ID: 458973
Cookbook: browseurl.jbs
Time: 23:32:07
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

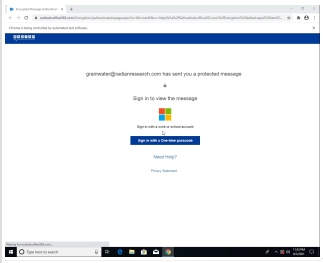
Windows Analysis Report https://outlook.office365.com…

Overview

General Information

Sample URL:	https://outlook.office365.com/Encryption/retrieve.ashx?recipientemailaddres...pSFUFyG6YbDvs4i0ZVqatNUFdh07tVh62OLJ9%2fEix1dt9V%2frV%2fLktpIvUxQ6RgA%3d%3d%3d
Analysis ID:	458973
Infos:	

Most interesting Screenshot:



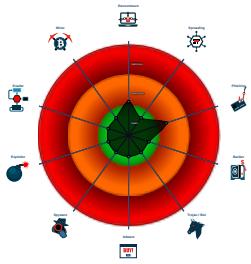
Detection

Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5476 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://outlook.office365.com/Encryption/retrieve.ashx?recipientemailaddress=ap%40gswater.com&senderemailaddress=grainwater%40radianresearch.com&senderorganization=AwGKAAAAAoYAAAADAQAAAL%2bPwYr4eztBl9bc2pXl9%2f9PVT1XYXR0aG91ckVuZ2luZWVyaW5nLm9ubWljcm9zb2Z0LmNvbSxPVT1NaWNyb3NvZnQgRXhjaGFuZ2UgSG9zdGVkIE9yZ2FuaXphdGlvbnMsREM9TkFNUFIwMUEwMTAsREM9UFJPRCxEQz1PVVRMT09LLERDPUNPTW3U2z0RbcxKmUtxcJ88CKJDTj1Db25maWd1cmF0aW9uLENOPVdhdHRob3VyRW5naW5lZXJpbmcub3NvZnQuY29tLENOPUNvbmZpZ3VyYXRpb25Vbml0cyxEQz1OQU1QUjAxQTAxMCxEQz1QUk9ELERDPU9VVExPT0ssREM9Q09NAQ%3d%3d&messageid=%3cBN6PR0101MB299654BC7612BE90121C8E74BBF09%40BN6PR0101MB2996.prod.exchangelabs.com%3e&cfmRecipient=SystemMailbox%7bD0E409A0-AF9B-4720-92FE-AAC869B0D201%7d%40WatthourEngineering.onmicrosoft.com&consumerEncryption=false&senderorgid=1abee47c-68ca-4166-a776-68475cb4c2d2&urldecoded=1&e4e_sdata=NAlD4xF5G7xsjCpoXLsrqcFvJk6j2vhVIIKSh98po4JUh8sQDhUS2lu3%2f27pCMtALumoYdxBZFlm2ASgEEpgP3NQkpb%2bn1kpgDgOCtqD09%2bG%2bs8heIeUlJTsqucw0Zz9OP7E6qTSm5hEj40bLIFk1SDbdplq9xz8N2Bf2l3k4%2fRwKrYELyDkr67ZSu8gKah3uOJUUSAuDu5R6fJPiAjKampBbQQqlsds8zLPJ%2b3ltpS0fbh4UsFYc2O7%2bUSJWWZyaqmvnnGyYWLFrZs%2fgtJGXGapSFUFyG6YbDvs4i0ZVqatNUFdh07tVh62OLJ9%2fEix1dt9V%2frV%2fLktpIvUxQ6RgA%3d%3d' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,8183373600241193 2,15524388546782287473,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1648 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

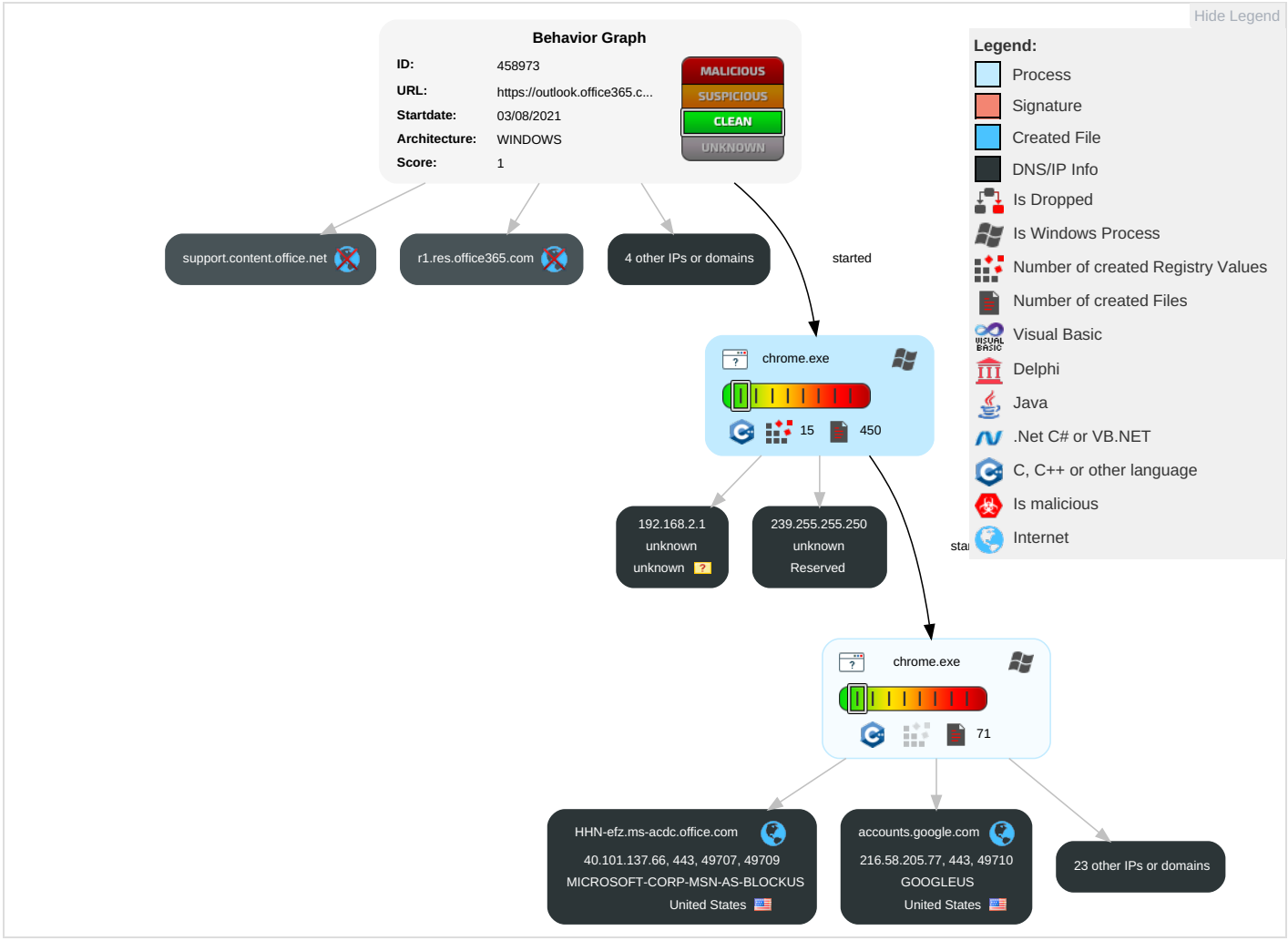
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
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)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

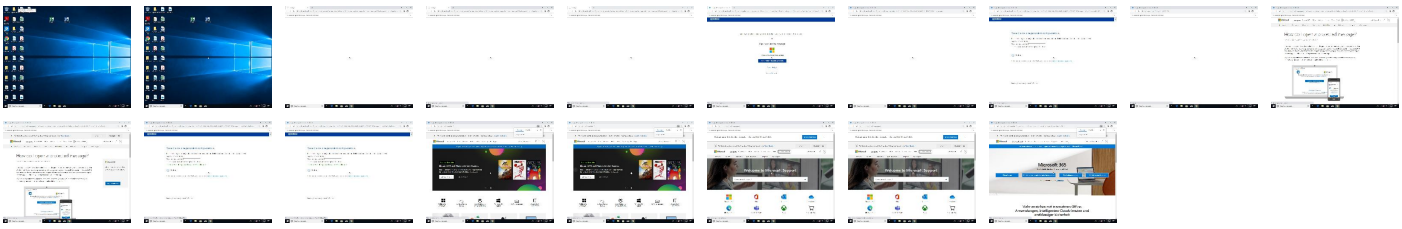
Behavior Graph

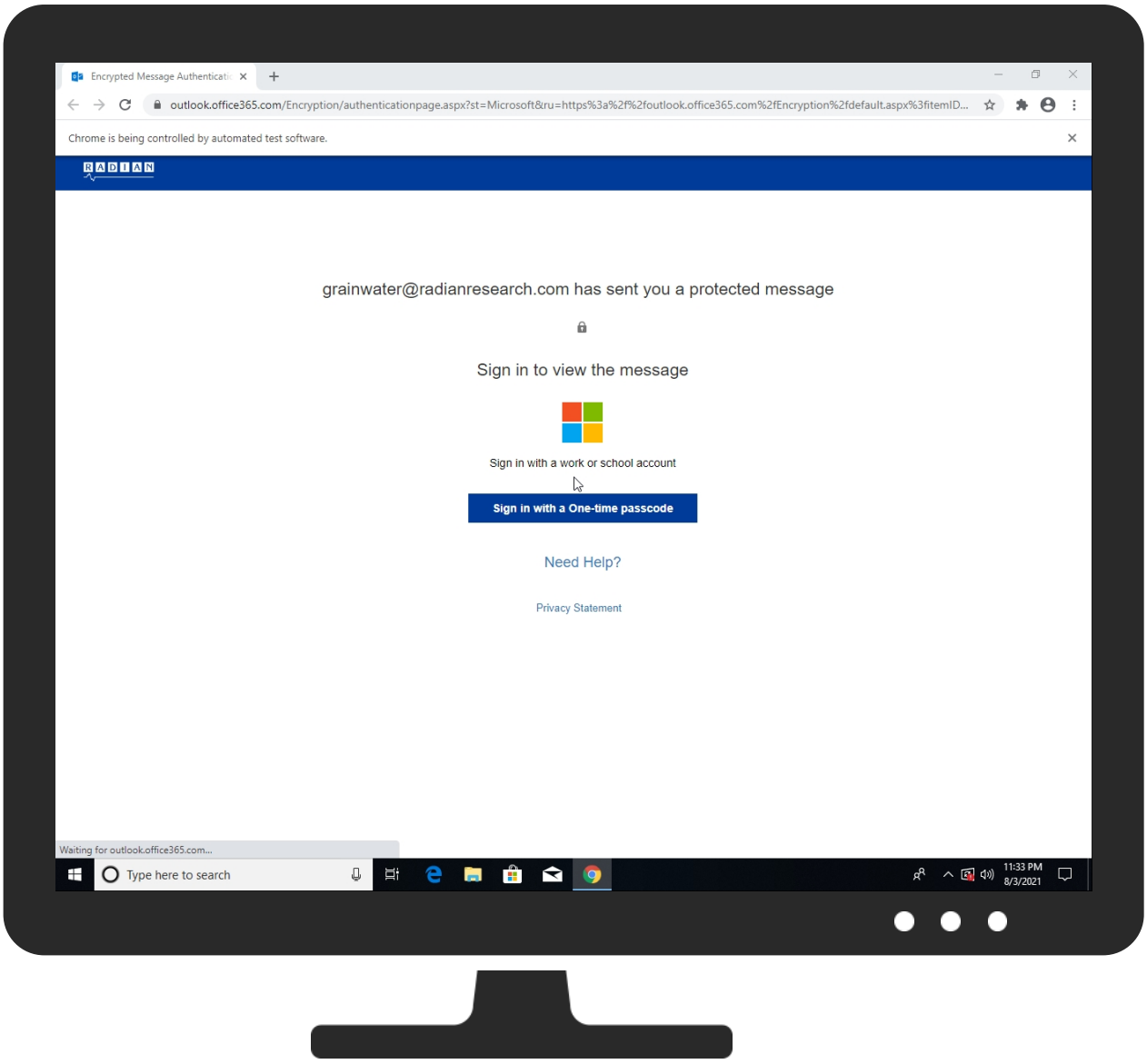


Screenshots

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://outlook.office365.com/Encryption/retrieve.ashx?recipientemailaddress=ap%40gswater.com&senderemailaddress=grainwater%40radianresearch.com&senderorganization=AwGKAAAAAoYAAAADAQAAAL%2bPwYr4eztBl9bc2pXl9%2f9PVT1XYXR0aG91ckVuZ2luZWVyaW5nLm9ubWljcm9zb2Z0LmNvbSxPVT1NaWNyb3NvZnQgRXhjaGFuZ2UgSG9zdGVkIE9yZ2FuaXphdGlvbnMsREM9TkFNUFIwMUEwMTAsREM9UFJPRCxEQz1PVVRMT09LLERDPUNPTW3U2z0RbcxKmUtxcJ88CKJDTj1Db25maWd1cmF0aW9uLENOPVdhdHRob3VyRW5naW5lZXJpbmcub25taWNyb3NvZnQuY29tLENOPUNvbmZpZ3VyYXRpb25Vbml0cyxEQz1OQU1QUjAxQTAxMCxEQz1QUk9ELERDPU9VVExPT0ssREM9Q09NAQ%3d%3d&messageid=%3cBN6PR0101MB299654BC7612BE90121C8E74BBF09%40BN6PR0101MB2996.prod.exchangelabs.com%3e&cfmRecipient=SystemMailbox%7bD0E409A0-AF9B-4720-92FE-AAC869B0D201%7d%40WatthourEngineering.onmicrosoft.com&consumerEncryption=false&senderorgid=1abee47c-68ca-4166-a776-68475cb4c2d2&urldecoded=1&e4e_sdata=NAlD4xF5G7xsjCpoXLsrqcFvJk6j2vhVIIKSh98po4JUh8sQDhUS2lu3%2f27pCMtALumoYdxBZFlm2ASgEEpgP3NQkpb%2bn1kpgDgOCtqD09%2bG%2bs8heIeUlJTsqucw0Zz9OP7E6qTSm5hEj40bLIFk1SDbdplq9xz8N2Bf2l3k4%2fRwKrYELyDkr67ZSu8gKah3uOJUUSAuDu5R6fJPiAjKampBbQQqlsds8zLPJ%2b3ltpS0fbh4UsFYc2O7%2bUSJWWZyaqmvnnGyYWLFrZs%2fgtJGXGapSFUFyG6YbDvs4i0ZVqatNUFdh07tVh62OLJ9%2fEix1dt9V%2frV%2fLktpIvUxQ6RgA%3d%3d	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Copyright Joe Security LLC 2021

