ID: 458789
Cookbook: browseurl.jbs
Time: 18:43:56
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

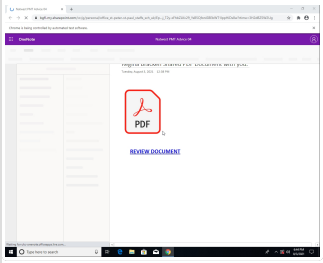
Windows Analysis Report https://bgfl-my.sharepoint.co…

Overview

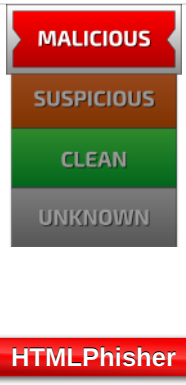
General Information

Sample URL:	https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staff...-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh
Analysis ID:	458789
Infos:	

Most interesting Screenshot:



Detection



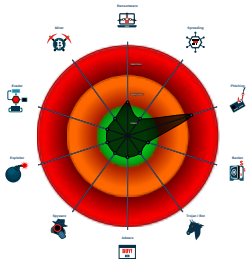
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4640 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2908 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1588,429362379618262116,4125680570342026079,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1760 /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

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

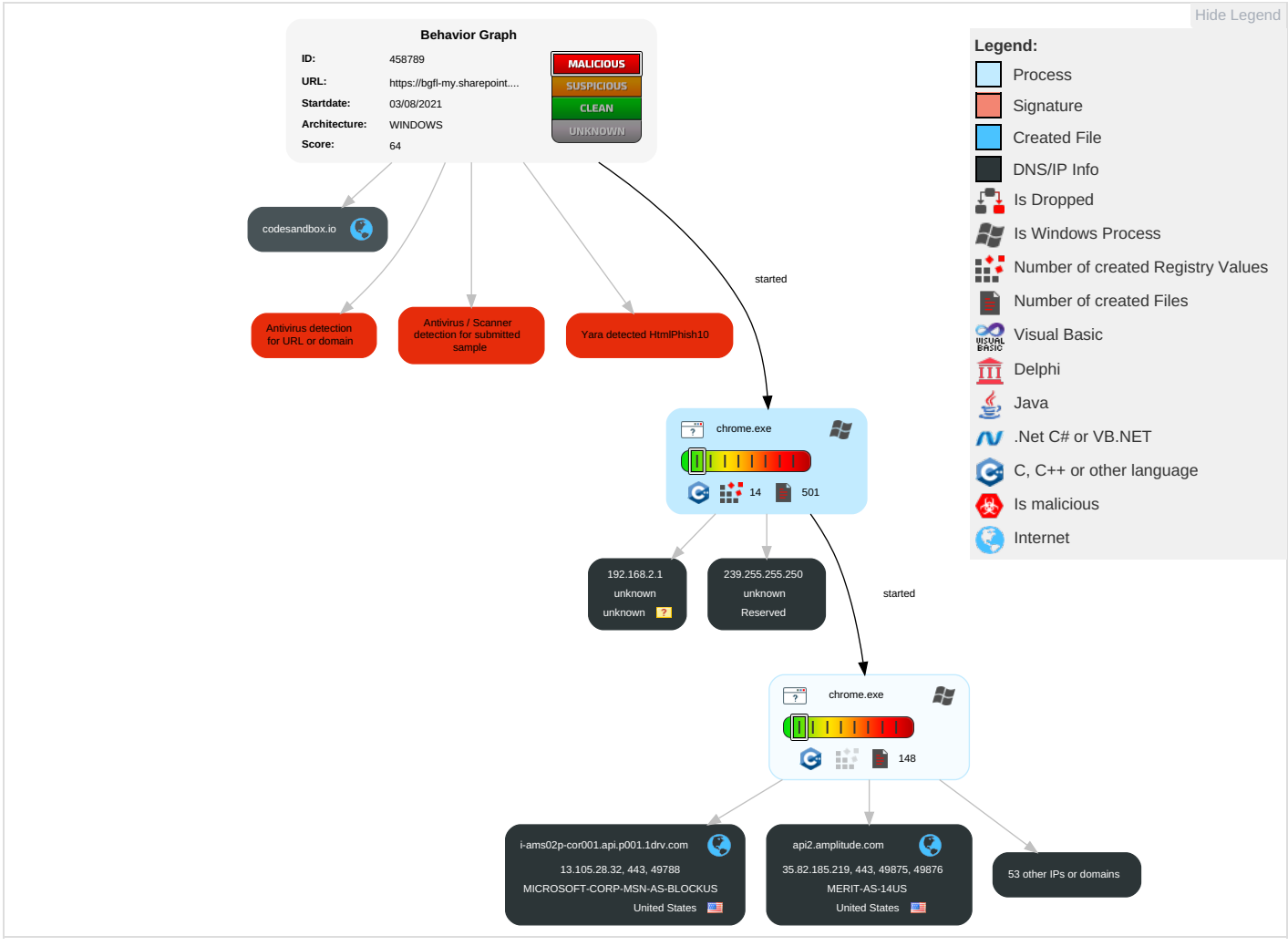
Phishing:

Yara detected HtmlPhish10

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

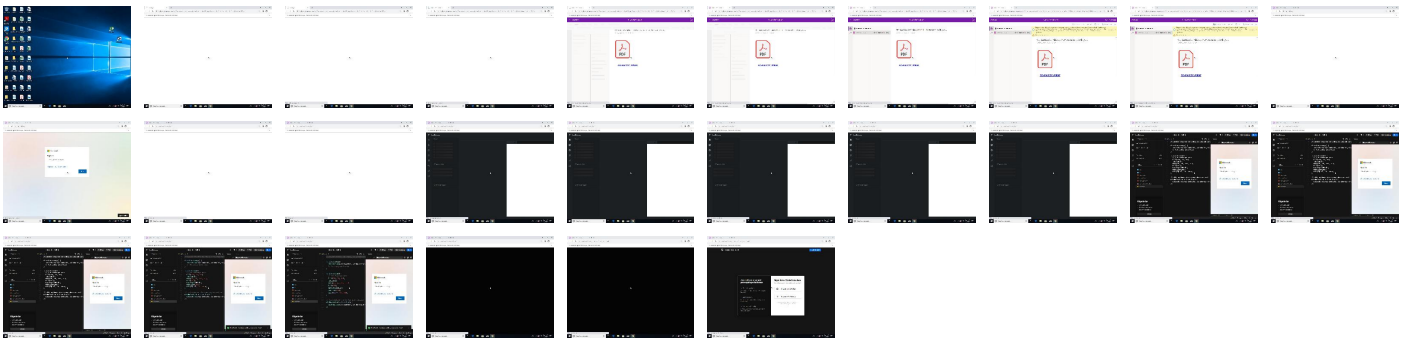
Behavior Graph

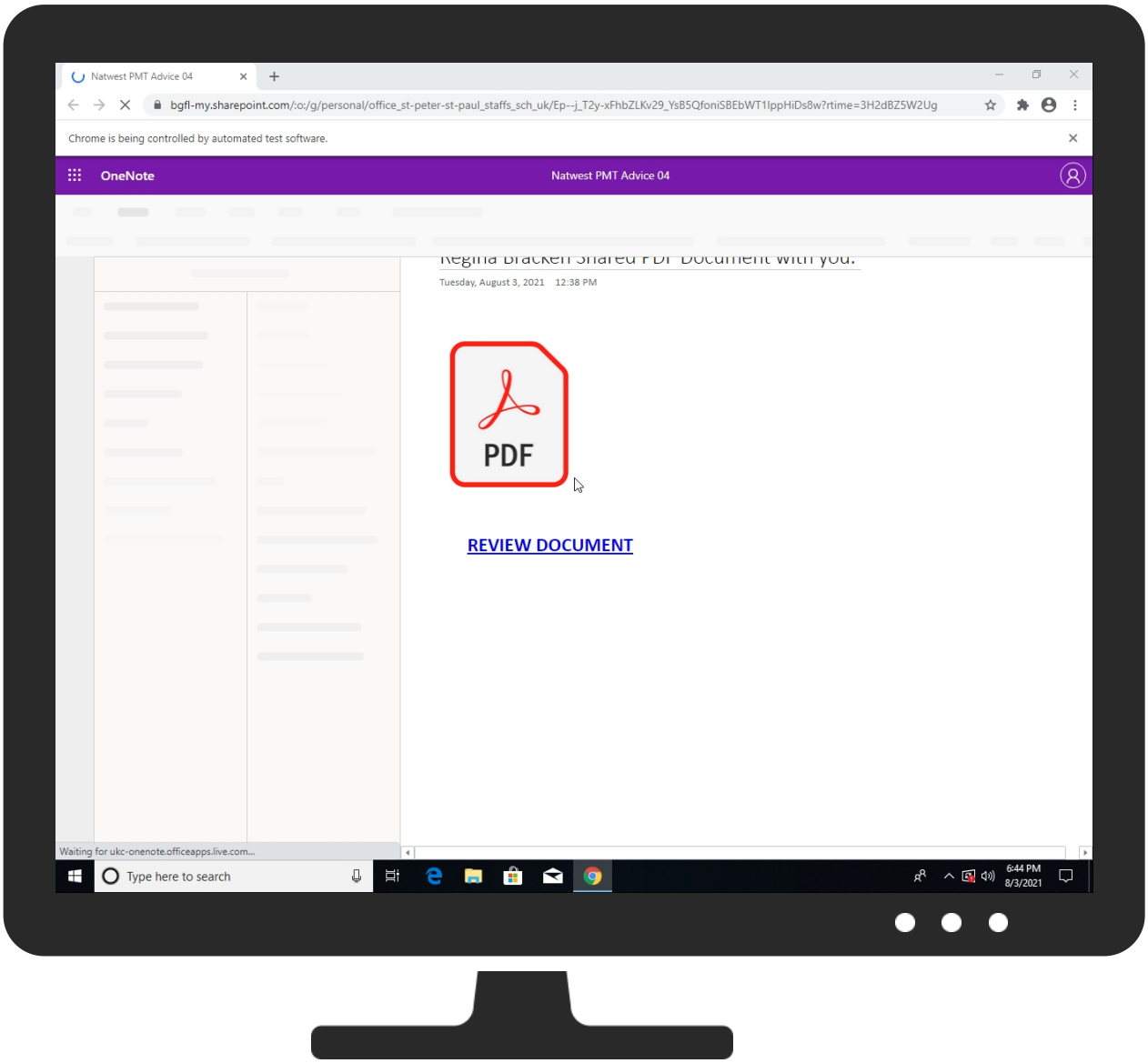


Screenshots

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://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh	0%	Avira URL Cloud	safe	
http://https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bgfl-my.sharepoint.com/personal/office_st-peter-st-paul_staffs_sch_uk/_layouts/15/Doc.aspx?sourcedoc={f48fbe9f-cbf6-45ec-85b6-4b2afdbdfd8b}&action=view&wd=target%28PAYMENT%20933901.one%7C40fd0dc0-1eba-410a-b830-3998646cdf57%2FRegina%20Bracken%20Shared%20PDF%20Document%20with%20you.%7Ca364dbd5-b7d0-438d-9aeb-168be6a7e316%2F%29	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://kedfl.csb.app/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://raw.githubusercontent.com/ajv-validator/ajv/master/lib/refs/data.json#	0%	Virustotal		Browse
http://https://raw.githubusercontent.com/ajv-validator/ajv/master/lib/refs/data.json#	0%	Avira URL Cloud	safe	
http://https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZL	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.185.131	true	false		high
jsdelivr.map.fastly.net	151.101.1.229	true	false		unknown
static.cloudflareinsights.com	104.16.94.65	true	false		unknown
codesandbox.io	104.18.22.207	true	false		high
kedfl.csb.app	104.18.26.114	true	false		unknown
api2.amplitude.com	35.82.185.219	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
d3qxef4rp70elm.cloudfront.net	143.204.214.47	true	false		high
www.google.com	142.250.180.164	true	false		high
data.jsdelivr.com	104.21.35.47	true	false		high
glcdn.githack.com	104.21.234.230	true	false		unknown
www.google.de	142.250.184.99	true	false		high
ab-testing.codesandbox.io	104.18.23.207	true	false		high
accounts.google.com	216.58.205.77	true	false		high
www-google-analytics.l.google.com	142.250.184.206	true	false		high
stats.l.doubleclick.net	108.177.126.155	true	false		high
www-googletagmanager.l.google.com	142.250.185.200	true	false		high
raw.githubusercontent.com	185.199.108.133	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
cdn.amplitude.com	13.32.23.160	true	false		high
prod-packager-packages.codesandbox.io	104.18.22.207	true	false		high
api.getvero.com	44.194.179.189	true	false		high
i-ams02p-cor001.api.p001.1drv.com	13.105.28.32	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
unpkg.com	104.16.123.175	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ka-f.fontawesome.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
messaging.office.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
schemastore.azurewebsites.net	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false		unknown
www.onenote.com	unknown	unknown	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
bgfl-my.sharepoint.com	unknown	unknown	false		unknown
dc.services.visualstudio.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
35.82.185.219	api2.amplitude.com	United States		237	MERIT-AS-14US	false
104.16.123.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
104.18.22.207	codesandbox.io	United States		13335	CLOUDFLARENETUS	false
104.21.234.230	glcdn.githack.com	United States		13335	CLOUDFLARENETUS	false
108.177.126.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.180.164	www.google.com	United States		15169	GOOGLEUS	false
142.250.184.99	www.google.de	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
44.194.179.189	api.getvero.com	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.16.94.65	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false
143.204.214.47	d3qxef4rp70elm.cloudfront.net	United States		16509	AMAZON-02US	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.200	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
13.32.23.160	cdn.amplitude.com	United States		7018	ATT-INTERNET4US	false
13.105.28.32	i-ams02p-cor001.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.184.206	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
151.101.1.229	jsdelivr.map.fastly.net	United States		54113	FASTLYUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
104.21.35.47	data.jsdelivr.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.131	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	false
104.18.26.114	kedfl.csb.app	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1
192.168.2.255

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458789
Start date:	03.08.2021
Start time:	18:43:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@35/641@40/28
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://kedfl.csb.app/ • Browse: https://codesandbox.io/s/kedfl • Browse: https://codesandbox.io/dashboard
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:45:09	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,.":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.139205445116624
Encrypted:	false
SSDEEP:	6:kKn8doW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:U5kPlE99SNxAhUe0et
MD5:	D90E7C3C05AC14443AE5C142A64CD76E
SHA1:	0310556DCDDA65A6D498223F42DE6A511FF0E8C9
SHA-256:	0428BE184AFBC9DC945C055003859FC9DC8186C495A0888099A25F0DA5F84E3C

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-512:	910B7253DA8C3CD795C02D1A0780980A830279673FF6B726970B2E856DF6BC525CF5A36032AE7CFBDAE1D0B65C401F5312EDA65350A76CBA4227BE3D8D7D8FE6
Malicious:	false
Reputation:	low
Preview:	p..... .....Nv.[...(..... .....T'._.....$.....\...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a423e9b-e5c9-4065-b655-b8d0ddc75c73.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.747808746884563
Encrypted:	false
SSDEEP:	384:D3e1dD4CHjM54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mc/43JJh2OjDJNI1xIp:i2BlabCawerhXboH7GjKFbBpB
MD5:	C9A2830C0847675B67A30DC1804FD474
SHA1:	9129D2EE60F51ED95D0D0ABE1272F5BA0FB31DBC
SHA-256:	2A1845E6F35D3A2366ED7AFAFBB71D3CC009F4140849D7E5D546F202CF158892
SHA-512:	9CBBA0B9339E81ABF4225B416E7DCEB18FE9A4B85BCA387AB6C30D4858113E02E312878F1CAAA0F0B486A6BFE91D4BBA29E8FC8DA857DB7A6C850B0C7229027B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...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\30dbe49e-544b-4bd2-ad3e-d25a65d0ae90.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):	365208
Entropy (8bit):	6.0152065108912085
Encrypted:	false
SSDEEP:	6144:rlpUubUv8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBJ:ZpUubUcxzurRDn9nfNxF4ijZVtilBJ
MD5:	07DE2F3537CD570CC4320420971F0F64
SHA1:	6E863CD4D00CDC99B7D58ADA6C0A51A405749025
SHA-256:	E2D0EB494EDBA1C611171161CFDFB453B2BF2F0793A5AAF9DFEF83B7EDF22463
SHA-512:	6A4370BD6A50FEEAD5B6F42680C4B0708128176B50D25832202C0337F90B99620A41E50E9BE96529630D508557328DF51CDFF0136175EF99AA9E3438590F7532
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":1.628041493862074e+12,"network":1.628009095e+12,"ticks":5850385126.0,"uncertainty":4375069.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjBylY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327251508901

