213B2D8E56EEEFD101C23A73E5F9699BEA1 B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651718834.826006,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182834.826012},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651718833.402122,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182833.402126},{"expiry":1651718807.160284,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620182807.160291},{"expiry":1651718825.556405,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182825.556412},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0f96e568-8533-49f4-bb6a-0e7f81cf8af1.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):	5861
Entropy (8bit):	5.185771262671199
Encrypted:	false
SSDEEP:	96:nIFDJ/TfNY1M5fSVXpIk0JCKL83pkv1jYk9hZQbOTQVuwn:nI/fvSjC4KSpkvyk9y
MD5:	9AB7E72F7BBE59ED916C020BE6FF0DB6
SHA1:	EB643CE4A530F6576F2927E4A098BC678CF0F6DF
SHA-256:	6A84739A9D05E46591EAE2A091E5DEC8D872C89FD515143F4537A97C2EF92C88
SHA-512:	64C5E724A118876D0EAD72E1DD744CECC69048202AE0259BDE5FA76DEF231E42619A0D2E1911423D330093484B5C9B22A15DC7FC0CD44DE48458B8072D7745
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264656394919701","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","1538886"],"daily_received_length":["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\19480760-04f7-416c-b509-6fb989b37d2a.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):	2212
Entropy (8bit):	5.570607621042072
Encrypted:	false
SSDEEP:	48:YQUC6UUhNUbxeUkU0DKUeEUcU1tRUp8aOUPUeC4wUbUeh:BUHUUrUbxeUkU0DKUxUcUJUp8aOUPUHa
MD5:	8FBB3F01466A1B244EBA640F677D6CBC
SHA1:	C68EEFEBF8E4FDBE61674EDFADDEF7C1AEFA428E
SHA-256:	381F93ED2B32DBFC07A1C640E4A8C988D4B81FCB9BCAB96DAF829C31833D987A
SHA-512:	768CA94A7F6021CCDAE8E751470CBD66E6C266D56B55837426177057BF0EDC0095541877BEEECE33006718EBAA77BCE31F16A7A4CE46CA426AB50258B77E18F C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\19480760-04f7-416c-b509-6fb989b37d2a.tmp	
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651718836.869369,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182836.869373},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651718836.858379,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182836.858384},{"expiry":1651718807.160284,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620182807.160291},{"expiry":1651718842.275775,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182842.275779},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1bb6e6f9-7b0f-4989-84be-56a9b40525f6.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):	5038
Entropy (8bit):	4.969388169432119
Encrypted:	false
SSDEEP:	96:nIFhGGfpSVX/Ik0JCKL83pkv113bOTQVuwn:nIBfpS1C4KSpkvD
MD5:	8440B1843337F40B4F53E3A2DEEB7073
SHA1:	EBDD0AA880DEA756542BC16B78EB4643EAFC8111
SHA-256:	F1D00926A2297D28F633F678D3074795EA040EC7F8BDD5D256AB23624C74725F
SHA-512:	597C2987F15F6F092FF8CC0B2532666E38B021687F7B09750F9BE5391120201F223D9345C78D9561ACACCC683D95F940591B2A37B6F9FF514FD303998081BA26
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264656394919701","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","1538886"],"daily_received_length":["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\4008cc86-4ba3-4be3-9cf6-359ef989c609.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536259656633655
Encrypted:	false
SSDEEP:	384:6lltbLlJiXP1kXqKf/pUZNCgVLH2HfDZrUGHGPnTgZhWN34b:+LlOP1kXqKf/pUZNCgVLH2HfdrUmGPnI
MD5:	A41FCA0D0CE250EC8F6F40D244ABE625
SHA1:	DB9E2E858B0B445A377C98AD49095F1B8E3348A6
SHA-256:	6129605BF40439F496DBA572441947B6DB920C88955FEC15CC09181CC51650A4
SHA-512:	53A6420BCE439FE5E4C43EA402C28B7C50975277B3E0857D2D241FB9AC0F48303942339477E7BBF8E4C805A33B9734B6D5E57BFDAF6885391B4A2ADD95720BB
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":"13264656394591924","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ed80575-7a24-428a-b1d4-ba5194805ce9.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):	5039
Entropy (8bit):	4.970386062646488
Encrypted:	false
SSDEEP:	96:nIFEczTfpSVXEIk0JCKL83pkv113bOTQVuwn:nI/fpSGC4KSpkvD
MD5:	0A5A73C5EBDFA96F6A0D4042551CC341
SHA1:	09E75F05C09A6F111B4F255A26A7AC23BCE2AF71
SHA-256:	A83DBB961953AD92CE5923E6D79F88480785399BC1343B8121167B2F2A2029C0
SHA-512:	F15D6548EDAD391DF7B0210D9A897D0CAD9D89046C743EB3CCF3965EC5C4F3BE656EA1A1259255AB122A0B30295E5D0A21360455B71E4329B6A1DBA9BCB3C CF
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ed80575-7a24-428a-b1d4-ba5194805ce9.tmp

Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264656394919701","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","0","1538886"],"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","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5703ca06-bf7a-46ab-b8b7-8a209145f104.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5983c13b-a561-4a3e-ab61-7b97d5068539.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577736732379996
Encrypted:	false
SSDEEP:	384:6lltSLlJiXP1kXqKf/pUZNCgVLH2HfDZrU2h2N34V:NLlOP1kXqKf/pUZNCgVLH2HfdrU2cN3a
MD5:	49976A6B437FE7A0631E2855F0DAF3FD
SHA1:	F58EEC0DF5B76D0249638D67510F8227A4834F98
SHA-256:	BE644E3BBCEABB81D6107E78F380D285CD5BBF7CDA5D0B3862AE1DC434E73400
SHA-512:	3BAA9DD6E3DD600A901A5EB32AB86D9FEB0B9DC5AE9ED573C5B3BA63506452CD0C37B055F72886EE4AB620C9832AC68E6AAA27604FC7F7AB113B0D409D112514
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":"13264656394591924","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6bf45214-0143-45bc-b2ac-8d7b0a940340.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6bf45214-0143-45bc-b2ac-8d7b0a940340.tmp	
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7630cb86-5e8d-4a52-ba35-111751caa80d.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):	1208
Entropy (8bit):	5.553360898307606
Encrypted:	false
SSDEEP:	24:YT6H0UhHm/ZeU8kG1KUem6F8atwUE7aUeCG7wUFRUeIQ:YT6UUhGxeU8DKUe78aOUPUeC4wUbUeh
MD5:	3C1E481E9728F3D2D58432244E9BC95F
SHA1:	C323A55B49F58DC0E8F30127C0987054BB37BEF4
SHA-256:	93585B9972978B81B6D404E6D0369979EC203E7D6838021E8E6DF64C200C3C84
SHA-512:	442D4B24DA3A7181978E0D93671E40A72EECF90E1B5615E95BF3F3E88D0ACCEB591439469686DE57469E30B262892C704B519671E37833F86BA2D2DBC5C590B5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651718807.160284,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620182807.160291},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1651718798.025817,"host":"2fyp6Zj7wfyniJVJxhIrUTsXM1PZeyziOe2tmKst6To=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620182798.025822},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1651718797.55261,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ae5b71a-19cd-47fe-9bdb-b45f4cf9210c.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):	5861
Entropy (8bit):	5.185638275766861
Encrypted:	false
SSDEEP:	96:nIFDJ/TfNY1M5fSVXqIk0JCKL83pkv1jYk9hZQbOTQVuwn:nI/fvS4C4KSpkvyk9y
MD5:	825205BFC6F093AC8FC04A1F67E9D7F6
SHA1:	9ACF27B04574288869B45C0B11BFCEE240C8291B
SHA-256:	9276DD2E56AF000ED5B7E0A5D2D92DD79FD50FE2C330A8B2B5310CA21DCCA5D7
SHA-512:	85301335966B4143D68264DE966E81A512E83265BF62F28D1A395944EDA230FC74DCF9FF81FD0274F1BAAFB144E5551E5735E260FA9E3DED1EBB26A2E55DE45F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264656394919701","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","0","0","0","0","0","0","0","0","0","1538886"],"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","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):	336
Entropy (8bit):	5.2494414919550545
Encrypted:	false
SSDEEP:	6:msmaJQyq2P923iKKdK9RXXTZIFUtpdY4SG1ZmwPdqQRkwO923iKKdK9RXX5LJ:tJVv45Kk7XT2FUtpdY4SG1/PdqI5L5KU
MD5:	87D650F4654C9F99200F26C0765AC5DC
SHA1:	572D13A66519672A5ACCE1965EF4BE4C2C5149A0
SHA-256:	5A7CEAF48EFA357175D6DB24AE2E700D76FBD19F4A4379674437E4D1642A2120
SHA-512:	C0F280BF001FF3BF9EA9EDC23F80AF288791A5546E5009C25D3576A6EAD07284080C65390653FD5F73F95C9CEB731EB685475AEC87498BD12CF07FF4757C638C
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:54.474 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-19:46:54.639 1b70 Recovering log #3.2021/05/04-19:46:54.648 1b70 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.212887236178032
Encrypted:	false
SSDEEP:	6:msLupQyq2P923iKKdKyDZIFUtpdJvYG1ZmwPd4NVSQRkwO923iKKdKyJLJ:tSpVv45Kk02FUtpdJvYG1/Pd4NVSI5L2
MD5:	88B47DC323CC1BBB44302D3467683B86
SHA1:	A75147204551180CDE83A7581033AA85490BE27D
SHA-256:	1B18142E62EB25F06085E57F81E930235D41DEB104F57D3FB029CA3C7504261B
SHA-512:	C6505CBA37A9567BB57D9E9AC625FC1AD1380581984A9ADD34DC9047FD46575507B451B69BA2A583295D8FB29ECB1A7335C3306CDDE4E2FC5F634EDC4FCD5 07
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:54.444 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-19 :46:54.446 1b70 Recovering log #3.2021/05/04-19:46:54.447 1b70 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0481116f3cd8293f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.51798310831975
Encrypted:	false
SSDEEP:	6:mlYL8vc7ZALSRTVLx1D5aqwF32Lr0nK6t:z0c7ZZTRD5w32U
MD5:	9FB1B70BECD6E7EB89678DD51BAF4665
SHA1:	0393756BDC2F52BAA04F7F3CB80D4B131D6282F2
SHA-256:	A6B3AC39BA27092F4CD8559FA470B3EEB54BF7BEECC520E6C34915C2EAEBE6CD
SHA-512:	FDD9F03C072EC28720D8E32896F4158E955D59C40D42E27AC75EF65CF5B0F02F44089A88515D0F8322F6A2E15CF2F35AEF855F346396AEEB20BE02D87F2275EE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...O:....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meCore.min.js .https://microsoft.com/D.?." /.....b.....DMB#R...>.....m$.....A. .Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04b9cf4c7c39886f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	299
Entropy (8bit):	5.716694744671919
Encrypted:	false
SSDEEP:	6:mQdnYcBD631XAQi8RuadTxUydwPzXcY3QDXHTapIFv4r3llZK6t:9VDu1XAnAuadTxUOsLhQDXaIFvI
MD5:	05FAA7C5F0EF004E4486DF1D83F6C756
SHA1:	D20C482337CF1BBE0D9DD54DC581E59652CFC381
SHA-256:	A92103D07F069B27727D21BE3D6DA1B3DFE0EE2C52D07D0082E51B7ABE36D5C6
SHA-512:	D511F069323B1EACE2B64D3708F02DE5528E7027C21FC6AC1A89FD2683C4115CC24AE7956B093482AA7DDC6680B7D95A13BE34B47D7D0C1AA02FB34C38A5F2 E
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://account.microsoft.com/dist/oneui.razor/public/scripts/amx.min.js?v=B51B71CD1157AD7895177C07B006CB93F95CE755838286D 2A7F725330B3E2467 .https://microsoft.com/<..~" /.....rI.....p.54t.....I...M.9.- ....Tt.A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\087e843a6a77f2e0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	6.231169385731735
Encrypted:	false
SSDEEP:	6:mydqEYWIcjAfbUy5Qhw1r3wmAvYxsYmzKa7KSTqSRjrHitj3dBCgC15Nal78hRK+:1dqfcaJH8/YeVzaIRPCtjdYxa5q
MD5:	CC883045AC16EF6E167C37E598EA9AE3
SHA1:	8CAD770FDCE8051E4763D9270DAA2715A1F305DF
SHA-256:	24F904D56F1F10FCA7A76AFA61506163FD642F2D73D11C58EE68F36B6FD32DBB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\087e843a6a77f2e0_0	
SHA-512:	2CE1D3DB50C2AA2F6AE7CFC6D1338B6B40D0CB1A820143B5F71B03ED4973976362A9BEF0C8FE404FDBE7976299E55FFAA2B006452A86E80ED362F593710E171
Malicious:	false
Reputation:	low
Preview:	0\r..m..... ....._keyhttps://cccounty-my.sharepoint.com/ScriptResource.axd?d=XLHvvuqUg5InnNgZ7caYxePwb7iO9lfyUqU9z6CieiK1SeY7yBm0gNcAOuZf0MzFuL mKkfu58X2GVY3x4M52CDdNMEhQq0CmVo3OdaFfc6_9k1CLdxRllcdgIpx2hdxMS2J_lenCy-Qic2F5StaYTp7sZ-cx2zIS6f4_-gaPMsn1QDVCRxnbjf-lEcPZmHWo0&t= 363be08 .https://sharepoint.com/...|" /.....g.....,..<..M..uj.S.9...qGy=l3~x..AU...A..Eo.....D.'.....A..Eo.....