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.gammacdn.net	0%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
logincdn.msauth.net	2%	Virustotal		Browse
assets.onestore.ms	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://static2.sharepointonline.com/files/fabric/office-ui-fabric-js/1.2.0/js/fabric.min.jsa	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meCore.min.jsaD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meBoot.min.jsaD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meBoot.min.js	0%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com/files/fabric/office-ui-fabric-js/1.2.0/js/fabric.min.jsaD	0%	Avira URL Cloud	safe	
http://https://consentreceiverfd-prod.azurefd.net/v1	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorryc	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com/	0%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com	0%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com/files/fabric/office-ui-fabric-js/1.2.0/js/fabric.min.js	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_EgJbqJOU_WgTDwJ3YZdEcg2.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://login.microsoftonline.comh	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=OfficeProducts&market=de-ch&uhf=1	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=SMCConvergence&market=en-us&uhf=1	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/content/js/MeControl_EgJbqJOU_WgTDwJ3YZdEcg2.jsaD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meBoot.min.jsaD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meBoot.min.js	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion?partner=SMCConvergence&market=en-us&uhf=1aD	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meCore.min.jsaD	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
sni1gl.wpc.gammacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
microsoftwindows.112.2o7.net	15.236.176.210	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
HHN-efz.ms-acdc.office.com	40.101.137.66	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
logincdn.msauth.net	unknown	unknown	false	• 2%, Virustotal, Browse	unknown
r1.res.office365.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
static2.sharepointonline.com	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
support.content.office.net	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
amp.azure.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/Encryption/OTPSigninPage.aspx?itemID=E4E_M_91d82880-d398-4e45-87e4-14d1f09b1851&OTPMessageId=35fe9d4e-7cc6-4b62-855d-ffa889425e4e%40MW2PR0102MB3531.prod.exchangelabs.com&OTPReferenceId=4473	false		high
http://https://outlook.office365.com/Encryption/OTPSigninPage.aspx?itemID=E4E_M_91d82880-d398-4e45-87e4-14d1f09b1851&OTPMessageId=a557b07c-3e5d-4f44-9102-c532f82c6ab9%40MW2PR0102MB3531.prod.exchangelabs.com&OTPReferenceId=6261	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.101.137.66	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
152.199.21.175	sni1gl.wpc.gammacdn.net	United States		15133	EDGECASTUS	false
15.236.176.210	microsoftwindows.112.2o7.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458973
Start date:	03.08.2021
Start time:	23:32:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://outlook.office365.com/Encryption/retrieve.ashx?recipientemailaddress=ap%40gswater.com&senderemailaddress=grainwater%40radianresearch.com&senderorganization=AwGKAAAAAoYAAAADAQAAAL%2bPwYr4eztBl9bc2pXl9%2f9PVT1XYXR0aG91ckVuZ2luZWVyaW5nLm9ubWljcm9zb2Z0LmNvbSxPVT1NaWNyb3NvZnQgRXhjaGFuZ2UgSG9zdGVkIE9yZ2FuaXphdGlvbnMsREM9TkFNUFIwMUEwMTAsREM9UFJPRCxEQz1PVVRMT09LLERDPUNPTW3U2z0RbcxKmUtxcJ88CKJDTj1Db25maWd1cmF0aW9uLENOPVdhdHRob3VyRW5naW5lZXJpbmcub25taWNyb3NvZnQuY29tLENOPUNvbmZpZ3VyYXRpb25Vbml0cyxEQz1QU1QUjAxQTAxMCxEQz1QUk9ELERDPU9VVExPT0ssREM9Q09NAQ%3d%3d&messageid=&cfmRecipient=SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}%40WatthourEngineering.onmicrosoft.com&consumerEncryption=false&senderorgid=1abee47c-68ca-4166-a776-68475cb4c2d2&urldecoded=1&e4e_sdata=NAlD4xF5G7xsjCpoXLsrqcFvJk6j2vhVIIKSh98po4JUh8sQDhUS2lu3%2f27pCMtALumoYdxBZFlm2ASgEEpgP3NQkpb%2bn1kpgDgOCtqD09%2bG%2bs8heIeUlJTsqucw0Zz9OP7E6qTSm5hEj40bLIFk1SDbdplq9xz8N2Bf2l3k4%2fRwKrYELyDkr67ZSu8gKah3uOJUUSAuDu5R6fJPiAjKampBbQQqlsds8zLPJ%2b3ltpS0fbh4UsFYc2O7%2bUSJWWZyaqmvnnGyYWLFrZs%2fgtJGXGapSFUFyG6YbDvs4i0ZVqatNUFdh07tVh62OLJ9%2fEix1dt9V%2frV%2fLktpIvUxQ6RgA%3d%3d
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:	9

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:	CLEAN
Classification:	clean1.win@42/267@17/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://outlook.office365.com/Encryption/OTPSend.ashx?itemID=E4E_M_91d82880-d398-4e45-87e4-14d1f09b1851&OTPRef=SigninPage • Browse: https://go.microsoft.com/fwlink/?linkid=849297 • Browse: https://outlook.office365.com/Encryption/OTPSend.ashx?itemID=E4E_M_91d82880-d398-4e45-87e4-14d1f09b1851&OTPRef=OTPSigninPage • Browse: https://www.microsoft.com/ • Browse: https://support.microsoft.com/en-us/ • Browse: https://www.microsoft.com/microsoft-365?ocid=oo_support_mix_marvel_ups_support_smcuhfm365
Warnings:	Show All

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\19539538-d8b1-4dc4-a6f1-0a44e45145d3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.75002232917252
Encrypted:	false
SSDEEP:	384:xrjYgKNvGpSEVFHs/Ngr5vcY3zQWPHKfG3ar1Koqxz+GG5r1omhtHZaQMMPOSWsV:1Wq1ZCmQr8eHOEekHH+sKicMJX
MD5:	8FE0D4548FDCF195F54AE35F10651BD8
SHA1:	12C70B26ABE97C59628B7F4418FC2D2ED0D2E9D1
SHA-256:	C9BA2461590E406DC5B58E23BCED31784CC4CDBE5FBE80F285A3758DE48DAF00
SHA-512:	15C8C993AE315636E51F2A3D4CA5E0511D7927A8C3BFBD320D4DB9F02042332167EE9C96EC19708486CAE6006C35BA4404BE1468DDD796C62587EAB90CAA308
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....A8.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\39eec20c-825c-4532-8a97-99c87a155249.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):	174336
Entropy (8bit):	6.079367491741129
Encrypted:	false
SSDEEP:	3072:cgLGaYTJQE+mugy9+QV1T7IRwdfLSNP9FcbXafIB0u1GOJmA3iuRh:PKxaV+QfT7GSmhbaqfIlUOoSiuRh
MD5:	F096429D305DA8B15A9FB8B601695D25
SHA1:	774CE00887D053F5884883CA0827608E44CFE6EC
SHA-256:	CD4097AB47A03007F9926E9E4B1D7D94620E6B15D606FF765777510B38752A44
SHA-512:	78E2193460C7DEF216D5512FA55F8A74275D40316ECE48228B45F622FCAB9E133BCE94C8969C5BB5BB2DCEDE9FA872531F8ABBD4F4F84D50C5A7BE77D749387
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":1.62805877960018e+12,"network":1.628026381e+12,"ticks":6533305014.0,"uncertainty":4372824.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016002084"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6098a914-205a-4d5a-aaa7-704c6e64a986.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):	174335