C:\Users\user\AppData\Local\Google\Chrome\User Data\7527f47f-39db-4577-af54-cb7e129e0a1a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.748218627776533
Encrypted:	false
SSDEEP:	384:d3e1dD4CbgjLVkq54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mcIe43JJh2OjDJC:da2Blab4awerhXboH7GjKFbBpg
MD5:	9AA065FFFC53BBD8AAFDFD9487D80023
SHA1:	D4E3F5BA31D50856EAA7AC4996D5AF09170E1314
SHA-256:	ADF67A1019050FAEADE00BE3C5DC3A44C46FD1C7854121C4D7A1FC543185E645
SHA-512:	95F426E554A8BFA0F4ADABBF3A1A7D7ECD7E21960261B6551D6EDF54BCC4CB51B8E355FFE28D78567CA8895515C17F9DC713AB88802CEF920E8C718E779E185
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7527f47f-39db-4577-af54-cb7e129e0a1a.tmp	
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\88d0699a-3ded-426d-8b5a-847f65ad4b8e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748270505369668
Encrypted:	false
SSDEEP:	384:t3e1dD4CbgjLVkq54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mc/43JJh2OjDJNl:Na2BlabCawerhXboH7GjKFbBpF
MD5:	669FC6E2F812A8D41FA39F4E3C57EFFF
SHA1:	692C930BD58F1B17BE3705C58A73F7497108E96C
SHA-256:	5CFECBA4BC9BC4F9D81BB368350304C7AD516CF542AFCCE060E9CA78E7DBC011
SHA-512:	D4002E68149823D2BCA7FFC1A815948A24D07982EAC444A1D60C1CE4BB62AAE8A430648B077E3CD27F0293923350E4A297E66CB90934A247A3A8016B34D6E531
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\96f28efe-65b2-4053-bfde-c4bbf4b5686e.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):	365208
Entropy (8bit):	6.01520692879174
Encrypted:	false
SSDEEP:	6144:MlpUubUv8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBJ:ipUubUcxzurRDn9nfNxF4ijZVtilBJ
MD5:	4B3AF24213463A1D129C9A6F41553AAF
SHA1:	66CF96C2C65B4EC17DAEF3810E0E8760DB75FD53
SHA-256:	8B87072791F7BBD7284BBB2C9884EA4E9FAA12F7020850FB57FB28DAE13A2E93
SHA-512:	A14F32608F105821A5F05A0F9E58B8ED16DF8E965DE18984295842A7FC2C32C4003BC9D8029504D5D03712C62B13F2B06F5EB3B630822652E6B350B25EF1F2CB
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":1.628041493862074e+12,"network":1.628009095e+12,"ticks":5850385126.0,"uncertainty":4375069.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjBYxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327251508901

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2e5f892d-9e3b-4d1b-ba45-354c68ce58ed.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):	5694
Entropy (8bit):	5.186249475702404
Encrypted:	false
SSDEEP:	96:nArwkb9FxWXASKIlIk0JCKL8zkx116bOTQVuwn:nAr99LQASXC4KMkxA
MD5:	D756355E3E898AF16BB4A675EC933BD9
SHA1:	5D61AB4DCE3035A3FD5FCAB4E5064DEEB72E5C7C
SHA-256:	6480195F73C5394C7537BFB2EED79223A82167EBC2ABC911E0F556ED142FE528
SHA-512:	031529C24D5730C081639E3E95A144A75C9C39FB89FE001CE03CB7D99E18FA6B25D69657F939B14C9AF8AEEAB53AB056A2DCEC3BFEFAE39982F61E6E83B7A0D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272515089464209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2e902a2a-e76a-4181-b40a-b6e089368daf.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):	3855
Entropy (8bit):	4.861787213953784
Encrypted:	false
SSDEEP:	96:JnOTXDHz9Sm5gNAVn+Id6MGFNai6x5j6YrClGl3NwhVD:JnOTXDHz9Sm5gN+n+c6fFNai6x5j6Yr2
MD5:	3A1C5800D4B0327653F5320AD1843FF3
SHA1:	5144321EC86CFEB11B9370E6F04088BFCD5D0A1E
SHA-256:	A876E11216B8714235430A0522C71F35A5AC4566DDDE3D61C484D8DBC7FBB3EA
SHA-512:	D225C8E38B0C42597FF076287799F6DFF1AEA956858F382B69FB1FB8A31F923EA861B397FA83CB538F97F1405DA0DBA374EE4B27FD553D3A18CFAEA1D3BDD325
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.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":"13275107094273800","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275107094275894","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275107094443035","port":443,"protocol_str":"quic"},{"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33d4d364-c15a-493b-be5c-148a41124539.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\36f9dc75-aeee-4f48-94bc-d5e17edc63e2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\36f9dc75-aeee-4f48-94bc-d5e17edc63e2.tmp	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.5357748076692035
Encrypted:	false
SSDEEP:	384:e2ftvLlrkXk1kXqKf/pUZNCgVLH2HfDyrUjHGWnTJZA47:5Llak1kXqKf/pUZNCgVLH2HfOrUDGWnj
MD5:	726091CA373DDCDD070FECC360E54645
SHA1:	2216937F322637887FE78DC65C69925A45539D3D
SHA-256:	0B6DF9E748E362F1C8623A07060EA42154C8B26C442260BFFED48D0205F9F087
SHA-512:	4008E80C9C4A35E2AAC41D50AD35AC93C9BD8FE972DC09B15BA310C8D9DA7E4AEE717573A3C7CD438E9BD2898253FB2672CAB3702A6239067470B85A4442B3E
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":"13272515089110329","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\525b1bc0-6a06-4406-b969-67a0d8a10231.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):	5084
Entropy (8bit):	4.975042993982597
Encrypted:	false
SSDEEP:	96:nAr6ib9pSKIIlk0JCKL8zkx116bOTQVuwn:nArh9pSXC4KMkxA
MD5:	64059D929F2E1D2DBBEF319A6E5A256C
SHA1:	68820102B8F1B0565373E2DD162FA2C0F6D9ED7D
SHA-256:	5225607F717158E5EF376B984BBA3CEE24ED653D6D6CF3B95DB0788322527F58
SHA-512:	27D57306290AC48F555FC7F98C89F643508D1155FF3CFCC52346215FF3E13CFCD78D2DACFD48C8C0F4B7E96F2E09E5722B98775ED1EF1B56163676839D52EB8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272515089464209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5939e492-13cc-4bd3-b4b3-c1fc86a80446.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):	5.57733135716745
Encrypted:	false
SSDEEP:	384:e2ftqLlrkXk1kXqKf/pUZNCgVLH2HfDyrUYHA4rZ:sLlak1kXqKf/pUZNCgVLH2HfOrUQA2
MD5:	5E577D37D8951E12C48DB5B248749DED
SHA1:	6FB823A28D4441D148D6BB3A0A3D8BFB415CC29F
SHA-256:	AAA6490C3539CDD8C0779708F7EC4496B7F677C95232559DF4B9B41F22E66055
SHA-512:	8DAEC400361AEE60BB5609B8F05B3669FBC5E32078C907C7EEE491C6A2B1B90B0CC73FF9B9E621853F42085B4C7669CE299B540006071B0E95A419716A65AC7
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":"13272515089110329","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59eff11f-6bc5-4b8c-9165-ec670c7d694a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59eff11f-6bc5-4b8c-9165-ec670c7d694a.tmp	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5bc73fb8-07d6-4f17-aa33-2d947e7a680b.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):	6260
Entropy (8bit):	5.184040562952196
Encrypted:	false
SSDEEP:	96:nArizb9FxWXASKIlIk1qvJCKL8zkx11KbOTQVo1wn:nArW9LQASXiv4KMkxG
MD5:	70853F486709EFCA1DC61CAB142EAD66
SHA1:	8970A65F6794DEE4FBE8EA34191F27AAC898E2F3
SHA-256:	4C55E232F6523545AECF06BA8A889B75546D1DA5BD9B71D765D11C9CBE626D56
SHA-512:	641C37FE8E826BBCE15FEFAABCC5FFD1BB7D61ACE1517006018EC76994C0C68FB9B221D35DFD19D7C47E691EE47EB74582B0E2551D1C3C1D5F20E08EF2DDE 196
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272515089464209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64433c07-dd88-4d4d-afee-2a4daca84416.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535574427580993
Encrypted:	false
SSDEEP:	384:e2ftvLlrkXk1kXqKf/pUZNCgVLH2HfDyrUjHGtnTJWbCA4/t:5Llak1kXqKf/pUZNCgVLH2HfOrUDGtn7
MD5:	493AE4F6F73B031A99CDA9C3C519DA28
SHA1:	EB2CEB3CB4755E8ADCEF878DBE2957B367784177
SHA-256:	C174BED3CF82FBDA2C2D151019087577C0442E30E3C0CDC282787A32B33D0DAD
SHA-512:	07CCAD19BA5B95BC77E36F3FA26647706299EBC84D16D2050476266E517274580F3EAC538B66AF96AF7E51FD81536A1A5EB6A8038A0991F98732E319A1AE3C5C
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":"13272515089110329","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7320dce5-2a48-42a1-94f7-85e2e1df7982.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):	3722
Entropy (8bit):	5.6033227798399965
Encrypted:	false
SSDEEP:	96:4UyUUAKUCOeU6ieU9UOUUGUtlwU18UHpKUmTUbUnWUpbUZUHBUF+UMUkYUvUzUc:4ULUPUJeUOU9UOUUGUtlwU18UJKUmTUb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7320dce5-2a48-42a1-94f7-85e2e1df7982.tmp	
MD5:	3E579DA20B4D092D070338C1FE5E2E47
SHA1:	80741656911CC2D8881192909F90AEB2565E1357
SHA-256:	8CE247D57019D04AC44F65660FB48500CEA9A715AE24DC5514981517E8824197
SHA-512:	CEDBB8D7B855C07AA0D70527A55FA3E03E8A1B115A35834865845915F624245FC7AECAAB5187A8DD9380B3996C460EF7FC75181DFEF8689326B57766444201AD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643821509.157152,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041509.157158},{"expiry":1659577505.576594,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041505.576617},{"expiry":1643593500.803905,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041500.803909},{"expiry":1638927962.761693,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041562.761698},{"expiry":1659577557.635695,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041557.635703},{"expiry":1659577506.066484,"host":"NRbo+SJrMiydIRb8dNqQFXJu7cvIkr1nN8dDkqo4V0g=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\78f092d3-94de-4d17-aa4d-741efc7b121f.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):	5694
Entropy (8bit):	5.186249475702404
Encrypted:	false
SSDEEP:	96:nArwkb9FxWXASKIlIk0JCKL8zkx116bOTQVuwn:nAr99LQASXC4KMkxA
MD5:	D756355E3E898AF16BB4A675EC933BD9
SHA1:	5D61AB4DCE3035A3FD5FCAB4E5064DEEB72E5C7C
SHA-256:	6480195F73C5394C7537BFB2EED79223A82167EBC2ABC911E0F556ED142FE528
SHA-512:	031529C24D5730C081639E3E95A144A75C9C39FB89FE001CE03CB7D99E18FA6B25D69657F939B14C9AF8AEEAB53AB056A2DCEC3BFEFAE39982F61E6E83B7A0 D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272515089464209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7fec6623-555c-45bf-a08d-93c566c62c81.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):	4224
Entropy (8bit):	5.601881432460798
Encrypted:	false
SSDEEP:	96:4UyUUAKUCOeU6ieUUU5UOUUGUtlwUQUR8UHpKUmTUbUnWUpbUZUHBUFYUMUkYUvA:4ULUPUJeUOUUU5UOUUGUtlwUQUR8UJKs
MD5:	16E29049E09C193A3670BA34819CDBA9
SHA1:	03AE323E8286B13773A6C7490F9FDD68D697EAD3
SHA-256:	D2B11C529825E3B4BB26614637DB8774257F0D6BA619CC15953DCE53D5BD4E5C
SHA-512:	9BD05A47165B0921F43EB1DD0BF9AC862A5492C04A1A1D969E9959A07D0430297F42282372A13BF561C8E9EF24F06D8B766DDEE8CE073A982237F2BB99A5B694
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643821509.157152,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041509.157158},{"expiry":1659577505.576594,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041505.576617},{"expiry":1643593500.803905,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041500.803909},{"expiry":1638927962.761693,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041562.761698},{"expiry":1659577557.635695,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041557.635703},{"expiry":1659577574.766652,"host":"NMLQxqDDrKzvJ5uwNgFmHdfFxDbK/FZNH+bU6hgJkoo=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91fd4404-b15b-4015-94d5-aeb150be8ae3.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):	1713
Entropy (8bit):	5.59644225117742
Encrypted:	false
SSDEEP:	48:Y1KUR6UUhvDKUe2U6a1UgUsUeCBUFywU/Ueh:OKUoUUlDKUbU5UgUsUHBUF/U/Uc
MD5:	1613603A76DEB93B1D8AA816CA2338F8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91fd4404-b15b-4015-94d5-aeb150be8ae3.tmp	
SHA1:	8A679E43319537355C695692064938B24732A0FB
SHA-256:	62379C7F8FB7B50F468210E71D7F39684DA102AECBDB73D9D8CF6B3923AB758E
SHA-512:	5E7E3706B3AC463079E5721B44111DF1EE33FA63BE8E789ABA27BA7A29AEFD4373E101BAB3C49E14473533E0F948D7E90141C1899BA23E25B37F0A4A3233CCBE
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643593500.803905,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041500.803909},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1659577503.601852,"host":"oJeZa9k/4NUpoWfTN04TBBWMu8281HpJq/GUqQJYkYU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041503.601856},{"expiry":1659577494.708842,"host":"oesgIJYXa0V7ktJrhnuZwGghRudqC6787cOWc6GvTBM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041494.708852},{"expiry":1659577502.787807,"host":"uSz0LqsujUW9DtrOFVcxgtoFF/cHnZgLvpRYE9IL618=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.245396888677642
Encrypted:	false
SSDEEP:	6:ms+q2P923iKKdK9RXXTZIFUtpVR+ZmwPVJNVkwO923iKKdK9RXX5LJ:gv45Kk7XT2FUtpVR+/PVJ5L5Kk7XVJ
MD5:	0910D09C56DB36E15BBF44AE286ABE0B
SHA1:	A122BB0A69464CD6CDEC8841CC580CA895C267E0
SHA-256:	49BAA30598BEBD4AAA310CB680F37A1F488FADF400320849D94054B285C0D4CE
SHA-512:	EEAE654EEACB2FED28FAE7C477D28665CE98A427F92689986A9BAEAC9E151A48E823C065F68B8DCC943474EF2FB37B81C97628911AC58B8F7A1FE292BB1949E0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:06.899 1578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:45:06.920 1578 Recovering log #3.2021/08/03-18:45:06.921 1578 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.oldB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.245396888677642
Encrypted:	false
SSDEEP:	6:ms+q2P923iKKdK9RXXTZIFUtpVR+ZmwPVJNVkwO923iKKdK9RXX5LJ:gv45Kk7XT2FUtpVR+/PVJ5L5Kk7XVJ
MD5:	0910D09C56DB36E15BBF44AE286ABE0B
SHA1:	A122BB0A69464CD6CDEC8841CC580CA895C267E0
SHA-256:	49BAA30598BEBD4AAA310CB680F37A1F488FADF400320849D94054B285C0D4CE
SHA-512:	EEAE654EEACB2FED28FAE7C477D28665CE98A427F92689986A9BAEAC9E151A48E823C065F68B8DCC943474EF2FB37B81C97628911AC58B8F7A1FE292BB1949E0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:06.899 1578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:45:06.920 1578 Recovering log #3.2021/08/03-18:45:06.921 1578 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.256515048623945
Encrypted:	false
SSDEEP:	6:m9S9+q2P923iKKdKyDZIFUtp0JZmwPNN9VkwO923iKKdKyJLJ:V9+v45Kk02FUtp0J/Pn9V5L5KkWJ
MD5:	6683D1732742831443B6AE90B64CAFF9
SHA1:	81EF46E80E07608AEA40A4BBF663B2744AB2D5C7
SHA-256:	053F433C02E11438809BA403B0619D39669A7705BB9437C621EB68C70C70B0C3
SHA-512:	311BBA085C5834B5B50FF6973A0DED55CABA60FF94BE22E73A5B173489A163B4911C635DD18416247472CDE6FDB91410C9602FF48501ECC3949102B4D15A3408
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Preview:	2021/08/03-18:45:06.895 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:45:06.896 194c Recovering log #3.2021/08/03-18:45:06.897 194c 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.oldcl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.256515048623945
Encrypted:	false
SSDEEP:	6:m9S9+q2P923iKKdKyDZIFUtp0JZmwPNN9VkwO923iKKdKyJLJ:V9+v45Kk02FUtp0J/Pn9V5L5KkWJ
MD5:	6683D1732742831443B6AE90B64CAFF9
SHA1:	81EF46E80E07608AEA40A4BBF663B2744AB2D5C7
SHA-256:	053F433C02E11438809BA403B0619D39669A7705BB9437C621EB68C70C70B0C3
SHA-512:	311BBA085C5834B5B50FF6973A0DED55CABA60FF94BE22E73A5B173489A163B4911C635DD18416247472CDE6FDB91410C9602FF48501ECC3949102B4D15A3408
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:06.895 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:45:06.896 194c Recovering log #3.2021/08/03-18:45:06.897 194c 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\037a117947eadf82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.554577772353773
Encrypted:	false
SSDEEP:	6:mQnYEYpRlM9V6EzUiIaCuefH6d//R82oE7Fk4hbK6t:dDY/lOIiIaOfH2XRoE7FkEN
MD5:	CCAF687A1F01BD02517CB72195E8BA0C
SHA1:	B39DE5226790A3838B20F743A6A856D81BE8E444
SHA-256:	8251D94FEA1ABEFF41136CE56C44242DB3CF66B0D754DD8932F69FBAB411AE62
SHA-512:	6CA1C47816F132BC8F8206B1DF7A7C8ED12F758AA5A8F046DB7B2687038F79464DCCF4E331A42A563C809E49735B1464C3705B66059CA3E08DA020B028963B56
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....A...._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/aria-web-telemetry-2.9.0.min.js .https://onenote.com/.M1<H'/.....C0.....h!.0.f&e...M.$...;Y.U.A..Eo.....p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\047447b274c22c54_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.568501536226431
Encrypted:	false
SSDEEP:	6:mioYxPERW7ctsyrhNdTp/4vMYMB/ESCm4AnK6t:xERW7As4jdmvMNB/EGFp
MD5:	3728A0299ED57367EFCC41CF54A0C4B4
SHA1:	CC938984902390F1E91ECE337EC0F26C34E52EAE
SHA-256:	6A672889D9883EA7BA4AD63038B80EBBB339994FF3371D5720DAB7517B6257C2
SHA-512:	1C137EFE88E9119BDDC99E97C3C7E8B88C23B7A31F9FA8293F82A760EB7D8BE27500CD910ED723084CAB87FE68C7C1C341E25431E49F7579D3FBEAD3A7F8D0C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q....B.j...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h4553A1519A41E5EA_App_Scripts/1033/OneNoteIntl.js .https://live.com/.I.;H'/.....<y.A..[M.....A.=.....w(.b.I.A..Eo.....Ot<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04ffe34ebd2761c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.544913004401362
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04ffe34ebd2761c7_0	
SSDEEP:	6:mwPYEYpRlM9V6YWWWeue/yTh64esi4jll/hK6t:1bY/lytj/AoYll/7
MD5:	EE70C6C8C4CBC13F11A0541E37E852A4
SHA1:	B620EEA219097036DD0CA4683359F1433C938079
SHA-256:	F417A4383D7882A8C541E17818972DFED870ADB6EF0759029D2E58DBE0E6002D
SHA-512:	88F3575E73F342D9467CE5A6C169F25172B22D8462C55AD59F9E959129CDAB91306B523C738027873D3CDE681A87DF6F201B08D083D35B46F4110C8004E1060E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....X,....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/LearningTools/LearningTools.js .https://onenote.com/..1<H'/.....Nm.g.E..=a .2k....u9L.wX.I...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\089da834c75847e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.624014795855968
Encrypted:	false
SSDEEP:	6:mUDPYxPEWg7450NdCetAThQv0u66nDWDK6t:nIEWg7MUddwGv0QW1
MD5:	0941553225D89848A395B5F0B8E549CB
SHA1:	FC22F5435191FA87B5542F3F6E29E2A0F71AA782
SHA-256:	72BDBF81409A467A5E0F7DD6A15D125E758587CE88411BA17F4C770821F02CA9
SHA-512:	31BEDC1316E3EA6AB83A9490A20FDD4917EA8C1413A05788B9FA09847EFBFE3ADA30CBA613573311B41CE8C06112410C7F097614F22747D156B84A3FADDA897C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h..`.Q....._keyhttps://c1-onenote-15.cdn.office.net/o/s/hCF8E38AF39F430EA_App_Scripts/jSanity.js .https://live.com/.w.;H'/.....Y...8.a.kC..-@.....w.-|...p.A..Eo.....`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bb91d310fc8f48c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.574077897536975
Encrypted:	false
SSDEEP:	6:mpNYxPEP9NUAFnd/ycBgulgvfqzrxhK6t:KiEPUAFnd/pguOvWd
MD5:	7688854BD34A82F579792A2F22153C24
SHA1:	4203BD00F45076EAFBD0AB858BF7895FAA553509
SHA-256:	A8ECCA5BB3268E4459AFAB60A69A697D0C46456C9788915EA40C30F20CA3B8B2
SHA-512:	76B04906FAAF7241125444AD73C87FA5691C10663B631DCD265F8C3DE5010763629A5AA11CC8732AC85BABDEA9D9F7F702DD1F870E9C023F5798C5A67BDCE4BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m.....d....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/OneNote.box4.dll2.js .https://live.com/.%.;H'/.....}.....-l..).=Cs_.... . ...A.....A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c1b3d52a9af7b69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.5933953423602025
Encrypted:	false
SSDEEP:	3:m+lYt21A8RzYFLlpEPw0XdE20uFvDzTJxyr11lHCydmYrSzekbzrH5mW5lXlpK5M:m7SYxPEP9NxdAc22v4W7DK6t
MD5:	0E8B288D2C35B9BC1F4F1C8720AB7155
SHA1:	843499EE027F69545BF0EB49927FA1307BA3B146
SHA-256:	D84034B0C611B4ED688E19A4B2DC7CA4F7B651363AFC5D998EE92F05FC83B140
SHA-512:	78FE8B9437D6E3F326E693926304592CCA6048B36FEEBE7323D21C0A6D499D0F92DD675A23118AB221C884E882555B462F81F87658280523F25052A9D6254A1C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....v....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/oreolazy.min.js .https://live.com/.G.;H'/.....]<2.=.ISS...p.AK..I.-.Mx..A..Eo.....m..z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e92be4d4afa6709_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.642016418344622
Encrypted:	false
SSDEEP:	6:mkRPYxPEP9NQo0eAMdJyC1s/dubRO6bsrS/bK6t:4EPRdJyv/dURO6bsS
MD5:	4E36BA1E9B88274393D649ECC8AE89A8
SHA1:	6988707E145683480640FF9B64034A6E1E00B93D
SHA-256:	B63B37508B56DC7F869FFB79C78ACD6B3F93A868CB9DDB6E7978628703AF849A
SHA-512:	D4E7D55C825E266BC327F29F5F3E99E84E35215B448146DA8E78FE0AA53D54737F0D00D4630B15A89889266F883DD2B54CD2BEE6394BEDE6D2DD63C86E9576E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/suiteux-shell/js/suiteux.shell.core.js .https://live.com/...;H'/.....N0..L.>..M.KDPHW.....&...A..Eo.....c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ed937f35102492d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.607346424424394
Encrypted:	false
SSDEEP:	6:mYPYxPEP9NQo0ClJSnNdjawEtgzmrWAatK6t:aEPodj9sGtJ
MD5:	9A9F52A17F43BAE0FBBE649B45BB3690
SHA1:	3FBA55F31B163D37545F6F3CF96BE6F91B7E9669
SHA-256:	1266208CC7EFF06D66D40C9F31C0D9635BDB3D2F74EAB57BF1462042A55DC9D2
SHA-512:	8282BC25A31E91910E445A2F53C399256B2477DF795700FFC8E7357DAA8697E65A9523BED06EA8C4D02C2927CBA079EF8BB4B72C7D643373FA01957C227E4C11
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/suiteux-shell/js/suiteux.shell.consappdata.js .https://live.com/3..<H'/.....7.....e....Rh../.F.zoL...e..TgE..Y..u.A..Eo.....Q|(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1265835cefa35904_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.538411851899489
Encrypted:	false
SSDEEP:	6:m5YxPEP9NwWpMIfd3+Au14bYi8H4nXJhK6t:NEPwZAdPbYi8m
MD5:	7BAA9EC996CF3284DE7EAA5021835B96
SHA1:	64C615DA29AA6816A1826D160A2BFF1060C8F23C
SHA-256:	BD2465F778A0C5A1E598FB74DFA1F1CDBF595DA353D0C137491260CF47C70AAD
SHA-512:	E91D2ECAD464FBF96BD910D34D2833D4C5715890187B3DB938D1670D6C3524AA44CBC7E96895F8D3C8A9C2F3383BE1D63D2D803A753D92C65B331B57A112D5C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....,....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/1033/osfruntime_strings.js .https://live.com/..&<H'/.....,..G-...5!.=.e.x..Vgc....zf..%.A..Eo.....o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\198d33026813b811_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196256
Entropy (8bit):	5.771616558521249
Encrypted:	false
SSDEEP:	3072:QQ0dn/D5D3hUw2bwCBtfHCPBvJxJs3K6/eaMW9w7CNY/uqwCCJzDHmu9:QQQn9D2wPr8PGy
MD5:	31F3D006135691A15B879E4C2E5498C5
SHA1:	3115862E73610DA8BDB47043A30DF8A3FE00A15C
SHA-256:	3743C2ACABE9D1799F4D076DFC703019C9EEE7A876E8CC1CC4CE9E696332D4F4
SHA-512:	29C444040858685597A6BF9A989A438767C2010F9A25C2B8FCED6418A7D088AC224DE8C7D87CA67ED94F3F2C93362FA284F0DD63D657D2C6CB58A236AFA3700