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):	351
Entropy (8bit):	5.951032303320987
Encrypted:	false
SSDEEP:	6:m3VYyK08fNH1DUFlYcSyL6jeVbK6to5TMJX1UZbUIL62q:aKjfNH1DUfnSy8ej0K1KJH
MD5:	9EE671ABB49E3401D55143960EA2E073
SHA1:	51AA79F215D28D029212BEFBBA73A10B689127CD
SHA-256:	B18CFF9D840F8F58E941D1BE6DA66628752FCAC213DFD461B0D05C3237D05206
SHA-512:	1EF02891B7347A232F575710E8249C86055ADF9C2EE972108C483C2EB1A6119B83AF47B35A8945498307D9C8B2046A6C9E2DA186EEEF1F24B3517FC3FB17012D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/..z}" /.....=.z-.7.K]..~..=..9.....8...A..Eo.....4z{..... ...A..Eo.....z}" /.`...DD662A76FBB4881B2273B6392C26D582E4D3171AD0A622C05C00C76FF33037DD...=.z-.7.K]..~..=..9.....8...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b6a779b97f6aaad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	53714
Entropy (8bit):	5.965975121438062
Encrypted:	false
SSDEEP:	768:Nkd+n+uL+NdMzjwhsQdGQPNQdGQPyQdGQPHQdGQPXQdGQPJVLvL/iyuL/mWh1:KqiHMzjwhsWlWqWfWvWhVLvL/iyuLDb
MD5:	5A42ED589A08C8B080EA117986FA3B84
SHA1:	F26D8403DB7C70A130BBAB7F3ED030505D4AEF3B
SHA-256:	3E6F124A5888911DCEE1BE2C531A1FA9E6CE5CFEE601CD90C08D7183F723CDA4
SHA-512:	C0ED41DB8C7D7441DBC2F51A1B76C2F0267C03CE9F1826A4A81AECA3244CCC89FBEAAB9866A573FB9E447D63B3A36B8821C23BBFEA45668B90A7DC7E024F0 43
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.....&...._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meBoot.min.js .https://microsoft.com/...~" /.....1K.....H_.s5.ux\`..y.e.B.$.V.]./xZ. .A..Eo.....G!.....A..Eo.....'..g....O....8.....E.....L.....(S.H..`L.....L`.....Q.`..+z....MeControlDefine...Qc.."....meBoot.....`.....M`... ...Qc.....exports..$QgZ..v....@mecontrol/web-inline....(S.....IaE.....6....P...fj..@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@...(..@.) .*..@.*.*..@.*.,..@.,.,..@.,0..@.0.;..@.;.=..@.=.>..@.>.>..@.>.@..@.@.@..@.@.@..@.A.B..@.B.C..@.C.D..@.E.G..@.G.I..@.J.J..@.L.L..@.L.`..@.`.l..@.l.m..@.m.p..@. p.r..@.r.t..@.t.{..@.{.|..@.}.~..@.~.~..@.~....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.. .....@.....@.....@.....@.....@.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1316511c4faf2fc7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	515
Entropy (8bit):	5.384654332642804
Encrypted:	false
SSDEEP:	12:/DFam08xEjsKlITP2RTzgoz3Pl1rKDoQK:/ham0yMstb2RTb3PPrK8l
MD5:	515800FFC7B1595A2164DDF094D6B787
SHA1:	70510C34394446BB00C2719A42AC0228E0666FAD
SHA-256:	1B699C514828C38317B0C0938288F9F45B12BE6039979EA30853278E0B0D5286
SHA-512:	079AE578D22F9A0C533E0CFD259E99CF01FA1B68F03EFA38140A72B43357BD7DDEDA5B2A86E4D46905BDC27AA279D054476235E41037664FD5574A30573D930
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.q...._keyhttps://www.microsoft.com/mwf/js/MWF_20210208_31270267/actiontoggle/alert/ambientvideo/areaheading/autosuggest/button/contentplaceme nt/contentplacementitem/dialog/divider/drawer/glyph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/mosaicplacement/multislidecarousel/pagebehaviors/ productplacement/rating/skiptomain/slider/social?apiVersion=1.0 .https://microsoft.com/.p." /.....#F.sN..zQ)<.....9X.. .....A..Eo.....A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\136d745a1210e64e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	43089
Entropy (8bit):	5.873065837706352
Encrypted:	false
SSDEEP:	768:2SjpyZf1zj6tN0XEHDh9nmH3adW2JXcy7XpNk1FycV3Vt:SZ00S98H38W2Jr7ZNkjzt
MD5:	55ACDF6B7793919F28A0952CCB5BA94D
SHA1:	C85BD4C9126488DCE19B50E128098398F6D58C76
SHA-256:	50FB0B42E7EC359FBA6BB69039B8AF789C7DDC8D4BAE6215261CB36470618E54
SHA-512:	2357491DBFC583BC82BB6F5F835A3973C335535022AA3FCC020C1110222266CC404AACFA11B6396A641F97D2B0BF7B12DA44D0AB816210931AD71A06BD598A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-bcc229/94-3cd1e0?ver=2.0&_cf=20210415 .https://microsoft.com/@..." /.....|.....5f.....w..I(1..Z.n.>.a..A..Eo..... .....A..Eo.....'.....O....P.....1.....|.....(S....`....=.L`.....L`.....QbrA.....awa...QdB>.....behaviorKey...Qc.....define....Qd.....jsllConfig.....`.....M`.....Qe.....rawJsllConfig....(S.....IaB.....IE.@.-.....P.a.....https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-bcc229/94-3cd1e0?ver=2.0&_cf=20210415...a.....D`....D`....D`.....`V...&...&..A.&.(S.t.`.....<L`.....@Rc.....Qb..}....t.....QbzO.....n.....S.b.....I`....Da.....(S...Ia.....Qb6.....r.....!.d.....(S...Ia...../