C:\Users\user\AppData\Local\Google\Chrome\User Data\6098a914-205a-4d5a-aaa7-704c6e64a986.tmp	
Entropy (8bit):	6.079367090035555
Encrypted:	false
SSDEEP:	3072:/M4GaYTJQE+mugy9+QV1T7IRwdfLSNP9FcbXafIB0u1GOJmA3iuRh:UJxaV+QfT7GSmhbaqfIlUOoSiuRh
MD5:	FCE2A797D450EFCE3784F2485C00BCE2
SHA1:	2639A9956201CB085CA299880C8E1B3F8E812A5A
SHA-256:	D4A67C402E2586CC768E53740E3056B8327634D00BF6866AE26F538FE5FEEA15
SHA-512:	B18F99173629BA3C321802C16061C44ACAC2FDB5DD28046AC0D1A8C17BD1A8ACCB3C0624C5779D9E13F76225D50202A607D68317D98902A4E52F5732C7C04BA
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":1.62805877960018e+12,"network":1.628026381e+12,"ticks":6533305014.0,"uncertainty":4372824.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8fb7abc0-17e1-4c42-848b-3d04112069ab.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.750155857492192
Encrypted:	false
SSDEEP:	384:BrjYgKNvGpSEVFHs/Ngr5vcY3zQWPHKfG3ar1Koqxz+GG5r1omh2ZaQMMPOSWsNt:lWq1ZCmjr8eHOEekHH+sKicMJh
MD5:	8C15D137F53F3A4ADE3FF188B1661DEE
SHA1:	489209B882857AAC8C36F2F2517B28DC74AAC2BF
SHA-256:	90B7B41968B151B8B4E3F1D11C34BD602FFBD3AB971F4A5D17A0DA89B612480B
SHA-512:	5518632231384D711649CC4ED05ECB047B1D36054D3C2958930A52166E32CEE47761015D39691C2F4141FFD9AA963B0446B1F20C369EB4C3BF6AE32F2A75A917
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\361b6e30-734e-4d00-941f-733b89b7075a.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):	5886
Entropy (8bit):	5.200122906055468
Encrypted:	false
SSDEEP:	96:n8Cb0729GWGcKIkok0JCKL8fkD1DbOTctVuwn:n8CL9CcJ4KKkD9b
MD5:	EC088EA2A9AA071379E86500210497C6
SHA1:	E94DEE2C76E55559DED6FAE30881F578D5B9AD75
SHA-256:	40B1B42D2D5708A935DCB64C1571178D7700AFF98684D34184480639921DD14E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\361b6e30-734e-4d00-941f-733b89b7075a.tmp	
SHA-512:	28F861AF4C9A353CA6F1C01128FBF4CCEE08EE678D7726DA2D66B6134D0A10D4A018F7489320CEF56673FB0AF708603242EAFC9753799C50F95E5DCC349A345
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272532376341481","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\415ddf19-0564-4f35-b4b8-62482e9ee79d.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):	5778
Entropy (8bit):	5.2005956932446855
Encrypted:	false
SSDEEP:	96:n8C7q29GWGcKIvok0JCKL8fkD1RbOTQVuwn:n8Cl9CcU4KKkDj
MD5:	1E0CFFE4CFDA6644ECD226664DDFE5A3
SHA1:	DE23C363E400FC12B0DBE54117F25801B42C5672
SHA-256:	A8AD665FC5A5CA3C081E86EC6E41729BC57654A00EFA562595104E412597C528
SHA-512:	B6CB55FCF14B52DFB1AE8475A729058D3C529A3C3EAEF052D9FB66748F3F4DFBC686898A5A21CE230CCC37E1E01720B6030D7D663A3DBE497A91F24727D5BA D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272532376341481","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4fb7962b-d760-4cde-b891-f422da9bd01b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ef90ca6-f568-4f43-b106-4e7725230326.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):	1039
Entropy (8bit):	5.566229259665207
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvr7wUoRUenHQ:YI6UUhVseKUewqPeUer2UefnwUMUenw
MD5:	F8FC15B0CC3B5EFD27F5572C4CC491D1
SHA1:	5EB0809AC8FC13F7151B8EE851ACE25EAD555EA1
SHA-256:	CA1F4AC9A883D9A38760DF27F7CA7F30BBA7A9EA5AAB3D7360627B262561963E
SHA-512:	353833680CAA25845A69B22405816B936D32F2B05279BBDF49741BE342359AE3C267C5F3C615C27C4C140A41A7E566E34527E5073FB9FD207F9D5E5A77EBB58C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ef90ca6-f568-4f43-b106-4e7725230326.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659594780.036031,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628058780.036036},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\67606d7d-aa9d-4fc8-85ec-570432687f68.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\74fef32d-db62-40ef-93c7-89bd2c2c8141.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):	5.577670760386156
Encrypted:	false
SSDEEP:	384:hRMtTLllVXy1kXqKf/pUZNCgVLH2HfDArUiSS4k:ELljy1kXqKf/pUZNCgVLH2HfkrU3ST
MD5:	DC2D873573C9AE518D0F744F9CEEA305
SHA1:	6FE79375341C29276911653A17EA1E6527D62A34
SHA-256:	37FEA90A982800F7AC57548E57B4E29155705EA3E69EF1BB3FEB7C862A6C6AC4
SHA-512:	3F99E7C3B1B2B469C20135DE12DD300929662599BE3CD0E884C26F1712680E22ED68EF7BB385883679199B7FC82E3A9A71EE9C021F6F2941528B42E44EFDF4B6
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":"13272532376001082","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b8d1cde-8e11-45d9-a452-83da7f69e15f.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):	2374
Entropy (8bit):	5.6039015186521315
Encrypted:	false
SSDEEP:	48:YIUVU66UUh1UZweUcz4U1seKUep2UXUiqPeUerueUMUefnwUMUenw:1UVUvUUrUZweU84U13KUdUXUJPeUfeUs
MD5:	FAB9469E9A88E1CED58A48A6DBC30D5C
SHA1:	7D3E63A152881263F171B6CFBA3600EF0D9DAE04
SHA-256:	0331E07DD48F284D44FD3810B6035D6B008B6B1FDF485C65CB157FF9FE0285B0
SHA-512:	E47D54987D85B2D779649C45C320B9DBA5A5068C0918077F3FEF0A25EBF1A9C819650A0B449870B88DFF160113678DEA23E926FB3E1CE9D51CA0988872AAAF0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b8d1cde-8e11-45d9-a452-83da7f69e15f.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659594815.9025,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628058815.902506},{"expiry":1659594814.949581,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628058814.949587},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659594815.766781,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628058815.766786},{"expiry":1659594813.343611,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628058813.343616},{"expiry":1659594816.021561,"host":"dUymlFcJcEIuWrPNRCRXYtREHxXDHdPfT47kO1IQnQ0=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8292e245-de15-4a9b-a5ac-37bf54bf0ec5.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):	4865
Entropy (8bit):	4.955520738727046
Encrypted:	false
SSDEEP:	48:YcqUklSLklwHjvc2qA8qqTlYqlQKHoTw09H3CH3G/s8C1Nfct/9BhUJo3KhmeSnz:n8CmHX9pcKItok0JCKL8VbOTQVuwn
MD5:	83E2A133DAAEE3B7D626BFDD2083FF9C
SHA1:	1C78B0C942698411EEC437289DFD68782B23DB9B
SHA-256:	CE432BDC0F66E30B0A3443E055EFBA5B881F5FA33148E452A71A78915489322D
SHA-512:	FE7680BAB8E723FC5A3D9961ED103B4493C84BECF366A04DF1D89A5FA6C90D15B41D23674454025B5C7C4A1B31C309462CE0E41DB5F9920D4EAE5F6F53E062F3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272532376341481","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\88ff584c-be93-4054-abeb-1f3c399e4dcb.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):	2373
Entropy (8bit):	5.6053811598524685
Encrypted:	false
SSDEEP:	48:YmUpm1UNf6UUhGUvY2eUcz4U1seKUepLUdUnlqPeUerueUMUefnwUMUenw:DUWUQUUkUvY2eU84U13KUcUdUnwPeUf+
MD5:	CE0B142DF2CB04987AFEAD8EDFF44792
SHA1:	7E047650A656109BDA37C082BC39433A9C29D1B1
SHA-256:	498947875ED5D23C9DA84748D48CF8E10E28023DE62B259880929919917B72C7
SHA-512:	C4E693391056BF4DE4408E274416CB4B20FEF13DF5E0193C5A451E1ED1009737A258CAB74914DE85852C8AD5137CEC8F09124C7BFA0DC6DFEC2BF3BC14ECB35
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659594844.666543,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628058844.666548},{"expiry":1659594839.632767,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628058839.632773},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659594844.56511,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628058844.565115},{"expiry":1659594813.343611,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628058813.343616},{"expiry":1659594816.021561,"host":"dUymlFcJcEIuWrPNRCRXYtREHxXDHdPfT47kO1IQnQ0=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\99511c22-5d76-4cbf-af42-17ec31a106ff.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3078
Entropy (8bit):	4.863074272112497
Encrypted:	false
SSDEEP:	96:JTnOCXGDHznd/X0R4TaZ67WGG6XYFFVi+neVxhH:JTnOCXGDHzdv0RuaZ67WGpXYF3TnQX
MD5:	E106F16FCB73B1FD2EE1013E24894F32
SHA1:	47AAF59E535CC79065B52091AE9247B6124DD9F9
SHA-256:	2C4EBC9BDDDEF07348F380D22010BEA5F1D315F6109DE0D2CA98D1CD68EC7EF0
SHA-512:	14E7BE899ED43087E3743CE520CDDCAA5F7203DF4268ECB640C221E94189D23CB61E013AB99EE8A45F11E95D2780EE53CE924C87B84172C470DDD85D2C0D0F3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\99511c22-5d76-4cbf-af42-17ec31a106ff.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275124380035951","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275124380038028","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f902b39-2e69-4be4-b41c-97c747353afa.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):	1206
Entropy (8bit):	5.579997462767777
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby8VkReUorqUeXvr7wUoRUenHQ:YI6UUhVseKUewqPeUerqeUZUefnwUMUD
MD5:	958BEEBB9D8FA61912E89D4DE81D1939
SHA1:	849B540678F4EC7AFF365EC874FAF9B5BD6F1BEC
SHA-256:	D753CB3B65FD8D7DA3BBC4FC4095D17A53174B06457276693733469707DB702F
SHA-512:	E2BB800882F9D3F5196B24014A8AD07ECC8EF888A6EA810862210D39B1D15F79EEDA4993DF612CD5A08E75E98C63A995D0F0434B758B65CE33B1C7C0F89FC4E2
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1659594800.529968,"host":"0gDcw19KLZhujrdyGYI0dgjyBKJM3paDRz4baiU55SQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628058800.529974},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659594780.036031,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.200822115082252
Encrypted:	false
SSDEEP:	6:mgk+q2PWXp+N23iKKdK9RXXTZIFUtp7JzZmwP7ENVkwOWXp+N23iKKdK9RXX5LJ:L5va5Kk7XT2FUtp7F/P7A5f5Kk7XVJ
MD5:	E643BD88F40B1A7B4EA3B9F808AA06CF
SHA1:	C1205D99ECBC9B56F36606F3B5374FA1AC5C2FCC
SHA-256:	4D6A3420DBCD2C2DA867659B9FCCDCCCD16EC7AF5DD8041767ACB1A97B1B88CB
SHA-512:	7225A7164040F75CA135DF858AE8A8D4EE743688EA02C6AC2613DC9D85ABA1CF51FBFC15C16B25E1919ED72CC00988F0FF9552C195DB3939D327082E1B5D58EC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.371 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:33:22.383 15d8 Recovering log #3.2021/08/03-23:33:22.384 15d8 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\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.200822115082252
Encrypted:	false
SSDEEP:	6:mgk+q2PWXp+N23iKKdK9RXXTZIFUtp7JzZmwP7ENVkwOWXp+N23iKKdK9RXX5LJ:L5va5Kk7XT2FUtp7F/P7A5f5Kk7XVJ
MD5:	E643BD88F40B1A7B4EA3B9F808AA06CF
SHA1:	C1205D99ECBC9B56F36606F3B5374FA1AC5C2FCC
SHA-256:	4D6A3420DBCD2C2DA867659B9FCCDCCCD16EC7AF5DD8041767ACB1A97B1B88CB
SHA-512:	7225A7164040F75CA135DF858AE8A8D4EE743688EA02C6AC2613DC9D85ABA1CF51FBFC15C16B25E1919ED72CC00988F0FF9552C195DB3939D327082E1B5D58EC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.371 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:33:22.383 15d8 Recovering log #3.2021/08/03-23:33:22.384 15d8 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\AutofillStrikeDatabase\LOG.old (copy)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.200685228758359
Encrypted:	false
SSDEEP:	6:mgsJrFN+q2PWXp+N23iKKdKyDZIFUtp7FzZmwP7FjVkwOWXp+N23iKKdKyJLJ:LGOva5Kk02FUtp7J/P7D5f5KkWJ
MD5:	2CC2F4832E26EC6BC8DF7DDF87A97BC4
SHA1:	EDE65EFFEBEF31EA56C745D0FD26266423D86554
SHA-256:	05BE22245F9B765BBB9A59B713F15AF19CBCFAC7A7E03528C63A04DE9AA362C3
SHA-512:	335D793374DDB8CA123DB2353ED4F37F779911DF5EE222AFD1BB961FF3346AAB92A3EEAEA4DBD30B6BB05A2674F2C4370E0FE8020F4935ED0E2D9E01E4EB2E49
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.364 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:33:22.365 15d8 Recovering log #3.2021/08/03-23:33:22.365 15d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.200685228758359
Encrypted:	false
SSDEEP:	6:mgsJrFN+q2PWXp+N23iKKdKyDZIFUtp7FzZmwP7FjVkwOWXp+N23iKKdKyJLJ:LGOva5Kk02FUtp7J/P7D5f5KkWJ
MD5:	2CC2F4832E26EC6BC8DF7DDF87A97BC4
SHA1:	EDE65EFFEBEF31EA56C745D0FD26266423D86554
SHA-256:	05BE22245F9B765BBB9A59B713F15AF19CBCFAC7A7E03528C63A04DE9AA362C3
SHA-512:	335D793374DDB8CA123DB2353ED4F37F779911DF5EE222AFD1BB961FF3346AAB92A3EEAEA4DBD30B6BB05A2674F2C4370E0FE8020F4935ED0E2D9E01E4EB2E49
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.364 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:33:22.365 15d8 Recovering log #3.2021/08/03-23:33:22.365 15d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07018f0058501c54_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	452
Entropy (8bit):	5.570543093086548
Encrypted:	false
SSDEEP:	12:EHfW7RDvUzDJN0VzNSHfW7RDvUzDOiN0w:sWVbUz1N0RNCWVbUzPN0w
MD5:	A23DCD32234B97494BDFC1C9BB438186
SHA1:	E773B262BDAD3056E05AA5EA348121CC74DDA838
SHA-256:	A36066611B0F2D2C7C25CAF528E36720E1B718A08F2E3381B0E170426C69B4FB
SHA-512:	C9063491D4892E249BC314CFB8A644FD8BA5107BE725B0570C2A924BD0B4E2D8497BCAD305EED4D4DFA8E45F23E61FF5325F6BC6D48B111C65789482C58A821
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...L....._keyhttps://az416426.vo.msecnd.net/scripts/c/ms.analytics-web-3.min.js .https://microsoft.com/0..CL'/.....]..... ..K....].I....,...$....A..Eo..... .A..Eo.....0\r..m.....^...L....._keyhttps://az416426.vo.msecnd.net/scripts/c/ms.analytics-web-3.min.js .https://microsoft.com/+RLEL'/.....oi.....K....].I.. ..,...$....A..Eo.....Hh.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07e591cc9237b16e_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\07e591cc9237b16e_0	
Size (bytes):	53898
Entropy (8bit):	5.966819215608049
Encrypted:	false
SSDEEP:	1536:CJZVkHMzjwhAWlWAWfWLWhVLvL/iyuLyf:GZVf
MD5:	C3A6318EA7E2A27CB2CFA0FAF3CBC8A0
SHA1:	1A1FC8981E3EEA77FF9595B5879C1DF0A2DD4707
SHA-256:	29D2281C1A07B4DF7A014ABDD9823A3DAA0F725D918453FCF403EE627B78596C
SHA-512:	2ADBEFDDE146A9BDD2E81EB29AFF4D1BC68F4917D0235FEA5A43726C4821AED5B78F4DB12611FB92BD49CBD103CF6093BBBD857D003FE1E9724F7E1B5AD77 873
Malicious:	false
Reputation:	low
Preview:	0\r..m......b...q._a...._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meBoot.min.js .https://microsoft.com/...CL'/.......................}L.j2..@[..v.P'l..?..o0f0.. .C.A..Eo......*m...........A..Eo..............................'..l....O........\.m............L..............|.......................(S.H..`L.....L`......Q.`.,. ....MeControlDefine...Qc.kB....meBoot.......`......M`. .....Q.@.(......exports..$QgB.......@mecontrol/web-inline....(S.....IaE...............6....O...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\08f1a8bfdd0963ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.4644239828608185
Encrypted:	false
SSDEEP:	12:EXLDQLsFhhBoK7u2vHOX797DjNC1Ngw9jMuweP1DCD4oL5or:SL/hHK2/OXB7DRCrMuFNDC+r
MD5:	74AAF0F308FEAACE1B14DE3BFEEE75F8
SHA1:	CD1290A4B1B4A301D150D40029DDBE1683DF0D8D
SHA-256:	4911ECE3630ECFDA02D489178310C83A8AE00708CD0DBA4CDEBFFF0D95CBA02D
SHA-512:	937A5E70A31C88B70807D20CA2983B25EA16CFB4734E754E01980B2A40FD35A7811A27002F8CB3E6505E117A5A96FC1135A823ECD0259AC4C515B4DC50C25AF
Malicious:	false
Reputation:	low
Preview:	0\r..m..........mU......_keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/2f-63ce8f/45-f9a0d4/aa-dc1460/2d-7a9063/8f-165e61/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/1e-2692a3/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/6a-234a32/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210618 .https ://microsoft.com/...EL'/.............\........[.D.D.S...1OK.|f...>.e.....&.A..Eo......n...........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0dc8e4beee7ad97a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	406
Entropy (8bit):	5.523296221557826
Encrypted:	false
SSDEEP:	12:YDFaj9uLesKlIT7Teq1rKDo1m2ANtuZGv:YhapEestnTH1rKF22cm
MD5:	E095B771FF765084539382750901985B
SHA1:	82AC6A2417629937C4966A6C18EE8248BB8C3434
SHA-256:	F2F921F3FF38E1CD6393E764C2F49EBC2DF4B67C24833DB7E74A3069FB0BE0F9
SHA-512:	625C843881331D8AFCA09BA4157190F87744C994D57BA036F4D8710AC30A90EEFBB513E8CAC961B9A4FA861220A18F6A9C4F90F06398842EA3B4551ADDA5D80
Malicious:	false
Reputation:	low
Preview:	0\r..m...........K......_keyhttps://www.microsoft.com/mwf/js/MWF_20210208_31270267/alert/autosuggest/contentplacement/contentplacementitem/dialog/flipper/glyph/ heading/hero/heroitem/hyperlinkgroup/image/list/pagebehaviors/singleslidecarousel/skiptomain/social?apiVersion=1.0 .https://microsoft.com/...EL'/.............6].........0...^.....F ....([.....]s=.A..Eo.........f.........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fa6b51446c8bf26_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.5199211404064785
Encrypted:	false
SSDEEP:	6:mGPYWFW7RPo8Dqik4nNrYrZK6tWGPYWFW7RPo8DaAeXTk4nNrfK6t:vzW7RPo8DLePFzW7RPo8DaRB/
MD5:	A1CCE20BD61FCB3776CE17719CE920CA
SHA1:	196BB7FB518957E74F512EA286608A0DDA798C6D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fa6b51446c8bf26_0	
SHA-256:	D6E9B79033C2228DDA427188F83627771859F16D6B0E647C66A9F48CF070D633
SHA-512:	019AEEF3BB058CD892765FAFB5DE5E4991FAAC797A13976A9E4E92F8A2D54F38F8E0C36343F52AB60311B71906AEC90F9C13D6A8843F5731C8081C1018DEC0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...X....._keyhttps://az725175.vo.msecnd.net/scripts/jsll-4.3.5.js .https://microsoft.com/...CL'/.....T.....li..Hw.(a...A.....unT..2.(...A..Eo.....A..Eo.....0\r..m.....P...X....._keyhttps://az725175.vo.msecnd.net/scripts/jsll-4.3.5.js .https://microsoft.com/rDLEL'/.....hi.....li..Hw.(a...A.....unT..2.(...A..Eo.....l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10048766a3a6676d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.738643848896612
Encrypted:	false
SSDEEP:	6:mU6EY4BLIMZDP638vnOAQhvwWD2DZKyjoxSmt6P4N65XhK6t:kl9TDP6ujQhYK2D0bYmmX7
MD5:	0CDB9FED9273C9A55F55D3487B9C3C3F
SHA1:	BBAC27932D9370572FF70B6509C33D08F381B400
SHA-256:	000AB341019244854A3F81D1FEB4FE5C5BB64B13BBA6A93AA5685C45DD1C9366
SHA-512:	7C6346D4401DB5E9E4FE0388341A749AC6C0CEEC8B47BE14CE09A4E2E25F7906AEB6602293FD984DFDB0B478C3F4278F201D9F5B3DB46462CB4677620B5331E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...7.yz...._keyhttps://support.microsoft.com/socbundles/TopNav?v=XYJZrw0yvSWJRlrR7vC3uLGzcXwCX5AMXhrSLUSZJ9s1 .https://microsoft.com/...CL'/.....td@H.....Q.te.7.p9=..+hS....MR.A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\166ee82c52b87e97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.878177765109015
Encrypted:	false
SSDEEP:	6:mY6EYmcRR3/wZdDfryR5i96VrYK6tOsJvRS8GQjud8Sn+4hS96VrL:RLcj4ZdDfIE9Xp0Iud7VS9
MD5:	4EA54701A19908439CEC6D032A6FDB8B
SHA1:	20C5DFA649841F59F9EB8DE4B78986CA0EEC5457
SHA-256:	3799392E114389978F47C0E5043997996A8B2937719DBEF22E75C9525B4CE198
SHA-512:	717B32F3BC3E29304DED5D142FA9A134AF38978E4EBED5D71D1984E18F293AD0393B7A03F07AB622E167B1E5B1F05A6D502E9E8094CAA27E554F699DFD6176F F
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/..EL'/.....(..A=Z....F...1/.k....s6...A..Eo.....`.....A..Eo.....EL'/..w..BCAA09D902FA7A31D5647F5BC49F0BBDD12E7DE25A73E4E5E381B5B9CD8C6AE2.....(..A=Z....F...1/.k....s6...A..Eo.....gL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\185fb8be4e716935_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	514
Entropy (8bit):	5.830834915254187
Encrypted:	false
SSDEEP:	12:7J9TDP923/Dc7+rzN1J9TDP923/DKo7+CI:lpiQ7+vNbpieo7+v
MD5:	5DE8E3C89A0C26B32F313923E1481D99
SHA1:	9EEEEE3D5C751ECA0051BB620C4F8469D2627C87
SHA-256:	2E30619823F36F06CCE11367C16D5168B935022C2D2671664D7DD8CEB185244C
SHA-512:	5961ECCB40C31CC7A76D46A625D2F55CC7A259349E491AC1E191C20ECCBAEEC01BF873E42BB919B2C0B27AE0DD8B629C0FD87734FD905427197F0E8BE6CC7 E6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...F....._keyhttps://support.microsoft.com/socbundles/floodgate?v=N7a-gpEJQkN6bthY4nvjISnR62g8lnmiDB2WXm1P3aI1 .https://microsoft.com/~..CL'/.....c.-.....%.#.i..I~-.\l...A..Eo.....?..%.....A..Eo.....0\r..m.....}...F....._keyhttps://support.microsoft.com/socbundles/floodgate?v=N7a-gpEJQkN6bth Y4nvjISnR62g8lnmiDB2WXm1P3aI1 .https://microsoft.com/.~PEL'/.....k.....c.-.....%.#.i..I~-.\l...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cadb05993d4cd38_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cadb05993d4cd38_0	
File Type:	data
Category:	dropped
Size (bytes):	461
Entropy (8bit):	5.442370354209141
Encrypted:	false
SSDEEP:	6:mzfYIEYGLTDFSVjKhaBokqPSuwykNWXeFODOtyIgoG0Y17vKDxryBImbP4ZbK6t:KAxDFajJEPjTxTjoq1rKDqHM
MD5:	AE5A96F92787136AA678564AA85913A5
SHA1:	D3FE99F410328B3D8DE1388E7408D4B5CDA7CD54
SHA-256:	AE999AA3847CEBD392B191E6D298BACF09FF6D23EF3E09EB9F0C26F613B866E8
SHA-512:	EE787366CADA793BCB5AC70F106254A7083F63B41BDEBEE871EDB1C234DE45191550D161FB040AD16FC95C9C1587A97271EDE0864E23EE3BD7278DF15C4963 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...+U.<...._keyhttps://www.microsoft.com/mwf/js/MWF_20210208_31270267/alert/ambientvideo/autosuggest/button/calltoaction/dialog/divider/feature/gly ph/heading/hero/heroitem/hyperlinkgroup/image/imageintro/list/logo/mosaic/mosaicplacement/multislidecarousel/pagebehaviors/rating/skiptomain/slider/social?apiVe rsion=1.0 .https://microsoft.com/..EL'/.....O}.....|.....`...>..Qi..mq...i..3Ah.K.v.A..Eo.....@z~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\282edb9c7e8884e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.8400024854727794
Encrypted:	false
SSDEEP:	6:mTVY4BLIMZDPyBsYqkPpHlBeRQD1C1xPWAOeULA3pnK6t:AL9TDPyBsYqkPpFBeRQD1AP7p
MD5:	FC9BE9327D4823999AFE84B3FB4C66A7
SHA1:	AB94A22433A67E923EA9E565F6A945E474F445BB
SHA-256:	15947A56CCD9BBADC46886B916B995C52CD5189EA22707C46E4B9464EA01A495
SHA-512:	02FD6E47A724C00643A5AF1BDF9343AEDBE8ECF4F4D719D4A574A20A41DD7E55618CC118780B02540F0E577EA16BBD36F4065967D066322065D441EEFE177B2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://support.microsoft.com/socbundles/ucsCreativeService?v=rLatTOmgAUzH_Hj-oxMb0g13eiTFM1vUQQRSCPIDl5k1 .https://microsoft.com/.. .CL'/.....~.....n..W..3..&..&.f...Eu.A..Eo.....A.?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2847712ffa08e54e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	489400
Entropy (8bit):	5.9859454777480305
Encrypted:	false
SSDEEP:	6144:e4CIrsdy8H42+MdwxyP87z1JeiF2XAjwPh5Dr0+vR73j726j05Hohs1qoG:N0y8Y2+1xyq2F/o0sG
MD5:	91D92DC052F7B9F9D38F7B8BFD29E3E0
SHA1:	47C8089875D8D8F7B55F76ECF85573CD324DCEFC
SHA-256:	6621A5D3B40F2FB983BB5AF9BF9DC56E67976E766886EC3BE44B1AA13C5D41EE
SHA-512:	6B356EFB31E31299E16E1A5DD049AA3902F54D7D1DE10949B109CAC6005A9C9C79EEEA1CCB46D356CAF438457FF58F775BFEEC9CA14B12AD7833552CB1D891 46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....y....BCAA09D902FA7A31D5647F5BC49F0BBDD12E7DE25A73E4E5E381B5B9CD8C6AE2.....'..0....O.....t.....(...L.....p...d(..... .....T.....4..... ....2.....H.....<.....H.....`.....0.....\.....(S...M...`NV.....L`..... ..pL`4....(S.....Ia`.....d.....(....$Qg..v|...._handleMultipleEvents...E.@.-....HP.....<...https://amp.azure.net/libs/amp/1.8.0/azuremediaplayer.min.jsa.....D`....D`F.. .D`.....e(...`....&...&....D&...(S...Ia.....d.....P....Qc.8U....._logTypeE....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29fd944161e42a84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	745
Entropy (8bit):	5.287828528273069
Encrypted:	false
SSDEEP:	12:6DQLsFhhOpuhHKJtaYONkS70me9iTMhKcOZG1/NlHJUdQWjmH9mJRCDMI19G44b:6/hXhQFO970mJghKcPUdM6Cvcb
MD5:	C5E3E170AE4419CDF93C38237FB6B851
SHA1:	473EFAE481193B12298EDDF0372CA9A1BCA010B1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29fd944161e42a84_0	
SHA-256:	C977F145BDB1933F247301BDC14EBC29969A097FB57712A0A6224E64BCBF872F
SHA-512:	6ADFE90C3362FBD5F11CCC00B4BFCFA0669459C6EB46A984D09C0BFFB11B9C15D3EA5BB59ABD5CA9C7C69C61173669CEF60C1B18111D977A9DA653118EEE5EB7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....7.#...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/e1-a50eee/e7-954872/77-04a268/11-240c7b/5c-0bb0c0/81-a5a694/2f-63ce8f/6a-f6eed8/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/ab-b04110/fd-7cc407/a4-fd2a9b/7b-131f20/66-c19a96/d0-633018/74-b70f5f/84-e0fd46/cb-abee28/1d-c29f1e/80-c05e42/a5-ef9ca1/f8-6a3735/b8-96db64/b4-d9c6d1/59-aa2448/d5-2b21b0/c5-346220/d6-6bf74f/8b-0d15c7/b8-527d75/57-0776c0/7a-fdafe7/18-91dd3c/88-3094ff/bf-4fabe5/a5-6014ce/12-fd63db/85-b1c94b/24-d5457e/64-02965a/37-f22d3d/33-eb67f7/fb-890cea/c9-860587?ver=2.0&_cf=20210618 .https://microsoft.com/.lmEL'/.....+v.....3?.J...'Z..j/.!J....dDfm.....A..Eo.....z.N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2ba56d1e276a69f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.75783715726588
Encrypted:	false
SSDEEP:	6:mC5Y4BLIMZDPZjB3QDofHb/B3NpGrmal/hK6t:l9TDPf3QDo/93NYhl/7
MD5:	5B2BA4618AAB759136E01FA760F199F5
SHA1:	95E12D7EDD4B3241549E624E2DA753AEA96E02B9
SHA-256:	665F624738825C37B72DD4C43FBE09406615F4C2E26D43C02B7340BE4C80886C
SHA-512:	2AF9898D3F8FB403C1BCEF266AED255C26DA2313E0B58B961C0AC8AFD1CBD1B769D6533B077CE73599E12E7B105AEC57AEA9BD33AB5160C66FCD51105F1B8D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....5.5...._keyhttps://support.microsoft.com/socbundles/homepage?v=3jvh_tz5JJrzNs4D8sjDMbG0CR3HHBpdqMXidZ-5Huw1 .https://microsoft.com/z%PEL'/.....k.....N...5wV.+v.F..11...Q<.^;..A.v.H..A..Eo.....j.s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2ca3f69ffae31103_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.617050493481704
Encrypted:	false
SSDEEP:	6:mkYGLTDQyKfZ+OsFRzhxfaTCEFDady2y5GuQwlfF4fnbK6t:pDQLsFhh4TCCDaw2WXF4N
MD5:	7FC45A4A064AE74414493CF7C7566B37
SHA1:	BA2A4740B1B9E41308B82EFC2912D6F0433A0BD2
SHA-256:	6085AB5ECFC979D1E1DC2AF26A86D46EFD15473F3DA72A98B8898F654F970870
SHA-512:	43C0DA9F9DDC94C218DF354BF93BAACD141B5675208F0362CEDABD455C89F3E0B89AE47B9EBA34F28D3B527D6DEB9DA08E2AC3893F0F8DE298A1BDDEE5BD48E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....-t.|...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/a4-539297?ver=2.0&_cf=20210618 .https://microsoft.com/.8.EL'/.....\.....1..}...c-...b..|..G....e..3....A..Eo.....#p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42019e3973afeed0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.8590898815816015
Encrypted:	false
SSDEEP:	6:mc/XY4BLIMZDPql3QDyc/mIoOicngK6t:5/J9TDPi3QD2IoOikC
MD5:	8EFD7CA5667716660A1596CEDC7420AB
SHA1:	B4D3433F977EEC710DAE1A496E47B49F6F45550D
SHA-256:	DA21F6E55DADACC9979DC07F38F08D8EA894C7B15AE06E47DFC6C74B8C444EBD
SHA-512:	BF5032F37D2961EA105402ABE8C0B1F6DA52B3786D2A95A8A0A219366761F50BF7FB0DFCFA5528119A2399D537427A32E5016D8DD9770A97422F282FBA9FB169
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...._keyhttps://support.microsoft.com/socbundles/stickyFeedback?v=qQkT_1VC3j-0Q-KC-UNSe-mjZ0UpEjddXcn2GxlYgvQ1 .https://microsoft.com/.}.CL'/.....w.D0]}@Z^.q...=,.. ..PJ-.....A..Eo.....$.....A..Eo.....