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\198d33026813b811_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....E6B14762876525594AFAC71E7ACDCF319CE053095F993D6D48A892A0A1DC2ECD.....'.`.....O>.....y..... ..... 6..`.....p.....(S.<..`4.....L`.....(S..`.....L`.....Q.@.....expo rts...Q.@.K.....module....Q.@bd-W....define....Qb..D.....amd...Q.P.0.....BrowserFS.....K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.|.&.^.....&...s.....&.\..&.-...%. ..\..&.-...%.....(Rc.....I`....Da..... ..f.....`...p...0.....@.-....HP.....:...https://codesandbox.io/static/browserfs12/browserfs.min.js..a.....D`....D`....D`.....`....&.. .&....&...(S.Q..`X.....L`^....(S...`.....LL`"....@Rc.....Qb.....t.....Qb.....e.....Qb..~....n...b$.....I`....Da.....(S...`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a049a383c9f2c9a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.645461380553512
Encrypted:	false
SSDEEP:	6:mayYxPESQ4dedCcdCP8okr56N9hnjk/ZK6t:PnEH4dedFCPuYdET
MD5:	28FAA48D55324AC5ECD59C9DB788853F
SHA1:	628663AD1C85A9A983E92E2ABD776F99CE880D1F
SHA-256:	86620736ED483E878C143260894656153E0BA3CC0C790365A70E06116C582E58
SHA-512:	06531CB84D2DB86D99FBD44BC593545769313E419F97BED894CFB9A692D2F6BA7637A7D6D49AD7F6E3ED27C218C2E768C819E642C098B126DA2E3D08AEF8A60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....w...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h9F67ECA760252947_App_Scripts/OneNote.js .https://live.com/~}.;H'/.....u..*\...A.<U..0z4E..F ...'$b.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c6ef0d7255b46f9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.536602413275672
Encrypted:	false
SSDEEP:	6:mUZVYxPEP9NT37MdZyxaP+D5mlk4RrK6t:poEPsdweE5Qd
MD5:	E2F9C98078CD33616FDCBAB263BA4D48
SHA1:	7EB0C85760DCDD75C8A229A4BD8A77A88944D66C
SHA-256:	FE8BF8D4AEE17C9267C931118211F3F5DEE85F27F94B69768479930AA74D4579
SHA-512:	96B53A3A02C9E64981183BDADCD8EA3F42BC28FD10D38720B2FD86784C6CDF55711D9B75A729142881591D997047F240CC43FE10F033A7CD0D04E341B15A243
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....4(...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/oreonavpane.min.js .https://live.com/U@.;H'/....._..w.....5.l9.... .v...@...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\205ef0c584d89ac9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	267
Entropy (8bit):	5.657612470368588
Encrypted:	false
SSDEEP:	3:m+l/Cq08RzYFLlpEPw0XdJUw+6lzDWqKlVDzTJBK1lHC+Xu0WB9V9hm5mrpK5kt:mF6YxPEP9N/+6MXqNdv+Xu0aPm4FK6t
MD5:	17E80718D3B49E09A68823334D64C7CB
SHA1:	A7295B1A8AD30E0F063A961770FA519C66454E26
SHA-256:	414099064FB32D94A44040C9FC099BBCD008DB50630BAE8B68970250E414A74F
SHA-512:	C4D371167E9B5188C4B71443BFA86BE4801F602799E12BC608F31EE84F77F420BBBE2C9E02C6DA1CA7B43AE2C79F0CF73C12A9CE7C6FA4743E8878EFEE4C8B20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/OneNoteSimplified.Wac.TellMeSuggestionModel.js .https://live.com/...;H'/.... .....D.....:.p..Z3...m....^F..XG8.....es`..A..Eo....._.au.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2838345e89c8fff3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2838345e89c8fff3_0	
Category:	dropped
Size (bytes):	97736
Entropy (8bit):	5.787281584964093
Encrypted:	false
SSDEEP:	1536:LK/xYOPG8FzSkQZXIQdzc7eVF/d93k5aOZzt6rcCFveKecPXkRDrjcCs1/9G1qvc:23e8xIYQiUH905aOpzC1e3ciDr47G1q0
MD5:	AD6EE01C6A210816E0CE3FAA08A868AB
SHA1:	2E1C7A4A10C760366C66F0630C13786F0B05EBB5
SHA-256:	10C90CAD6E59315C4C9E51F379873A0291DD4DC28BAE29F1B7B3BAF87BB0EEB0
SHA-512:	A36704879396F96E6BC8F5B096DA76E2F9557A1E23B92014027C4DDBD95EE1C83B4DFB01E08B9F8E3F24F5E2DE7DF218389C43E331A78692D238830A8E83A17F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.../..j....86DB9F8A56E1908C8F3D3F739EBF79A1393B5B3EDAFCC9A5EF058614D115A2AB.....'.JN....O!...p|.....!.....L.....(.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@.t.....module....Q.@.q.....exports...Qcj.1.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa.....D`....D`$...D`.....`z...&...&..!.&....&.(S....!..`.C....q.L`.....Rc@.....M....Qb..Z....d....Qb".U....e....Qb:.....f.....Qb..7D....h.....S...Qb.....j.....Qb.I.....k.....Qb.3.....l.....Qbju.....n.....Qb..V....o.....Qb.Ql.....p.....Qbn. .....q.....Qb.....r.....QbB..O....s.....R....Qb...@....v.....QbN5[}....w.....Qb.....x.....Qbr....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b8c9d08626be354_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.888096611394609
Encrypted:	false
SSDEEP:	6:mUIPYeD1cJflrzXKyBc//PF7PPi2m4sK6tPKFDSXCXWUFWVeJtQF7PPi2m4Xlll:puDCJflrbLc//N7ywOXqW0WVeJo7Jl
MD5:	67C67B8DC78B88899B971DADB09FF5EE
SHA1:	83300AD147FB5B95D1FF30BF935EEEE5654C4784
SHA-256:	62597BC1BCE12B07B82E8E9B7F3ADA2FB2AF9D9A090B94A07E1E949CD61E3C46
SHA-512:	4EABA144C536791D2C9578BF76717D1769C5D7A28F1F1EEFD011C63E17933D9EB25AC7D4536CC1B602C6F53E959C43EE93220A272DF38A35E7AC48106D73A10
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://codesandbox.io/public/sse-hooks/sse-hooks.f648b14c15c640a14a557113a991cb8d.js .https://csb.app/.]Q<H'/.....$.....{.n..D.....*.#....;5NfI.G....A..Eo.....G..|.....A..Eo.....]Q<H'/. 5..94BB5C4E1302719F602A9C6673B5E722936B61182459BAAA0C938817E7B07ED7.{.n..D.....*.#....;5NfI.G....A..Eo.....B.]L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30df1dad39595b20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.580491817728003
Encrypted:	false
SSDEEP:	6:meWNXYxPEP9NiGvtdWNdeeaCFHJnBP/yP4izbK6t:JWSEPhMdBrFj+h
MD5:	E33C318D5CE9707D3E9D0AADAEE86968
SHA1:	B19452849ED0B2052B2E28FC6A0BD65A975C4233
SHA-256:	9A683CE61DF0316D2610705E4F2FCD239961E18BDE8BC8B6C1C1446DF51027E8
SHA-512:	0C6BE846805C82EE398D48382C404743900BEC3C39238B41C5E45C90948B73BB140C27D0AAE073BFFCCC3A3097F940E39DD97DBF0EBAB693AE3243BA6BF5F5C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....6....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/OfficeExtension.WacRuntime.js .https://live.com/.';H'/.....h.....FHO'...V../.Rr.....B...'b..U....A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\322736b04cb79fd8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11703
Entropy (8bit):	5.560713703880966
Encrypted:	false
SSDEEP:	192:8WXe6r5FFDbtghIpIDRUEJVYoTi9Dg1DlC5Ai3nNg+i7:8X6haJdUkOFhgplClNg+o
MD5:	DF0AE1ADAA8720F84EC4E4FEC7B8FE22
SHA1:	DCAE49CFF259EB9FDADD512B4827DFF23D9EE3C3
SHA-256:	BA1E3414DCDA9F220FB32880BA1B9E49B98A2FBF76636D05949B3FBFDA19D84C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\322736b04cb79fd8_0	
SHA-512:	676EFD54B9DE0B146FD278B1E7508EF31DF3C1D4D9C5FBDE2B4CB77834D2DD227168D4A8A5BC85F7E7E50E189C3F6ED0D64C2538658D404906ABBF61C84617 2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....Z...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://csb.app/.s[<H'/.....'.....TWx.,...V.-.*&s....kc.s...6..L:..A..Eo..... ...[.....A..Eo.....'..J....O....(,....M8.....(S.<..`2.....L`.....(S.I.`.....L`.....Q.@.q.....exports...Q.@.t.....module....Q.@.E.....define....Q b.O.....amd...Q.@r.d=....Popper....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da"...8.....e.....`...p...@.....@.-....XP.Q. ....I...https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js...a.....D`....D`T...D`.....`....&...&....&.(S.U..`b.....L`.....Rc.....v.....Qb".U.....e.....Qb...(.. ..t.....Qb..V....o.....Qbju.....n.....Qb.....r.....Qb.Ql.....p.....QbB..O...s.....Qb..Z.....d.....M...Qb.3.....l.....Qb:.....f.....Qb.=3....m.....Qb..7D....h.....Qb.5.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\338b843602030d09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	41633
Entropy (8bit):	5.918082066094366
Encrypted:	false
SSDEEP:	768:xiR0Jw4fTn+f5v59k6fNwlwcmf/hwEfFFdfeDVfNQZLIu9p7bX:1a4DE5R9kwNo7c/q+FFJeFGIuHvX
MD5:	1A07C89190E9F9A375DCB5D622C36243
SHA1:	31D9C34A04374A0BCFB84CF6FC3425E57FC6CDE0
SHA-256:	9C30DB8EE44B6082150A5B91F8A2CAA693CC90AC0A1E53E11A8210E6A544DDC7
SHA-512:	C300F9E1F10F63F22D4C64DFFBB03970F5B5B13FF578CFA1398901D7773FC3ACB36117658BAEA250041EC0077114613F67FD343BCCDBB9BA2CC997297279538
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y....e/(...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://csb.app/.[<H'/.....K.....k....._.....L!.5(.h...Bod.BT.A..Eo.....d\.[.... .....A..Eo.....'.0.....O.....|-.....(S.<..`4.....L`.....(S...`.....4L`.....Q.@.q.....exports...Q.@.t.....module....Qc..... require...Qcn.....jquery....Qd.^.....popper.js.....Q.@.E.....define....Qb.O.....amd.....`.....M`.....Q.PrJn.....bootstrap.....Q.@.v.....jQuery....Q.@r.d=....Popper....K`.. ..D.!.(.....s..3...s.,...&....&...&.]...&....&...&.]...&.[.....A...s.....&.(.....&.z..%&.^.....~&.-...'.(...&.(...&.[.....(Rc.....I`....Da.....$..g.....`...@...`..L.....@.-. ...PP.1.....C...https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js.a.....D`....D`V...D`.....i....`0...&...&....&.(S.....`.....%.L`.....Rc|..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\346aaf183ce99f27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.675257782629911
Encrypted:	false
SSDEEP:	6:mpnY5TYpQyCEP9NFmbR4nGIfd5KyrAiQNj/YK41K6t:UrpQLEPFmb3Ad5fQR/Q
MD5:	A269E53F2FBDA7574C32828AF9FB653E
SHA1:	3E103ED516A0ADF7266420BC4A9F1125F09FC445
SHA-256:	7DD23C726BC2017F7EE772CDFB496DC194A42F9E7F407EA987A8C45E6EC34EE6
SHA-512:	AACE1BB3F50EB68893C324C9B00228E62A565334A271935549D7BD36C4529FF2DA35F0F3C3C41BB06851227F08A46610E2CB6B97E815F2B41ABD98AE86976E30
Malicious:	false
Reputation:	low
Preview:	0\r..m..... l...._keyhttps://c1-officeapps-15.cdn.office.net/o/s/161432541018_App_Scripts/Feedback/latest/Intl/en/officebrowserfeedbackstrings.js .https://live.com/...;H'/.. .....x.....M8eh.....".%NK.+....|"r..A..Eo.....&VR.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3480aedfbd38243a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	349
Entropy (8bit):	5.933195177350186
Encrypted:	false
SSDEEP:	6:mBAlVYEEUoSdWXD1VVYWgmHYLjwwK4P6nK6tpwa3AvrFtGGHBlv+mHYLjwwK4A:Wc5dmD7XHYLkwryrw0ArFtGGhlfHYLkw
MD5:	DECE60ECC96EAF1A11E8474625B45B00
SHA1:	B8891FD11BE90E5B76F8A2472B200344803371E4
SHA-256:	C44B97AABF97330D7CF4AC2937702C5E98ED777F078651AA4538403E740B85D7
SHA-512:	814455C88BE5A7C53AFDB3A6D97A1F1EE582CC575F4023E65AC9759E6CFAE82B0437E81E77E0EDFF293D18D4238426AABCB1440F3882FFAFF18E5C0DFF0D80 EB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U.....:...._keyhttps://cdn.amplitude.com/libs/amplitude-7.1.0-min.gz.js .https://codesandbox.io/..]?H'/.....L.....=.w..84.C.e.....F....\.t...A..Eo.....2.>..... ..A..Eo.....]?H'/.....37AFD7C964E148DCEA471949146C140423528AAAD2548118E86FD764D242D738...=.w..84.C.e.....F....\.t...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\372202cbfea5803e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.4022901978056135
Encrypted:	false
SSDEEP:	6:m2vnYeD1cJZIE1nD1T/9Yp8E5ztE6gK498bK6t:Z5DCJZL5Ddi8QztOx4
MD5:	0A1252EB35FDB0BF537740BB12BD1148
SHA1:	FDE2BB99CA691BD1A5AC0CB40AF8ABCBAD19C848
SHA-256:	83689064992F864A609A4C21034D3558B47FE459B5982E4E740CB56986824267
SHA-512:	96A3FB92223EA33A43D9AF2E507B94ACF6724F4961711A7195346DE2708377A33181115AB2F291B6230253B93E0CACC9109C11833B548338347DBC2D6C4E33D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....@.J...._keyhttps://codesandbox.io/public/vscode30/vs/editor/codesandbox.editor.main.js .https://codesandbox.io/z.)?H'/.....a.....S._....Z.l..i..Vd..f$%.. .P.x...A..Eo.....?].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\387591b72ede2a53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.659334689087785
Encrypted:	false
SSDEEP:	6:mfXYxPEYPcjwEFNduAYWD8awcuGvAVK6t:DEDjwEfdunano
MD5:	098B03FC4123C4EA1E8E6C6FAB6D4A81
SHA1:	5B304974B7DFD5BF67BCC5B8C7F937F906D8712E
SHA-256:	C0AC4AC1AB4B727694522A82F813C8F7A002D7162EB289549A6C467B56E563EC
SHA-512:	FA1FA329904D52EFE2B5486851EEC441870D99191E53DD91D5E984B04A3D6270E2AD04B13B8CD73DCC16B3877F2B1F25635A67B0B215CA4115C41A9F4E150DD E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://c1-onenote-15.cdn.office.net/o/s/h29DB8AD8C3F08967_App_Scripts/1033/WoncaIntl.js .https://live.com/^;.;H'/.....~.[&..&..(.[q QM.%....=/..[.A..Eo.....c.o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e2045da28285ce5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.545957112430879
Encrypted:	false
SSDEEP:	6:mRYxPEP9NQo0g0fduwlW8XxDGx9hyAvK6t:9EPhUdzQWFGx9km
MD5:	1A7BBF74A9566899588C517A8C802CE5
SHA1:	441BF85EA7A2244AD6DD18D821CA91DE4BCEA403
SHA-256:	63A9AD6B1FA1840706E314BD857996FA8F14F78C5613A0DEBF000588EF3F6C0E
SHA-512:	8D906B4C56D00753AA83F981A28E9F9DD4D1351F786D7795450CEB174456E684A8C6AAF9C99AC3CCE6CC63AF007E6FEDD68BD85E8DB44C6816905C07BE1F2E A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....NG....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/suiteux-shell/js/suiteux.shell.plus.js .https://live.com/.n#<H'/.....a.....H ....nO.>'.}.>..}k/.Mp.I.-.....A..Eo.....O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\400f20d94b676f8e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	86904
Entropy (8bit):	6.093252900324719
Encrypted:	false
SSDEEP:	1536:K63yteDiUB11rv1jzruLrWaGfWHbjcN+z4BmI0RCIAPFKMsF9dzR:r3eJUBLz1j/QWaEW7jcN+8QIsp0FKMsv
MD5:	59B019DE45509CC091E70CCB85275724
SHA1:	F6E7EA7D4B4DC89041BBFAC7A0A064AB2781BDA6
SHA-256:	DB1529525BBB7FDFA26052D7DD526B5D07C3F6D81F142056D0E7CB249B3FD135