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\14557f4877e37a1a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	104456
Entropy (8bit):	5.791986350077854
Encrypted:	false
SSDEEP:	1536:jT0N2gu5pDmkblrL1CzP5sJ8YnV5KDZy644PFEFDKMfb7OSj+qkqc:jlNm3L8zmJ8Yn+ZywPFlfnLj+D5
MD5:	3601F677858C5563311EE94547911C7A
SHA1:	09CDBB6B5A16677572CFADCC9B62751134D7031A
SHA-256:	E77DC0207727AC71E40C51CACA42FA812B15BFE3EEC6EB19ADD9FD40AF287F54
SHA-512:	6A8D32580E2E8319A1AD867B55F91A3260ED09320DE3E4049526CA32F3305594F6C600556808241C838EAB9FF59152CD5297395C7B9155D3F7D3381085410FF3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....DD662A76FBB4881B2273B6392C26D582E4D3171AD0A622C05C00C76FF33037DD.....'..v....O#.....y.....d....&.....`.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....N.....Q.@.LR.....module....Qc..D-....exports...Qc..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...Qb.[.....c.....QbZ.....d.....Qb.?.7....e.....Qb&.;|....f.....Qb..e....h.....S...Qb>.....j.....QbR.T.....k.....Qb6.Gl....m.....Qbz9.....n.....Qb...z....o.....Qb~Vd.....p.....Qb.....q.....Qb*7.3....r.....Qb..b.....t.....R....Qb.....v.....Qb~5.....w.....QbN.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\14c06f6781117c4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16983
Entropy (8bit):	6.103583959453751
Encrypted:	false
SSDEEP:	192:fxlxSMldeVVe+s6JMnxacjJvOHj2yEHuOJdYvZduHheDtXxka334DGQhtqO/MKzi:fxlxSkis69cjJvutEHu8OiWnOrqKvaX
MD5:	E522BEE48D59DBEBEE4F5E774313F422
SHA1:	5E7447A2902963EE216FE67BDB382B183DB1CBDC
SHA-256:	ACD516B78F98D58E378C8DB751F219651DD0EB23D56A1C8ADF24125F3BE19A5A
SHA-512:	F8E1CB21E94D1FE43170A1B3939E1681EE152C9A3FFBCDAFC775CAE84F852E5E29E17BD3201C8424B6BAA5DED1AEA72A6A44A702DD7B26D2FCD37EF7C2FFB017
Malicious:	false
Reputation:	low
Preview:	0\r..m....._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-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.]}" /.....o..m~v....*>...p....a..K..o..M..A..Eo.....A..Eo.....'.z....O.....?...p.E.....4.....(S.0..`.....L`.....(S....`.....L`.....LRc".....Qd..Y\....requirejs.....Q.@..u.....require...Q.@.c.[....define....Q.P.....__extends...d.....I`....Da..... ...(S..`.....L`>.....Rcf.....*.....Qb..P.....n.....Qb...t...r....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\166ee82c52b87e97_0	
Size (bytes):	220
Entropy (8bit):	5.441108370250081
Encrypted:	false
SSDEEP:	3:m+lkLI6v8RzYmfksCVbKEfQXtkMEOZuFvDFYtRbueflHCtwt5yZ9aPjGWTh/z4mt:mY6EYmcRR3/wZdDKVtCi96Vr1PK6t
MD5:	38F8D3ED79B4D35A0CD09DA91D9FBEFB
SHA1:	4CFB353FFE8F3392AB39A185A59F482296C55228
SHA-256:	3DE0CBD24EE084A7ECD30BB6DE2A34A7753B510E96B812F8E2196D8CF7E053AF
SHA-512:	7748F3D6E132CAB1ACE649A75918734280CAA30E11A71D633C39498A7A04D5CEC523E8640E71AD4E47C15DF5790C75391D6C50AA07950205F6E68F93A807D395
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/..K." /.......................(..A=Z....F...1/.k....s6...A..Eo.............. ...A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1addd37645bc92bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.548745506147608
Encrypted:	false
SSDEEP:	6:mZYklyBLg1iyPfwvKXxmWBdBCqAFHlYividrrZK6t:kELg1iyPmihBdzgKRT
MD5:	D5BA7C150CDB3FE5DBDFE5C3C9280F98
SHA1:	87E2C4B9DD64B3AD81029B59956FA4495CFDD3FF
SHA-256:	7E9CB40BEAC4A457BD73FB974B6EFABC521AF2BC6690836F22523769DA4E6698
SHA-512:	5992D5AD2703D9C363A5EF32C7F0B60C7CF5EC939AF50FFC269ED5F447961602912CF9AD86D37B143C4D7BBC171A52ECADCDDD6D464AF2F5E9910AE7F4EFD DB
Malicious:	false
Reputation:	low
Preview:	0\r..m......s...V......_keyhttps://statica.akamai.odsp.cdn.office.net/bld/_layouts/15/16.0.21221.12005/require.js .https://sharepoint.com/.K.|" /............. ....I..8#...T...w...uxU....I x...b|.A..Eo........f..........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\225853b3d3cc9c98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59890
Entropy (8bit):	5.294011692822004
Encrypted:	false
SSDEEP:	1536:yOLIIheFoceBkUq6L0z4KjPJXzzZImtNAzLwRwJpkP5xYi1rMQtcDtdsYqO9rD12:A
MD5:	495A81BD86CDDBC24605079276EA3090
SHA1:	CACC9CF5430D2A804F50109C066C5D35BDD35C52
SHA-256:	0EF9C7CFBBECCC957066B5253FBFDB99642095499012FCE00008F6C07680A93D
SHA-512:	ED2BC0B5677EB3C394BFF6E6BAB484ABE744AA5F2D716560BAC3C18EE8C45B8F250631F2D37328E4808E70DE34C2BAE2A7FF4624B432DEE752F2DE7F55959E 71
Malicious:	false
Reputation:	low
Preview:	0\r..m......b....D......_keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meCore.min.js .https://microsoft.com/...~" /.............xM.......@...T.U..i.~I..r...|.q.`..H.9 .A..Eo......A...........A..Eo................................'......O....`....#......................l........................(S.H..`L.....L`......Q.`..+z....MeControlDefine...Qc.......meCore.......`......M`......Qc..... ..exports..$QgZ..v....@mecontrol/web-inline.... Qf...x....@mecontrol/web-boot..(S.....Ia[...~.........A.........~....@......@......@......@......@......@......@......@......@......@.. ....@......@......@......@...+..@.+.,..@.,.-..@.-./..@././..@./.3..@.3.?..@.?.A..@.A.B..@.B.D..@.D.D..@.D.D..@.D.F..@.F.J..@.J.J..@.K.Z..@.Z.]..@.].]..@.^.d..@.d.f..@.g.i ..@.i.j..@.j.j..@.k.l..@.m.o..@.p.q..@.q.x..@.x.{..@.{.}..@.}....@.......@........@........@.......@.......@........@......@......@........@......@......@.......@........@.......@........@.. ......@........@........@....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\300bb9fb98ab63f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.538987158023906
Encrypted:	false
SSDEEP:	6:mNtlXYL8woG/8mLD2D+Ajwyz48pC6AZanK6t:0XizUmLD2D/jYyCIp
MD5:	6B0C152BD1A8608D39A6C4DB648093FC
SHA1:	AA8D000040F0112CC4FB1418B0CA4F4571A1C69B
SHA-256:	71F064D1A72D193C452CD20D51A8654861771A1C894F557C8C32D6283AA438F2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\300bb9fb98ab63f0_0	
SHA-512:	DBA4B67E8232EFA7587A1C29E80DA45C94D854EED4FABD9C0C88F97DBD27262DFEF04D8DD39FC28EB766A68F91CDC42B07DBE992407D74A648AD0B656B8A 26F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....&....._keyhttps://mem.gfx.ms/meversion?partner=amc&market=en-us&uhf=1 .https://microsoft.com/q..~" /.....l.....y@.+.....KC+.wjL..l...Z.yD..LO.. A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30411d1af682235b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.705231418231579
Encrypted:	false
SSDEEP:	12:mqDQLf+5KWFhhozgGjBzIszpbZrYW1DIoNQX:mqj5FhYlzICp9YW1coNY
MD5:	A80B3C18DE1D4C12B86380D6BBF6A197
SHA1:	E03B4A754E92A16938459FB0DFC190A4D9E9D8C1
SHA-256:	331EECDD72E722E4B422F668E29A794C38CF868601C545D889DF4EB966331FAF
SHA-512:	E1FB93AF3487E7D7B9C9C6DEC2E3268AA47AE1BB09890C8753A752B0D9760891B567232275B3EBA987DDEE8C332D2112299FA79BE6CE0B87E7EDDFA114E3EA E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!...2b.A...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-6ade99/91-3596be/2b-b6ab60/e8- e8a01f/28-8f59e1/ed-a05786/58-f3fc85/d6-6e76d0/19-9c8e36/1a-3fe6fe/3f-7b39c7/66-afd0b6/f5-7e27a5/d7-de3320?ver=2.0&_cf=20210415 .https://microsoft.com/...." / .....s.....1e!.V"...d.....7GDSe..L.^..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328b75cf02d95d5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5992
Entropy (8bit):	5.812967409487188
Encrypted:	false
SSDEEP:	96:XTxi1OfjMiEjXdysuCBqFyU6mD+4sqTsBfj6iuXA84PxUMfAtvMKT:COrjQXUdFyU6QiB76nXA84Pxnf2
MD5:	62BC44C0B1BA8EF9675052284418B2F1
SHA1:	7C50E72827E5E189230F76AADC97C05B4184C119
SHA-256:	D2CBC7E55EC8B35CD4064BCA6DC5BE973D23BA4EBE0815F4302EEC6C1530188F
SHA-512:	9DFC0FC72E92D2BC3CF574C3F1E43073C764AABDA5300544848EF2F011130A2E116BA8A69306C269C1249DC68ECB1F395642242A7368F3A2181184D592EC2C5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...?....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/..{}" /.....U..0. ....\.oQ.8gD.r*{.....A..Eo.....B.....A..Eo.....'.0u....O.....F7~.....(S.y...`.....L`\.....L`....(S.....Ia&...m....,Qi...?....ShowSelect edComponentKeyPress...E.@.-....hP.....\...https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70a.....D`....D`....D`.....Q....` ....&...&....&.(S...Ia.....,Qi*)O. …SetRightSideNavigationMenuHeightE..q.d....).....&.(S...Ia.....$Qg..=.....ShowSelectedComponent...E.d.....&.(S.....Ia..... (..f.....-.....d.....4.....d.....-.....d.....!.!.....Qd.}.....ShowToolTip.E.d.....D&.(S...Ia....>.....e.....-.-..... Qf.$.(....AssignToolTipTo Href.E.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\347259540ff04e44_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.77667239744045
Encrypted:	false
SSDEEP:	6:mOotYcBD+Iw1M6fyQEfDD8AC69Jt7nK6t:ID+IwG67EfDRp
MD5:	2C56177AAFB56435715C5181D7387049
SHA1:	4F73E825B9344ED82E656CC6ADFFD769B66708F9
SHA-256:	5C5E80E1C022C93105298DFA0266ECC500647FE9B8DE71D4F45C415AE1B6D9E3
SHA-512:	F49B3A572D1F3A6A35159701545AEE2FD8FD961C8C1C2C91998F759EC2A7CC46969B92A74052225E0F3CE985D6A5D5B4174E3889255ABC2E1CAC4469E05C849
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....$.H...._keyhttps://account.microsoft.com/bundles/scripts/webi?v=Hr6sQs8agKb6EPaXzJIDUSK5w7Ll68eh5Kh2Ki56i1g1 .https://microsoft.com/.[.~" /..... E.....8P|…I.A-.....(+"...1%x.&..-`.V.A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38c7c19d1d0ee3c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17753
Entropy (8bit):	5.6357134457079825
Encrypted:	false
SSDEEP:	384:88KzJ+K0SH8hNSc9OEJiyILn8lsHS3beba3IWi:TKtPcHSc9D8yIQlfe2C
MD5:	86B8C9CF5E4A706C36735566E19AEFCA
SHA1:	637E49303460B3B6F837839F13894C9549A1F3CC
SHA-256:	DC63B19F5F82E3044CF1F72CB1F772BD375FA7DA53239AC3F8E185C25CF40238
SHA-512:	01DD4DC15C011C820B6C50998286B295374C601A8C6A4D3E9B27B4889F28243444D3EF7B77731A74F091773993E8D57844D3A1F885A1B0F6A6B098F1A6C8D08F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....5....._keyhttps://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.js .https://live.com/QB..'' /.....O.....B.K.f.zF[U.m....b....`..<.%"%[..A..Eo.....M<.....A..Eo.....'.nC....O.....C..;.6:.....(S....`.....L`.....L`F....(S.<.`2....L`....I..K`....Di.....%.....g.....g.....g.....(Rc.....Qb".W...._iz.`....Da....h.....b.....B...@.-....`P.q.....R...https://logincdn.msauth.net/16.000/content/js/MeControl_cT3-bL3bZ5AAnjmz77cksQ2.js..a.....D`....D`....D`.....)....`....&...&..A,&.(S.....Ia@...X.....Qb.4....._Du.E..A/d.....&.(S...Iac.....QbF@....._J..E.d.....&.(S...Ia.....Qbz..J...._BD.E.d.....&.(S...Ia.....Qb>..o...._F..E.d.....&.(S...Ia.....Qb"Ze....._BE.E.d.....&...(S...Ia ...8.....Qd...\....strOrDefaultE.d.....&.(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\462d64d34aad30da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.550157414477394
Encrypted:	false
SSDEEP:	6:mUv/gEYL8uCKxwVOW8mLD2DHktkPfAtm4rLK6t:/vI7rbwVcmLD2DEAfA7
MD5:	A1D24DE45296A04AB23E491037592E66
SHA1:	239334BB15C29EF1FCB8FA5DCE32AEDC77B18A17
SHA-256:	EBE8A86E0851A534764427F77DF666687E5B15A2F8A6179C94FF0724151D1FA2
SHA-512:	E3CADCE497D20264A2EB232460003006C9CD81C94B72CA7F57195C0DF2FA5392D91ED20C8DB4E7467C44F72453B5491936256326BC65CD2D8A42ABFD85D754(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://mem.gfx.ms/meversion?partner=OfficeProducts&market=en-us&uhf=1 .https://microsoft.com/.)w." /.....y.o.W.*.5...=.....+..v.....A..Eo.....x.X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a7b0a16eebe4c59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19454
Entropy (8bit):	6.01159236756297
Encrypted:	false
SSDEEP:	384:exLxeknx6H1cwJvB1eFS5GWdooFm8qKvac:i0K1Wyo4Kf
MD5:	D3B0F9DC35B7AC2160802116895819E7
SHA1:	35058AE1083B38A9D9A633F9B7FDB26BB5BBDA13
SHA-256:	7A35AF39B3CD170D1DD6EF3369A6EADEF3B49240FA95D2D110BA89D090376519
SHA-512:	0FE5B90EEFFD2A62917E4F4E7CD71CC4CB655F5127105C4E580398BAF005B391CB4F62A5238385B1F0A48B0ED3373E1E672433198CA9D0137D4F3D2728D509D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.a....._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-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.w~" /.....(.....o..r&.@..I.....a._.?f..~...A..Eo.....m].....A..Eo.....'.z.....O.....H....-[.....4.....(S.0..`.....L`.....(S...`.....L`.....LRc".....Qd.....requirejs.....Qc.....require...Q.@.V.7....define....Q.P.2....__extends...d.....l`....Da..... ...(S..`.....L`>.....Rcf.....*.....Qb*/.....n.....Qb.e.....r.....Q