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):	5.563550090396766
Encrypted:	false
SSDEEP:	6:mCVYL8uCKxwVOdD2DtscT05df/CxJWom4FQK6t:irbwVgD2DadfyWHL
MD5:	B863CDF34C178EC7061F1C0F04644903
SHA1:	04309FC9939A444AB68ECD1E58620CBD2A976735
SHA-256:	BC49BE01BAEE8BEB922860121E5FE8955A595B5C4A9A0FF45624CDC9C01552C2
SHA-512:	3866F7E4E997F4E7B4BC6D7791F9465BC6F72996F49488D05BD238AB633EF44940A965CB67FCA2525DF3F97684DA846234286CB0E464B3FA2FFC2E4F937A7B80
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/...EL'/.....}.....*d..,.....cP..Tl.*...A ..Eo.....>8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59a8cca6e4f3998e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.751026711210495
Encrypted:	false
SSDEEP:	6:mC9Y4BLIMZDPO8vnOAQhvwWD2DCQ1xtWWkJ2V9hvK6t:pD9TDPjjQhYK2DV7gWp5
MD5:	72651FE5CCC8D60ABE96E5E4EC0F8411
SHA1:	F59EFF57AA7C04CE1B88C2784207F6251D7BCC94
SHA-256:	CA7D29A0A0E214A1A30E3A765F4692C4D282171C72F081D2F4A7F66A37643836
SHA-512:	F05972DCA3638B0B371B9878C663B6698D697F7A262CB8313980B4C33BE34DDEF3B9C78FCE221BD38384347B9426A783A2FB5847CDA1BF66518DA916047FCEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...t=.V...._keyhttps://support.microsoft.com/socbundles/topNav?v=XYJZrw0yvSWJRlrR7vC3uLGzcXwCX5AMXhrSLUSZJ9s1 .https://microsoft.com/.lOEL'/..... .....k.....d..lf....&l...j..d.,I5.%...(..A..Eo.....0C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e26752cdd389193_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.823230104290296
Encrypted:	false
SSDEEP:	12:OD9TDPVd0/DJd5m+IoD9TDPVd0/Dim+U:2pRgVOvYpRglP
MD5:	DA90CD2A2F74E3F6184BD6A6D065EA46
SHA1:	A251BBF93C8EC7D0EB56266BE574B1F5AE1D11A5
SHA-256:	75BD442CB96C4AAAF2C0DC4A78E23D343FA95583348F86333971F737E7A1BC70
SHA-512:	994C511E50B605EA08DF80A2CD7CD043872B34F0A921D5F74D858975983107D7D8CB0A38EA83786C1A00404C4823BDB50F3A314FDC5A09D29CA44F4719164DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...-....._keyhttps://support.microsoft.com/socbundles/article?v=n3WzlKRRyiNLv-ORJi3GWBqOG4FGm_LqYA33W8Qo3z01 .https://microsoft.com/.d.CL'/..... .....K.....-.9?.....w..4V;&..1.A..Eo.....#.s.....A..Eo.....0\r..m.....{...-....._keyhttps://support.microsoft.com/socbundles/article?v=n3WzlKRRyiNLv-ORJi3GWB qOG4FGm_LqYA33W8Qo3z01 .https://microsoft.com/.=PEL'/.....k.....K.....-.9?.....w..4V;&..1.A..Eo.....A.C@.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6424745969b4f2a1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	53906
Entropy (8bit):	5.969051312448432
Encrypted:	false
SSDEEP:	1536:2JZVjHMzjwhAWlWAWfWLWhVLvL/iyuLyy:yZVn
MD5:	7D7C5002FC53CF955A36C64879553B33
SHA1:	F7FDCDE9B56F77F8183DF37224A57EE9587A0C96
SHA-256:	7207A89EFC123EB781F4AA7D19C38F4CB8B94625FC48F4B63C6693737D34C31F
SHA-512:	246DFD070F6D82488B7F2DEF99208E7E3B548137817F217BE814C9D71CD35A2E94B469B1B39697B2427E3D0EB0DC7A9823DB5CCCE53DE9E60573E903DCB0BF C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6424745969b4f2a1_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meBoot.min.js .https://microsoft.com/.. EL'/.....[^.....|.....e.s...9.%.g~.._.x9J....^. .A..Eo.....v.z.....A..Eo.....'..l....O.....m.>.....L.....|.....(S.H..`L.....L`.....Q.`.(G7....MeControlDefine...Qc^.....meBoot.....`.....M`.. ....Qc.v.....exports..$Qg.....@mecontrol/web-inline....(S.....IaE.....6....O...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\6a8c63844138b23f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59890
Entropy (8bit):	5.296626523457005
Encrypted:	false
SSDEEP:	1536:iO8MlheFoceBkUq6L0z4KjPJXzzZImtNAzLwRwJpkP5xYi1rMQtcDtdsYqO9rD10:D
MD5:	D828FF07D7748D6C8D52BF0B3FD9B7F5
SHA1:	A5CB0298F068EFA274B1F4C1809F0E5FB4EDA990
SHA-256:	20D4C703B4DDD089E880DE68E39EAB07ECD3C5D4BC015E8477A18B779C313C54
SHA-512:	D52F6661EC7D2D020AAFF2776AC02FF389DD5384468C11466878E7D76F38A60F2EF4DB8FEE02780312C65004849AB017D58E00BBFCA129F49010C5CBBE4A2DF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...K9....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21162.3/en-US/meCore.min.js .https://microsoft.com/...CL'/.....5?q.@n.q5?df..... &.wL.h..Qu.A..Eo.....*0.....A..Eo.....'.@.....O....`....$.....l.....(S.H..`L.....L`.....Q.`.,. ....MeControlDefine...Qc^.....meCore..... .`.....M`.....Q.@.(.....exports..$QgB.....@mecontrol/web-inline.... Qf..M.....@mecontrol/web-boot..(S.....Ia[.....A.....~....@.....@.....@.....@.....@.....@..... @.....@.....@.....@.....@.....@.....@...+..@.+.,..@.,.-..@.-/..@././..@./.3..@.3.?..@.?.A..@.A.B..@.B.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\7801a9a904161a21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	43091
Entropy (8bit):	5.876606279312446
Encrypted:	false
SSDEEP:	768:eZnESoJdhT2TlkG75Mcm0F4COMbLGNguoCJe73US:eZnxo7TGS50F4f0LGNgLme7kS
MD5:	0ED9F03F6CF98B362DFC4B607F3378AB
SHA1:	DBC32A3B59BD04A65D321FD12ADCADCAE4267218
SHA-256:	4544989A29E43EE97BACE3306B5CC80BF1F034378A92ED4D27880A1D5AA6E8E1
SHA-512:	8DCDF2455A7DD224DF845678516BD954CE2E402855BE0297C4956482CEBADD9602DF349BF0744E64E124C7252AA3FA245A48EB1033C18DDB6CD3FDDBF4329C E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~.A....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/78-6f121b/f4-c426d8?ver=2.0&_cf=20210618 .https://microsoft.com/.k.EL'/.....#].....~.....9.x.....0.K./Dc..S..A..Eo.....z.....A..Eo.....'.....O....X...o..X.....t..... .....(S.....`.....=.L`.....L`.....QbJ.X.....awa...Qd..z.....behaviorKey...Q.@^..x....define....Qd..K....jsllConfig.....`.....M`.....QenoZt....rawJsllConfig....(S.....IaB...O...IE. @.-.....P.A.....https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/mscomhp/_scrf/js/themes=default/78-6f121b/f4-c426d8?ver=2.0&_cf=20210618.a... .....D`....D`j...D`.....`V...&...&..A.&.(S.t.`.....<L`.....@Rc.....Qb...|....t.....Qb...|....n.....S.b.....l`....Da2.....(S...Ia....H.....QbV.....r.....!.d.....(S...IaR. ..J...../..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87aef5dbae583360_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	441
Entropy (8bit):	5.721676293269104
Encrypted:	false
SSDEEP:	12:GDQLf+5KWFhhzNK2hEt4HfhlbepbZrYWCDUmgTllT:Gj5Fh1ho4HfWp9YWCImQlT
MD5:	A4A397719AEB27D91AB6ED7F3DCE8BD3
SHA1:	A88837F47CEB770DAF0AB8A307066B8677B554A2
SHA-256:	F63CED7B40B4AE5F66A85459F7D61C60D257E1959D1BE4C5B22637DC57BBCDF4
SHA-512:	C5838B5153A11C541E4C3E549164A373D0E1ED8B703D94897789734AFB68FD280A9B77895B7B2B80830B2C1F8E8F85213861A89574B13269286EA4B9CC79BE4F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87aef5dbae583360_0	
Preview:	0\r..m.....5...W....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/c8-0b0bf1/99-5b2d94/f9-5804e2/2f-d255e3/f6-c46fbb/7e-a075ed/24-71291e/51-342e75/58-f3fc85/74-06cc32/35-b7738f/df-046a69/8b-1546f0/66-afd0b6/f5-7e27a5/d7-de3320?ver=2.0&_cf=20210618 .https://microsoft.com/.w.EL'/.....H}.....N...w(...\....d@.]..G..8pE.O.A..Eo.....s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87c9707040e653d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	293
Entropy (8bit):	5.666127924055845
Encrypted:	false
SSDEEP:	6:mS7XXYGLTDFSVYKLsnWXnRKWJAytUvKDII2yAllWP9cfVnH4Z7DK6t:vzDFanLsnW330KDINPllWP9cdHE
MD5:	CC95EE05D0DE10920E08F318807A0665
SHA1:	35A593FC9746EF04E4208A4EAD9CC1B4E6882C64
SHA-256:	3EEBFC688D3734729EC8C422586FCC6058B1AD2D4A931F09953374623F56FAAC
SHA-512:	1C7575D9E9572493CF1E10CACF154C4EFA4911555DF9591392239F5294D13FAFE866628FB461866F346B540F955C880EFD753B020C259ED3DE43BD273CFFD95E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....+[...._keyhttps://www.microsoft.com/mwf/js/MWF_20210208_31270267/button/glyph/heading/image/list/pagebehaviors/selectmenu/slider?apiVersion=1.0 .https://microsoft.com/E.mEL'/.....ev.....OZN.;.J.HMS.Kth..{C.....,U.A..Eo.....40.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8a41173cbadc68f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24490
Entropy (8bit):	5.912192600579492
Encrypted:	false
SSDEEP:	384:lefYnLS7y+hIotbB3Psq+PSRscISfXtBEESFdCCybvQRHaQ5u73vR:IWmWxD3PsqFscxXtGRLD4QlaCu7fR
MD5:	A345C61D304E1B84FCB3D9636CCF1D4A
SHA1:	9C3203A8E1CA442AC2E7184791F3DB291B33A11B
SHA-256:	097710B6E4504E7AA21F78B27D2DF90288258B48B22026EFB1DC365E104207B2
SHA-512:	1F7F63A1B8DE863B162AD48457AC7FDD9183691F96F5E6DCCB704663759DD416E665F19BF3EE70F3EBC156B471461439D8A2A2066EC0F1672381224968F0F692
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....C.|...._keyhttps://mem.gfx.ms/meversion?partner=SMCConvergence&market=en-us&uhf=1 .https://microsoft.com/...CL'/.....)3.8=..p.O.....@ !....&s...b.A..Eo.....59N.....A..Eo.....'.?I....O....^...:I.....P...@.....(S...`....<L`.....Qc>..V....window....QbB.~.....MSA...Q.P..... ...MeControl.....aN.....QbB..}....ver...Qd.._N....10.21162.3....Qb.....mkt...Qc.....en-US.....Qb.*.....ptn...Qe.?.@....smcconvergence....Qb".....gfx.. Qf..R.....http s://mem.gfx.ms....Qb^.8b....dbg.H..Qb...z....aad.G..Qb.....int.H..Qb.x.*....pxy.G..Qc>.....msTxt...H..Qb.0-.....rwd.G..QcR}|.....telEvs...pQz...b...PageAction, PageView, ContentUpdate, OutgoingRequest, ClientError, PartnerApiCall, TrackedScenario....Qc.\....remAcc..G..Qb...^....main..Qc2.....meBoot....Qd..NZ....wrapperId.....Qb..T. ....uhf...Qc.Y.!....cdnRegex..Q.A.....^(?:https?:\/\/)?(mem\.gfx\.ms(?!\.)|contro