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\400f20d94b676f8e_0	
SHA-512:	2551264F9AEB48786DDFF7AE1F6FAC736F8BD44F06563DB71B99DBEED89DE919797DC18BBB50B07D57BD7AC039491781CC7FE9A84A7B4CB48188E4BE383C85 20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...T.>.....9DA1FBFAB2D7F0E412DF8E28CAA50D64EB36D26D7D03E2E8015E2D3232E7C1C9.....'.....O....0R.....8.....`.....D..... .....D.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb>y;....n.....Qb.....q.....Qb..=.....r.....Qb.|.c....t.....QbN.....v.....Qbb.....x .....Qb.../....y.....Qb..).....z.....Qb.....A.....Qb..Q.....B.....Qb.5J@....C.....Qb..Q#....F.....Qb"X.....E.....Qb.X.....D.....QbZu6`....G.....Qb..h....H.....Qb...3....J.....Qbn.....I.....Qb.. .z....K.....Qb.....aa....QbN:.....L.....Qb.T.O....N.....Qb.....O.....QbvsG.....P.....Qb..i.....M.....Qb.....da....Qb2..&....ea....Qb.|.c....Q.....Qb.Yy.....S.....Qb.....R.....Qb.....ia.. ..Qbj7DA....U.....QbV/.D....ha....Qb.6.A....T.....Qb.....V.....Qbv.....W.....Qb.].T....Z.....Qb..v.....Y.....Qb*..f....X.....Qb...z....ba....Qbr.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43114edcb3e31bf1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.514871309993814
Encrypted:	false
SSDEEP:	3:m+la0TA8RzYP2D1HGLMkBGKuKKBXgEB/LE2LNRM2D1HGLMzYHlXlHC5lvlNPrbt3:mWdYeD1xQEB//NXD1eFY79rQAhlhK6t
MD5:	9AD6B142351A6AFBC9F60240952385E6
SHA1:	FEF2A13E31649A499E16812F80332B6E86EA8B86
SHA-256:	6237555FA53AE320C59D6FD679EBDDB8661F8E593DA1606CEFCA2725D1829680
SHA-512:	76B931B49C1B7FC3CAA6B5984308A8A8F88357588CD53CD695B502964CF31CBFD58C96465134FA4BE2C1F7B4C58B5B520ACED5467B1B64DD6C1B3AC1E808FE 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...0Q....._keyhttps://codesandbox.io/static/js/vendors~app~monaco-editor.bba89dfbf.chunk.js .https://codesandbox.io/.Y)?H'/.....b<.....]....._F..+..w}.Q..9 ~.Q.....A..Eo.....:..=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\434fa832c3021df6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197
Entropy (8bit):	5.3957488067729455
Encrypted:	false
SSDEEP:	3:m+lr2llLA8RzYP2FycyG8ZFvDQ/bi/lvXlHCuPBXRf3RdSm/lpK5kt:my2/VYeMS4YSBBf3HVbK6t
MD5:	2F1B1E343301B74EA5170C317D1DCEC3
SHA1:	75D8786338015817F80479242A7AA0E4FF837141
SHA-256:	DBD9EE07B2E7A43B1AC0FFCF1A08F4CD6EFA7271319EFED535F5132265E6C29D
SHA-512:	C1B6729DB1E5F3E42283BB27B093E17A0360DCD7869EABFECAB53909EF40AD57ED44A6E6EB5DA4A42E6E130CB142506EB4B0FF7A2E907DABE8A8BF5DE59E BDB1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A... d.e...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://csb.app/~{u?H'/.....M.....G...`.)..)... .T./.:..Y..<.....A..Eo.....us n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\454625a839ccbce0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.572588545862763
Encrypted:	false
SSDEEP:	6:mcYeD11FQEB/mtDJXD1OwYhVD2/jBZK6t:XDFOHXDmsT
MD5:	79034AD88E32E21DB07F9520BD3D400D
SHA1:	F0F4050FFCB0CD97F230D2AF9A84D730AD930AEC
SHA-256:	4DFF2538159A8D28BF121CF72143AAD7F7E6F0B697DCA10FBAF94D9FEF0B850C
SHA-512:	BB0F14B782777619BBC58DEA7CDCBBF79B58D1F465F4121099CE3584F4EE3FB6A1B009CD94DCB5D1F999DDB5DCB56CB56D5CCC8F10482109CF36CEEE03592 98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...Z.|....._keyhttps://codesandbox.io/static/js/default~app~monaco-editor.7aa2f93bf.chunk.js .https://codesandbox.io/..)?H'/.....<.....{.&4]..Ohmu!..3.Z..W...(.. {."...A..Eo.....%U."".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\457c24354a740aad_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\457c24354a740aad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.554248349094404
Encrypted:	false
SSDEEP:	6:m2Yq9YxPEP9NwIKLxTLxMd3atATRMCTfk/l7K6t:HYqyEPwIKdHxMd3AkTfkL
MD5:	85F623AA841396666FF25DEC14EB60D3
SHA1:	D725EF92D265DFA2B4A7692CFB0C918CF9F48F52
SHA-256:	A0F022B0EF8FE48B454600CA8D2E818973E85D4686C310CA41BF48EF9491677C
SHA-512:	023CEFBEDED175C14CC7E986ECDA16281D8EC91123A90A2279DB757C38FF6DFB0DFC7C417C90BE1A09D5BDD52D9696FBEC3571166FA292FDC93F41B6BBB2 32E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x.....}K...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/1033/onenote-ribbon-intl.min.js .https://live.com/. .;H'/.....D2..Y.ZO. ..b$...F.I.H.}....c.*.z.A..Eo.....0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47694da069754152_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.530395077764418
Encrypted:	false
SSDEEP:	6:mxYeD11N6FjSXD13/9YQn/TB19ftba/nX0K6t:SDYhSXDhBrBxae
MD5:	7968D25FF1FA0F4FF65FA6FD9FA70A68
SHA1:	CD4D3513A29CBCF60FEBF8C52867A8D6767B6F70
SHA-256:	9C97C3ED3AB5259ED8985B842D3B02C30D46360F96EF7350DF258271B1234445
SHA-512:	2F4FF9A84EABB76A4D8A3D7D54BB6CC4F1FF990F981B081CFCE0B73CB7ED3443820841D114B65AC7F2E53F677F708DFFE51EB95A8012B5E241046330253C5D2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...^....._keyhttps://codesandbox.io/static/js/default~app~embed.0ed4b8b23.chunk.js .https://codesandbox.io/&.)?H'/.....<.....4.u3.~$k?X...x...y.M.I.O....-.~. .A..Eo.....{.`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b163325e46bc0bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10068
Entropy (8bit):	5.499465848350941
Encrypted:	false
SSDEEP:	192:Q5McwO1fGYqnSMzdMejWsoEzJlx2o2Aa6fW:ewO1uX/Myrljo2A9fW
MD5:	F9207E9BA4CCB2E4BBB6366E781A78F4
SHA1:	23C163B66C11E87CF53DD7FE84BD33EC65A36973
SHA-256:	7773F46E5B31C7AC09CB2B3AAFD7A5C000777B9ED27B92A2D12D940467D3A8FE
SHA-512:	24B7A91E61BF880E681B36D10D51DB5D1209724F5E5FDE68BEFD12510660DB28C46F787D5051A62150C9A7507389483111F1BCFFB8CB472A51B296C0313B61AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....._keyhttps://ajax.googleapis.com/ajax/libs/webfont/1.6.26/webfont.js .https://codesandbox.io/y.*?H'/..... 8.....}...?p.:..s.+C.f.;.....T...:.6K.A..Eo.....P?{ .....A..Eo.....'..3....O.....%...n.....(S.0..`.....L`.....(S....`.....L`.....A.Rc.....Qb.?.....aa....Qb6.....ba....Qb.J.W....p.....Qb..k .....q.....Qb.9k.....ca....Qb.....da....Qb.....t.....R....Qb.I.h....v.....Qb.D.T....w.....Qb..T.....y.....Qb.;^P....z.....Qb..5.....ea....Qb.-.....A.....Qb.4&M....B.....Qb..nr....C.....Qbv.....D .....Qb.....F.....Qb&X.....E.....Qbr)`G....G.....Qb.....H.....Qb.F0L....fa....Qb.#.....J.....Qb.s.l....K.....Qb^.....I.....QbJ`.?....ga....Qb*.X.....ha....Qbr.y.....ia....Qb.V5.....M.....QbV.... ...L.....QbFH$1....ja....Qb.....ka....QbJ.w.....N.....Qb.8FO....O.....Qb.....P.....Qb.....Q.....Qb.....R.....Qb~.....S.....Qb.w.n....T.....Qb.9.O....U.....Qbb.L.....m