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):	5.554854438222852
Encrypted:	false
SSDEEP:	6:mCVYL8uCKxwVOdD2DlH1X+5df/CxJWom4QRK6t:irbwVgD2DTQfyWHjr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ac2f448771ab57b_0	
MD5:	F4064DAC5F15781E2561FA87693B330B
SHA1:	6AC5EB4B5C31658B337AB36093FCB53D165684F3
SHA-256:	67BD50C4CE0FD15B0834E6D1278EE9B08C734032AAF39A181526DBB5F8D5AC09
SHA-512:	D34A7F45B6A4194C4B12A59ACDB66F22ED1354492C6401EDEEAE1F844E519A3C6A3F0FE14203E68C34D8D6E3AB6D9613293A2E26BB0F4EE21B84D547F52C36 9
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/.Q&." /.....*d..,.....cP..Tl.*...A. .Eo.....63.D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5563163b962da706_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	6.168257057971434
Encrypted:	false
SSDEEP:	6:mqlgEYWIcjAfbUyiiWMQH11BQyE8r2/rIu9pgK3FYTU5lXdBOHXltlwomFTIxg7H:rscaiVfg8AQK3D7XdulA/L/N
MD5:	82D8F681C482D5DD84937B33DFF91B6E
SHA1:	D29B17C6E17D07049184EA70D65FC205DA4394CD
SHA-256:	67B977CBA690D293277772813CBE7A411BED6E39DB413F6D693256CC8763F2FE
SHA-512:	F78B13B1685C0F2CF8916FCE69002250A62F72356EA32E83EF91E3671B60099D213BC9C16727C59B5933DEF2E1715069BBAD3C7E3D442878AFA76E968AB73A8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q;.j...._keyhttps://cccounty-my.sharepoint.com/ScriptResource.axd?d=XjLkEB_vSvznU474E48kPJA1H9JTKlbxQRrF9mf4oevbHPo4Rsxshku2KRWdAyEvGe JXtGeRBr6q8THhytVreob8zoco7vSKH0VxNm-OjFffgsrM8_4XygNX6xBPyWb2EwmKReXoheA2Yv5LHydJ7p_w-QiZxE8PK3WazHfXSSs1&t=ffffffffe191061b .https://share point.com/...|" /.....".....^...p..w4.a...p..$.2.*Xdy...A..Eo.....U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6686b0c92e7fc912_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.499674533498059
Encrypted:	false
SSDEEP:	3:m+lWC6v8RzYLLIvc7QGMXLSRTk2FvDFYtRTcqNlHCvt6p6QC7R+mg7T/pK5kt:mi6EYL8vc7ZALSRTkVDQlp74f+lK6t
MD5:	41F567B6C527390F6E89BC6396B1B26E
SHA1:	C75A99F1BA48DA44ADA0D1769FF4B57543512280
SHA-256:	E5D9A4448F9348EF5D5E32D2FC7EB1152EA545C08726D4CF759E58567DE73DCD
SHA-512:	E85A2D251C191248A20DD0B0F8E6EF7FF2AD4155CE4CC9EA00A4D3D095FE65BC89BA25D2BBEFE782755EE7849BBEFC333EE2A69645D28997DDF0A1610576F3 AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21035.1/de-DE/meBoot.min.js .https://microsoft.com/..9." /.....*L....^>.....#(....S..t..^...4..A..Eo..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76c0ccd3a8d876aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.580417786690455
Encrypted:	false
SSDEEP:	12:MzDQLf+5KWFhhBoKRtCOXUDjNC1Ngw9jMuwe9l1D1DA+357:Gj5FhHhtCOXUDRCrMuFpD18+p7
MD5:	AD60ABD566402D34FA1428F92B570E95
SHA1:	ACBB05718A7EDB0FAEE50A05A187E60DF03D5D98
SHA-256:	D1F98B7BD71A343189C52C885DB9B1A65AF7333DC0640DFA68EA117E2EF2D70E
SHA-512:	8E2E91F4BF4EC7607997A95AA3A82DE7B88CEDBF4C4778CFCCF1D1F702F8B929B6981FC279E6A978816BBBD653E3BC7F2A42CC51D03C107C25F8F63C1A6EDI CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76c0ccd3a8d876aa_0	
Preview:	0\r..m.....:.W....._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-c07ea1/9d-b58f60/f6-aa5278/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-cda2d3/69-13871c/b7-0ad59f/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210415 .https://microsoft.com/...." /.....[.....<.c...R.%...>..!g...s..{Z..B.A..Eo.....zs`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\839dc2a9677b3e84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96472
Entropy (8bit):	5.828166198200441
Encrypted:	false
SSDEEP:	1536:ppdXZec5lKaDHZkeugbUrpiAyTaTt5LPkkFnw5O43:6qZ5NugHnTaTj1Fnw5Oi
MD5:	F673A335D70371CBB7A9AB3C8BD5345D
SHA1:	2FC882A011977AB3E9BAB78111EBF4280DF3C4C8
SHA-256:	5E05FDC24A64FA1DF6C0B6823FCA94EEF72F4D62415E23B3BBECFE78DEC2CF9E
SHA-512:	12A03995B4CC60153697E52A58E00A7DE3CB125E91478CA7222FE153C6D8FAA1059276749D26830F737D52189799080CDADFBF18241B16E79089BD1ABF3CD67C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...8)Mg....758A17C84FED3F5C44C96C1EAEF992FC4813F5911792E7AB1C9971D6295AB33F.....'..S....O!....w....}\.....H#.....,.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb..}....t...`....I`....Da....I.....Q.@j.~"....module....Qc.....exports...Qc...4....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..R.....e.....Qb6.....r.....S...Qb.....o.....M...Qb".....s.....R....Qb^%.....I.....Qb'"u.....c.....Qb..4H....f.....Qb.WD2....p.....Qb.K.....d.....Qb..=.....h.....Qb.U.....y.....Qbj.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83e647e14a56f97a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.775896638432376
Encrypted:	false
SSDEEP:	12:2MDQLf+5KWFhhozgGjBQaIepbH1DdKF1r:2Mj5FhYlPIepb15c
MD5:	C69EE62BF99EEE5EEFF16D3794A94351
SHA1:	F19007FB6BC628ADE82A728DFCFB010C6B84EC68
SHA-256:	EE85499CCAD020BF8B7C07F641A2911579A5251B32B310A264EC00FCB1C74CC7
SHA-512:	709E7067CBB1A34E1C34CB190E659464C1514F689945FA54B1D8791A47D2717F31BADB3FE7BF5FC8F412934FB6DAB36B03270DCA8E11B68B3821E61E1DABA544
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/9e-6ade99/91-3596be/2b-b6ab60/e8-e8a01f/28-8f59e1/ed-a05786/58-f3fc85/c4-301a8f/19-9c8e36/1a-3fe6fe/66-afd0b6/f5-7e27a5?ver=2.0&_cf=20210415 .https://microsoft.com/..q." /.....5....M.....e...*S.....[RX.T.A..Eo.....{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86aa07f121a6237f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	5.77054014108674
Encrypted:	false
SSDEEP:	6:mgXYcBD+IwaG5wHfCfxsxKNlDV+gDwyxJ8cWygr5thK6t:xLD+IwXKHfCfxKKXAgDwoyr
MD5:	D74338D6A13D2BADBE2E7180D4AD58EA
SHA1:	8311E38294B000D3CCED8D720E8631A78BFB9DFC
SHA-256:	2BF7DCE2E53EEB1F6C7693F577DDA9CAA1A01EE5CEE4476C687B569DD17849A8
SHA-512:	CE182BA720E7F5C58011D3E2D644586EAD9FBB9652FBBBC6BA89481E9B611CB8CB3B80EB783210A56E10CD19C77F61F6310C6EADAEC073D523147B7C9F0DC38E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....._keyhttps://account.microsoft.com/bundles/scripts/experiments?v=dhMHbKozrGOgxx2MYXfMMYMDxUo0UcLjtgcfK8uL2iA1 .https://microsoft.com/.&.~" /.....E.....Q...JKd.,.P.U...Oy9@.Du.>..#...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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.8550697298961945
Encrypted:	false
SSDEEP:	6:mXYI4McTDsJegDCM1TrlENtK6tBMA2XVanndC2iTrlE9:e+TDsYgDj134EAiannAF3
MD5:	ABB3415CAAB181F4DA105EE57A7D5DE6
SHA1:	977A008FDFF10A7FFCC13783DCCC04AF4C23F597
SHA-256:	E1BF8B07FD9F0FCD7F94547FE1F1781B5ECD65B08BF7FB3C3D131E2AF676A8AD
SHA-512:	2AC995975BE2ACE2BA50E698D82374FB912AC4CECD231A455090D2832DC53C62517E03C9A8B5C467005A6D6B137A64695AC0C7F7EB18E75F3681B6429ACA3E 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/.'.~" /.....I.....<.S....I....*.W.U\..E?`..r.A..Eo.....H..... ....A..Eo.....'.~" /.p8..F1485456FB862634B6F64526C3B5BCAA9EFD460DF5BF5D9B235D96278D52B2F9....<.S....I....\*.W.U\..E?`..r.A..Eo.....IL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\94d12f6ce814ffd5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.566988009488165
Encrypted:	false
SSDEEP:	3:m+l2w/l6v8RzYBREI/plPbp5S/QaxLLuFvDFYtRHF5elHC1tlNwdAa1KRe9A2dMA:mi/gEYsYpl3ax/dDl51vlWZARipTK6t
MD5:	9A9BD8521A64D93A0C92A2EECB9832AD
SHA1:	74EFB56E128C9AEB5301DEF23693C65BFAA216DD
SHA-256:	07A30B35D162768E38E69E2EC7E40BE1EAF79B7732C209CF3E06F0D7C8B36218
SHA-512:	57A7B7102C14A121C3B392CCBCAE3CDF7CCF057ECCB95DBBC16C02754D44DB8EF4D0CE3AFF0948518C613D9FCD7B22E374C674496BEA62145777FDF24C33E BBD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...@'t...._keyhttps://mwf-service.akamaized.net/mwf/js/bundle/1.57.8/mwf-main.umd.min.js .https://microsoft.com/k..~" /.....qI.....j.k.D2.Ek%.....M.N...JO .jK..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):	5.91327886713989
Encrypted:	false
SSDEEP:	6:m0iYGLTDQyKfZ+ONNKM3IGRWm8SIyDWVOU0Jf37eTZK6tyl8ZUdJMX60Jf37fp/:D6DQLjl4mxlyDWpM3+Tsl8qzM37p/
MD5:	EAF0D252A5EEC08496D71079F242D574
SHA1:	FB787ABF830B4781E67F9100BE7FF15B70A68152
SHA-256:	65B4ED06DDAAE9306E7B6A702986DA81801F95ADAE8E07DF944725E91441D511
SHA-512:	01AD071CED73EBBE2E034528E43B37FDE0BC145F59C0F7D2288F100AED385568828651E86345983E13F780D3C14DC184A2B355BAC0F3009662DE303AA80F541
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/:.#." /.....'|.....C..j.,c%X.i.Y-....F...N.A..Eo.....,X.....A..Eo.....:.#." /.0x..758A17C84FED3F5C44C96C1EAEF992FC4813F5911792E7AB 1C9971D6295AB33F.'|.....C..j.,c%X.i.Y-....F...N.A..Eo.....G..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4e37f7fb809c2dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	5.668220160581615
Encrypted:	false
SSDEEP:	6:mQaXYEcOjyBLgsHaYCOziRzqy9KVBdBLEsX5+1iy4dDhq7DK6t:zOmLgshCOmReyMVBd6sX5+1iyIDgp
MD5:	A40A098903CDC5017F3FA247A915C406
SHA1:	DAD665B81503A9BC440E449DBEF253AFB07B09D0
SHA-256:	A83EF4637B742DD41EC624AF536FA024EAAA2A79A01911CF677B74CD364D851A
SHA-512:	AE9ABAC3A9C795EBC5219DBCC792A812432229FC66FA2A13522E2B5ABB763D8E4AB3B71519A8CFB49E3B310519E59ABC91E99C356D3041A8B499D05FACE528 53