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bd751b01a0ac2c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.901055195214128
Encrypted:	false
SSDEEP:	6:mr9YyK08fOiQGAJLD+Ahqkt/2Pip4u/bK6turVdMOZTW0hBW1luCip4W:iKjfOJGmiEqkte6Z1uVdMQTku57
MD5:	5D58BD6E1F4CAB26F0B08584B85EDC5B
SHA1:	D0FEBF9AA1009B0B8D9C695F44BB5DAD81F4AE16
SHA-256:	A049A38ADE950FC6C570F0D329E231F82F8C9A347A5A693FD87E58B5F263925F
SHA-512:	63AE64BD3B810D7C6F69478F57FA73225CC007D9D9458021B85DFA9F41F0A6B25E7AA9B70550DB1286645AD089785B21E4C7FFC8FB74D05E8777840E4AB2D0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....?....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.12.4.min.js .https://office365.com/...BL'/.....0..<.....3`]F.7k*kS.zRb.n-...A..Eo.....@.%..... ...A..Eo.....BL'/....7E5A7CAA6407BEE12B42C3061FA215EC55DFE50350CF46AE46C7C6BBEA1F9927..0..<.....3`]F.7k*kS.zRb.n-...A..Eo.....G~m.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Entropy (8bit):	5.826340365531952
Encrypted:	false
SSDEEP:	6:mXYI4McTDsJegDNrlAFC1TrlEfFK6teClDwURafm+VuKWVTrlEF//:e+TDsYgDdlgC13eflDwlles3
MD5:	F63E9874606DFC015D2CB853850BD7D1
SHA1:	633833F17E42A34D0B6B1FF55D23DA8C3F204533
SHA-256:	921A52461CE5721EAF95DEB2463CFA6243FC796C22D18D4D170B7C1EDB1C43BF
SHA-512:	124C680EF4A835CC7F9EF217970DDCB003263F934FD9ADB98FC00A58706D33526875DCB120F7E2178E79B9C5AA93310A55CC7E1FE1A630EB2E467ECEFF5485AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/M..CL'/.....<.S....l....*.W.U\..E?`..r.A..Eo..... .....A..Eo.....M..CL'/.p8..2E9ED0901FC97404F264F835FD84A666BC46159DA8C5838EE0E347DA5569742B....<.S....l....\*.W.U\..E?`..r.A..Eo.....,GL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91e887711a548594_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.424053899392158
Encrypted:	false
SSDEEP:	3:m+lZn8RzYrSLZRtRJKj1ZPNTyRA27FYtRphpjlHCQ1oIrTnyeEgBQAL4mR5/tpK+:mXYGLTDyxBrxDZcQeouNq/LK6t
MD5:	2CB9A6B957ED4D8DC41F86C1C3AA139D
SHA1:	742D9FB331FD4A94D400475675ED09088AEC0BEB
SHA-256:	7002D1561E7480AF083F267A29CBF471C7B4FBCFCCA05B5BAB1A8A5A44C028FE
SHA-512:	83054344CB72C003D9C9D0FBF92F1E6D7665B8AD4E6E3A4B4A39CB9851EBDD28510B7B6F8FB7882E1A23136DBE58AB91580A4F6570AF1756810FEDA3F0EC9C52
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...'....._keyhttps://www.microsoft.com/videoplayer/js/vxpiframe.js .https://microsoft.com/.-TEL'/.....k.....n..":.....T....q...x.C..>c.A..Eo.....4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a638cd841fb21f98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	301
Entropy (8bit):	5.761306536327967
Encrypted:	false
SSDEEP:	6:myrEYGLTDQyKfZ+OfojOW7kXWFRzhtHb8LXmEFDV5AF5jV1bK6t:XrsDQLf+5KWFhhZeXmCDzAFJN
MD5:	4FE96445084B484CC300C0B7DA65698E
SHA1:	AD6689A474A16E3372147BED26020EA96754EEB3
SHA-256:	0543799C50F9348F5F5302AF43E6F91ED724423C46CD3F249409C2BE11002D8D
SHA-512:	023394E277C1CC5F8738E386E16688168D2A772C662E069BF3D028FB74FBC07B969CFEA313A44E4CF799E840F693405220D0C08F35D4F8374208665D531C7A8A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Gz...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/MICROSOFT-365/_scrf/js/themes=default/f0-8efc89/f4-c426d8?ver=2.0&_cf=20210618 .https://microsoft.com/..EL'/.....L}.....)tk.."j..eI..b.....R..O.A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8edac07534ab3ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	60226
Entropy (8bit):	5.302303760311967
Encrypted:	false
SSDEEP:	1536:3OfIheFoceBkUq6L0z4KjPJXzzZImtNAzLwRwJpkP5xYi1rMQtcDtdsYqO9rD13m:c
MD5:	1F65BFB29174EA0A8C85E49611A4AA7C
SHA1:	82474A7A7F83AC232B75EFCC15317FAAA914AD8F
SHA-256:	6B9A6C870CF1240E64053DD9D96CD4E7C1594A9F11DEA2E4B7CD19679E2CC7DE
SHA-512:	15A9E2507FFA20B6E0A1E2EA7B51F38205B6E4682AAEF905BD7EF01AFB957F5444F2FFBCB08022278B025E76042F95354794F8F1AD95115CBC4F5E071BE8AF30
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8edac07534ab3ec_0	
Preview:	0\r..m.....b....f....._keyhttps://mem.gfx.ms/scripts/me/MeControl/10.21162.3/de-DE/meCore.min.js .https://microsoft.com/<l#EL'/.....,_.....K..,_.....M.k.M.[.:.\z...H.. .A..Eo.....8.....A..Eo.....'.....O.....l.....(S.H..`L.....L`.....Q.`.(G7....MeControlDefine...Qc.p.....meCore.....`.....M`.....Qc.v .....exports..$Qg.....@mecontrol/web-inline.... Qf^.UO....@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\aff8b63bdc36cb2b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17753
Entropy (8bit):	5.631005570100666
Encrypted:	false
SSDEEP:	384:WvLs7K0q6xnjvyluT4FGGVhliP7obhsa73IW2:QI+AryluTIGG7liYL7W
MD5:	7114EEB2E98D39D4277147C3063C481A
SHA1:	C17911AFD6AFE187D1477A523CB7CBE72A0EDFF6
SHA-256:	5BE74423D75366F26A0D0BED4CA7DEA52603966DD5239CFD93D02C75340618EC
SHA-512:	EEB26AD0DBEA6011F676B12F25590B76EB520F1379A1BCD6BCB089F34A7B6C86EE8E141B2248B1D393294CC1FAD0E45AB4066B123B429F72179C83550C6FDD B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....e.r...._keyhttps://logincdn.msauth.net/16.000/content/js/MeControl_EgJbqJOU_WgTDwJ3YZdEcg2.js .https://live.com/3..CL'/.....8`.....^..>.Q..E.3.\ &.8....>/@]!"J~a1.A..Eo.....R&J.....A..Eo.....'.nC....O.....C....?.....(S....`.....L`.....L`F....(S.<.`2....L`....I..K`....Di..... .....%.....g.....g.....g.....(Rc.....Qb287...._iz.`....Da....h.....b.....B...@.-....`P.q.....R...https://logincdn.msauth.net/16.000/content/js/MeControl_EgJbqJOU_WgTD wJ3YZdEcg2.js..a.....D`....D` ...D`.....)....`....&...&..A,&.(S.....Ia@...X.....Qb....._Du.E..A/d.....&.(S...Iac.....Qb..D....._G..E.d.....&.(S...Ia.....Qb v....._BD.E.d.....&.(S...Ia.....QbRmz...._F..E.d.....&.(S...Ia.....Qb....._BE.E.d.....&...(S...Ia ...8.....Qd.....strOrDefaultE.d.....&. (S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b180e6523891105c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.823346113762013
Encrypted:	false
SSDEEP:	6:mc/gEYyK08f2yDyr1MnloUeR3vY934nbK6tDdrYcgK9uG5EoaR3vY934Fe:/vKjf2yDyOloUO3vMONxNYXK9CD3vM8
MD5:	3C0E5F86BF88C7705105DC3449DEEBC3
SHA1:	BFC54DF94FFABC5D6A0F50353E72E182FFB8BF19
SHA-256:	1EF7D939B645F682BCC3649B4D08ED5F2D60CA5E32C113487909EEE3254617BF
SHA-512:	7C3BEF9710AE139397BAF82CAA0CAE706C7849A8A8D92A24F8EB3A709547DBAD9E59129C3E8AEC6FC456A1B1BD7C89719900EB6B6AC6E969C766EE797E43F7 C7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....2...._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.9.1.min.js .https://microsoft.com/.y.CL'/.....~."1...W.9.w.....C.oe.7.GS^.%7..A..Eo..... ...1.....A..Eo.....y.CL'/.....89F4C4BE8A7DC01F9E6EA91AF77080A791A329C1478A405297D8EE75C29B0170~."1...W.9.w.....C.oe.7.GS^.%7..A..Eo.....L .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b20b274cdd4d9114_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	498
Entropy (8bit):	5.49129790680526
Encrypted:	false
SSDEEP:	12:9L59TD9z7xDOZcwBl7TL59TD9z7xDM/s0jw3q:N5pxz7xWcwBl7f5pxz7xis0jw6
MD5:	77628F4B90868A34641131675F5E403B
SHA1:	4E9E200A3CEDC7D5963682DD0D23326B8932A1CF
SHA-256:	6426524917C92C54A270413A95184CB3C8CE1D7CDA362B6FB5C381F1477394A7
SHA-512:	58EF6411942810A7BECCC69969E9B283D484D7075E6A815EC88321562F636805943AA7C5851FBB633B7C5C592799F35ED569A8D4F08E91DB911BE1B1C0D813A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....'M....._keyhttps://support.microsoft.com/SocScripts/floodgateintl/en/officebrowserfeedbackstrings.js .https://microsoft.com/..CL'/.....~W....!V.O ..M....teI....~...A..Eo.....3.....A..Eo.....0\r..m.....u....'M....._keyhttps://support.microsoft.com/SocScripts/floodgateintl/en/officebrowserfeedbackstrings.js .https: //microsoft.com/..ZEL'/.....l.....~W....!V.O..M....teI....~...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b595a7abbf56db39_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19486
Entropy (8bit):	6.010191980259637
Encrypted:	false
SSDEEP:	384:60Gt0Fk2+6H1cwJv2uK4By4j24pkV+8qKvaQ:1PhHdpkQKt
MD5:	AC7D909434F0C5FF70B4C6B2CDEA454E
SHA1:	0429FF20DFBC47049D10205D73CBDCF54EAE40B8
SHA-256:	8A54106B42EEC66C145C2AB5D482BED9DBB40A9B0B6D86C4A451DEE85DF869E8
SHA-512:	16771C0F0086542FFD84E0CC288790D13BE7A05E6C9EB70578813835D626B61364AC6E339FEF524D0E9D81B28313645D13DF24713A1DE71737417BEB782E57FB
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-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-c07ea1/1e-2692a3/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/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210618&iife=1 .https://microsoft.com/,'.CL'/.....1.b.....t.....$....;...\a1.A..Eo.....&.....A..Eo.....'.....O.....H...&.....4.....(S.0..`.....L`.....(S....`.....L`.....LRc".....Qd.....requirejs.....Qc~qsl....require...Q.@.@.....define....Q.P."OF....__extends...d.....I`....Da.....'...(S...`.....L`>.....Rcf.....*.....Qb..z_....n.....Qb"]*.....r.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bba728cf7d8d85ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97968
Entropy (8bit):	5.835514848354048
Encrypted:	false
SSDEEP:	1536:ZVWFklkt8o2Sq+toi+UhmonhTI4LuaPgaDFT/vua/6/l1wpRVamP:S+I/jKODrs6P
MD5:	8D17A796D87662D12B8B6892FAE48999
SHA1:	26D34D282220B199FE8BE23CFEEB586F58AD7732
SHA-256:	2BA27753927DF6B180E71A3EE9049BA3A731370F0C29AD0A34D0E8FCB4C82BDF
SHA-512:	29F6E11A7DF4758926895C8206DA24AC1B751DC98E21DFA0EAEF8872DE308CAC0FC61BF4635F4EC6B5D82BA493AD1BAC976EC684C0F69131A900D2094E9455D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....14FB2B8F223A99AC18DA90444CCBB39829A6DAD9D432803A68A8A2C0B4A5BF8C.....'..]....O!...X}..f"n.....`&.....`.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb...|....t...`....I`....Da....l.....Q.@.....module....Q.@.(.....exports...Qc.v.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa....0...l.....@.-.....P.1.....https://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/dfa0b592/coreui.statics/externalscripts/jquery/jquery-3.5.1.min.jsa.....D`....D`p...D`.....`....&...&..!.&....&.(S...a&..`|L.....L`.....Rcd.....*.....Qb...p....C.....QbV.....r.....Qbr,T.....s.....R.....S...Qb...|....n.....Qb.J.....o.....QbF.....v.....M...Qb..Oe....l.....Qb...V....y.....Qb.....m....Qb.f.@....x.....QbB.....E.....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d2f1203102966a36_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.577666319015415
Encrypted:	false
SSDEEP:	12:MqDQLf+5KWFhhBoKRtCOX797DjNC1Ngw9jMuweP1DCDc45op:jj5FhHhtCOXB7DRCrMuFNDCP5op
MD5:	B5F7D1B1F1069C8982BC1B5423F3DCE6
SHA1:	92A3D19B1B9FCF85F66E3ED657ED7116E544096F
SHA-256:	CBB55E57DC11FE821B61F92DBFCFA97209A8FCF13058C6C3BD17B9D523C2AD87
SHA-512:	42CC0C986160C46C243FF209A145B907A6A4D2BD20CC80845F665FF71C90EA741D772BF85489B87086663D639F4B5F3C076A87B77740F39C62359ABD33D85C8F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}7...._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-c07ea1/1e-2692a3/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/6a-234a32/91-97a04f/1f-100dea/33-abe4df/17-f90ef1/e3-082b89?ver=2.0&_cf=20210618 .https://microsoft.com/c?.EL'/.....@}.....y...x.N...B...6.....C.....yR..A..Eo.....V.>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da5d5e3543c44acc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.94334517569374