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c768a03884be887_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.611749791756422
Encrypted:	false
SSDEEP:	3:m+lsoV6A8RzYFLlpEPw0XdfqaR2FvDzTJxRelHCmo//tfd9/Om3WO71pK5kt:mUSYxPEP9NCaRsd1XtF9J3WiDK6t
MD5:	ABCEF8A365EF02027AA63E7CABC48A8A
SHA1:	8AF85780A9D7C310316B53C447C331CBB4A7A7D8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c768a03884be887_0	
SHA-256:	76FD96B812602CBA2186C44826DE69C69704F69D80AC740B26DEE93DE2C629E3
SHA-512:	70240A61FFAD84D1ECD120C1FC2C14C29FAE05EA41E487A87DA25E82962527CCE6DB8E634B43D08F74476F36E07819399E7862A063A252143C4AE597301A879F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....40....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/otelFullNext.min.js .https://live.com/...;H'/.....[ZJ.b.G.WJ.3G.C..8.]....|d..L.A..Eo.....n.3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\511f06892f5a721b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.426744890988962
Encrypted:	false
SSDEEP:	6:mz4PnYyeDM+uDCn6JoFVueZwK612zqrpVK6t:RPsM+uDG6JoF/OKRI
MD5:	017551F9C4B57E656B2AEBEC3E152628
SHA1:	4813DF82BBD8D3E2930BB93355E31F13D30C5429
SHA-256:	09A47305832FB305FD3D2E644F5C678F0056FEAA79BC12C6D8AEE82448A28F27
SHA-512:	EC0A708D0612E240DE524A1EECB6B6EB310D5C19A4D856395C17AE4F9B6CDE8CDA3B80BEC61152848E04AC9873E5D46B9355FE8DCC65ADC03D57786F84D89 29
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...e].v...._keyhttps://appsforoffice.microsoft.com/lib/1.1/hosted/onenote-web-16.00.js .https://onenote.com/.=3<H'/..... .....=i.....}.Yo.F.....t.A..Eo.....~ .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\579843132a44b5b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3362
Entropy (8bit):	5.470414282667569
Encrypted:	false
SSDEEP:	48:nzet7DfEBAOtA64BLtKwuQLTjC4tPSzrlwHn1FfIwjLPqv++eOR+lbNszOSZbv:za/fnOtA/BbvC4taAXfIwjLPD6H
MD5:	071DB7282B394ED8D891720E19CCE4D8
SHA1:	720B013D9A772509A6CAD8F1D7C65E5819370D96
SHA-256:	11B6E5D4AB30CE6520B6FCEA09D2C3BEF10F1E2D88B87052B51EFB55A5EA280C
SHA-512:	7D7AEA8397C2B9F0AEA4561940596325E1C9733345F9A238D5296621C80076AA5E7BC2A7A690397380E9B588C517EA0C73F9CF0E898356BE42BCE5A0F2BCD1A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J...p.z...._keyhttps://codesandbox.io/static/js/banner.be879265d.js .https://csb.app/.8Q<H'/.....(.....x..'#...4..uup.n...UF....J.c.A..Eo.....C.W.....A..Eo.... .....8Q<H'/.....'.:.....O.....b~.....(S.@..`8.....L`.....(S...`.....PL`$....@Rc.....Qbju.....n.....Qb".U.....e.....Qb...(....t...b$.....I`....Da....n.... (S...`.....L`.....Q.@.q.....exports..$..a.....S.C..Qb.3.....I...H..q....a.....Qb.....call..Q...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&. (...&.(...&...&.'..W.....-...(.....,Rc.....`....Da@...8.....q.....e..... P.....@....@.-....@P.....4...https://codesandbox.io/static/js/banner.be879265d.jsa.....D`....D`@. ..D`.....X...`(...&...&....&..1.&.(S.....Pb.....t.d.a.....I...A.d.....&.(S.....Pb.....t.r.a.....I..q..d.....&.(S.....Pb.....t.t