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4e37f7fb809c2dc_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.z...._keyhttps://modern.akamai.odsp.cdn.office.net/files/odsp-web-prod_2021-04-23.001/spoguestaccess-74b74b08.js .https://sharepoint.com/.E.|" /..... .....#>.....r.....>G..[....?..A..Eo.....{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7088b4299cd1633_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	6.030584264633989
Encrypted:	false
SSDEEP:	6:mVzEYWIcjAf52QQpLGS0wgSbczs/GkkRpK3uVSXdByrANIrQnE+RfUDK6t:CfctSS0wXWsekIVudPI8nEAM1
MD5:	6DE519082FD11DF702CD3A3D06C30A11
SHA1:	B623A89276B0A68B7BD7504BB160DE0D90182E51
SHA-256:	8E866E6982FF8F9A0311C5FBFAE6783D85A6C36084FE7484F72918757D8328FF
SHA-512:	712502651AEC792D51A27FD48D3B17D5BDBC7427DB4FC8DFD7B9FD7FB6DDD978753ECD2238DC45D0E3C2C242C5323784C1FA74E0D21B5B84EF27AC3ACC7B F4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.r...._keyhttps://cccounty-my.sharepoint.com/WebResource.axd?d=M5O6KBnw2Kc30Ye7wKtYeOmA0-ax1yV1j7R_PuQmXE74ijK-p7VgGBmEo6i 7sWjj4CxNK4ny_sJkjVmnmnT2J8iLdBFN1JnZpJ_Ut4sc-so1&t=637453780754849868 .https://sharepoint.com/...|" /.....s%.\.k@.n'#_..o1.W....d..^.i.A..Eo.....:.?.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae966ea7cdbe242d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	6.263104157980455
Encrypted:	false
SSDEEP:	12:Rhscai/MyE2iGzCUa1jfUGgVw1ZdVsJz1:RhsejBa1jfUvKsX
MD5:	4914EA1AF458764E32412C81E7BBA7E7
SHA1:	637F9087BF86593A92E239BE10124DBAB5BAB22F
SHA-256:	3FB0DBD92F50E754C33653AB46FAB3B7D09720A4591A53FAF0627096F54B4E1A
SHA-512:	094A4917BC61600757F5B8D3887A11C226AC9E49D70F23A0F85D6235556DFA7BB6E139C1A72208F6684366C210ADFDDF2BFC7526F511E43349F02C6AF3C5830B
Malicious:	false
Reputation:	low
Preview:	0\r..m..... ....*K....._keyhttps://cccounty-my.sharepoint.com/ScriptResource.axd?d=1fDsP7T8iuixVwu-fVH5iZr4cSvnLTO52_v1doY-7FhgWaaWltCQ1YAVn6OLWhnjO4 H7Q0hEdA1ci1J-fF8SwwiK_XjvCszvOdLq3HG47Gn9D2Wbuzf6Is9ZoJa7py-uqHcZcRZ-iDHA51cgnYAH2x-Xl2y2cYbZfeTTjc0ofc4xAm4qzlUFF1qMIzXHyJlA0&t=363be08 .https://sharepoint.com/...|" /.....o.....8F...Z..PF.M#...u.>'..2".....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b5c044ed76bbe646_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18073
Entropy (8bit):	5.515539491208722
Encrypted:	false
SSDEEP:	384:5tGrXYjcb9c7sDOI15M+iPhne/9ogif1nvyqOwUvrQx:bGro/nuzo
MD5:	B270AD9997C411B3E02C0CE6222FB2D0
SHA1:	C312F0FCE604DEE1E42A054881AFFF068ABBAEAE
SHA-256:	DF5EC6A2D41FC260BEE7516B5F9969DB550423B967B3DBA4CEA40B5C2DBC807C
SHA-512:	F7C5A8D544DB02010457C14044735A05B00CB5B29E33FA513F127BDCE9EC9A4924E083B4511DD6275CF8543DB06368C7595BF0D4426A9949F2A3F4FD1F464B85
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=17e9fd93-8142-d2e5-0026-505db3628325_1545a2a3-f8ee-1941-5c04-a4b822c95e2c_bad c3012-6391-ec2a-3c4d-eda492f079fc_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_5c27e8aa-9347-969e-39ac-37a4de428a8d .https://microsoft.com/..w~" /.....*.....?.}.....L.lP.ZO.....Q.A..Eo.....o.....A..Eo.....'.7[....O....0D..%.M9.....d.....$..... (S.I...`H.....L`.....L`.....Qc~.zo....Privacy.....Qc*..N....document..Qc.b.....ready....(S.....Ia..... ..f.....P...../.....IE.@.-....%.P.....https://c.s-microsoft.com/en-us/ CMSScripts/script.jsx?k=17e9fd93-8142-d2e5-0026-505db3628325_1545a2a3-f8ee-1941-5c04-a4b822c95e2c_badc3012-6391-ec2a-3c4d-eda492f079fc_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_5c27e8aa-9347-969e-39ac-37a4de428a8d...a.....D`....D`....D`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c94540d4c86c0448_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c94540d4c86c0448_0	
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.517497964206236
Encrypted:	false
SSDEEP:	3:m+lP0xqOA8RzYJb9yKIf8QPKxWSZFvDFYtR5xK1lHCTn/tFPoNK01mMm45lXlpK+:mvnYyK08fuDtHPa1u45RK6t
MD5:	9896D2672AFD2B362A881463EAF73293
SHA1:	61AC3C6D1259197EABA15B8BCF4CDE8A2C826AB9
SHA-256:	0C2E05E656F063B67D28DD809FB2DE1A0FEDFA7930AEDCA31F47B2EDD6466357
SHA-512:	E46A7C9A1659129566FDF7C3F95902FE10D82FC0D0C505CC87696A57BE963E5F42B46C91CEDEA694910D91B57D75853EBB448F9B1AB9E37B15F181BD11F4A7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....n#C...._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.1.min.js .https://microsoft.com/...~" /.....E.....{Z..Kn.....>.z..F.z@....h.Z.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d0f7c6311eac26cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	473
Entropy (8bit):	5.4514753177545
Encrypted:	false
SSDEEP:	6:m/tLYGLTDFSVjKhvK6cXBokqPSuwykNWXeFODOtyIgoG0Y17vKDwIlGSd17ntnK+:u1DFaj08xEPjTxTjoq1rKDPdF
MD5:	F4114FA36DC7A45C4D2A081E9236BDAA
SHA1:	C5024941D02CE62B2D7075EC4766C6EF5CFD8772
SHA-256:	041114156DEA173043D87EC35C7FB0ED65ACC413CCA9F72B5AB47981FE02A8CD
SHA-512:	C9675664B7B635F45B2B7EE5D2B52CC280367C7A07DF9D3A122D18573073F34AC405A69B3834537FCA2C687883034380113A285B581552AD1C9E83F69DBBF672
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....|....._keyhttps://www.microsoft.com/mwf/js/MWF_20210208_31270267/alert/ambientvideo/areaheading/autosuggest/button/calltoaction/dialog/divider/feature/glyph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/logo/mosaic/mosaicplacement/multislidecarousel/pagebehaviors/rating/skiptomain/slider/social?apiVersion=1.0 .https://microsoft.com/...." /.....7.5...z.;.? tz8]..'..8..>.a..A..Eo.....[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d70d38ab121c5d18_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	272
Entropy (8bit):	5.809802395335878
Encrypted:	false
SSDEEP:	6:mCCYcBD+lw01D01fceM3j4ERzaH6SDelAQ2CSjohIprFDK6t:HqD+lw0V0eeEj4E/SDeZRSjo2pv
MD5:	093E423FD30882945E9BD8787CED3E31
SHA1:	03EFE6F8D50D6419A8D3E84653258C7078A11F98
SHA-256:	3A9FEE58007ED35B3E5BDD008AC9D516374FF08241D63F67F19770A26C006006
SHA-512:	8693AF01366564AD7E73DC202244196B599F7B0B356DFCB519CEE32D83436DD55E15D0C05B65425A0A0514CFA5C726324342C13F53E324A15C4E9DCEF7A9CE2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://account.microsoft.com/bundles/scripts/site-migrated-oneui?v=EDs9RKiO0Lek-YWoRxPRbacGTNVI9DiD973iUfT93e01 .https://microsoft.com/.R.~" /.....Fl..... .!.[.$..[T.C..1.$.2.....^..A..Eo.....I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e80e6e93d4807d92_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	276760
Entropy (8bit):	5.582015349456139
Encrypted:	false
SSDEEP:	3072:xJdb2Z/e5oIiJ/l+mjp9ALBaoydE/cEDjTzBEw6PK97sRtXZOIIRNmLe1C1Acojp:xJBNS5/mjE6K9ARtXZ/KNxB
MD5:	E0BCCEEB108FA7CE97490C6B4945C74D
SHA1:	EA6AB13666377870AA309F93F617F79636F576BF
SHA-256:	ABA13F73F1A57A3F8A116BC1693E87A1E082F67DEDC80E354513493A3375D089
SHA-512:	BDACD62AE0434E944CC287A3E42A7457AD8FE6C3E81EED85859EFF212ED0DBADB8FEECD4EAC48E7FF17F54CF98036D80122A6C876A31D3C3F8A50C9DA1B9588
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e80e6e93d4807d92_0	
Reputation:	low
Preview:	0\r..m.....@...@..|....F1485456FB862634B6F64526C3B5BCAA9EFD460DF5BF5D9B235D96278D52B2F9.....'.tT....OP....7.....\....%.....(.....4.....H...,.....H.....d.....|.....L...L.....$.....$...`...,... ...|.....|.....$.....p.....p.....P.....(.....$.....|...8...|...(S.`..`|....$L`.....L`.....Qdb.....WcpConsent...(S...`.....LL`"....@Rc.....Qb.....e.....M....S.b$.....I`.....a....F....(S...`.....L`.....Qc.....exports..$..a.....C..Qb.....I...H..!....a.....Qb.....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\e9e05c56f0030d6b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270
Entropy (8bit):	5.880669338000547
Encrypted:	false
SSDEEP:	6:mzYcBD+IwX1aJMVQ0oQsDoc1OwNVCie+43RK6t:KD+IwX/uRQsDoRwNVB4r
MD5:	91F6EC121BFB5923FB407587E5D68919
SHA1:	016953D748E425C6F4F95E9F63BC681467BD4F07
SHA-256:	C9827BA5DAE8F9DD643A47F60A051A73329F13CCA019DAFC8C45368DD32C44C8
SHA-512:	524E9D4C537A3953884583CC533F96DBEB12D7278BC3449E5075B3200A1FC0CAAD523E91AC7C34226261ABADFEAD4CCCE16451FF2D8F31F8566DCFAB446B886
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://account.microsoft.com/bundles/scripts/FeedbackXS_AMC_UX?v=bqX0CpSRm5F9TyqPkh5S37dI7Qk2RAM5-zFb1TJuAdY1 .https://microsoft.com/./.~" /.....I.....s...(re(.....h.....<..J;.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ee5d3a8d13f7d9ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.531033999058694
Encrypted:	false
SSDEEP:	12:aGLDQLf+5KWFhhz59K7uCOXUDjNC1Ngw9jMuwe9l1D1DyLoZNroK1:aqj5Fh31COXUDRCrMuFpD1G9G
MD5:	C395C8EB056898EA8DB29256F3DB8F22
SHA1:	49C69905C1EC15B055F07186DE8E8E55DCB57062
SHA-256:	056CBC54EB2BEC69D5EB6B50B75BFB1745A5E552498234ADF907D476A138C046
SHA-512:	8FFF51D3361BE028A4E1B2945F6C3463B6C65E07F97505423D7EEC7B9406A63A918902E6B5DF3F2122AB0FC3815FBA405CF3AF2D2597D2293E1CF84D84E789AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....].[...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/c9-7b8600/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/9d-b58f60/f6-aa5278/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-cda2d3/69-13871c/b7-0ad59f/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210415 .https://microsoft.com/..o." /.....O."..$.D_S...Z.&.)...I..7~"D0..A..Eo.....5;X.....A..Eo.....

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):	1.9410121630856685
Encrypted:	false
SSDEEP:	96:dNw0NwypBEPFtuPJQ9Ai7L8L8qJN38qAdvrG+7B3nOaPo8AiYCBGRuy2mhX:du0uypuCib7uPrENi65dUH
MD5:	45CE88034DDBEFA373F36887655CE062
SHA1:	3AE1FEC0CF4060F978A9ABA16367F42572B3BB82
SHA-256:	335A0ACCD6B0FC14FF4E997C31A6C8C1EA8525DD66BEE09307BAAC8861E57608
SHA-512:	BD394C4DBE9F6D65B65C70E28D69B4A15427268A470754F5ABFD19E539D1FB534BEDB1C5D594CBD47106B0CA992478FD30DD9E9696517838B97A265BB57EFEA
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.8386067349192138
Encrypted:	false
SSDEEP:	48:VI+iq5LLOpEO5J/Kn7U+pjqekLLOpEO5J/Kn7UX8:y+icNw6MNw4
MD5:	CD1426E4EFE69BB58A7F618DD7152D45
SHA1:	9E507447B1E59EC4FA87F126ADF83CDABB022B91
SHA-256:	74C6337C8E52309E5D30D6C4F9C60AD48A24C2E0BB0AE826CAC1FD1B1104494A
SHA-512:	9ED699DC9237C6FFA9494E963E17A3B8CD31774405CE22D71A8329734D54FC4D5E7BDB46049F93AA449DF841E3A94A5B5EF80C410AEF6E04AD587A7EF30D828D
Malicious:	false
Reputation:	low
Preview:	.....k[..... ....

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):	16275
Entropy (8bit):	3.458332092199852
Encrypted:	false
SSDEEP:	96:34j9C0dG854DMjGICRu53bRuTs3Nbb3/Al+XD+1/XDlBj63oSxftRfqRr+H0qvz9:3o9C+8Mjd2+jFkP65j75TyTPDk+kh
MD5:	CFF1A84935F92B75CEB85303AFABF250
SHA1:	EC3CB0039718C2E6B25C49654183F839CE94B726
SHA-256:	DC882C698F5B0EB3C889C3B7C6488263895B5EA3BECCD48C1D41B43C09F21024
SHA-512:	B10163BE3E89A7657D84DC0E89AEE77A9B39223FAAFE3B4D1544CE566F903065E6314B0215EDD3DF708F5AB916E9A67E129781B8437D57744A322408475F421C
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...d3933373_3166_4ed6_ba6f_94143dcaa47b.....2.|..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....https://cccounty-my.sharepoint.com/:b:/g/personal /dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9.....S.h.a.r.i.n.g. .L.i.n.k. .V.a.l.i.d.a.t.i.o.n..... .....h.....`.....:g&4....;g&4....8.....P.....&.....h.t.t.p.s.:././.c.c.c.o.u.n.t.y.-.m.y...s.h.a.r.e.p.o.i.n.t...c.o.m /.:.b.:./.g./.p.e.r.s.o.n.a.l./.d.c.d.r.e.s.o.u.r.c.e.s._.d.c.d._.c.c.c.o.u.n.t.y._.u.s./.E.X.T.c.a.b.N.A.l.P.B.E.s.5.P.2.S.2.t.s.k.y.U.B.h.Q.h.F.Z.w.B.k.m.1.y.x.j.B.c.G.A.2.Y.Q.5 .A.?.e.=.4