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da5d5e3543c44acc_0	
Encrypted:	false
SSDEEP:	6:m4RgEYGLTDQyKfZ+ONNK6iXfRWmO2xD02FEpnK6tbVhjL/gXXWkRs4HEon:nfDQL+v4mOOD00kpd3H/gDRsCjn
MD5:	E432AD8A9A2023A8DC61F728BE52725B
SHA1:	4AA09305EEFAB04C03BD0420B097CFDD26D5F419
SHA-256:	ED2C53A4B4C264D2C2AAEFF5165666F847B25EAE861873DA7F9822CCECD85EE0
SHA-512:	855F384BA8DED1BE7CD316FB208B4DA786489A248C6C81737FDF14FD38BFB207FB47124CC02ACA4EA724198B87BE629786568A94DD977D2BB42DBEEE52C0614
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/_h/dfa0b592/coreui.statics/externalscripts/jquery/jquery-3.5.1.min.js .https://microsoft.com/...EL'/.....w].....K.....w.3...8.@CVi...P.$!..A..Eo.....M}.....A..Eo.....EL'/..~..14FB2B8F223A99AC18DA90444CCBB39829A6DAD9D432803A68A8A2C0B4A5BF8CK.....w.3...8.@CVi...P.$!..A..Eo.....FtL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dfb81c1b3493e456_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	276760
Entropy (8bit):	5.581083427111711
Encrypted:	false
SSDEEP:	3072:qAdg0Zor2zJI6qwLZB8bpdoFavyjE/cE3jTKBTwWkh1Tl5tANOU5NLVLUEJHwcoK:qAO6RNlB8duch1R5tAN7zLGc
MD5:	3224A9E2B44B461295C0D8D567FF7C72
SHA1:	2C5EFD57E6F3677898234720BB4DFAB8512CDE2B
SHA-256:	66DFAA266392DA3A3576F7D169B269B7FCB67C1E2C3CEF28621C81D087F2E53A
SHA-512:	625514EB5FE762D01CB1EF938BAD6F3E0EFCC0F03DBED2F1690C78F954101A536DC1767DCF96F784672B256DC81B2895AF822AEE3EDF8E2AB462C5FC30B6506
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...b..^....2E9ED0901FC97404F264F835FD84A666BC46159DA8C5838EE0E347DA5569742B.....'.tT....OP....7....r.....\....%.....(.....4.....H...,.....H.....d.....|.....L...L.....$.....$..`..,... ..|.....|.....$.....p.....p.....P.....(.....$.....|...8...|.....(S.`..`|....$L`.....L`.....Qd.....WcpConsent...(S...`.....LL`"....@Rc.....Qb.....e.....M....S.b$.....I`.....a....F....(S...`.....L`.....Q.@"s9.....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\e3e88e3254f8115d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99888
Entropy (8bit):	5.792396753196211
Encrypted:	false
SSDEEP:	1536:JDfQ6iuHRall1ccOrkkFDBxnSGfsruEWS9GJuPX1RcUCZ:JrXiRQDnSesru5lGende
MD5:	EC1379D64A257372D2B5E87C003EEB3C
SHA1:	41A8D1D8ECB7DABF08301CF4AEAC6E26AFB61585
SHA-256:	814DCBDDA3F11E71BD9C2620487C13D55E8EF6B305821D4767E200B7C561E560
SHA-512:	9C5BE5952AB86E74AABEE69D3C5A32165F17B5E7B97BD4E4C5A1530C7922F0061C37F110BE3FBBBAE86502FD60E30EBD48E3E2BC2DD915C7D9716DCCCCA2CED6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...^.....89F4C4BE8A7DC01F9E6EA91AF77080A791A329C1478A405297D8EE75C29B0170.....'..i....O#.....K.L.....$.....X.....(S.4..`$.....L`.....(S....$.`.H.....L`.....Rc.....<.....Qb...|....t.....Qb.1.....e.....Qb...|....n.....QbV.....r.....S...Qb.J.....o.....Qbr,T.....s.....R....Qb..Oe....l.....Qb.....c.....Qb.....f.....Qbn.....d.....Qb.M.....h.....Qb.....m.....Qb...V....y.....QbF.....v.....O...Qb.iIB....w.....Qb.....T.....QbF.1.....N.....Qb...p....C.....Qbj.....k.....QbB.....E.....Qb.....S.....Qb..p.....A.....Qb.....j.....Qb.PY5....D.....Qb...s....L.....Qb...[....H.....Qb.....q.....Qb2.'M....M.....Qb....._....Qb.....F.....Qb.....O.....QbB..k....B.....Qbz6H.....P.....Qb.\?;....R.....Qb~0T.....W.....Qb.Y.9....I.....Qb.....z.....QbJ.:.....X.....QbB.9.....U.....Qbv.SP....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4b9b26cef092fbf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.595207958152845
Encrypted:	false
SSDEEP:	6:mcGRXYL8UdD2Di9RLtA96dGfGh9R4hK6t:6RibD2DyA96dGIi7
MD5:	13CDDC0015387D24289EDBA7CE6965FD
SHA1:	A6D3E20BB0AE11F0CE5959A3148345C346988A66
SHA-256:	D0C4139B8272ABDC778EC47FC436097CC97A9F0401C2F5A573D9C82E7EEF0B1F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4b9b26cef092fbf_0	
SHA-512:	88594D83323124294AEE2647AE827A5C52E2D8CF0F3877BC46BCFC0602FEFAA48D9CFA3CDF84CCCF367ACA6E191DFECD11FEE0751306108E5CCABB1948949 18
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://mem.gfx.ms/meversion?partner=MSHomePage&market=de-ch&uhf=1 .https://microsoft.com/...EL'/.....].....t..-...}~I.1..?D.=.#.& .6d..A..Eo.....G.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e562ecd571f64bac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	105600
Entropy (8bit):	5.797487652057799
Encrypted:	false
SSDEEP:	1536:vbuFH9mJH8NsI30zyzOEE32MX8uQe3J5Y9jMQaI/sCtAk/:vb4HUJE0zKFC8HSJ5Y9jMQppp
MD5:	DFB8DE28E24EAAF96468AC0826ABDF23
SHA1:	D47FF4203B2EE60554ADCA8521D7B11816C367A6
SHA-256:	BE171FD3BDA1AE1095E9A1EB1E4F0EAF6A5CE0A8C1FB8F9C5D69928447503E9B
SHA-512:	89BD5B5C79DBABE89527BAF9CFB1133CDBE3941025D0C9910B3BF14473A03642EF6783AB178AD35FD0C77EDD844AB927AA4D019CF04C5BB83E82F9EC485B0 65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....7"....7E5A7CAA6407BEE12B42C3061FA215EC55DFE50350CF46AE46C7C6BBEA1F9927.....'..{....O$... ....b.....4'.....x.....d..... .....D.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....,.....Q.@.i.....module....Qc.....exports...Qc .g.R....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....HP.....;...https://ajax.aspnetcdn.com/ajax/jQuery/jquery- 1.12.4.min.js.a.....D`....D`....D`.....`....&...&..!.&....&.(S...5'..`"N.....L`P.....Q.Rc.....J.....M...Qb.....c.....QbB.gd....d.....Qb.W.-....e.....Qb.).....f.....Qb.....h.....S ...Qb.....j.....Qb.r.....k.....Qb.R.+....l.....Qb.....n.....Qb.=.....o.....QbN.g.....p.....Qb.....q.....Qb.y.....r.....Qb...E....s.....R....Qb...c....v.....Qb.M.(....w.....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e76eeaeb7f6700e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.7775841206247955
Encrypted:	false
SSDEEP:	12:Qkq9TDPdxDrUQDJjT9Skq9TDPdxDrUQDehTe1:xqphxHltjT9XqphxHlqhTe1
MD5:	969028689B82CBE914FE3A154DB68621
SHA1:	335834BFC5AECA9F0FD7046BFB96BB0CF284C9A8
SHA-256:	CDB69E9D8CA5357FA89F722302377EB94D2F28200B4BEFE941F48FB71BACE8FA
SHA-512:	093829BE7F32B591D879DF546A6420C4C241D1744E3DFC8A860897FB61DCCC895410308EC2C018BC901D5E8AE0EFDD5023BD22936E40FB2F2DA96D957728915
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://support.microsoft.com/socbundles/autoSuggest?v=TrjWgBpbqSVnsY8NWPkXzoT_DDPbXdmWeLTXcH2lyLw1 .https://microsoft.com /.A.CL'/.....h?gB1.....LD.5Q9u..|C.C.K.....A..Eo.....Y.....A..Eo.....0\r..m.....o....._keyhttps://support.microsoft.com/socbundles/autoSuggest?v=T rjWgBpbqSVnsY8NWPkXzoT_DDPbXdmWeLTXcH2lyLw1 .https://microsoft.com/S.OEL'/.....k.....h?gB1.....LD.5Q9u..|C.C.K.....A..Eo.....}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\edce433eec3e6459_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48744
Entropy (8bit):	5.4545184681160235
Encrypted:	false
SSDEEP:	768:+Jk1nuijFDLe3DTImrvZ7XuL3wN+uItUEDOJiXsWklAZToNgwjlgpM:+JinuijF+vnuL3wN+RUEDOSuw0gwsz
MD5:	9475E480BCDF6F6DD07EA633DE617666
SHA1:	DD0242E6EF0647BCBB15D960F9C88EEB9F7C10D6
SHA-256:	70954522712D9EC1026BCF6B800F1E07437070A0B29F760581585D385F3710B6
SHA-512:	786D3A9D52FC5F4A73F55BADE39B4CC27B07F50D9F11EB5AAA939B7A2A709DB8A2B261B0048041D7AAC8F0D3CE664F9E9E705A0E714C431830095342E850B82 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\edce433eec3e6459_0	
Preview:	0\r..m.....x...j....._keyhttps://static2.sharepointonline.com/files/fabric/office-ui-fabric-js/1.2.0/js/fabric.min.js .https://office365.com/.k.CL'/.....'.w.}.g.WT.8.UL.6u 8g....!..O....A..Eo.....A.....A..Eo.....'.....O.....\.....(S....`.....L`T.....L`H.....Qc.....fabric.....Qd. ..&....STATE_HIDDEN. QfZ.:F....CLOSE_BUTTON_CLASS... Qf.....MODIFIER_OOBE_CLASS.....(S.@.`8.....L`.....0Rc.....Qb.....t...`....I`....Da& ...z+...(S.u..`.....L`n....4Rc.....Qb.@X....e...`....I`....DaT...\+....a..(S.....Ia7...;.....1!..a .@.-....hP.....\...https://static2.sharepointonline.com/files/fabric/office-ui-fabric-js/1.2.0/js/fabric.min.jsa.....D`....D`....D`.....1....`....&...&..q.&..a.&..q!&.(S.....Pd.....e.transitionaW.....I...Q"d.....&.(S.....Pd.....e.animation.a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f990a944bf0059f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.740993826220238
Encrypted:	false
SSDEEP:	12:M9TDPW1me3r0DulTY5pNS9TDPW1me3r0DDrMY5y:MpCB3r0ilTSNSpCB3r03rMb
MD5:	8CF6155DD2A3FD93F3AA954DAAC1B595
SHA1:	18221DDE5291CFE8EB889F3227E6DB5A6A98060E
SHA-256:	F54969B02787F327FF38719AFC0A30BEF95B523EC717B495A6934D1604D2FEA2
SHA-512:	CCC91A312BAC549275DA3DBB10E4DFCF166AEF77594E4605B03B4E681647E6AC5FA25457F99A2E015154BFF8061E36ACD2EBC8C9B3DB4BEE9921F9C841BF9E 30
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...N....._keyhttps://support.microsoft.com/socbundles/support?v=KZSfmSdvXd7lUlIcsr_04VzCt_Wr1cbAIRvbHspPcY01 .https://microsoft.com/.>.CL'/..... ....."....ZI...N....Ar....-.3..q.A..Eo.....}.....A..Eo.....0\r..m.....{...N....._keyhttps://support.microsoft.com/socbundles/support?v=KZSfmSdvXd7lUlIcsr_04 VzCt_Wr1cbAIRvbHspPcY01 .https://microsoft.com/dYNEL'/.....gk....."....ZI...N....Ar....-.3..q.A..Eo.....I.,.....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):	32768
Entropy (8bit):	3.5444559243367015
Encrypted:	false
SSDEEP:	192:du1C+R3SLvLrzT2XNkjMIfcRu3pfcT67qdC+R3SLvLrzT2XNkHMlW0EbnpXmvXGP:QZSjE0/xv78ZSjglvEbRmvXGP
MD5:	2532E50729F858A992294DA637630B04
SHA1:	4932953C50FEC8765F02054E2A9F95D1AB512628
SHA-256:	3FDDA20285B67882E6697C15C24737A3CC333197E24D26095AD5B8A24C093EE1
SHA-512:	A1039C44A322365FA8E8EF96034494F5B285075DC65A1E0AB48277C0BE343B27242B5D36D25888CAE8860AA8ECDD8B0AF2E567DF4A0EED0CEEB648B70F583D E
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):	2.1351012224959702
Encrypted:	false
SSDEEP:	96:mOpcNwTfcYp4CAzR+IAOuXoCvNhr0eWamE2XNVSjMyw6MNw8:mOpcuTfc9C+R3SLvLrzT2XNkjMaMu8
MD5:	09059E3DB327617AB6DFA7A1D09FFB70
SHA1:	8471B66B73BAAEF68C8281B5766A239E880CA674
SHA-256:	855D144A00392992FB7BF0B7F85F2ACF67D9725556AF3CCE27DFE082708E8552
SHA-512:	684322EF568821FCBAFD8DD7D259507B6173D3B66192DB9EBBE9F3F603D2BBB5B4DDF6EB358BF4BAF9A0753143F5BC41E6339162473F102B4A005F5611A0F61I
Malicious:	false
Reputation:	low
Preview:	.....0..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
File Type:	data
Category:	dropped
Size (bytes):	28735
Entropy (8bit):	3.767520591233567
Encrypted:	false
SSDEEP:	192:3F4TUlC9SEX1YOknV+GbBINgRWC7hsJzhsJhZ0RMnG8iWcvEL7PiaKiq:V4RBlYOknVTyLuhCzhChORMRqELVs
MD5:	F8950F9C1B884AAA1AF3F1CF00FF9344
SHA1:	0D2607E2A7221F9F91032A88BDCBB76F293472B1
SHA-256:	54D78A5B8650ED548464104FB8D7F47FF69221D8A243544ABA838132DC9ABCC4
SHA-512:	A86AC7102294ED042954D67C6735A45A853F60545859B807C4BA297EBA950CFC8C21F50F626D5204D0501F3862026CC417EE0347A693B442F4D2ABAACFF86A62
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...cb7452ab_05ba_4ce0_998a_f0a837e37018.....s7..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....5..0.....9...https://outlook.office365 .com/Encryption/authenticationpage.aspx?st=Microsoft&ru=https%3a%2f%2foutlook.office365.com%2fEncryption%2fdefault.aspx%3fitemID%3dE4E_M_91d82880-d398- 4e45-87e4-14d1f09b1851&e4e_sdata=BQ63pl%2fl1rHfMPpKaFXJB%2bg41DuU303zEwz9JyHBDz8kAqUWdGSJZmCHBjCyH2zT1S4bUXAM0DT5whGxxzJ9KJVLM45Y jveJfNbM5S8IIE0H5ikwwsjEd3KY4MQMvvkn99VMvHtfK9iK7OeXK26%2fFcjFjupnrekHme8FxoehlCVjn8iK3raspWGzoDJHCaqPznQhiMULGg32PYvyjftskicaNDdn I4zk8NYzRhV45ubepJ%2fpCIzSJZ9Pj7zrxZQIAHdndn0gCZ%2fMxPucpLQwKwr5PsFXqPMnPy46o4V%2f5Dnl7JdkbGEHSeN9fzGSxAR3BFlHrZh4ahh0uV2IkOZHpQ%3 d%3d.....