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b3d6230afdb7f4c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.5369736269578675
Encrypted:	false
SSDEEP:	6:mYi6EYxPEP9NwKEEXodHMdWC1XGoY0KP1jCthK6t:PZZEPwfE4dsdFcT0KA
MD5:	692F361D89E5140B3EBFA337D505F358
SHA1:	0C0A6520667F79F17EA94A1D1B241132A84C03F4
SHA-256:	72060C12902FB5100ECF3D19253FBDDB74BCA30FB516CCE85E49AD55BBA1D0F4
SHA-512:	27CF5F3A74F58C9749FB79A7A952A082713D3BA8409C6C6A54B32115EF8177C67A9B4C8F70DA7652AAD2881F3A8B01017DB47A21F957544D6F712EB5CC7D50A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....P....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/1033/onenote-navpane-strings.min.js .https://live.com/.W.;H'/.....8. ..DA..j.=n\D..&.a...e...H.N.A..Eo.....3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d411a617ba1f1ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d411a617ba1f1ec_0	
File Type:	data
Category:	dropped
Size (bytes):	103752
Entropy (8bit):	6.001451545310903
Encrypted:	false
SSDEEP:	1536:9QMH/6Z6z8TbOd5+QVCQ2JfY64BpNlpFPkL4l7C8UKhRt7bu:abZ88Hy5+OCQ2JfqbNJPkSp7K
MD5:	B8BEC098B0B1E5ED896DF2816C76F723
SHA1:	56A15EDDB398FDB1E513E69204D901D5629D8B61
SHA-256:	5910338B7637D6087A1EAAC67A8FE571BF4177A96ECD2ABBA3FDA00A733B248B
SHA-512:	16E0BCF32173A1FDB4DC429FB486225C1D19C2706AA394FB8271258CCB7AB2A140347DDD9D1B367EEBDD09A2A1AC43EED0955649883337350F01175688FED7 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...tc.....37AFD7C964E148DCEA471949146C140423528AAAD2548118E86FD764D242D738.....'./.....O.....n.....4.....D.....HX..... .....`.....(S.<..`4.....L`.....L`.....Q.P..b.....amplitude....(S.q..`.....5.L`.....RcD.....Qb.....t.....S...Qb..~.....o.....Qb.l.h....v..... Qb.J.W....p.....Qb&%nE....c.....Qb^.....l.....Qb..~....n.....Qb.....m.....Qb..R.....r.....QbV.....s.....R.....M...Qb.S.....d.....Qb.oc.....h.....QbB.....f.....Qb..T.....y.....Qb.c....._..... Qb.D.T....w.....Qb^.....l.....O...Qb&X.....E.....Qb~.....S.....QbJ.w.....N.....Qb.w.n....T.....Qb.8FO....O.....Qb.,.H....k.....Qb.-.....A.....QbF.....x.....Qb.....R.....Qb..nr....C. ....Qb.....P.....Qb.9.O....U.....Qbv.....D.....Qb..k.....q.....Qb.V5.....M.....QbnK.X....j.....Qb.Z%.....V.....Qb.s.l....K.....Qb.....F.....Qbr)`G....G.....Qb.;^P....z.....QbV.....L.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e31981c3490d5f3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.505185580259378
Encrypted:	false
SSDEEP:	3:m+lJ7iK8RzYP2FycyGYWCULLuFvDQ/vPtvXlHCT2CRu/+BR/Rkn+lYH5mGvpK5kt:mu7uYerCUztYT/u0R/CnaI4GRK6t
MD5:	33CB753CC96A0227A9BD53D2F9DDACE1
SHA1:	B065E704E1E264FE9B2AC3E55DAF560EEA5E48A0
SHA-256:	9BF0FDABFE0843D9C29CE96B8160089DC8D6706C5D9EE112C351B8C87DB9CFEC
SHA-512:	F42A5A052E85A9CDAE559809C369CC7692EEF67CB277FDF4FA518FBC491295BD09E69BEC7AB6332C8831BBF7BFDE8F6D639115303ADD809F2D5C4369006EEE 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F.....z...._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://csb.app/.u?H'/.....N.....i.}..4?!Q?}x...[.(&....,C2Y....A..Eo.....Du.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f8f6380a3ff021f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.437742484551844
Encrypted:	false
SSDEEP:	6:m1nYeD19CQ3XD1cfYL/qwVvdOtWzbK6t:wRDigDO6LVvdgWzN
MD5:	63A192891B5DD97C63E4D7C0EF8F3C34
SHA1:	B980131091A7D2E25211579E7E2E99BA77C57A81
SHA-256:	A268F14CE2729196DAF68AB99DAA4BF549E86DEC6307F6379B49CB2F785C6F92
SHA-512:	8A24E413F24EA78D24BF83022AB3ED2AAD9138ECDB15319D08210E5479200B8A2590F16F0E9DD56DE65A11B915BCE7B8A4249AF89D4564D9E3C6DF379316A76 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....C...._keyhttps://codesandbox.io/static/js/app.4be7dfb72.js .https://codesandbox.io/IH-?H'/.....B.....N...&U.#....gl-...C*...@.ef."}.A..Eo.....aB.s.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\600feda4c6f1d023_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.5455178405961325
Encrypted:	false
SSDEEP:	6:mYtVYeD1Q1O6QNXD18zYf8QXUkF16d2thkhK6t:FRDu460XD7PUU16d2ti
MD5:	B21FF8B6F1796B57FF2B0DEACB7DCDC1
SHA1:	543D0FE8D8D74CE8F1FD2DDE6424093934A20ACC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\600feda4c6f1d023_0	
SHA-256:	7F1328577D787552AD6E23CA3A80C1422A5A14652C6B4B8A996788BFE498BBC1
SHA-512:	112A14BA2D30F88C742734E4CF78A50811E564D10B6F997DE0858E68AC46CA793099F5D353D2CCF489C1AA99C90B47846B3E1A2BDE4708D54B23C59B20425DD
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....:...._keyhttps://codesandbox.io/static/js/common-sandbox.7be24d846.chunk.js .https://codesandbox.io/H.)?H'/.....D<.....4..>...Q.yp.WC...B>{_.7R.....z...A..Eo....._..K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6127d4bd9cdcd01a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.5703106734301215
Encrypted:	false
SSDEEP:	3:m+lq0bs8RzYFLlpE/QAPklQIdFvDzTJGMEflHCaFAyFGI3m2mO9l//pK5kt:mCb9YxPEYlrdV/TU/mBsZK6t
MD5:	D395A11D56AB18D0A689DFE9FB928100
SHA1:	8ECDD8D57A9C51FBC06D1428A9D6AD5F60229F70
SHA-256:	06220362F089064D910B10FBA4C8343D56C82A5B281065A63313509D680D03A7
SHA-512:	A14D24040BAD83927E1E2E2B7B75BC27776F4C17BFA39F6E53AAEF96A542CFA09316120473C541C35BF5B3E46A330EFF7C88CF1825690497E15C4EE644435ADF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....ET....._keyhttps://c1-onenote-15.cdn.office.net/o/s/h9559DFA267B44DDC_App_Scripts/onenoteSync.min.js .https://live.com/t..;H'/.....2...7)....a.F.s.]..?..h.3.....A..Eo.....r1.f.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\617f78aaa544a720_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	5.606496690188346
Encrypted:	false
SSDEEP:	6:m+hY5TYpQyCEP9NFBUKm2ndjRycesCwokA1OK6t:JBpQLEPFfdvnAw
MD5:	D1B2E681D0400B9F9E20AD9AB60BF4F0
SHA1:	00ED7BA198F971F1758C1349092BCE8C7DBBEB5E
SHA-256:	18AA80674F3F1CAB1393058CDEB90A1C5C318378D804E0109BCAB95E4A3E7050
SHA-512:	48CC5C892A212F38F362822D3634E7C5648CB718FD251D46B3F5ACA0EF04224F2FA9907CD01DEB33B1A67E9378C279C187B27E9A2CEBFA858EADCE5350761A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.J....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/161432541018_App_Scripts/Feedback/latest/officebrowserfeedback_floodgate.js .https://live.com/.a.;H'/...../.}!)a...pgr....^a.=.q\.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\62eb635e4e337bab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.497661243382202
Encrypted:	false
SSDEEP:	6:m5yEYeD15SvOSXD1R/9YUlyYt8vDZK6t:rODLSvOSXDFyAsT
MD5:	74963D2EF09E65B7417302961FFCE120
SHA1:	547D448D1184049D615A78B0D12C77B81D1FFB7F
SHA-256:	BA1EE9C6F0EE00053F2E1E4E9028A88F59EB057D5BCF67390701BAAC9205B0A7
SHA-512:	4E2B666D33FA8F6B33F50C39FB07023737410CBB05D9D7CA3742CA736EF9AEB19B47BFBA824AD6D8D7CF04DDAAB6C9540FF7A2EEEC216C8DEFB5EAAC9B9AFA9A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://codesandbox.io/static/js/common.9517b6661.chunk.js .https://codesandbox.io/..)?H'/....._<.....%_.h..aV...Z.&...y.3...o^.....!.A..Eo.....g.h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\65001a11f70945da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\65001a11f70945da_0	
Category:	dropped
Size (bytes):	264
Entropy (8bit):	5.5562894213375165
Encrypted:	false
SSDEEP:	6:m5KEYeD1xe/sgMB/ykyWHXD1szYbBUaz+062GYbzbK6t:vOD/qAa0XDd362GWN
MD5:	D3DFB705BFEB491D63F53BAE87031023
SHA1:	EE7DA51B8BA22FD78D432CB50C969A18B0B17A69
SHA-256:	E0557D8814E95856654458F52E57FAD8F11CA43C22170B9FD04A6B1EC0A6EA6B
SHA-512:	DC08940EA1A96E423BD17DDC88EFC1C7A5CF786B9E76E9C31F57BDF477DF053AA808EEAE23DC63282082039A7A355295D943400BFA0CC3448EC4CFF7A68B72 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u..".._keyhttps://codesandbox.io/static/js/vendors~app~codemirror-editor~monaco-editor~sandbox.5ca13c344.chunk.js .https://codesandbox.io/..)?H'/..... .....><.....'.Do..MM...D..W.?..4..S;.Y.A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ce673d9d43c7a3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.590988466699044
Encrypted:	false
SSDEEP:	6:mxYxPEP9NaP6VfdHBaFtIttEvqAr4klthK6t:5EPnNdHBuIttuzEo
MD5:	C7F7BF717F57DC05215388FAC8290CBD
SHA1:	FC823599FB214824A7E3A2BF509E9A11F0691FF2
SHA-256:	E4AC9B359909D00688607CA4390CC71979FE71902AC4E460A164B854E93700AF
SHA-512:	5B9C1600E1571FDE69973546AB713FF98D18B3D409B63A88F0032F3FEB95D99BBD3A0B1FC080D2469C57652ACADCF645F9DDBD3384EB3EDF7404EF723C284A D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/OsfRuntimeOneNoteWAC.js .https://live.com/u..;H'/....._.....<.....+.....!.. .....@...Z..W4.f.A..Eo.....M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d6a4f3b7a75956a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.470850637731655
Encrypted:	false
SSDEEP:	6:m63zYEYpRlM9V60OZ8xCueJTh6wnPUp06YDK6t:hY/l5mo9h3G0D1
MD5:	16F508AA90BA28776592323F01B6C49F
SHA1:	5B9BCFC99E00B4D28C6E5B7A3811AD4D6822D90D
SHA-256:	9010DA28FB616A4A3FC72905D066A9ED2CCD174F77C55B82FD93AF4E0E3259A9
SHA-512:	AACB5328C16C91DE4C2FB5E5485165F3F07C740275E0ED762AE099BF15932E5759E61F6247356273851812 7A84777BF32C9567711D2794B83F985C0E54276F12
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/pickadate.min.js .https://onenote.com/.Z1<H'/.....K.Z..'.%.xQ.....VhA.g`. .t.A..Eo.....&d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6daa52f36522edb6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.502074913445483
Encrypted:	false
SSDEEP:	6:m3kVYEYpRlM9V6yduefH6kklwwX3w0+m4iXhK6t:bNY/lGP1sN3B+mlr
MD5:	5402575D74E9D7F9D114F07FDAF3E819
SHA1:	4BCC298718C82C4BF3F80D8CD5F431BF7BEEB123
SHA-256:	494085CD5F8B14BF7B059C3B8DBF64FD68F351455A7E696F5773C0B499708D8F
SHA-512:	E20E23711F5A64C7DA557676ABD959918D50D760DE636401F9D2C97B454FEDE8634EF429B79FAA4FD443BFFC86431232FD7699925A2C091319E9EB13AF06C723
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6daa52f36522edb6_0	
Preview:	0\r..m.....h...S....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/CommonDiagnostics.js .https://onenote.com/K;1<H'/.....;.....DZ.....V. .U....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\72cb71b2dae842c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.574729151798472
Encrypted:	false
SSDEEP:	3:m+ldf/lA8RzYFLlpEPw0Xdw6IIJbx/uFvDzTJArflHCmtpQSc59KSjEM9RmzlpK+:mo/XYxPEP9Nw0Jbx/Ud+AmejE8A/K6t
MD5:	B02B3A9A7F2BAA7983CB84D71B3D0511
SHA1:	05A6E34C6BF6E0BD427E96C523C32B42E1FA811E
SHA-256:	DCCB57712D730A892EA6D7577009C6F7DB2B3D0CA1232AA9B4D3242B5F745334
SHA-512:	6335946B121CEB34C823CED93B47212AC8BA47D79DC2A8DE3EEDC2DAAB71137F644CAA2DFCDA6849AD25919BA64D26A91E257225280D879397632FB807BC43 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u...b;QX...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/1033/onenote-intl-mlr.min.js .https://live.com/E".;H'/.....T'....9... M...@....Q....1.0.&.A..Eo.....;.K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7444ea2da1317cfb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.445352459545222
Encrypted:	false
SSDEEP:	6:mMYyK08fz1ueOth6cXABR7M9hnPnlDK6t:TKjf7MHqqdl1
MD5:	95FEC1551B288DBDED3980372BBF5B9D
SHA1:	F0B44F8F7833FC4A411373536C384ABC36059BC6
SHA-256:	DF6653D70B77AB522537DF9339293DC9F7EBA52F6AAF5692F89E8A956BC7D1BB
SHA-512:	F1ECFB7858B5EC1FF8B02EC8F0BCFD68914C868EE26C68324EE842B11CD069FDD854B454E603609F56A8A08D0F85ACC0C97A2AE8435E419A66B51C47B9374B A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....%...._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js .https://onenote.com/.L1<H'/.....Z.e...3]OO....B../...e..!.A..Eo.....k.>.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75a8617f4be7ec63_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.510426946157492
Encrypted:	false
SSDEEP:	6:mWXYeD1xSYOWEiqGJAWSXD1HYSn/leKJvLrDK6t:HBD/Ss3qXDvJ
MD5:	F419714A5ACC0D6FA94B7AD42A6EC075
SHA1:	8A421BE9A718C63B7553CD35E131862E52152EA4
SHA-256:	1DC9F47F1667C2A475EFBA0694D078C091C182A227D787D5E88DAE4B8C3698DC
SHA-512:	EAD1894B0941AEB277ECF4F8ED3239B7ABE966750D4D8D6A44BEE53B3EEF03521CE6422A73E130A29F64EC443F7CC4D02C7DC2FB6C15C5505AEB1EE6E7251 16
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....,....._keyhttps://codesandbox.io/static/js/vendors~app~embed~sandbox~sandbox-startup.bcc15d438.chunk.js .https://codesandbox.io/#.)?H'/.....?<.. ...../.#.Y."o.x.A..2...k...b.h..A..Eo.....n:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78bedd258028e0c4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.541914654527297
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78bedd258028e0c4_0	
SSDEEP:	6:m0EYxPEP9NGMGKdN4Qkl/Y/rGlz4UDK6t:zZEPDdVsQzGlzV1
MD5:	7A1588241249AAA42E8F1539FE2D86CD
SHA1:	EAB200939A10036967F3D1C8A50B6DF093AE873A
SHA-256:	58094D60F4B74A1CFECACA968726E50B12F3D692357BC8825957F025D7A2B1D9
SHA-512:	5FD7B34FED959CE70D4061405635EFFFF9686EE81C68FA0EBCBA4359AF3BC0C9749B3E1FAA5EC6DC81297B83E7D7AD56F81CB1C5CE0598625E5EB6922A2288 88
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...4..$...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/uiFabricLazy.min.js .https://live.com/t./<H'/.....f.....po...u"...O.8...h.. ....m;.@_..A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cd4eb7d184ef6b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.594093970063739
Encrypted:	false
SSDEEP:	3:m+lBADls8RzYFLlpEYSdP9kRGVQB4LKVRzTJ9yjlHCQmsltWdW+zh/MqyL4mQW7H:mjYxPEVP9YGVQB4L0Nd8cYatsl7DK6t
MD5:	2ABB80AF64AEC69EC6DEACCF57F17853
SHA1:	478A2F81501C03A2CE0BA612A2D34C2413017CA7
SHA-256:	E959B79E6BF79FF647AE748AA902F82C6C679B998D414B50D4DEC9BEFE1D65B7
SHA-512:	114D1FD2E2C228670D0CC6ABB76F83D181887207AF1DED18D8F54C94D9F9446C68CEDDF78CA6CDE3D0FB54869AAE419AA66D99D2EACFBB613EDFA1077CE3 91B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....%.'...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h06FE78141D1F3A43_App_Scripts/Compat.js .https://live.com/_.;H'/.....3..n....c..."...s.&..} ..Q...A..Eo.....+oh.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\810e53cf61aed9ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.474212343058479
Encrypted:	false
SSDEEP:	6:mSEYyeDM+uDCnHAO7OrNNueQAIL2Si3uDs4iK6t:NpM+uDGpi0C3MO
MD5:	F2D7911692D0DEFC22EC1773F2EF4F41
SHA1:	674F51F7FDF06126AD1C1F5B54B470DD51E53703
SHA-256:	450DA76E049C18D019D0E76D280856824FBA1D45ADA57AB59A12ADC227A506DE
SHA-512:	63313A94F62B234942A74F3429F913B43525FD4D4DC5A74454D382DE6B92D09CC11554780FE9BFA78B22B805EC23E76A577F7034EFA8014A1D59B18E3134B280
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://appsforoffice.microsoft.com/lib/1.1/hosted/telemetry/oteljs_agave.js .https://onenote.com/..6<H'/.....<..W.).....,..J|.Yr[)....C...A..Eo. .....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\81e5469d23adf390_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	5.606676940888094
Encrypted:	false
SSDEEP:	6:m9lEYExZyBLgsHasmVbEV/dBxyDLtPbTH+4nyRK6t:iI1LgsaZO/dwZH+9r
MD5:	664C94ECAE83630034ADDA4FFDAE81CD
SHA1:	FCFD6A4BFF56861ACC19AFC6D6905568C30745FD
SHA-256:	F7E59E0A93B016C63B093B6AC1B25E16D8F60ABF4FAC6CF458F05011BF96595F
SHA-512:	11F16987F75774D44C689F844781BA2971EF35A317C4BDE70ADC601AC828DAE74EFD4E4845F69CCDDA417BC3E2DE71A64C03CB53015EC5EE9DB066CB43B3A 46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T7gf...._keyhttps://modernb.akamai.odsp.cdn.office.net/files/odsp-web-prod_2021-07-16.007/odsp.aria/odsp.aria.lib-e79781b2ea62341d53ce.js .https ://sharepoint.com/...;H'/.....7..).....T+|.hgU.X6|..]....-_.A..Eo.....?.y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85dcdd750ea0ab0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.501853806092712
Encrypted:	false
SSDEEP:	6:m6YxPEP9Nd/17MdxDyR1fhK0l7vLKd9G7DK6t:IEPd/ydFKN7T71
MD5:	C24F16ECDED4947D64E1C96B2D5C6402
SHA1:	8BFB7D34D9133217783575519F12CC62CA796440
SHA-256:	621162B42D09AEEE5D1159AA17D6D2166D2125D8015DD1E5ADAF487919CD8180
SHA-512:	90A48C90B73B4AC7A74CA62F156B29845F61E82DD1F59BC9E84C4CAC5769C756B7D69DFF067985146CFD5F794865E167E0E5CD0017F87BAD401D427B2E0385C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....Rg...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/oreonotebookpane.min.js .https://live.com/...;H'/.....HGo...G.A.: .vP.[h....#Lt.A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86da0adc7a337dd1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.556820481504107
Encrypted:	false
SSDEEP:	3:m+laWs8RzYFLlpEPw0XdbpW7WFvDzTJCNH1lHCd7v++mAyde99ykvgK5m0/XpK5M:mK9YxPEP9NbpW7MdYadbxR3H40/ZK6t
MD5:	DAA5B6606D21FDC459C6A2797E1476E9
SHA1:	D13306C782A70F328582C646433BA97FD682CDEB
SHA-256:	7BC60A2670569EE4DFD2340A9B973BEDAA4DE5D2A2CBD0E34CDF2E41DF947148
SHA-512:	E1491204BA325F3284E657EA4DDC8E820F3B926701520DF0737A80A6CB55C8A1A6FA89BC96A3B0D5C693B0B800CA6537CAACA589D886E6F43542B68281297A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....1."...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/oreosearchpane.min.js .https://live.com/R..;H'/.....Y.d_b9.k7.C..5m..3 .^.}....WN.8I.A..Eo.....].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8a6f46adbf302e29_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.451042961462787
Encrypted:	false
SSDEEP:	6:mmYeD1cJZIE1SD1f+Y5tDWxqKJvAy5RK6t:1DCJZLADdBWoAp
MD5:	DFA73EBAB86D7E0DF099A27AB22D89DA
SHA1:	892EB46730248ED4CA1FCFE49BBA34E0955245C7
SHA-256:	B151B2AE4885623639BB93A54CBB4F1B5358BDD6F91D566E61E5AE3380F1486B
SHA-512:	99C83A1350725DD931B1DAD9ACCC021699182712A160388993FD4D04627638A84B1448FCD2C9709FA548AACEDF39E358A034B6D344811621CA038969EF93ABE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...pq.X...._keyhttps://codesandbox.io/public/vscode30/vs/editor/codesandbox.editor.main.nls.js .https://codesandbox.io/.".?H'/.....oe.....18.T...|....[...9 ..t...Z..O..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bfe08d7fd7aee5f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	144840
Entropy (8bit):	5.870560772341489
Encrypted:	false
SSDEEP:	1536:L7RKu1t7Vh53DotZBhiHfQwH9TNoUe3HuVxVI6qm5yM+n6FxWcwB4D0OIZUoCXVp:vRKu1tL53a8dtLX5H+nJ4D
MD5:	DE7F34932C2A432C887E08A53B56BED2
SHA1:	E50CE8B842D53BE90DA71D3DD021BCFA86D8FE02
SHA-256:	1B2E07C6D2C2920F08153B7B9C69F0D80ADDFD08F326043FC300EFEB8CA08BC2
SHA-512:	1917EA885CF0217358758EF94BB573C90FC6B6BDF55310F65C1D82D04C07F45AC6C0F6F20650A7B1D5368C26C5FDB99473E9BE08319A33B3B06710FF5FD58833
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bfe08d7fd7aee5f_0	
Reputation:	low
Preview:	0\r..m.....@.....Q.....94BB5C4E1302719F602A9C6673B5E722936B61182459BAAA0C938817E7B07ED7.....'.....O!...p4...[.....4....*.....(S.<..`4.....L`.....(S.x.`.....(L`.....Q.@.q.....exports...Q.@.t.....module....Qc.....require..8Ql.`..+...@codesandbox/common/lib/utils/url-generator...Q.@.E.....define....Qb.O.....amd.....`.....M`.....Q.P&."....urlGenerator..K`....Dx.....s.....s.....&...&.]...&.]....0...s.....&.(.....&.z..%&.^.....(...&.].....(Rc.....I`....Da.....e.....`...p...0.....@.-....dP.....U...https://codesandbox.io/public/sse-hooks/sse-hooks.f648b14c15c640a14a557113a991cb8d.js...a.....D`....D`<...D`.....`....&...&....&.(S....*.`.T.....L`B.....Rc.....QbB..O....s.....Qbju.....n.....Qb...l....B.....Qb..V....o.....S....M...Qb.5.}....c.....Qb.5.}....Q.....Qb.3...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d9ca5c9f4f18f7e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	496
Entropy (8bit):	5.853168873950381
Encrypted:	false
SSDEEP:	12:vVpnplDlDz4/B4u1omerxVpnplDlDlX4u1omk:vVRBRuorxVRB2um
MD5:	0B73DC80FEC42148387D045AE60A1495
SHA1:	9752A71EA027BB71A652C5C289263C8B8ACAD145
SHA-256:	223830DC499EB43D1038C81147A8BED56C83C30E519D7A2B3DCD1590F038E5FD
SHA-512:	B2D27C13638ABFB00426BB9AD48653D83A554C50B147C357131F564879B3D4BB1F58B80B7ED3C6C229A79A3AE84B6856CD6A632464C31C781D11C9F64C3EDCD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t.....!x...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TLB9J48&t=gtm4&cid=2138525702.1628041532 .https://codesandbox.io/;..?H'/.....N.....Z.....p.q.....X79.....p..A..Eo.....A..Eo.....0\r..m.....t.....!x...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TLB9J48&t=gtm4&cid=2138525702.1628041532 .https://codesandbox.io/..&AH'/.....Z.....p.q.....X79.....p..A..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e68e846adc437ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	676
Entropy (8bit):	5.951666265561989
Encrypted:	false
SSDEEP:	12:yIwvgDhbqKc9ivOqFZpPIwvgDyplnNhX8m/YyL/:yIQgNbqKc9iGKpPIQg0lNhsiJ/
MD5:	B3A00634E84D94AB6DFBFB695A3847C1
SHA1:	DD1486FF24B9C6468AE0E9A6CF400234858759D7
SHA-256:	A08CCE2283ED5CB46BA138C25CD4AF9EDBC15ED590F4DAB99D83D38C0937C764
SHA-512:	2867CC5EDF932D15456EBA7D4E4842E18CFF0905FE744B4441340DCED748A36838D9D9B0F71F7684CD60D92236E49F08AE2019DD509A64550195BDD955D78B4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J...P{....._keyhttps://www.google-analytics.com/analytics.js .https://codesandbox.io/p4^?H'/.....L....."...z.x*.9\gk...L.}.2.-1.l.A..Eo.....C.....A..Eo..p4^?H'/..R..9DA1FBFAB2D7F0E412DF8E28CAA50D64EB36D26D7D03E2E8015E2D3232E7C1C9....."...z.x*.9\gk...L.}.2.-1.l.A..Eo.....~.fL.....0\r..m.....J...P{....._keyhttps://www.google-analytics.com/analytics.js .https://codesandbox.io/...AH'/....."...z.x*.9\gk...L.}.2.-1.l.A..Eo.....}.26.....A..Eo.....AH'/..L..1776572D0E76E7AC4F403DF17D5843D2EBEEBC1A749916610E8DDDE51A85F86D....."...z.x*.9\gk...L.}.2.-1.l.A..Eo.....,.VL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ea059dec7e49470_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	138480
Entropy (8bit):	3.2932463334141557
Encrypted:	false
SSDEEP:	768:D5f7DvKLhCwTx+jDieULMdLPWAEsY2J+47JK2ZzK0hKcIbG9mCcHML46HjLE14iv:D5fv/eoDAoxR44Fi
MD5:	9F48E247A518081468ACF44C2C17DF56
SHA1:	831A13C0207C03C4EC38342957BA1DCD6166B32D
SHA-256:	DEBA1B3BDE6FC545AF75F613D9356F022DBB02F73338E602ABEAAD5B188EC346
SHA-512:	2AEE2C929EA48DC3763DEC200E1472A7DBA69FBE8F8644D679C5360AFD98AC1241AA506C99B5CEBE7E97F724B5FF8F9C7CAD19E82914A829721633C02A3DC4DA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ea059dec7e49470_0	
Preview:	0\r..m.....@.....7C7BB6C63FBEC6AFE43BB0DD03B2B1C7228D2151A8140B8AFDA98696AE7B8101.....'.....O.....t..c.....8....(S....`.....(L`.....L`.....QcR....._0x127b...Qd2.Q...._0x3af821....(S.4.`$.....L`.....(S.<.`.....L`.....K`....Di.....%..A....&....&.%.*..&.....(Rc.....QcR....._0x269d.`.....a.,...,.....b.....@.-....tP.....f...https://glcdn.githack.com/manageroffice990/drjoe/-/raw/bcb817436cdc46e3b377279ed8bd1475c5721129/ukk.js..a.....D`....D`J...D`.....`....&...&....&..A.&.(S.m...`..... L`.....Qc6.#.....parseInt..Qb:V\[....push..Qc..3.....shift.....Rc.....Qd.F.*...._0x437167...`....`.....Kd .....D.a.@.....&.|...'.....&.....&.]...&.]...&....&.....&.]...&.]...4..&....&.....&.]...&.]...N.&....&.....&.]...&.]...6..4..&....&.....&.]...&.]...4..&....&.....&.]...&.]..!&....&.....&.]..#&.]..%6..4.'&....&.....&.]..(&.]..*N,4.-&....&.....&.]...&.]..0N24.3&.%.h.4...G