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):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..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):	319
Entropy (8bit):	5.242546259286191
Encrypted:	false
SSDEEP:	6:msfxq2P923iKKdK8aPrqIFUtpdrNJZmwPdIkwO923iKKdK8amLJ:t5v45KkL3FUtpdrX/PdI5L5KkQJ
MD5:	124821E7E81C44F8E011C9F653BD25F1
SHA1:	FFDF2C71FB82970E49C4AB3FE8AD2938BFEE73CF
SHA-256:	F03FE75B3A5D9357ABA4DC16E500F5B45AA4522E7A2899E307830DFDD5EAC94E
SHA-512:	C4FA9236B625A4BC69D23D8DAF5DF95669020FD1D75B572B92BFCF989BF5DF79EE6078EE09F5EA06A268079152B203D02D2A6DD34534704AF30CE77FF819A72
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:34.984 c94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-19:46:34.987 c94 Recovering log #3.2021/05/04-19:46:34.988 c94 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):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	319
Entropy (8bit):	5.247990435108819
Encrypted:	false
SSDEEP:	6:ms25N3+q2P923iKKdK8NIFUtpd2eXZmwPd2lVkwO923iKKdK8+eLJ:t25NOv45KkpFUtpd2eX/Pd2L5L5KkqJ
MD5:	9798F70DE235864E0DD085B1A0C75A9D
SHA1:	7341908DAD15BB67A77243B48666C3EA4F043798
SHA-256:	0ADB17BD2DFE5072E69D0ECC53C12CB7D41581C8D1765F0C6BC3C772FFDE4453
SHA-512:	0194211EDD1A0C2F235968C522E2F354A57430DB0171C0F888FB4AAA24AA6F04B360ED81E4796573F50118F94CCFCF7CC2FB4FFCB7BF9E08BBE8ABD5E1819092
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:37.312 628 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-19:46:37.313 628 Recovering log #3.2021/05/04-19:46:37.314 628 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","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):	2.5833749657037135
Encrypted:	false
SSDEEP:	384:wvBfHIurySBH6BP6HIuroNBXTzX6BpqVHBP6HIurl8PAevBgnBR1E:cluCSluGceSluMV1E
MD5:	3EF8FAD2454543F161510FE43A5D8A97
SHA1:	AA8D3699856C21117485FCD0592E7B63F6F465EF
SHA-256:	046205E68BF1AA294C947E56FC8AD9EC23D7AC9AC3CB9D0978455084CB03326D
SHA-512:	FC3B4E5300513DB1353D8D09173391EFE7347EE9EC79E85D927F561B533FADF3F27197B8562EEA4EF731202F0E4C544C54274D51726FD3B02E511CC845732458
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):	1.9295865854595369
Encrypted:	false
SSDEEP:	384:JZBKBHHIurlpK+wBHBw6HIuru8yGVNBBU6B/231:mIuBSIu+iC
MD5:	25129B0B7BC8DEDC99CAE9FC29A1B073
SHA1:	0F40F9DAEBD521D18F87F214788BC9382E132C9E
SHA-256:	6203BE90CAC4AA7D08CE185AA8B109F28E3E506E9FE8040A269E4610F61ACB42
SHA-512:	56D904810773575BEC76423C9944F7125398DA3893C190D1D288400C5C0C31A956B7548F87A469ACD3AD38ABBC11E95D18477296057DB0222A8270D4226637C7
Malicious:	false
Reputation:	low
Preview:	.....U..... ....

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):	374
Entropy (8bit):	5.268154380214087
Encrypted:	false
SSDEEP:	6:msGWNSQyq2P923iKKdK25+Xqx8chI+IFUtpdKSG1ZmwPdKSQRkwO923iKKdK25+M:tBAVv45KkTXfchI3FUtpddG1/PddI5Lk
MD5:	ABE11BD164AB383AA98CAF2F45588B1E
SHA1:	63D3A83A827F8F98F7C4989722E1EB8F1B5D5634
SHA-256:	B12754BA1A81FA9DC165762BB596B39A7A9A77ACF8258A8A0AC05B2A0ADDC1CC
SHA-512:	D164E8F18A2822AF0C4B3186B986D938DE8DE3B120D6112B379D462D47F9F1F6709B64C670AFAE169C25D1BC8471448936181B6BEAF22EDB70AC336015B0C58
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:54.213 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-19:46:54.225 1b70 Recovering log #3.2021/05/04-19:46:54.225 1b70 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):	360
Entropy (8bit):	5.245326430198787
Encrypted:	false
SSDEEP:	6:msWQyq2P923iKKdK25+XuoIFUtpdDVSG1ZmwPdDVSQRkwO923iKKdK25+XuxWLJ:tWVv45KkTXYFUtpdDVSG1/PdDVSI5L5X
MD5:	A22E40CF3FB4068CFFD25BE2BDE25B41
SHA1:	032ECFE344E48AC65AE1E3C48759482AE047B818
SHA-256:	EDFD06A536CA2C350868AE47B994B72AF274DC5CA7E38AEBB192F48D557FD804

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
SHA-512:	5D7F2435F2D19E7017B5D0DA102DCBC2ABAC222A0DE6715D49720C62DBA343DD8DF6B2B5CBFBBC57D49324E42360B0B1476A7149BBC118542774DFB59839575
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:54.165 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-19:46:54.167 1b70 Recovering log #3.2021/05/04-19:46:54.167 1b70 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):	332
Entropy (8bit):	5.3064178989628745
Encrypted:	false
SSDEEP:	6:msMAQyq2P923iKKdKWT5g1IdqIFUtpdhYG1ZmwPdaFyQRkwO923iKKdKWT5g1I3e:tLVv45Kkg5gSRFUtpdhYG1/PdaAl5L5N
MD5:	523BBB00D57C0D0EBCE41B7B19E43D97
SHA1:	2F61164789DED24FB4578FFF1DDC34F536565EE3
SHA-256:	88CF3EB98D7C19707B3199A7D85E0CE742C24EC58EB0667B13B3BBE460A1E711
SHA-512:	7C25E43C948C3106CC91B95D20F567BA07255FA1DC026D703C7B23097E135006B0C999EC4D9BC977B00E3A33981303A484A94CFC9495D8C17BE720FD07899F5
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:53.844 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-19:46:53.885 1b70 Recovering log #3.2021/05/04-19:46:53.886 1b70 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):	1.130725917313618
Encrypted:	false
SSDEEP:	384:qd2pd9UVvd/fk6cvdfHk4F4Qpvd19kIxEQQpvddbk2B85U:8FQR2Qpp3Qp3R
MD5:	4882CFCDBB01D79D35019D71FB9D555A
SHA1:	96420441B21EBF2DA9BAAF31137E57DD4DA21221
SHA-256:	2C5814B6F0258A8ECFE4F2B22EBDE55DB33DC50FE3FC6F4826D554C54FE4B151
SHA-512:	A843C4281A427A576854F7A0802F6A6DEF5A8E247BDBF53E032A06931FBF4119AD639D6E1CB28D605AEB8117E8BCB49899DE1B57AC577A24E56D1D4754D4355
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1895
Entropy (8bit):	5.828308517001116
Encrypted:	false
SSDEEP:	48:QMzY+b+hpWzj9Qh8vf304EOsILJFEw98SSGzjHpRuHA47:QmVbk4j9V3304xtrUSSGzjHpRug47
MD5:	01DBDB7EFC920A360BA9DC72A63FD693
SHA1:	7913D8AFB8D8846AC04758A49BCDCA0ACA35545F
SHA-256:	ACB1364E1EF7B6E2FFFE229930759EFD219F00E2AE6729551CA554310F6969D6
SHA-512:	02B8ABEC2F414F4546BC9F17635EE0A7DB91401BAA4AC87556242683A5D881E18AD50E008AE8B82A1617E153152C80BD06E28A098A2686501D7BB501BB97B059
Malicious:	false
Reputation:	low
Preview:	.....".....845480..com..fwlink..go..https..linkid..microsoft..en.$maincookiessimilartechnologiesmodule..privacy..privacystatement..us..4..9..at..b..cccounty..dcd..dcdresources..e..extcabnalpbes5p2s2tskyubhqhfzwbkm1yxjbcga2yq5a..g..j55mhg..link..my..personal..sharepoint..sharing..validation*.....4.....845480.....9.....at.....b.....cccounty.....com.....dcd.....dcdresources.....e.....en...2..extcabnalpbes5p2s2tskyubhqhfzwbkm1yxjbcga2yq5a.....fwlink.....g.....go.....https.....j55mhg.....link......linkid...(.$maincookiessimilartechnologiesmodule.....microsoft.....my.....personal.....privacy.....privacystatement.....sharepoint.....sharing.....us.....validation..2...!.....0.....1.....2.....4.....5.....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):	0.8611780249298233
Encrypted:	false
SSDEEP:	384:ahwdCzdv7NvdkfkRvd3gBHkuE5Qpvd549kg:yMkIwQpoz
MD5:	75B60FA4AE6E4D3E9BF5F1EF7096374A
SHA1:	C0060B793960DEEF83FE5FFA94D4D638B8379A5B
SHA-256:	08D58DB17529401B6735F6CB373B12564F157D0095C0B75A5B7A660398A333B4
SHA-512:	2A88C321733DA79EE348C5EE5A5F7F97F68C451E48E585CFFB2DC7AC14D108BAE95703F62E1A77C6B17C91BC9EAEB817082C2AE127D56C63DA85A3649D9EC0 1D
Malicious:	false
Reputation:	low
Preview:	.....t..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.489934872893162
Encrypted:	false
SSDEEP:	48:8W5IxGTJZCsa7ssML8db2Yo4bQSefgG6pNrS0U9RdiN9r/:7a7pMYdb2Yo4bQ5fgG6jrS0V
MD5:	57CF4E4639B7C922A2E23FB205BB0478
SHA1:	973EC906BCADCD85D4EF54324649C65E51BCD8C4
SHA-256:	90CFC46E78D998EA8BB8B5DD548734AC2090298CC65F56D4CB2024EBC12ED224
SHA-512:	0F01AE7EF9CD7C3DBB908A1614607EE088054075DCCEAB6937F9DE454996092BE906D0BABC5B8F35FFB84C41A7EF2FBDC2B007C872296C9C8B36B5505180275 E
Malicious:	false
Reputation:	low
Preview:	.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..512604000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-04 19:46:59.33][INFO][mr.Init] MR instance ID: 5148ef45-f3e0-4317-8715-3f41722c8ece\n","[2021-05-04 19:46:59.33][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-04 19:46:59.33][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-04 19:46:59.33][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-04 19:46:59.33][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-04 19:46:59.34][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-04 19:46:59.34][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.204968728943176
Encrypted:	false
SSDEEP:	6:msqpM+q2P923iKKdK8a2jMGIFUtpdLZmwPdOaMVkwO923iKKdK8a2jMmLJ:tN+v45Kk8EFUtpdL/PdkV5L5Kk8bJ
MD5:	7A9825963895841FCA2D4D939EFDC29F
SHA1:	B7D727E5BCE1DFA7CB899354690895D4A1C51199
SHA-256:	F0C53C9E81B8B416388452258A724549E619BB3B78822DC729A30966B741E26C
SHA-512:	1669E7A7DC20D5385B3DA24018EB35AA935BFB262811519CEDD7BEAC5ECB3597B08A371BC4B609AB85553F7A61D41EE00EB2BC5641E89AC9CDA8C4872270D4 97
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:34.736 151c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:46:34.741 151c Recovering log #3.2021/05/04-19:46:34.744 151c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	135168