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
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
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):	314
Entropy (8bit):	5.21656717817845
Encrypted:	false
SSDEEP:	6:mAHl4q2PWXp+N23iKKdK8aPrqIFUtpJHtZmwPJHE5vAIkwOWXp+N23iKKdK8amLJ:ZF4va5KkL3FUtpJN/PJk575f5KkQJ
MD5:	2599EBB79AF3117619B10EC144E14532
SHA1:	634B6EBCD9241934BC008E2D9F3E2766F9CABDC1
SHA-256:	0342AC4973E068BF84F0EA0CC1E182877895015068EF0209103A4AD18B47C60F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG

SHA-512:	6D5FE45ABEF345D47A51B919E7B584E4999053A00EBE96DDD52484F43E5D0A141B3070942BECAF688D45630D667AC35EA64433B73FE956EA348FEFDE38EF99A F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.349 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:32:56.350 f0 Recovering log #3.2021/08/03-23:32:56.351 f0 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 Rules\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	314
Entropy (8bit):	5.21656717817845
Encrypted:	false
SSDEEP:	6:mAHl4q2PWXp+N23iKKdK8aPrqIFUtpJHtZmwPJHE5vAIkwOWXp+N23iKKdK8amLJ:ZF4va5KkL3FUtpJN/PJk575f5KkQJ
MD5:	2599EBB79AF3117619B10EC144E14532
SHA1:	634B6EBCD9241934BC008E2D9F3E2766F9CABDC1
SHA-256:	0342AC4973E068BF84F0EA0CC1E182877895015068EF0209103A4AD18B47C60F
SHA-512:	6D5FE45ABEF345D47A51B919E7B584E4999053A00EBE96DDD52484F43E5D0A141B3070942BECAF688D45630D667AC35EA64433B73FE956EA348FEFDE38EF99A F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.349 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:32:56.350 f0 Recovering log #3.2021/08/03-23:32:56.351 f0 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....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):	314
Entropy (8bit):	5.241903514569077
Encrypted:	false
SSDEEP:	6:mAevIq2PWXp+N23iKKdK8NIFUtpJ1SgZmwPJOXkwOWXp+N23iKKdK8+eLJ:ZeIva5KkpFUtpJ1X/PJOX5f5KkqJ
MD5:	2D96681EABD354AB555D8BB8044C5ACB
SHA1:	ECA30ED0030F8105A239BF78B39698DFFBE7591C
SHA-256:	D7EDD713A7562B4AEBD1B35FAA0AD4989CC18D664D4A805B8D16E4F68941CA72
SHA-512:	AFDC538DF93A18CA084C359893CE240CA6051DFAE41BB12EBC0548C0592B9AA44C33F451A059854AE39FC515C2BDBB656A9DC17CB0EA57BAE311AA898CAE8 C0E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:59.459 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23:32:59.461 f0 Recovering log #3.2021/08/03-23:32:59.462 f0 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\Extension State\LOG.old. (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	314
Entropy (8bit):	5.241903514569077
Encrypted:	false
SSDEEP:	6:mAevIq2PWXp+N23iKKdK8NIFUtpJ1SgZmwPJOXkwOWXp+N23iKKdK8+eLJ:ZeIva5KkpFUtpJ1X/PJOX5f5KkqJ
MD5:	2D96681EABD354AB555D8BB8044C5ACB
SHA1:	ECA30ED0030F8105A239BF78B39698DFFBE7591C
SHA-256:	D7EDD713A7562B4AEBD1B35FAA0AD4989CC18D664D4A805B8D16E4F68941CA72
SHA-512:	AFDC538DF93A18CA084C359893CE240CA6051DFAE41BB12EBC0548C0592B9AA44C33F451A059854AE39FC515C2BDBB656A9DC17CB0EA57BAE311AA898CAE8C0E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:59.459 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23:32:59.461 f0 Recovering log #3.2021/08/03-23:32:59.462 f0 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=","3mBGNAiRlTANEQkqzU3TEi+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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Category:	dropped
Size (bytes):	67584
Entropy (8bit):	3.4103874232832463
Encrypted:	false
SSDEEP:	768:+uVM0RDCrK6V0PxRDC9fuVM7Tf39xRDCwg:+udYZ4+fuqz3vM
MD5:	BD04338F59C9A7C48E6456AF8072CFBC
SHA1:	117E3284037AC1F1EBB19C9DB27784637B97EA8C
SHA-256:	9AE6E200128B0AA106C8A74D7422A25316D62CC2098EF695DAC0210B6AAF1C34
SHA-512:	A4CDEA34E2977D89C368C85F92328396D487C793DAD387886FFC51F92F6C5F41F667A4A046F1D937592DEA301EF349BB1B84F0DD239F398A87049A46FD20C75A
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):	57608
Entropy (8bit):	2.624541859670829
Encrypted:	false
SSDEEP:	384:f9YMYOknVTIocRDG7EjLEYhZxRDG7JuA4LEY6d:1NuVMjRDCZexRDCFX
MD5:	026C3269C475E4D753A23863B5D55B89
SHA1:	FA5F25768C902CE6E6636D6D3BFC3F01FD2AE615
SHA-256:	BFA38CFD739A7F22E69A6CD1AECC461296B0D0B4DDF41EF2E2EF09FE82EB43EB
SHA-512:	F1EC75F5F7B5E5B358E2F0B59763A3019102C5F9A9F3DF8C4D0FDBB0531850B5BA2574EFF29E9E0D6855982BEA1327891EB3A0CCB63A14380C285F8EF021DBFC
Malicious:	false
Reputation:	low
Preview:	.....~T..... ....

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):	372
Entropy (8bit):	5.239138318349408
Encrypted:	false
SSDEEP:	6:mgQ+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp7luAZmwP7jUdFNVkwOWXp+N23iKKN:LVva5KkTXfchI3FUtp7p/P7jUdF5f5KN
MD5:	58F762A3975853A688E5C6CE3337A0C5
SHA1:	F5258F1C77C79DD744DF77C3BE26CE20DA2CF945
SHA-256:	6E482E122F8AB3A6F81ADDB693BAF96DB33CF90C34AFC3924044223CB9D22668
SHA-512:	FEF95F45734A5A7E67E3C2F563D38F98335E103777408A52B8963F2E45FF9B8FE4F58E31926636D395053160C013670E402B0C865392C8745B9CD457CE26609E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.340 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:33:22.343 15d8 Recovering log #3.2021/08/03-23:33:22.344 15d8 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\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.239138318349408
Encrypted:	false
SSDEEP:	6:mgQ+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp7luAZmwP7jUdFNVkwOWXp+N23iKKN:LVva5KkTXfchI3FUtp7p/P7jUdF5f5KN
MD5:	58F762A3975853A688E5C6CE3337A0C5
SHA1:	F5258F1C77C79DD744DF77C3BE26CE20DA2CF945
SHA-256:	6E482E122F8AB3A6F81ADDB693BAF96DB33CF90C34AFC3924044223CB9D22668
SHA-512:	FEF95F45734A5A7E67E3C2F563D38F98335E103777408A52B8963F2E45FF9B8FE4F58E31926636D395053160C013670E402B0C865392C8745B9CD457CE26609E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.340 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:33:22.343 15d8 Recovering log #3.2021/08/03-23:33:22.344 15d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.1633186495551815
Encrypted:	false
SSDEEP:	6:mgG3+q2PWXp+N23iKKdK25+XuoIFUtp7HrXZmwP74VkwOWXp+N23iKKdK25+Xuxo:LGOva5KkTXYFUtp7b/P7w5f5KkTXHJ
MD5:	259A6E7B2D3EC1CE600B905CB1A1C487
SHA1:	073216BDAB4C382EEB7247730E09B6093E644808
SHA-256:	D85391F3ED9373AEAC7170139CF96B94A905971631C8C29DE61EE5C95082567D
SHA-512:	18572763FAFECDCBE5D87782F00B48315B8718888B0544B73B395ACE7024CC037367A37A482E0005922F5714C9152A8D5CA7EBEC7E20A26ABEC9D2E0949C2E6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.328 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:33:22.330 15d8 Recovering log #3.2021/08/03-23:33:22.331 15d8 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.1633186495551815
Encrypted:	false
SSDEEP:	6:mgG3+q2PWXp+N23iKKdK25+XuoIFUtp7HrXZmwP74VkwOWXp+N23iKKdK25+Xuxo:LGOva5KkTXYFUtp7b/P7w5f5KkTXHJ
MD5:	259A6E7B2D3EC1CE600B905CB1A1C487
SHA1:	073216BDAB4C382EEB7247730E09B6093E644808
SHA-256:	D85391F3ED9373AEAC7170139CF96B94A905971631C8C29DE61EE5C95082567D
SHA-512:	18572763FAFECDCBE5D87782F00B48315B8718888B0544B73B395ACE7024CC037367A37A482E0005922F5714C9152A8D5CA7EBEC7E20A26ABEC9D2E0949C2E6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.328 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:33:22.330 15d8 Recovering log #3.2021/08/03-23:33:22.331 15d8 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Size (bytes):	330
Entropy (8bit):	5.200681554745712
Encrypted:	false
SSDEEP:	6:mgXj+q2PWXp+N23iKKdKWT5g1IdqIFUtp7cfZZmwP7wVkwOWXp+N23iKKdKWT5gZ:LX6va5Kkg5gSRFUtp7cR/P7o5f5Kkg5i
MD5:	2803AC502346EF9B994C28B22D76B412
SHA1:	0E1562737FD7C25DC6F1EAA748958585372829C8
SHA-256:	82282950BA0BD7804E2117AF77057127EE794CE81EAB4998CCB69BA6889E0553
SHA-512:	A2FA36900ADF7676A671C90FB91BC4589288A77D12B1D8EECAA288842E7BAAF7700A554237EB600D00D25AA66F36CA2E34E3A45A2813CFF6DFD89685DECF7D8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.305 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:33:22.306 15d8 Recovering log #3.2021/08/03-23:33:22.313 15d8 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\GCM Store\Encryption\LOG.old.d (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.200681554745712
Encrypted:	false
SSDEEP:	6:mgXj+q2PWXp+N23iKKdKWT5g1IdqIFUtp7cfZZmwP7wVkwOWXp+N23iKKdKWT5gZ:LX6va5Kkg5gSRFUtp7cR/P7o5f5Kkg5i
MD5:	2803AC502346EF9B994C28B22D76B412
SHA1:	0E1562737FD7C25DC6F1EAA748958585372829C8
SHA-256:	82282950BA0BD7804E2117AF77057127EE794CE81EAB4998CCB69BA6889E0553
SHA-512:	A2FA36900ADF7676A671C90FB91BC4589288A77D12B1D8EECAA288842E7BAAF7700A554237EB600D00D25AA66F36CA2E34E3A45A2813CFF6DFD89685DECF7D8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:33:22.305 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:33:22.306 15d8 Recovering log #3.2021/08/03-23:33:22.313 15d8 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):	131072
Entropy (8bit):	1.818632364112577
Encrypted:	false
SSDEEP:	384:2YOknVTaU2/YOknbTZYOknVTJ/N1G/YOkngYOknVT7/4JoG/YOknuyvMUGYOknVj:2uVuZ/ubduVFy/uguVH0/uDvRGuVU/uJ
MD5:	3A8A3C955CC9E51A8C20B54F76C33793
SHA1:	68766ACD8077C40E21E28ED56D14799E06DB4DCC
SHA-256:	2FEC1678291D2FE45413FDB2AD646670176CA5033E50D51D256034A0B9DD8E67
SHA-512:	20DB99ECE3EA0805DE592F9041508C6F52C5C1034543F46A0FADCE9A5E3BBF1F46B662A2A91BD16BA19D58758878A393DDB8E5B1E541194B190E508921F5049
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):	6915
Entropy (8bit):	6.385338504095548
Encrypted:	false
SSDEEP:	192:Uz0yuWWW6z53XVi0LksRthPci0kvF4vsVYOknV+G5+V:UXu5bNysvhPj0kdXVYOknVT5+V
MD5:	B8DEE78098569431C514A96B013BAB14
SHA1:	18315ED514BD782573D74BBDCD0AF42661D4425F
SHA-256:	47BE115F1045F77A0D8C88AC8D67DA1BC46914C75448C908E61767A7E464854B
SHA-512:	C3850AB41562568F5726E91AE5D090934211B0163905B2DDAC3F6E838EA0CF9C53393E3385E98DE3796FCA7C219F81F954ED00F68B019CE5C1FA827E05CBF1A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Malicious:	false
Reputation:	low
Preview:	....."...G..1..1abee47c."27pcmtalumoydxbzflm2asgeepgp3nqkpb..4166..4720..68475cb4c2d2..68ca..92fe...9pvt1xyxr0ag91ckvuz2luzwvyaw5nlm9ubwljcm9zb2z0lmnvbsxpvt1nawnyb3nvznqgrxhjagfuz2ugsg9zdgvkie9yz2fuaxphdglvbnmsrem9tkfnufiwmuewmtasrem9ufjprcxeqz1pvvrmt09llerdpunptw3u2z0rbcxkmutxcj88ckjdtj1db25mawd1cm..a776..aac869b0d201..af9b..ap..ashx..authentication..awgkaaaaaoyaaaadaqaaal..bn6pr0101mb2996.(bn6pr0101mb299654bc7612be90121c8e74bbf09..cfmrecipient..com..consumerencryption..d0e409a0..e4e..encrypted..encryption..exchangelabs..false..g..grainwater..gswater..https..message..messageid..n1kpgdgoctqd09.8nald4xf5g7xsjcpoxlsrqcfvjk6j2vhviiksh98po4juh8sqdhus2lu3..office365..onmicrosoft..outlook..prod..pwyr4eztbl9bc2pxl9..radianresearch..recipientemailaddress..retrieve.-s8heieuljtsqucw0zz9op7e6qtsm5hej40blifk1sdbdp..sdata..senderemailaddress..senderorganization..senderorgid..systemmailbox..urldecoded..watthoureng ineering..14d1f09b1851..4e45..87e4..91d82880..aspx..d398..default..itemid..m..5

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):	129320
Entropy (8bit):	1.3104119778146441
Encrypted:	false
SSDEEP:	384:HM/YOknkYOknVTafIG/YOkneYOknVTJ/F0G/YOknrYOknVT7/n8t:s/ukuVut/ueuVFH/uruVH6
MD5:	6895A5257905CA1AF132EB3D20A4024C
SHA1:	A4AEFBA066641BEC6AF4E96D252B67AE984B06FC
SHA-256:	F09BEC298247E30C8C691F86E4E02354E13BAA64CD31C0ECB60941926DDC6890
SHA-512:	63506221B10CA827951DABABE330F9D897E143CD24DE3B74772181B4FB05D10A725383F66422C974E68B7C8EA6B16BCEDD9FEAAFC8BA2379B00D5EC94FCB76E
Malicious:	false
Reputation:	low
Preview:	.....0c.O.....SQLite format 3.....@ .....C.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28735
Entropy (8bit):	3.767520591233567
Encrypted:	false
SSDEEP:	192:3F4TUlC9SEX1YOknV+GbBINgRWC7hsJzhsJhZ0RMnG8iWcvEL7PiaKiq:V4RBlYOknVTyLuhCzhChORMRqELVs
MD5:	F8950F9C1B884AAA1AF3F1CF00FF9344
SHA1:	0D2607E2A7221F9F91032A88BDCBB76F293472B1
SHA-256:	54D78A5B8650ED548464104FB8D7F47FF69221D8A243544ABA838132DC9ABCC4
SHA-512:	A86AC7102294ED042954D67C6735A45A853F60545859B807C4BA297EBA950CFC8C21F50F626D5204D0501F3862026CC417EE0347A693B442F4D2ABAACFF86A62
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1..,.....$...cb7452ab_05ba_4ce0_998a_f0a837e37018.....s7.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....5..0.....9...https://outlook.office365.com/Encryption/authenticationpage.aspx?st=Microsoft&ru=https%3a%2f%2foutlook.office365.com%2fEncryption%2fdefault.aspx%3fitemID%3dE4E_M_91d82880-d398-4e45-87e4-14d1f09b1851&e4e_sdata=BQ63pl%2fl1rHfMPpKaFXJB%2bg41DuU303zEwz9JyHBDz8kAqUWdGSJZmCHBjCyH2zT1S4bUXAM0DT5whGxxzJ9KJVLM45YjveJfNbM5S8IIE0H5ikwwsjEd3KY4MQMvvkn99VMvHtfK9iK7OeXK26%2fFcjFjupnrekHme8FxoehlCVjn8iK3raspWGzoDJHCaqPznQhiMULGg32PYvyjftskicaNDdnI4zk8NYzRhV45ubepJ%2fpClzSJZ9Pj7zrxZQIAHdndn0gCZ%2fMxPucpLQwKwr5PsFXqPMnPy46o4V%2f5Dnl7JdkbGEHSeN9fzGSxAR3BFlHrZh4ahh0uV2lkOZHpQ%3d%3d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabske (copy)	
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabske (copy)	
Preview:	SNSS....

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):	5076
Entropy (8bit):	5.569892696064634
Encrypted:	false
SSDEEP:	96:za7HMldbd4WIWabQ5fgGkrS062mV681bgWiUP2w4GtPAAp1PrdgzEFfnUoUI9ZsG:zyHidx4WIWaE5fgJ0A81bbiUj4Gh1DdX
MD5:	83531DAD8C23C13A7313DA3471BB0E30
SHA1:	308A072150EF951441CE8D9F41B84C3E12F4E26D
SHA-256:	D7914CB691D631B0E1ADBBD7F8867FBD52F93915BD7B9B143E18A7032332B419
SHA-512:	6C902D3C18EA85E02A6B34BED13DE36BF9B8775AEF27AA27BE0C09FBDEB026FA2F197DB170433DF4D19B2787DFFDF414B246D3998BF4395B6855A8FF23B9AC17
Malicious:	false
Reputation:	low
Preview:	..B...*.....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..939013000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 23:33:24.12][INFO][mr.Init] MR instance ID: d2b1c3d1-c867-4c4d-b3d4-1c418646496d\n","[2021-08-03 23:33:24.12][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 23:33:24.12][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 23:33:24.12][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 23:33:24.12][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 23:33:24.12][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 23:33:24.12][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):	329
Entropy (8bit):	5.152340169175218
Encrypted:	false
SSDEEP:	6:mAHCqq2PWXp+N23iKKdK8a2jMGIFUtpJH/ZmwPJHXzkwOWXp+N23iKKdK8a2jMmd:Ziqva5Kk8EFUtpJf/PJj5f5Kk8bJ
MD5:	E98FEA9F4047D2FD751402D7E975C7F8
SHA1:	75949A844E39FB4D1BBFCE08BC7D5216362FE7CE
SHA-256:	A582283A4B4FA4EB86D35FDBFBF6463AF496E45D80057F1A0E0516F921680CE5
SHA-512:	58F1026599A7D143CAC8E83B2C2399E6343CD77E79A36D43CC5124EA552B36B4F63D4061560A3A3D22611D4F908F945058F7F5B4D0F60086C5163B032F674A34
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.102 d20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:32:56.105 d20 Recovering log #3.2021/08/03-23:32:56.107 d20 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.152340169175218
Encrypted:	false
SSDEEP:	6:mAHCqq2PWXp+N23iKKdK8a2jMGIFUtpJH/ZmwPJHXzkwOWXp+N23iKKdK8a2jMmd:Ziqva5Kk8EFUtpJf/PJj5f5Kk8bJ
MD5:	E98FEA9F4047D2FD751402D7E975C7F8
SHA1:	75949A844E39FB4D1BBFCE08BC7D5216362FE7CE
SHA-256:	A582283A4B4FA4EB86D35FDBFBF6463AF496E45D80057F1A0E0516F921680CE5
SHA-512:	58F1026599A7D143CAC8E83B2C2399E6343CD77E79A36D43CC5124EA552B36B4F63D4061560A3A3D22611D4F908F945058F7F5B4D0F60086C5163B032F674A34
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.102 d20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:32:56.105 d20 Recovering log #3.2021/08/03-23:32:56.107 d20 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Size (bytes):	86016
Entropy (8bit):	1.3160104241206199
Encrypted:	false
SSDEEP:	192:Hf+tC+hadnT+waQmnT+S0omP1Ufsn7R1UfG:Hf+tC+hadT+waHT+SNmP1Tn11v
MD5:	6AA8B40105569FFE6805C806BA272864
SHA1:	C1EA4B64BFCAF0AAAD2FE66990BD7C81F84838E6
SHA-256:	3ED4B279841570783FDF873A8F6D2FA34A667D2EFF4D2C07D8DACD3D6E8BD880
SHA-512:	D9970150B0E268C3CBDAABA392278AC44149250DEBE5ED738A399A0ABE7A37B1248F9236D0CE373EFACFA1A679B32A1CAF892C0157B2AD37A196FFD1E584BD79
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):	89852
Entropy (8bit):	1.170357509458354
Encrypted:	false
SSDEEP:	96:eUUOqAuhjspnWODoRypUp0kOqAuhjspnWO/98wgOmRypUpS0OqAuhjspnWOqzGwP:Vyu+uiij+MS4nT+wCK/yxZiO1UfWLm8
MD5:	FF32C0C390A17EC6CFFA3BDA70975EDD
SHA1:	2038012DC39F339A09176ED1A6DC08C4D33AC302
SHA-256:	2E893726B02A6B7CF2C4842DE8FAF87FC22B97F6387F8BC3BC67D516C5030277
SHA-512:	860F6FDCB6E274429C8D90A8851E559C0F9B4AB75AD7AF91E7039B2288C2772C3CE8853D60CC048F96346FFCDE0960CB594782ABD8D356D08BB2B835BAFEE53
Malicious:	false
Reputation:	low
Preview:	.....p..$..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statea (copy)	
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):	3078
Entropy (8bit):	4.863074272112497
Encrypted:	false
SSDEEP:	96:JTnOCXGDHznd/X0R4TaZ67WGG6XYFFVi+neVxhH:JTnOCXGDHzdv0RuaZ67WGpXYF3TnQX
MD5:	E106F16FCB73B1FD2EE1013E24894F32
SHA1:	47AAF59E535CC79065B52091AE9247B6124DD9F9
SHA-256:	2C4EBC9BDDDEF07348F380D22010BEA5F1D315F6109DE0D2CA98D1CD68EC7EF0
SHA-512:	14E7BE899ED43087E3743CE520CDDCAA5F7203DF4268ECB640C221E94189D23CB61E013AB99EE8A45F11E95D2780EE53CE924C87B84172C470DDD85D2C0D0F3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275124380035951","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275124380038028","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statemp (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statemp (copy)	
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.203180542069283
Encrypted:	false
SSDEEP:	6:mAHRVOq2PWXp+N23iKKdKgXz4rRIFUtpJH+xAgZmwPJHLzkwOWXp+N23iKKdKgXS:ZxVOva5KkgXiuFUtpJE/PJrz5f5KkgXS
MD5:	237EBC037EA4C40F5D2958B4B1CC333C
SHA1:	094D4AF24FD72B4E2CC06A73A13704180002F51A
SHA-256:	7439EB66E30D2AF621B1720AF78996B61A35219862BFBF00277916B18D46D162
SHA-512:	3EB09C1FEBFCAE201499C643C40D2495B88012F27251AE8907EA7CF067DE3AB26851BDA964C8C333731FEBCB3F8FEA8CDF0954653550D9388AE61B3AD483762 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.370 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:32:56.371 f0 Recovering log #3.2021/08/03-23:32:56.372 f0 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\Platform Notifications\LOG.old.7 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.203180542069283
Encrypted:	false
SSDEEP:	6:mAHRVOq2PWXp+N23iKKdKgXz4rRIFUtpJH+xAgZmwPJHLzkwOWXp+N23iKKdKgXS:ZxVOva5KkgXiuFUtpJE/PJrz5f5KkgXS
MD5:	237EBC037EA4C40F5D2958B4B1CC333C
SHA1:	094D4AF24FD72B4E2CC06A73A13704180002F51A
SHA-256:	7439EB66E30D2AF621B1720AF78996B61A35219862BFBF00277916B18D46D162
SHA-512:	3EB09C1FEBFCAE201499C643C40D2495B88012F27251AE8907EA7CF067DE3AB26851BDA964C8C333731FEBCB3F8FEA8CDF0954653550D9388AE61B3AD483762 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:32:56.370 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:32:56.371 f0 Recovering log #3.2021/08/03-23:32:56.372 f0 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\Preferences (copy)	
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):	5792
Entropy (8bit):	5.201758323627837
Encrypted:	false
SSDEEP:	96:n8CMk29GWGcKIWok0JCKL8fkD1RbOTQVuwn:n8CE9CcD4KKkDj
MD5:	53D88C40312EBC8D52495C1468ED6B3A
SHA1:	694A31DED82516FE44B095FE697DED9D20320528
SHA-256:	713766C49D8E9EDCE2B56F9D09C451A95643DCC40BA9F51C9DC0E5390BDF6EFF
SHA-512:	6A8554B78B4DEB188D838A35015C2833A4AC19DA4AA8F94E40121340D4EDCA9C90C09E7E8C35FBC1B61EF2ACAFA56888974F2968C05BA943AB23411325DBCD D4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272532376341481","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:33:00.020473003 CEST	192.168.2.3	8.8.8.8	0x83f4	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.023257017 CEST	192.168.2.3	8.8.8.8	0x77cd	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.023664951 CEST	192.168.2.3	8.8.8.8	0xa9ef	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:19.804249048 CEST	192.168.2.3	8.8.8.8	0xc82e	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:20.734308004 CEST	192.168.2.3	8.8.8.8	0x1a43	Standard query (0)	r1.res.office365.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:21.918418884 CEST	192.168.2.3	8.8.8.8	0xa7d7	Standard query (0)	r1.res.office365.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.136609077 CEST	192.168.2.3	8.8.8.8	0x6c3d	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.657381058 CEST	192.168.2.3	8.8.8.8	0x866	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:30.593027115 CEST	192.168.2.3	8.8.8.8	0xef2f	Standard query (0)	static2.sharepointonline.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:34.293524027 CEST	192.168.2.3	8.8.8.8	0xb0c5	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:34.293603897 CEST	192.168.2.3	8.8.8.8	0x9a4c	Standard query (0)	support.content.office.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:34.709805012 CEST	192.168.2.3	8.8.8.8	0x4c32	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:36.298851013 CEST	192.168.2.3	8.8.8.8	0xdbc9	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:37.397579908 CEST	192.168.2.3	8.8.8.8	0x3688	Standard query (0)	support.content.office.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:55.706219912 CEST	192.168.2.3	8.8.8.8	0x8f48	Standard query (0)	microsoftwindows.112.2o7.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:55.708133936 CEST	192.168.2.3	8.8.8.8	0x8e4c	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Aug 3, 2021 23:34:03.589257002 CEST	192.168.2.3	8.8.8.8	0xfea0	Standard query (0)	amp.azure.net	A (IP address)	IN (0x0001)

DNS Answers

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.2	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.162	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.048110008 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	HHN-efz.ms-acdc.office.com		52.98.151.242	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.062371969 CEST	8.8.8.8	192.168.2.3	0x83f4	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:00.078129053 CEST	8.8.8.8	192.168.2.3	0xa9ef	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:00.078129053 CEST	8.8.8.8	192.168.2.3	0xa9ef	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:19.839684010 CEST	8.8.8.8	192.168.2.3	0xc82e	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:20.768491030 CEST	8.8.8.8	192.168.2.3	0x1a43	No error (0)	r1.res.office365.com	wildcard.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:21.952543020 CEST	8.8.8.8	192.168.2.3	0xa7d7	No error (0)	r1.res.office365.com	wildcard.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.34	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.18	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.210	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.162682056 CEST	8.8.8.8	192.168.2.3	0x6c3d	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:22.699970961 CEST	8.8.8.8	192.168.2.3	0x866	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:22.699970961 CEST	8.8.8.8	192.168.2.3	0x866	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:30.627384901 CEST	8.8.8.8	192.168.2.3	0xef2f	No error (0)	static2.sharepointonline.com	static2.sharepointonline.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:34.092418909 CEST	8.8.8.8	192.168.2.3	0xd9aa	No error (0)	sni1gl.wpc.gammacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:34.328217030 CEST	8.8.8.8	192.168.2.3	0x9a4c	No error (0)	support.content.office.net	support.content.office.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:34.332922935 CEST	8.8.8.8	192.168.2.3	0x89cb	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:33:34.333601952 CEST	8.8.8.8	192.168.2.3	0xb0c5	No error (0)	mem.gfx.ms	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:34.745089054 CEST	8.8.8.8	192.168.2.3	0x4c32	No error (0)	login.microsoftonline.com	ak.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:34.745089054 CEST	8.8.8.8	192.168.2.3	0x4c32	No error (0)	ak.privatelink.msidentity.com	www.tm.ak.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:35.510629892 CEST	8.8.8.8	192.168.2.3	0x54bc	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:36.343261003 CEST	8.8.8.8	192.168.2.3	0xdbc9	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:36.343261003 CEST	8.8.8.8	192.168.2.3	0xdbc9	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:37.440609932 CEST	8.8.8.8	192.168.2.3	0x3688	No error (0)	support.content.office.net	support.content.office.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:33:55.740071058 CEST	8.8.8.8	192.168.2.3	0x8f48	No error (0)	microsoftwindows.112.2o7.net		15.236.176.210	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:55.740071058 CEST	8.8.8.8	192.168.2.3	0x8f48	No error (0)	microsoftwindows.112.2o7.net		15.188.95.229	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:55.740071058 CEST	8.8.8.8	192.168.2.3	0x8f48	No error (0)	microsoftwindows.112.2o7.net		13.36.218.177	A (IP address)	IN (0x0001)
Aug 3, 2021 23:33:55.744787931 CEST	8.8.8.8	192.168.2.3	0x8e4c	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:34:03.626463890 CEST	8.8.8.8	192.168.2.3	0xfea0	No error (0)	amp.azure.net	160c1.wpc.azureedge.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5476 Parent PID: 996

General

Start time:	23:32:55
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Copyright Joe Security LLC 2021

Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://outlook.office365.com/Encryption/retrieve.ashx?recipientemailaddress=ap%40gswater.com&senderemailaddress=grainwater%40radianresearch.com&senderorganization=AwGKAAAAAoYAAAADAQAAAL%2bPwYr4eztBl9bc2pXl9%2f9PVT1XYXR0aG91ckVuZ2luZWVyaW5nLm9ubWljcm9zb2Z0LmNvbSxPVT1NaWNyb3NvZnQgRXhjaGFuZ2UgSG9zdGVkIE9yZ2FuaXphdGlvbnMsREM9TkFNUFIwMUEwMTAsREM9UFJPRCxEQz1PVVRMT09LLERDPUNPTW3U2z0RbcxKmUtxcJ88CKJDTj1Db25maWd1cmF0aW9uLENOPVdhdHRob3VyRW5naW5lZXJpbmcub25taWNyb3NvZnQuY29tLENOPUNvbmZpZ3VyYXRpb25Vbml0cyxEQz1OQU1QUjAxQTAxMCxEQz1QUk9ELERDPU9VVExPT0ssREM9Q09NAQ%3d%3d&messageid=%3cBN6PR0101MB299654BC7612BE90121C8E74BBF09%40BN6PR0101MB2996.prod.exchangelabs.com%3e&cfmRecipient=SystemMailbox%7bD0E409A0-AF9B-4720-92FE-AAC869B0D201%7d%40WatthourEngineering.onmicrosoft.com&consumerEncryption=false&senderorgid=1abee47c-68ca-4166-a776-68475cb4c2d2&urldecoded=1&e4e_sdata=NAlD4xF5G7xsjCpoXLsrqcFvJk6j2vhVIIKSh98po4JUh8sQDhUS2lu3%2f27pCMtALumoYdxBZFlm2ASgEEpgP3NQkpb%2bn1kpgDgOCtqD09%2bG%2bs8heIeUlJTsqucw0Zz9OP7E6qTSm5hEj40bLIFk1SDbdplq9xz8N2Bf2l3k4%2fRwKrYELyDkr67ZSu8gKah3uOJUUSAuDu5R6fJPiAjKampBbQQqlsds8zLPJ%2b3ltpS0fbh4UsFYc2O7%2bUSJWWZyaqmvnnGyYWLFrZs%2fgtJGXGapSFUFyG6YbDvs4i0ZVqatNUFdh07tVh62OLJ9%2fEix1dt9V%2frV%2fLktpIvUxQ6RgA%3d%3d'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 1708 Parent PID: 5476

General

Start time:	23:32:56
Start date:	03/08/2021
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=1544,8183373600241193 2,15524388546782287473,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1648 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021