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fcbaf7266cbf6aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15624
Entropy (8bit):	5.744083392404805
Encrypted:	false
SSDEEP:	384:UI6mPP03h6iJga6Qnvb9Jf1RKAYZ3BOYCPUDtlkxYi:UI6mPP03kaWQnlR6ReC
MD5:	B7E6E5FAD8BB9C9792478697D8E07859
SHA1:	8FD36EBC83436C5FB9874DF5785C6449C012F8D4
SHA-256:	8D18127127C11B1BE96E1CBB79F4F40C224664656582D7B10E5D62174F393A9B
SHA-512:	5AFFE33612BCF34C6DAC3059AE3D10C2C001CE50F55BDB5C87042040D6485DD67A9C42A08302CE34A4F7EDCCE497EB84AF843983459046B778441608453972A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://static.cloudflareinsights.com/beacon.min.js .https://codesandbox.io//->?H'/.....B.....y...l.8..S.F..@.....H.K....z<.Q..A..Eo.....^.a.....A..Eo.....'..5....O....;...kQ7.....D.....(S....`.....L`.....(S...`.....<L`.....@Rc.....Qb.....e.....Qb.....t.....Qb..~....n...b$.....I`....Da.....(S...`.....L`.....Q.@.....exports..$..a.....S.C..Qb^.....I...H..A....a.....Qb...j....call..!...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&..'..W.....-...(.....,Rc.....`....Da....&.....A.....e..... P.....@....@.-....@P.....3...https://static.cloudflareinsights.com/beacon.min.js.a.....D`....D`<..D`.....`....&...&....&....&.(S.....Pb.....t.d.a.....I.....d.....&.(S.....Pb.....t.n.a....v.....e..... I..A..d..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\930f6afc487f275c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85288
Entropy (8bit):	6.092017223778212
Encrypted:	false
SSDEEP:	1536:KEodQDlu4VbMBntBULYlBEQlcaP+5nkfmmmJJEBIR5+VxPF9dzH:VodT4Vont1l9lcaG2f9m/EOT+VxPF9t
MD5:	9C7592951C936835FBE72F1F6CC8C0E1
SHA1:	F6EEBAD0F62350ACC997CFF163A200999AF85EB2
SHA-256:	77DD4F0E74412C16969549A9DC5162CA09CBA0C4E66CB6A289D5005A7E291EBB
SHA-512:	5FCFA5BF65B15F28AD5C70516843B7F5AB79E890409280CCC9D59D12BC882A060633502FFC8A0395018F8680175D755A98102608E280F4E501C88393EAB402CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...a.W.....1776572D0E76E7AC4F403DF17D5843D2EBEEBC1A749916610E8DDDE51A85F86D.....'.....O.....K..0.....8.....`.....D.....P.....T.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb..~....n.....Qb..k.....q.....Qb..R.....r.....Qb.....t.....Qb.l.h....v.....QbF.....x...Qb..T.....y.....Qb.;^P....z.....Qb.-.....A.....Qb.4&M....B.....Qb..nr....C.....Qb.....F.....Qb&X.....E.....Qbv.....D.....Qbr)`G....G.....Qb.....H.....Qb.#.....J.....Qb^.....I.....Qb.s.l....K.....Qb.?.....aa....QbV.....L.....QbJ.w.....N.....Qb.8FO....O.....Qb.....P.....Qb.V5.....M.....Qb.....da....Qb..5.....ea....Qb.....Q.....Qb~.....S.....Qb.....R.....Qbr.y.....ia....Qb.9.O....U.....Qb*.X.....ha....Qb.w.n....T.....Qb.Z%.....V.....Qb..%.....W.....QbF.w.....Z.....QbF.v.....Y.....Qb~..7....X.....Qb6.....ba....Qb.9k.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\96709ab112708e7e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	5.621430290082535
Encrypted:	false
SSDEEP:	6:mmVYExZyBLgsHasHQTPnBdBqX1aiZs9nK6t:KLgsbAdUXUiZS
MD5:	9EB1C59FC46A32C96A09A611CCDB29DA
SHA1:	2CC0E6BD36EC547BB36B37DD6D67F36B67372044
SHA-256:	93FE8D1979E3E447A1C256C01EA32F1B4BD0A3C411C26566EB44E2E448D03980
SHA-512:	DA5CE822FE36A704EAA61B5FAE3F74A860A4D6788D5EB99363283EA45DA7E89231CE49A49E422DD96D2571A17DFC22940E5962D3CD5D7F4BB7EAF11161F21B4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A`...._keyhttps://modernb.akamai.odsp.cdn.office.net/files/odsp-web-prod_2021-07-16.007/odsp.react/odsp.react.lib-d0a14f9e7a2171683321.js .https://sharepoint.com/p.;H'/.....s.o~~!...4..v..6...M...%DBt.A..Eo.....?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98107553e418a554_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	390
Entropy (8bit):	5.467690984882233
Encrypted:	false
SSDEEP:	6:mTYlNYpSVkQXmaF0wa9MH7/bK6tWTYlNYpSVkOtzYfY0waPMbK6t:CpSVuOJH7/NEpSVLaYJbN
MD5:	3ED3A5B1A9AE8AB96910E1DBA1C5594E
SHA1:	A3601C7098065E25A345ED43081547E8925987D0
SHA-256:	8CB171CC44B7D789EDAEB71A435B892CF94144E1C06E7DDA888BC845C73B4182
SHA-512:	93F03FDF87E20C817DCD4DDEAC7FF84E1D52063AF459418238DCB56CCD0BF332239DB24BD9C395ED51EC36AB804D7400D3077B0273DFE03B2870EA539167F5 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....L.n...._keyhttps://kit.fontawesome.com/585b051251.js .https://csb.app/..[<H'/.....B..^.&.Q.x7w2...n..1R.....^K9.9.A..Eo.....ib.....A..Eo..... ....0\r..m.....?....L.n...._keyhttps://kit.fontawesome.com/585b051251.js .https://csb.app/.qo?H'/.....M.....B..^.&.Q.x7w2...n..1R.....^K9.9.A..Eo.....3.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99840c9a9136abf6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.580739788571806
Encrypted:	false
SSDEEP:	3:m+l2b/l6v8RzYFLlpEPw0XdmIKl7WFvDzTJVjeVlHCKaEoK3Pdglkc2oLYzmVhXB:mR/VYxPEP9NmZMdViaKaqVglc7KVK6t
MD5:	4A0EA6211C3A27C6D32F342E1F86DD18
SHA1:	857A72896E68AD5B91CA6376ED2F42B795EB62AD
SHA-256:	AA983CECCCE3EBDB1E70DCE4CDD40E9C20C28DD911C9B0B25FE6F024109BBC1D
SHA-512:	A3D36D837CBB80D7363F954D928CF10FD82940EBA21DA1FD8BD593DCD77892DDB839E5FBDC159FA472C45EC152CE80BAF2C05D22315D37562D5F1B56AC18A 56
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f.....j....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/common.min.js .https://live.com/gX.;H'/.....ZX.a...j.~T.....]...=M.1 ....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a61a1c32141d9d52_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.561801676201359
Encrypted:	false
SSDEEP:	6:miHYeD1xe/sgMB/KcWyUiSXD1F9YLWoZMsBK6t:DD/qA/WHiSXD3FHU
MD5:	231709B42D733030988085F342D76F03
SHA1:	923C5B7146DEF7AE3E8A15A9BC94F65BD0AD58CF
SHA-256:	095E4C8E06D64875F0B7B72009FEB3ACEDA775D11C4C9773499FF9CF6D6C6863
SHA-512:	D35366E82DBD66CE308BC1DBA54DA5945D65A6F68C822FA87765C4EE8692BE7795011050E69D094FD17028E74A70ABDB50D345B5747C7F7F0D015A99CC0F98D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...y_/....._keyhttps://codesandbox.io/static/js/vendors~app~codemirror-editor~monaco-editor.e9593b851.chunk.js .https://codesandbox.io/2.)?H'/.....E< .....T^....P2....r....n>....S.....N.A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a92bac04b4a26881_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.88219044611981
Encrypted:	false
SSDEEP:	12:5Mv8MtyMYB7pkty7uSXQltaWVkBZX7uSX:qkMtyZb7XQlv2X
MD5:	24A63B8A34652BFC62DAC8D614F766D2
SHA1:	C50A486D7CD7E07C8E94C1A3C561376CC41C5908
SHA-256:	7D94200F525639D9C0C0A43C3FC04C40ACA606C80C7937D9E5E6043D014B2D2C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a92bac04b4a26881_0	
SHA-512:	FF8D4C172A6BB7BE30491C4C2541AEB4BE681D6A8770C683161C220BC7D277A204CFA368E09F27A43C053A3633AA5AA0A8EA72DAD94802E1B5F9A8B68197E71 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...]O./...._keyhttps://glcdn.githack.com/manageroffice990/drjoe/-/raw/bcb817436cdc46e3b377279ed8bd1475c5721129/ukk.js .https://csb.app/.#V<H'/.....M. .....B._...QgD..x...n..u1.....A..Eo.....8.....A..Eo.....#V<H'/.H...7C7BB6C63FBEC6AFE43BB0DD03B2B1C7228D2151A8140B8AFDA98696AE7B810 1.....B._...QgD..x...n..u1.....A..Eo.....AH..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\abce5cb82b32ba85_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	5.5583930869179605
Encrypted:	false
SSDEEP:	6:mTYExZyBLgsHaslzGAoWV/dBWFM1BYktXUQkx5/lbK6t:3LgsBzG6BdYMLjbg5/lN
MD5:	5F96A555E1C5859004CDBFF61D1D12EF
SHA1:	4CA0CBBF2C9FD7FB6869D2735DE5A2E39296CC39
SHA-256:	479F42DF851E5B439532350AD887E1C28B2C6214391630C758A16FAC92AA6E51
SHA-512:	D61E527E7443AF1649C93003B5E87AA1324480E3248508BDD87260E1B23B781E6CC9D44A17432C29E6006A0948330F5D3F0231A0E5B215CC6634FEEC44D8C05D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...._keyhttps://modernb.akamai.odsp.cdn.office.net/files/odsp-web-prod_2021-07-16.007/brotli/wachostwebpack/wachostwebpack.js .https://sharepoint.com/ . .;H'/.....I.....SA.....M....Lk.mY.....y..A..Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ace4c4aad50ed743_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.708190623328762
Encrypted:	false
SSDEEP:	6:msmnYGLSmXZCLRCqD18ZzYglm/FYnP4kK6tWsmnYGLSmXZCLRCqD1CGKlYinlm/1:Bs/qDuZnk6P5Ls/qD2lNlm6PO
MD5:	6720414CDC020C00648BDAE9D1ABBF51
SHA1:	4E46FCE67A9C13C041179A97317DFFBA63DA1081
SHA-256:	BD9D81BE8957A3AF02186A3C78EF9E2C28AD533D0A42E2362DBB56701AE9BBAE
SHA-512:	E79FA9013E6987BD82E799DB4FCBF0349B9E3DFF478B5AEE832458DCC6BE31A1CF3EBDF1AB664E00527C4AD30E941A9D92025C173CA34BE42A792642120CF5 C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....D....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-T3L6RFK .https://codesandbox.io/..>?H'/.....B.....#1.Gg.].....JVC....*.8..1...A..Eo.....?.... .....A..Eo.....0\r..m.....S....D....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-T3L6RFK .https://codesandbox.io/W=.@H'/.....9.....#1.Gg.].....JV C....*.8..1...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae502b2351390b95_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.565602544956615
Encrypted:	false
SSDEEP:	3:m+lAyta8RzYP2D1HGLMkBGKuK29f/6kXLBqdLGXc1LGzSRM2D1HGLMabHlXlHCVl:mmXYeD11N6YfXcBWSXD1KY+Y7rBK6t
MD5:	0B23DC04BB735FE93838900646DEA0DD
SHA1:	F2BD6CC82044D0C5CDAD98B84B592CE1A95CC2CE
SHA-256:	C4CAABEFC3C67F6E633F947F53B921D7E0C178A0568F8B8C17D2C0C785E0BD03
SHA-512:	A4FC1F2DB46A40A211F4BBDEA667E5D6121AF3F218369E8082C464B5CABD81E555473BB0CAFBB07D556E42DFF9E630C09F06940C4A26D0865998710F0D575DE 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....z.h...._keyhttps://codesandbox.io/static/js/default~app~embed~sandbox.34c87297c.chunk.js .https://codesandbox.io/.)?H'/.....v<.....t..6.Z..5>`..7..N.C..a. ...>.E>.A..Eo.....9.7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af65d4b8e5657b69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af65d4b8e5657b69_0	
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.544903141747022
Encrypted:	false
SSDEEP:	3:m+l/Nl/a8RzYP2D1HGLMkBGKuKKBX1dLXa0RM2D1HGLMiYAvlXlHCjn/lhPrZST6:mYNtXYeD1xVXD10YA9Yb/PwTbAK6t
MD5:	21DAE52CD54EE61E5A22B0A726832145
SHA1:	4D0A4B8C924DB66CEC1736998C2446A1E4176271
SHA-256:	A3C17B043E9A23E69DC4AA3EDE46303121695215BF995AB7CC3892C964B58F49
SHA-512:	19C721A0F835EAABE866EFEBB5849F058DBBEA99F6F1D9F59B833D7D9B1301BE8ADD2C7C97DB6DCB0678948CF03D4AD37AACB768C9C2B386BD5BEDCA943F3197
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...{G....._keyhttps://codesandbox.io/static/js/vendors~app~sandbox.711ae7310.chunk.js .https://codesandbox.io/..)?H'/.....`<.....@...@r.....3....."e...A..Eo.....'.d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1237742af5738bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.488902813757615
Encrypted:	false
SSDEEP:	3:m+lQ5S/yOA8RzYP2D1HGLM8HJLGKxVbsDM2D1HGLMpvlXlHCUjt/ly8dPuCIZgG6:mviPYeD1cJZmD1/9YEtdyOaG+4tRK6t
MD5:	F0D1E54B05E25EE50647C88BF79D91A2
SHA1:	8978C98AB94681A209A6BD21CA6B4F087E024141
SHA-256:	E19C22C86A75DDDDBFCEC86FA471D90DA61A737E332943F2CF0052F191457A28
SHA-512:	6A2DF53CCC27299CB7D0A8311D1FF5D5E7E54B15027DF56D8C054922BBF20A1C8D798259F5E61699602A579C57CA3D832260C95AD55BE839D3439DAD9A368B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://codesandbox.io/public/vscode30/vs/loader.js .https://codesandbox.io/.N.?H'/.....^.....&..?t.*8.....<#.....A..Eo.....P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b24c7ce889c44bd7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.64704699184685
Encrypted:	false
SSDEEP:	3:m+liAls8RzYFLlpEfjTQndJyV8sRzTJMMrflHCek/8CGiJ0rLgUoMmwP5XllpK5M:mWnYxPEwdUhNdlAek532vGnc5XhK6t
MD5:	ADAE298C0D9F243BC643D38C0FC693FC
SHA1:	E743A9613002F38F25535AEFE2E237FE3477CA1C
SHA-256:	83459371F479F7CD65B716B68BEB0A0C39F2BBDA9BB07BACC92A6FE795FA8242
SHA-512:	0B68B4A810C6B89D6D9732201E4DF1ACB58012FA24761164DED1F0FC86792D1D0EE034E0AAD69722CA5CEE07C06F9F96EBEF54926202083274AA321FDBA6501C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...o....._keyhttps://c1-onenote-15.cdn.office.net/o/s/h59FC7B214127519C_App_Scripts/OneNote.box4.dll1.js .https://live.com/..;H'/.....V...aN#U..m.....{.\.....r8...A..Eo.....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2b369b661608142_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.634528043910918
Encrypted:	false
SSDEEP:	6:mr+XY5TYpQyCEP9NL+nNdxR+AcEtbtmU4RxH0+DwnK6t:LpQLEPwdxR+zENtsfwp
MD5:	0D27FAEC9A906E79EAF3484B8137B0CD
SHA1:	C00425D8393BA9DF2A79449F05D2F8D90AD70845
SHA-256:	29D6E46AE5678B5E407523988EB58C8972B5B66306720EA6C27579089BAECD2B
SHA-512:	D73BA666443AF350D35FAC7CAAC1264A2B9726A51E57245D21919E1CFB3B694CD8692E0956F84DDA809ECC9556FA413FA145B557AE06885DCFF902BDF7E2901
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2b369b661608142_0	
Reputation:	low
Preview:	0\r..m.....z....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/161432541018_App_Scripts/wacairspaceanimationlibrary.js .https://live.com/.}.;H'/.....y.....(.-P... .''.'..u.uc.....]....7..3.A..Eo.....Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b50016dedaf7d14f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.47360599793546
Encrypted:	false
SSDEEP:	3:m+lUx/lllA8RzYP2D1HGLMkBGKuKKBXfByO9LBRM2D1HGLM11lXlHCS260ZfbQ8v:mvXYeD1xP5TXD1/YSUQXkH4AZK6t
MD5:	CDC385B536136B83FD15F6083207F768
SHA1:	D1B10D9CF8573329ECE755CF2E32D3B3043F9312
SHA-256:	5ED5E8267431B8335FDA9DF5B768E4EC5D521E46A9A424B3902EC44F3879EAF4
SHA-512:	839D2486CFC827AA1E23158B592C1859E5AD0B895B80238E9CBD626A65A35E9FE39A25773A0BACA3B77A6FA3B0F6AD11626DDE382D319F23FF153C6E22405D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\.....\....._keyhttps://codesandbox.io/static/js/vendors~app.5dda64d70.chunk.js .https://codesandbox.io/..)?H'/.....u<.....@$...W'.....`...:..u\.y...cI..A..Eo....._.. .....A..Eo.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:44:54.234285116 CEST	192.168.2.5	8.8.8.8	0x35b8	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:54.243649006 CEST	192.168.2.5	8.8.8.8	0xc496	Standard query (0)	bgfl-my.sharepoint.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:54.250710011 CEST	192.168.2.5	8.8.8.8	0x5de5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:56.134342909 CEST	192.168.2.5	8.8.8.8	0xe10	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:00.871880054 CEST	192.168.2.5	8.8.8.8	0xaeb1	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:01.194426060 CEST	192.168.2.5	8.8.8.8	0x43aa	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:05.872014046 CEST	192.168.2.5	8.8.8.8	0x5d70	Standard query (0)	amcdn.msftauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:06.284733057 CEST	192.168.2.5	8.8.8.8	0x50bd	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:06.359090090 CEST	192.168.2.5	8.8.8.8	0xdfbe	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:06.670032978 CEST	192.168.2.5	8.8.8.8	0x3590	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:08.289401054 CEST	192.168.2.5	8.8.8.8	0xe1d1	Standard query (0)	kedfl.csb.app	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:45:08.704844952 CEST	192.168.2.5	8.8.8.8	0xaac4	Standard query (0)	codesandbox.io	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.050967932 CEST	192.168.2.5	8.8.8.8	0x5209	Standard query (0)	glcdn.github.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.291235924 CEST	192.168.2.5	8.8.8.8	0x9be9	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.291615009 CEST	192.168.2.5	8.8.8.8	0xfe8f	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.292490959 CEST	192.168.2.5	8.8.8.8	0xa6f6	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.292676926 CEST	192.168.2.5	8.8.8.8	0xe67f	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.327383041 CEST	192.168.2.5	8.8.8.8	0xd2d8	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.918833971 CEST	192.168.2.5	8.8.8.8	0xb37b	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:27.958213091 CEST	192.168.2.5	8.8.8.8	0x5933	Standard query (0)	static.cloudflareinsights.