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Entropy (8bit):	1.4404180065239311
Encrypted:	false
SSDEEP:	192:HIia8e2ULm7U5UuUUTZhsEgTqmgTu3FU5UuUk7lU3UPU4:HIiaZ2cm7WfHMiQVWfvBImp
MD5:	8636B4E40C566A4A67D9569DA6284BC4
SHA1:	C4AF3885ABB69C0CEEDE76890FFDC158B6DBD0C5
SHA-256:	62B4AD625AE0453297A2F823B74B051FE72E41CA1D7F9D4C4D74068A92A1FBC1
SHA-512:	87F58586FBBC4A01737F3E7E40EF129107DCDF70B73EA79A9A7B4990A7E3F9ABD2C800062E9F32FB6B2D429D01CD9DB4407BD45F352B558F9FCE0804656C123
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	141196
Entropy (8bit):	1.3196215160299298
Encrypted:	false
SSDEEP:	384:byviUSxCJyjny+eibLm+CfyQWffi4WfUSh:GaxYV+fnmfaQWfK4Wfxh
MD5:	380E42B2F1F45510D4B0BCBF1FCA63C5
SHA1:	57AE8E2F95A98801DBF7D6F367051C210259DA61
SHA-256:	4AA6E11D6F7957F617A216E90C64A1ACDEEB1B4329178DA10FE75B708A93DFF9
SHA-512:	DD6FA19CCC207D597779F87C032FAC848650346E73236CEAB884D6D8CF8C378D62787F56B19B7260761ED41D0DC8023B1EF0ABC36ABC17555E96D321D45F2F
Malicious:	false
Reputation:	low
Preview:	.....*..I..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.219543315583461
Encrypted:	false
SSDEEP:	6:ms6pN3+q2P923iKKdKgXz4rRIFUtpd255ZmwPd25VkwO923iKKdKgXz4q8LJ:t6qv45KkgXiuFUtpd2j/Pde5L5KkgX2J
MD5:	724B48651C0E2703CB2EAAEF24B273E7
SHA1:	4DF048A950CE121A2B5DDE24ABCFDD696408D62B
SHA-256:	6C186E9D9A291BBDDF142B4A87EBF4552EDF78C574602FD53347F5CD8FA44F40
SHA-512:	8BB9CE050B66F6581E96D53E4158F1C2A37205D89D286A21C0D0322ED3276D13EECDAE190297489A01E9C71BAF247748AE624A93789E2D68808A844A19E53C95
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:35.015 628 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/04-19:46:35.019 628 Recovering log #3.2021/05/04-19:46:35.020 628 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1317
Entropy (8bit):	4.613993309458421
Encrypted:	false
SSDEEP:	24:70LbOS3fkc5yFWsOFZwaxllfYA7bqOId72tWB1QbO7aAqZ55dG5P3q5bnCB:70nOScOyFWsOFZTYft7XldStWR7jqZ5M
MD5:	548FBD0326A032E2C0017EB2AA2ADC9E
SHA1:	F3F4166DBAB5F5FF4171F0AC25AB94C59B7A052B
SHA-256:	D76BD3BEBEFF881D5F2FC9FB07B6C6BB0D6702ABFFD3DBC8E415F88BEB35B3CD
SHA-512:	6FF0BD530B7C9AF087525B39D59AFFD8FF545995EB9D8716F53DD8C2F255CB3460926EACBB1B8549A8BD7AECF6D6AC0EC23695A68B25A4785FFA6F8B7360B01
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Reputation:	low
Preview:	..&f.....d..q.....next-map-id.1.Rnamespace-d3933373_3166_4ed6_ba6f_94143dcaa47b-https://cccounty-my.sharepoint.com/.0V.e.....V.e.....V.e.....V.e.....3&bl.....next-map-id.2.Mnamespace-1f97e185_0724_4731_84d8_33f7683d7a5b-https://account.microsoft.com/.1.s.. .....map-1-MeePortal-logs..{... . . . .".d.e.b.u.g.".:. .[.],.,... . . . .".t.r.a.c.e.".:. .[.],.,... . . . .".w.a.r.n.".:. .[.],.,... . . . .".e.r.r.o.r.".:. .[.],.,... . . . .".o.t.h.e.r.".:. .[... . . . .".2.0.2.1.-.0.5.-.0.5.T.0.9.:.4.7.:.1.5...0.0.0.Z.:.:.M.e.e.P.o.r.t.a.l. .-. .H.i.p.C.l.i.e.n.t...S.e.t.u.p. .-. .N.o. .h.i.p. .c.o.m.p.o.n.e.n.t. .f.o.u.n.d. .i.n. .t.h.e. .p.a.g.e. .-. .s.k.i.p.p.i.n.g. .s.e.t.u.p..."... . . . .]...}...map-1-msameidH3.7.8.1.f.4.3.9.-.f.4.f.d.-.4.d.3.9.-.8.f.0.8.-.2.9.d.d.9.8.4.c.a.b.7.0..f..h.....next-map-id.3.Inamespace-4c5b9893_7556_452b_9d9a_c3412be74684-https://www.microsoft.com/.2.n..h...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.195850344550323
Encrypted:	false
SSDEEP:	6:msCM+q2P923iKKdKrQMxIFUtpdGZmwPdsMVkwO923iKKdKrQMFLJ:tP+v45KkCFUtpdG/PdtV5L5KktJ
MD5:	FCBA8F79D23EE0AC496BB77109C0A5E2
SHA1:	FD9E6E1F48B2DB25CC4ECAEB4DC30AA9063F0A36
SHA-256:	18F9654C11314F9450AAAC6913BB49D2530D571FFC3949F5378DC53F833A4C2C
SHA-512:	193334BC19294813E231F9C6C7FDF55DFDEA0408C3B150811FDAA0196D179BDAC0335AC1FFF4783407E632F98D8989826B1837CBFE178C2865B610A0EE012261
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:34.891 151c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-19:46:34.892 151c Recovering log #3.2021/05/04-19:46:34.893 151c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.1995762558463765
Encrypted:	false
SSDEEP:	6:msSAM+q2P923iKKdK7Uh2ghZIFUtpd4eZZmwPd0elMVkwO923iKKdK7Uh2gnLJ:tbM+v45KkIhHh2FUtpd4eZ/Pd0KMV5LI
MD5:	A0228728931081B4A5CE89DF0E3F6F24
SHA1:	8C7C25B9B54192BCD57C5569B9AD211F074F0DFE
SHA-256:	CF43B2F48CF63E25E42C1CF49DE899C70309140AB799370CF068557A4D73328F
SHA-512:	E4CEC11CA5B96C79A1A16DF2D2DB00CC8C0AAE93A962F9544EA3296BCEB023A1199B83DA2324C1689352940A5C7C9F04E5F6A6331D701291775EB3A4895918E
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:34.582 146c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/05/04-19:46:34.589 146c Recovering log #3.2021/05/04-19:46:34.593 146c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.262137248633966
Encrypted:	false
SSDEEP:	6:mshy1yq2P923iKKdKusNpV/2jMGIFUtpdoc/1ZmwPdocpRkwO923iKKdKusNpV/s:thy1yv45KkFFUtpdX/PdjR5L5KkOJ
MD5:	31DF71137E6D094D12C49951310708AF
SHA1:	353A3AED106014B8D672800F2C02E183462DC97B
SHA-256:	D5BB527B95BEBCE8246C090AEA5CC642BC22D304F3F5BE39F240F90B6A1DA633
SHA-512:	A9C340B6C7B9CE20AE2E77648D2B74EBE42540AA5AB4E32BD901FD3E64E849A28EC985BCFFF686D79A7183A2235F2E9D01753080484C235A4123528BFB08DF6
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:34.932 b94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:46:34.933 b94 Recovering log #3.2021/05/04-19:46:34.933 b94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.287812709974381
Encrypted:	false
SSDEEP:	6:msnsq2P923iKKdKusNpqz4rRIFUtpd6DZmwPdbKMkwO923iKKdKusNpqz4q8LJ:tsv45KkmiuFUtpd6D/PdmM5L5Kkm2J
MD5:	63B1D81BC73A6571F3A4DA01EBFAF914
SHA1:	008DC90C9060D38495D4287B60B5982FB92D193A
SHA-256:	9B459491E473CEBAA7AD1924B2DB6D39B027BAC7C51C805BFAB64E7021D823C8
SHA-512:	965450E4679F57EF526CAD7D9097A220A77786E719D88CFE06FDB13FAFFB68E0F787176B440529F16A0CD2F8BBE818806775D975EE4C078894BF0ABD0DAAA05
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:35.012 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/04-19:46:35.015 1694 Recovering log #3.2021/05/04-19:46:35.016 1694 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.272622422024276
Encrypted:	false
SSDEEP:	6:ms1Gyq2P923iKKdKusNpZQMxIFUtpd91ZmwPdz9cL1RkwO923iKKdKusNpZQMFLJ:tEyv45KkMFUtpdP/PdzGR5L5KkTJ
MD5:	30BD2996229DC575C62EF6FD004382FA
SHA1:	B46CF083D18B9A3958D075415261ED7CB3B30C13
SHA-256:	EB0032EF2D0AAB124FE6014C5D39544A5AB4BB517A19ED7973A75957201EBF71
SHA-512:	0E30A2DB1D796D842B0FA86801E996D74ADA2A35530EE9A64E9F965B9AFED2AA66B31BAE9E65136B1C13C564300DAA5339391CE61678A8F0373A1B695305F88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/05/04-19:46:51.353 b94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/04-19:46:51.354 b94 Recovering log #3.2021/05/04-19:46:51.355 b94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\e72addbe-6b1d-45a5-b361-9657049270c6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\7bfb62a6-3a75-44fc-af2c-f79f44843a16.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.238123129123364

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Encrypted:	false
SSDEEP:	12:tiv45KkkGHArBFUtpdC/Pd25L5KkkGHAryJ:to45KkkGgPgT2gL5KkkGga
MD5:	34299538C6FB90F897997DFD3D5AA0FD
SHA1:	E114AB572845AFB53D156508A52194850E151D64
SHA-256:	3F98E97C6F378EFCC0E093F08FD507EE0409168B91C0CB599618011047756B30
SHA-512:	5E7E15750A367A51FF113F7027B4AB2854E1184A607BC10344F462188FF243604E0B47230F7FE868BBF34BDE5AA10B7F9D2B3AE64A17B0F41C5ADD36757964AB
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:53.335 628 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:46:53.338 628 Recovering log #3.2021/05/04-19:46:53.341 628 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.232783593911397
Encrypted:	false
SSDEEP:	12:tHv45KkkGHArqiuFUtpdP/Pd7P5L5KkkGHArq2J:tP45KkkGgCgTFtL5KkkGg7
MD5:	06D625DABD59A9CC60C768FC212965CA
SHA1:	51B807745D445D052AA3C1C2AAD1D2F3DE17F3AD
SHA-256:	153D916982ECB106741C2508DF8594BC40C5E41097E66B412531CD566E0C5353
SHA-512:	1EDF3AC39C5E78CFF0311C86975BB6561CFF2BAEAE8369A7B4AC756A57BA4F366C093D7491CD4C5AD440E4D356295622D30145238588869 37C885B56AA836D3
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:46:53.336 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/04-19:46:53.340 1694 Recovering log #3.2021/05/04-19:46:53.342 1694 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.204723112180629
Encrypted:	false
SSDEEP:	12:tM+v45KkkGHArAFUtpdSmW/PdSNV5L5KkkGHArfJ:td45KkkGgkgTXyEL5KkkGgV
MD5:	25342D59E29E654B9149E6D4C17A7289
SHA1:	E70CF68E6416881689F07C1EACB10CDAC51DF9C1
SHA-256:	20CB1B547B8026C109F66AEF11A01C734F7AE9F899F6CFFB057EA734C572F4F8
SHA-512:	EAAF0BE165837351F39377E960971D70836E1588C0C263206DCAF793C8CB8243B00A97A756CB424FBEE734E14530B013A011A90A0A8B9C7EC2ADACD6437601F
Malicious:	false
Reputation:	low
Preview:	2021/05/04-19:47:08.796 14ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/04-19:47:08.798 14ec Recovering log #3.2021/05/04-19:47:08.798 14ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

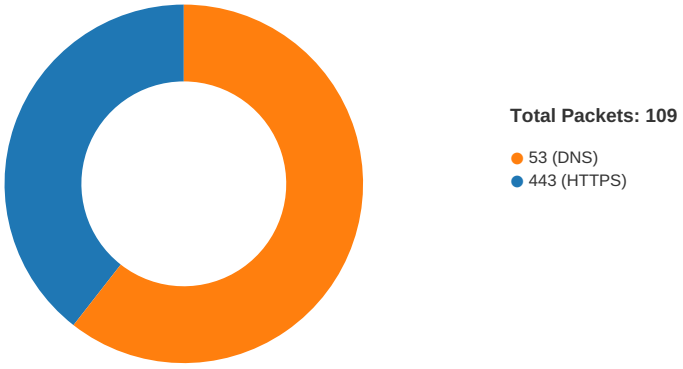
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9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

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:46:37.026989937 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.028052092 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.144402981 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.182147026 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.182264090 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.182286024 CEST	443	49707	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.182357073 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.182898998 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.183073044 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.299628019 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.299740076 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.300817013 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.338579893 CEST	443	49708	40.108.248.29	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:46:37.338613987 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.338650942 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.338715076 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.340092897 CEST	443	49707	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.340137959 CEST	443	49707	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.340172052 CEST	443	49707	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.340220928 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.385310888 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.390058994 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.455642939 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.455672979 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.455694914 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.455739975 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.458077908 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.539985895 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.540726900 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.547470093 CEST	443	49707	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.612551928 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.727044106 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.727065086 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.743206024 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809806108 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809844017 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809879065 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809921980 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809940100 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.809961081 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.809986115 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.809995890 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810030937 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810060978 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.810065985 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810098886 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810125113 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.810133934 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810168028 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810188055 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.810210943 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810249090 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810266972 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.810282946 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810317993 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810334921 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.810352087 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.810420036 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.963715076 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963758945 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963797092 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963834047 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963848114 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.963893890 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.963897943 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963957071 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.963995934 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.964009047 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.964032888 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.964071035 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.964082003 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.964107037 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.964134932 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:37.964163065 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.977097034 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.977685928 CEST	49707	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.979032993 CEST	49709	443	192.168.2.5	40.108.248.29

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:46:37.980698109 CEST	49714	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:37.981470108 CEST	49715	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.134896040 CEST	443	49714	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135056973 CEST	49714	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.135313988 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135353088 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135407925 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135423899 CEST	49714	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.135438919 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135445118 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.135478973 CEST	443	49708	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.135482073 CEST	49708	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.136403084 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136431932 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136465073 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136493921 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136504889 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.136538029 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136557102 CEST	49709	443	192.168.2.5	40.108.248.29
May 4, 2021 19:46:38.136578083 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136607885 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136637926 CEST	443	49709	40.108.248.29	192.168.2.5
May 4, 2021 19:46:38.136645079 CEST	49709	443	192.168.2.5	40.108.248.29

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:46:26.828223944 CEST	54302	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:26.888032913 CEST	53	54302	8.8.8.8	192.168.2.5
May 4, 2021 19:46:27.028551102 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:27.078924894 CEST	53	53784	8.8.8.8	192.168.2.5
May 4, 2021 19:46:27.452756882 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:27.456532955 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:27.501545906 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 19:46:27.505312920 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 19:46:27.925915003 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:27.986227989 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 19:46:29.292701006 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:29.344203949 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 19:46:30.229652882 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:30.278738022 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 19:46:31.209456921 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:31.259356976 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 19:46:32.260472059 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:32.321978092 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 19:46:32.517266035 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:32.570113897 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 19:46:33.589970112 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:33.641510010 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 19:46:35.377659082 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:35.430341959 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 19:46:36.891231060 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:36.891910076 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:36.897433043 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:36.897942066 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:36.940968990 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 19:46:36.956491947 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 19:46:36.959311008 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 19:46:37.025779963 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 19:46:37.379091978 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:37.454121113 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 19:46:37.551079035 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:37.615837097 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 19:46:37.910051107 CEST	55016	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:46:37.966764927 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 19:46:37.982917070 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:38.041997910 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 19:46:38.340847015 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:38.369154930 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:38.405776978 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:46:38.418052912 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 19:46:38.831382036 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:38.888669014 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:38.895979881 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 19:46:38.959052086 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 19:46:39.457330942 CEST	58530	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:39.505831003 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 19:46:40.081187963 CEST	53813	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:40.161326885 CEST	63732	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:40.214657068 CEST	53	63732	8.8.8.8	192.168.2.5
May 4, 2021 19:46:40.247519970 CEST	53	53813	8.8.8.8	192.168.2.5
May 4, 2021 19:46:40.845207930 CEST	57344	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:40.896701097 CEST	53	57344	8.8.8.8	192.168.2.5
May 4, 2021 19:46:41.782259941 CEST	59413	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:41.831012964 CEST	53	59413	8.8.8.8	192.168.2.5
May 4, 2021 19:46:46.543839931 CEST	65086	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:46.595428944 CEST	53	65086	8.8.8.8	192.168.2.5
May 4, 2021 19:46:47.027107000 CEST	52929	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:47.085524082 CEST	53	52929	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.101133108 CEST	64317	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.102519035 CEST	61004	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.114155054 CEST	56895	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.114917040 CEST	62372	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.115609884 CEST	61515	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.161170959 CEST	53	61004	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.164145947 CEST	53	64317	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.166210890 CEST	53	61515	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.185664892 CEST	53	56895	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.188203096 CEST	53	62372	8.8.8.8	192.168.2.5
May 4, 2021 19:46:51.535640001 CEST	56675	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:51.594387054 CEST	53	56675	8.8.8.8	192.168.2.5
May 4, 2021 19:46:52.137253046 CEST	57172	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:52.206433058 CEST	53	57172	8.8.8.8	192.168.2.5
May 4, 2021 19:46:52.837246895 CEST	55267	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:52.896135092 CEST	53	55267	8.8.8.8	192.168.2.5
May 4, 2021 19:46:53.939461946 CEST	50969	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:54.001004934 CEST	53	50969	8.8.8.8	192.168.2.5
May 4, 2021 19:46:57.941076040 CEST	64362	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:58.006624937 CEST	53	64362	8.8.8.8	192.168.2.5
May 4, 2021 19:46:58.384845018 CEST	54766	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:58.446520090 CEST	53	54766	8.8.8.8	192.168.2.5
May 4, 2021 19:46:59.156888962 CEST	61446	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:59.160852909 CEST	57515	53	192.168.2.5	8.8.8.8
May 4, 2021 19:46:59.205735922 CEST	53	61446	8.8.8.8	192.168.2.5
May 4, 2021 19:46:59.224471092 CEST	53	57515	8.8.8.8	192.168.2.5
May 4, 2021 19:47:05.933526993 CEST	58199	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:05.992137909 CEST	53	58199	8.8.8.8	192.168.2.5
May 4, 2021 19:47:12.061305046 CEST	65221	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:12.120538950 CEST	53	65221	8.8.8.8	192.168.2.5
May 4, 2021 19:47:12.747119904 CEST	61573	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:12.828610897 CEST	53	61573	8.8.8.8	192.168.2.5
May 4, 2021 19:47:14.377712011 CEST	56562	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:14.444089890 CEST	53	56562	8.8.8.8	192.168.2.5
May 4, 2021 19:47:14.761790991 CEST	53591	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:14.762003899 CEST	59688	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:14.764194965 CEST	56032	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:14.814589977 CEST	53	56032	8.8.8.8	192.168.2.5
May 4, 2021 19:47:14.834144115 CEST	53	59688	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:47:14.834184885 CEST	53	53591	8.8.8.8	192.168.2.5
May 4, 2021 19:47:16.218163967 CEST	61150	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:16.302992105 CEST	53	61150	8.8.8.8	192.168.2.5
May 4, 2021 19:47:16.940006971 CEST	63458	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:16.998713970 CEST	53	63458	8.8.8.8	192.168.2.5
May 4, 2021 19:47:17.032782078 CEST	53247	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:17.040848970 CEST	58544	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:17.100910902 CEST	53	58544	8.8.8.8	192.168.2.5
May 4, 2021 19:47:17.105592966 CEST	53	53247	8.8.8.8	192.168.2.5
May 4, 2021 19:47:20.355623960 CEST	53814	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:20.406197071 CEST	53	53814	8.8.8.8	192.168.2.5
May 4, 2021 19:47:22.526134968 CEST	51305	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:22.585341930 CEST	53	51305	8.8.8.8	192.168.2.5
May 4, 2021 19:47:23.855597973 CEST	53670	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:23.912502050 CEST	53	53670	8.8.8.8	192.168.2.5
May 4, 2021 19:47:35.091543913 CEST	55160	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:35.156433105 CEST	53	55160	8.8.8.8	192.168.2.5
May 4, 2021 19:47:35.902137995 CEST	63847	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:35.963658094 CEST	53	63847	8.8.8.8	192.168.2.5
May 4, 2021 19:47:36.896923065 CEST	61523	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:36.948764086 CEST	53	61523	8.8.8.8	192.168.2.5
May 4, 2021 19:47:37.066245079 CEST	50551	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:37.133958101 CEST	53	50551	8.8.8.8	192.168.2.5
May 4, 2021 19:47:37.332073927 CEST	62847	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:37.389228106 CEST	53	62847	8.8.8.8	192.168.2.5
May 4, 2021 19:47:37.755520105 CEST	57712	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:37.815305948 CEST	53	57712	8.8.8.8	192.168.2.5
May 4, 2021 19:47:38.345160961 CEST	61064	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:38.396653891 CEST	53	61064	8.8.8.8	192.168.2.5
May 4, 2021 19:47:50.064819098 CEST	61891	53	192.168.2.5	8.8.8.8
May 4, 2021 19:47:50.115808010 CEST	53	61891	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:46:36.897942066 CEST	192.168.2.5	8.8.8.8	0x4ede	Standard query (0)	cccounty-my.sharepoint.com	A (IP address)	IN (0x0001)
May 4, 2021 19:46:38.831382036 CEST	192.168.2.5	8.8.8.8	0xf089	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
May 4, 2021 19:46:40.081187963 CEST	192.168.2.5	8.8.8.8	0x9fb9	Standard query (0)	cccounty-my.sharepoint.com	A (IP address)	IN (0x0001)
May 4, 2021 19:46:40.161326885 CEST	192.168.2.5	8.8.8.8	0xd3d4	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
May 4, 2021 19:46:51.114917040 CEST	192.168.2.5	8.8.8.8	0xf7cb	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
May 4, 2021 19:46:51.115609884 CEST	192.168.2.5	8.8.8.8	0xb35f	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 19:46:52.137253046 CEST	192.168.2.5	8.8.8.8	0x894d	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
May 4, 2021 19:47:14.764194965 CEST	192.168.2.5	8.8.8.8	0x7241	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
May 4, 2021 19:47:17.032782078 CEST	192.168.2.5	8.8.8.8	0x3c67	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
May 4, 2021 19:47:20.355623960 CEST	192.168.2.5	8.8.8.8	0xf386	Standard query (0)	aka.ms	A (IP address)	IN (0x0001)
May 4, 2021 19:47:38.345160961 CEST	192.168.2.5	8.8.8.8	0xbc45	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:46:37.025779963 CEST	8.8.8.8	192.168.2.5	0x4ede	No error (0)	cccounty-my.sharepoint.com	cccounty.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:37.025779963 CEST	8.8.8.8	192.168.2.5	0x4ede	No error (0)	cccounty.sharepoint.com	214-ipv4.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:46:37.025779963 CEST	8.8.8.8	192.168.2.5	0x4ede	No error (0)	214-ipv4.clump.prod.aa-rt.sharepoint.com	20687-ipv4.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:37.025779963 CEST	8.8.8.8	192.168.2.5	0x4ede	No error (0)	20687-ipv4.farm.prod.aa-rt.sharepoint.com		40.108.248.29	A (IP address)	IN (0x0001)
May 4, 2021 19:46:38.895979881 CEST	8.8.8.8	192.168.2.5	0xf089	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:40.214657068 CEST	8.8.8.8	192.168.2.5	0xd3d4	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:40.247519970 CEST	8.8.8.8	192.168.2.5	0x9fb9	No error (0)	cccounty-my.sharepoint.com	cccounty.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:40.247519970 CEST	8.8.8.8	192.168.2.5	0x9fb9	No error (0)	cccounty.sharepoint.com	214-ipv4.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:40.247519970 CEST	8.8.8.8	192.168.2.5	0x9fb9	No error (0)	214-ipv4.clump.prod.aa-rt.sharepoint.com	20687-ipv4.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:40.247519970 CEST	8.8.8.8	192.168.2.5	0x9fb9	No error (0)	20687-ipv4.farm.prod.aa-rt.sharepoint.com		40.108.248.29	A (IP address)	IN (0x0001)
May 4, 2021 19:46:51.166210890 CEST	8.8.8.8	192.168.2.5	0xb35f	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:51.188203096 CEST	8.8.8.8	192.168.2.5	0xf7cb	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:52.206433058 CEST	8.8.8.8	192.168.2.5	0x894d	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:46:52.206433058 CEST	8.8.8.8	192.168.2.5	0x894d	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 4, 2021 19:47:12.828610897 CEST	8.8.8.8	192.168.2.5	0x1604	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:47:14.814589977 CEST	8.8.8.8	192.168.2.5	0x7241	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:47:14.834184885 CEST	8.8.8.8	192.168.2.5	0x5c1b	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:47:17.105592966 CEST	8.8.8.8	192.168.2.5	0x3c67	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:47:17.105592966 CEST	8.8.8.8	192.168.2.5	0x3c67	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 4, 2021 19:47:20.406197071 CEST	8.8.8.8	192.168.2.5	0xf386	No error (0)	aka.ms		95.101.18.109	A (IP address)	IN (0x0001)
May 4, 2021 19:47:38.396653891 CEST	8.8.8.8	192.168.2.5	0xbc45	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 19:47:20.569560051 CEST	95.101.18.109	443	192.168.2.5	49885	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 07 22:45:54 CET 2021 Wed Jul 22 01:00:00 CEST 2020	Fri Jan 07 22:45:54 CET 2022 Tue Oct 08 09:00:00 CEST 2024	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 22 01:00:00 CEST 2020	Tue Oct 08 09:00:00 CEST 2024		
May 4, 2021 19:47:20.569641113 CEST	95.101.18.109	443	192.168.2.5	49884	CN=go.microsoft.com, OU=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 07 22:45:54 CET 2021 Wed Jul 22 01:00:00 CEST 2020	Fri Jan 07 22:45:54 CET 2022 Tue Oct 08 09:00:00 CEST 2024	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=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 22 01:00:00 CEST 2020	Tue Oct 08 09:00:00 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4440 Parent PID: 3880

General

Start time:	19:46:33
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://cccounty-my.sharepoint.com:443/:b:/g/personal/dcdresources_dcd_cccounty_us/EXTcabNAlPBEs5P2S2tskyUBhQhFZwBkm1yxjBcGA2YQ5A?e=4%3aJ55MhG&at=9'
Imagebase:	0x7ff677c70000

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: 4940 Parent PID: 4440

General

Start time:	19:46:35
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,11341300835914849824,6073494584447434684,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1768 /prefetch:8
Imagebase:	0x7ff677c70000
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

Disassembly