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.187725067 CEST	192.168.2.5	8.8.8.8	0xef97	Standard query (0)	ab-testing.codesandbox.io	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.431931019 CEST	192.168.2.5	8.8.8.8	0xd163	Standard query (0)	d3qxef4rp70elm.cloudfront.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.667638063 CEST	192.168.2.5	8.8.8.8	0x21f0	Standard query (0)	cdn.amplitude.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.669508934 CEST	192.168.2.5	8.8.8.8	0xe885	Standard query (0)	api.getvero.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:31.244469881 CEST	192.168.2.5	8.8.8.8	0xcebc	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.337358952 CEST	192.168.2.5	8.8.8.8	0xe439	Standard query (0)	api2.amplitude.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.774024010 CEST	192.168.2.5	8.8.8.8	0x8753	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:33.704828024 CEST	192.168.2.5	8.8.8.8	0xa397	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:33.706535101 CEST	192.168.2.5	8.8.8.8	0xd077	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:37.419375896 CEST	192.168.2.5	8.8.8.8	0x389b	Standard query (0)	codesandbox.io	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.755326033 CEST	192.168.2.5	8.8.8.8	0x2ea	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.799350023 CEST	192.168.2.5	8.8.8.8	0x4340	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.801146984 CEST	192.168.2.5	8.8.8.8	0x668c	Standard query (0)	prod-packager-packages.codesandbox.io	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.941000938 CEST	192.168.2.5	8.8.8.8	0x5ae3	Standard query (0)	data.jsdelivr.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:52.011666059 CEST	192.168.2.5	8.8.8.8	0xf318	Standard query (0)	dc.services.visualstudio.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.579246044 CEST	192.168.2.5	8.8.8.8	0x4508	Standard query (0)	codesandbox.io	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.712565899 CEST	192.168.2.5	8.8.8.8	0x9b84	Standard query (0)	glcdn.github.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.712618113 CEST	192.168.2.5	8.8.8.8	0x28d6	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.739418030 CEST	192.168.2.5	8.8.8.8	0x2514	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:46:02.993635893 CEST	192.168.2.5	8.8.8.8	0xfb6e	Standard query (0)	schemastore.azurewebsites.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:44:54.266830921 CEST	8.8.8.8	192.168.2.5	0x35b8	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:54.266830921 CEST	8.8.8.8	192.168.2.5	0x35b8	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:44:54.277929068 CEST	8.8.8.8	192.168.2.5	0x5de5	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:54.317786932 CEST	8.8.8.8	192.168.2.5	0xc496	No error (0)	bgfl-my.sharepoint.com	bgfl.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:54.317786932 CEST	8.8.8.8	192.168.2.5	0xc496	No error (0)	bgfl.sharepoint.com	427-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:54.317786932 CEST	8.8.8.8	192.168.2.5	0xc496	No error (0)	427-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com	187776-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:54.317786932 CEST	8.8.8.8	192.168.2.5	0xc496	No error (0)	187776-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com	187776-ipv4e.farm.dprodmgd104.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:56.189677954 CEST	8.8.8.8	192.168.2.5	0xe10	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:00.926542997 CEST	8.8.8.8	192.168.2.5	0xaeb1	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:01.231261969 CEST	8.8.8.8	192.168.2.5	0x43aa	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:01.231261969 CEST	8.8.8.8	192.168.2.5	0x43aa	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.161	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:05.912473917 CEST	8.8.8.8	192.168.2.5	0x5d70	No error (0)	amcdn.msftauth.net	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.336839914 CEST	8.8.8.8	192.168.2.5	0x50bd	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.336839914 CEST	8.8.8.8	192.168.2.5	0x50bd	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.336839914 CEST	8.8.8.8	192.168.2.5	0x50bd	No error (0)	ams02pcor001-com.be.1drv.com	i-ams02p-cor001.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.336839914 CEST	8.8.8.8	192.168.2.5	0x50bd	No error (0)	i-ams02p-cor001.api.p001.1drv.com		13.105.28.32	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:06.409724951 CEST	8.8.8.8	192.168.2.5	0xdfbe	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.538255930 CEST	8.8.8.8	192.168.2.5	0x1973	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:06.705632925 CEST	8.8.8.8	192.168.2.5	0x3590	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:08.339345932 CEST	8.8.8.8	192.168.2.5	0xe1d1	No error (0)	kedfl.csb.app		104.18.26.114	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:08.339345932 CEST	8.8.8.8	192.168.2.5	0xe1d1	No error (0)	kedfl.csb.app		104.18.27.114	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:08.800568104 CEST	8.8.8.8	192.168.2.5	0xaac4	No error (0)	codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:08.800568104 CEST	8.8.8.8	192.168.2.5	0xaac4	No error (0)	codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.087388039 CEST	8.8.8.8	192.168.2.5	0x5209	No error (0)	glcdn.githack.com		104.21.234.230	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.087388039 CEST	8.8.8.8	192.168.2.5	0x5209	No error (0)	glcdn.githack.com		104.21.234.231	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.318604946 CEST	8.8.8.8	192.168.2.5	0x9be9	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:45:09.324219942 CEST	8.8.8.8	192.168.2.5	0xfe8f	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.324219942 CEST	8.8.8.8	192.168.2.5	0xfe8f	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.328114033 CEST	8.8.8.8	192.168.2.5	0xe67f	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:09.329276085 CEST	8.8.8.8	192.168.2.5	0xa6f6	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:09.363140106 CEST	8.8.8.8	192.168.2.5	0xd2d8	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.363140106 CEST	8.8.8.8	192.168.2.5	0xd2d8	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.557231903 CEST	8.8.8.8	192.168.2.5	0xe9a0	No error (0)	gstaticadssl.l.google.com		142.250.185.131	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:09.951239109 CEST	8.8.8.8	192.168.2.5	0xb37b	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:27.983911991 CEST	8.8.8.8	192.168.2.5	0xd380	No error (0)	www-google-tagmanager.l.google.com		142.250.185.200	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:27.993462086 CEST	8.8.8.8	192.168.2.5	0x5933	No error (0)	static.cloudflareinsights.com		104.16.94.65	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:27.993462086 CEST	8.8.8.8	192.168.2.5	0x5933	No error (0)	static.cloudflareinsights.com		104.16.95.65	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.222800016 CEST	8.8.8.8	192.168.2.5	0xef97	No error (0)	ab-testing.codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.222800016 CEST	8.8.8.8	192.168.2.5	0xef97	No error (0)	ab-testing.codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.468671083 CEST	8.8.8.8	192.168.2.5	0xd163	No error (0)	d3qxef4rp70elm.cloudfront.net		143.204.214.47	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.468671083 CEST	8.8.8.8	192.168.2.5	0xd163	No error (0)	d3qxef4rp70elm.cloudfront.net		143.204.214.220	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.468671083 CEST	8.8.8.8	192.168.2.5	0xd163	No error (0)	d3qxef4rp70elm.cloudfront.net		143.204.214.16	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.468671083 CEST	8.8.8.8	192.168.2.5	0xd163	No error (0)	d3qxef4rp70elm.cloudfront.net		143.204.214.120	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.694861889 CEST	8.8.8.8	192.168.2.5	0xc78c	No error (0)	www-google-analytics.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.701710939 CEST	8.8.8.8	192.168.2.5	0xe885	No error (0)	api.getvero.com		44.194.179.189	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.701710939 CEST	8.8.8.8	192.168.2.5	0xe885	No error (0)	api.getvero.com		107.21.40.39	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.703105927 CEST	8.8.8.8	192.168.2.5	0x21f0	No error (0)	cdn.amplitude.com		13.32.23.160	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.703105927 CEST	8.8.8.8	192.168.2.5	0x21f0	No error (0)	cdn.amplitude.com		13.32.23.194	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.703105927 CEST	8.8.8.8	192.168.2.5	0x21f0	No error (0)	cdn.amplitude.com		13.32.23.136	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:29.703105927 CEST	8.8.8.8	192.168.2.5	0x21f0	No error (0)	cdn.amplitude.com		13.32.23.71	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:31.272267103 CEST	8.8.8.8	192.168.2.5	0xcebc	No error (0)	cdn.jsdelivr.net	jsdelivr.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:31.272267103 CEST	8.8.8.8	192.168.2.5	0xcebc	No error (0)	jsdelivr.map.fastly.net		151.101.1.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:45:31.272267103 CEST	8.8.8.8	192.168.2.5	0xcebc	No error (0)	jsdelivr.map.fastly.net		151.101.65.229	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:31.272267103 CEST	8.8.8.8	192.168.2.5	0xcebc	No error (0)	jsdelivr.map.fastly.net		151.101.129.229	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:31.272267103 CEST	8.8.8.8	192.168.2.5	0xcebc	No error (0)	jsdelivr.map.fastly.net		151.101.193.229	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		35.82.185.219	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		44.240.192.168	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		54.148.27.20	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		44.225.145.135	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		52.34.17.104	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		35.160.216.213	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		34.213.216.29	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.364588976 CEST	8.8.8.8	192.168.2.5	0xe439	No error (0)	api2.amplitude.com		44.235.147.202	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.806411028 CEST	8.8.8.8	192.168.2.5	0x8753	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:32.806411028 CEST	8.8.8.8	192.168.2.5	0x8753	No error (0)	stats.l.doubleclick.net		108.177.126.155	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.806411028 CEST	8.8.8.8	192.168.2.5	0x8753	No error (0)	stats.l.doubleclick.net		108.177.126.157	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.806411028 CEST	8.8.8.8	192.168.2.5	0x8753	No error (0)	stats.l.doubleclick.net		108.177.126.154	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:32.806411028 CEST	8.8.8.8	192.168.2.5	0x8753	No error (0)	stats.l.doubleclick.net		108.177.126.156	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:33.729585886 CEST	8.8.8.8	192.168.2.5	0xa397	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:33.749079943 CEST	8.8.8.8	192.168.2.5	0xd077	No error (0)	www.google.de		142.250.184.99	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:37.454746008 CEST	8.8.8.8	192.168.2.5	0x389b	No error (0)	codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:37.454746008 CEST	8.8.8.8	192.168.2.5	0x389b	No error (0)	codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.793579102 CEST	8.8.8.8	192.168.2.5	0x2ea	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.793579102 CEST	8.8.8.8	192.168.2.5	0x2ea	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.793579102 CEST	8.8.8.8	192.168.2.5	0x2ea	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.793579102 CEST	8.8.8.8	192.168.2.5	0x2ea	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.793579102 CEST	8.8.8.8	192.168.2.5	0x2ea	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.828051090 CEST	8.8.8.8	192.168.2.5	0x4340	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:45:41.828051090 CEST	8.8.8.8	192.168.2.5	0x4340	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.828051090 CEST	8.8.8.8	192.168.2.5	0x4340	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:41.828051090 CEST	8.8.8.8	192.168.2.5	0x4340	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.840164900 CEST	8.8.8.8	192.168.2.5	0x668c	No error (0)	prod-packager-packages.codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.840164900 CEST	8.8.8.8	192.168.2.5	0x668c	No error (0)	prod-packager-packages.codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.978624105 CEST	8.8.8.8	192.168.2.5	0x5ae3	No error (0)	data.jsdelivr.com		104.21.35.47	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:44.978624105 CEST	8.8.8.8	192.168.2.5	0x5ae3	No error (0)	data.jsdelivr.com		172.67.213.229	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:52.069240093 CEST	8.8.8.8	192.168.2.5	0xf318	No error (0)	dc.services.visualstudio.com	dc.applicationinsights.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:52.069240093 CEST	8.8.8.8	192.168.2.5	0xf318	No error (0)	dc.applicationinsights.azure.com	global.in.ai.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:52.069240093 CEST	8.8.8.8	192.168.2.5	0xf318	No error (0)	global.in.ai.monitor.azure.com	global.in.ai.privatelink.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:52.069240093 CEST	8.8.8.8	192.168.2.5	0xf318	No error (0)	global.in.ai.privatelink.monitor.azure.com	dc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:45:55.613631964 CEST	8.8.8.8	192.168.2.5	0x4508	No error (0)	codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.613631964 CEST	8.8.8.8	192.168.2.5	0x4508	No error (0)	codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.734263897 CEST	8.8.8.8	192.168.2.5	0x9f2d	No error (0)	gstaticadssl.l.google.com		142.250.185.131	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.746283054 CEST	8.8.8.8	192.168.2.5	0x28d6	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.746283054 CEST	8.8.8.8	192.168.2.5	0x28d6	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.748380899 CEST	8.8.8.8	192.168.2.5	0x9b84	No error (0)	glcdn.githack.com		104.21.234.230	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.748380899 CEST	8.8.8.8	192.168.2.5	0x9b84	No error (0)	glcdn.githack.com		104.21.234.231	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.772721052 CEST	8.8.8.8	192.168.2.5	0x2514	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:45:55.772721052 CEST	8.8.8.8	192.168.2.5	0x2514	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:46:03.033808947 CEST	8.8.8.8	192.168.2.5	0xfb6e	No error (0)	schemastore.azurewebsites.net	waws-prod-ch1-001.vip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:46:03.033808947 CEST	8.8.8.8	192.168.2.5	0xfb6e	No error (0)	waws-prod-ch1-001.vip.azurewebsites.windows.net	waws-prod-ch1-001.cloudapp.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4640 Parent PID: 2892

General

Start time:	18:44:47
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' --start-maximized --enable-automation 'https://bgfl-my.sharepoint.com/:o:/g/personal/office_st-peter-st-paul_staffs_sch_uk/Ep--j_T2y-xFhbZLKv29_YsB5QfoniSBEbWT1lppHiDs8w?e=tfYhfh'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 2908 Parent PID: 4640

General

Start time:	18:44:49
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=1588,429362379618262116,412568 0570342026079,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1760 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly