ID: 458823
Cookbook: browseurl.jbs
Time: 19:21:50
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

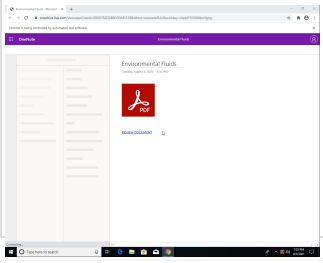
Windows Analysis Report https://linkprotect.cudasvc.co…

Overview

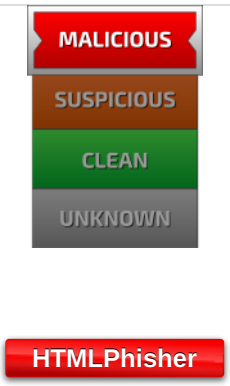
General Information

Sample URL:	https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs!B...wQx0qxxoPwhTl2ujgDMlbeQxn4ZdZQB-OFmNbdIvk9f4X00Afp0hXBwXDa-unMy-xntb&typo=1
Analysis ID:	458823
Infos:	

Most interesting Screenshot:



Detection

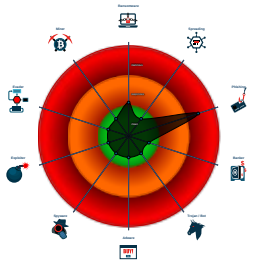


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4808 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs%21BKZQjSsteGBggQGWxWGDijKXGIKI%3fe%3dYSYU1OrRbk-OgIBVwfjzEw%26at%3d9&c=E,1,kIuIGEH799izsJ8ZzgEzo4vQsPME7QtXgthIwQx0qxxoPwhTl2ujgDMlbeQxn4ZdZQB-OFmNbdIvk9f4X00Afp0hXBwXDa-unMy-xntb&typo=1' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5940 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,16837710322178850958,12009668449574082098,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /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

Phishing:

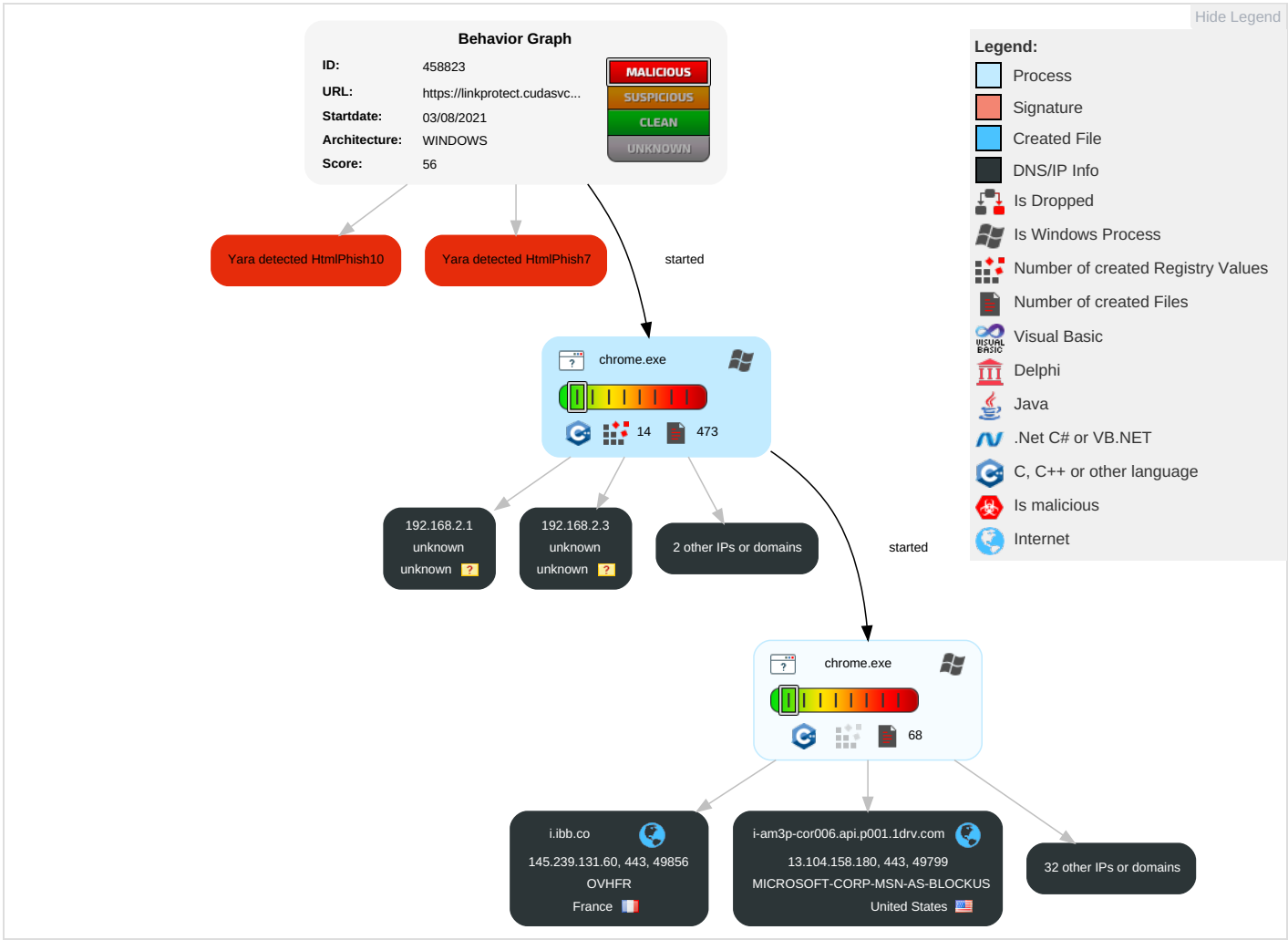
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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 1	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

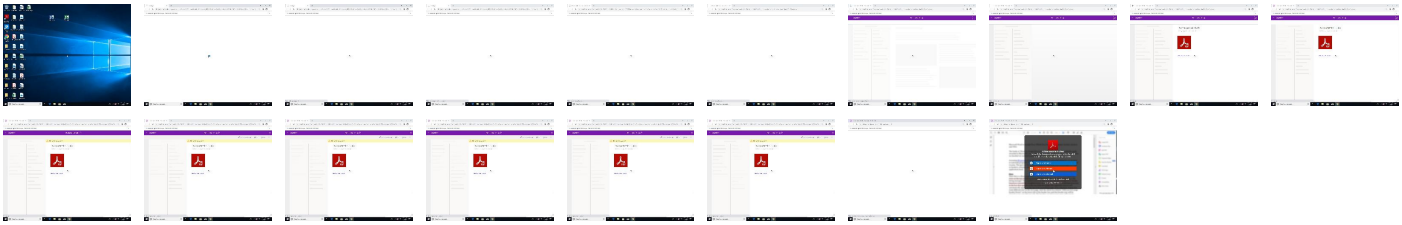
Behavior Graph

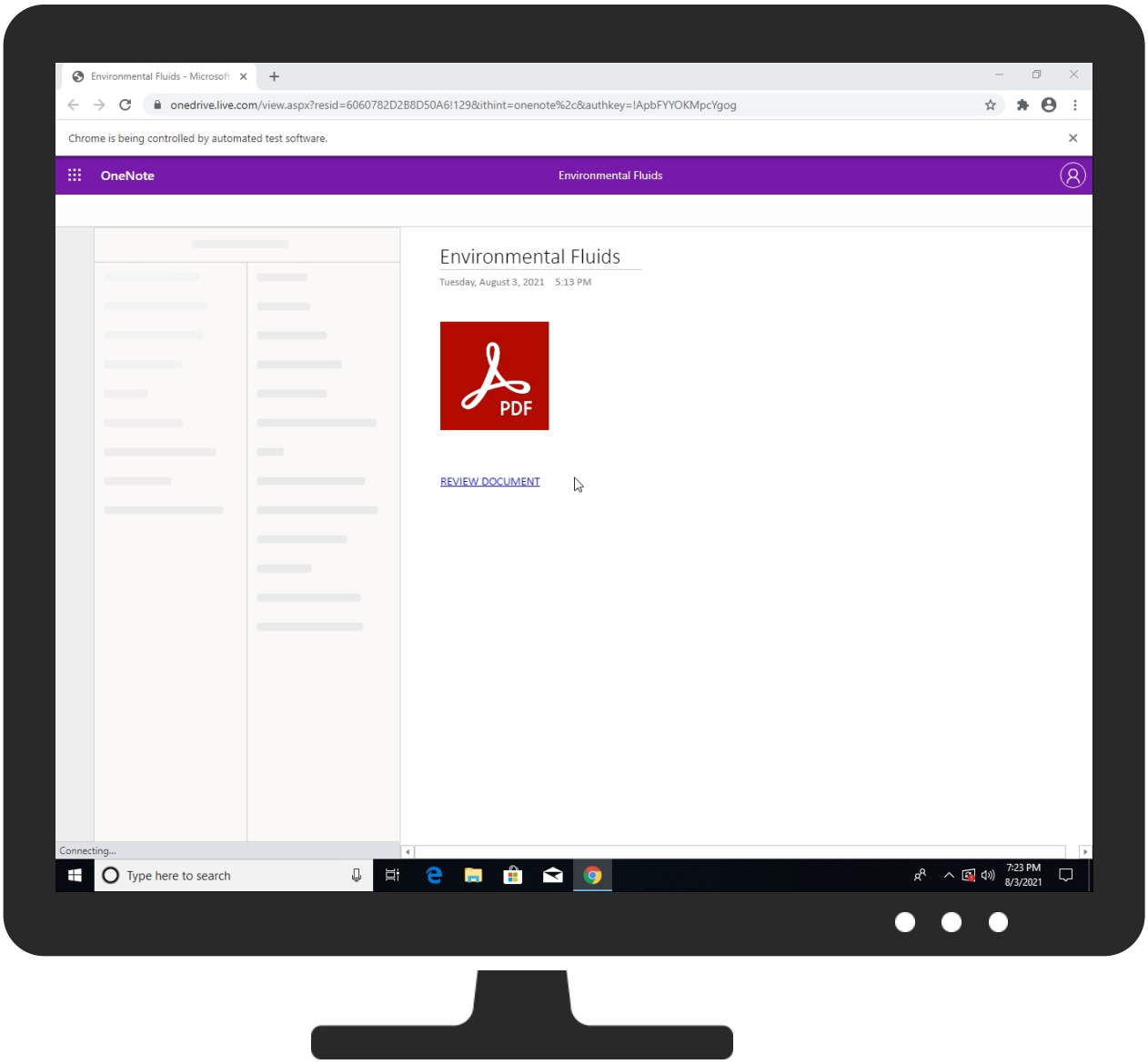


Screenshots

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://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs%21BKZQjSsteGBggQGWxWGDijKXGIKI%3fe%3dYSYU1OrRbk-OgIBVwfjzEw%26at%3d9&c=E,1,kIuIGEH799izsJ8ZzgEzo4vQsPME7QtXgthIwQx0qxxoPwhTl2ujgDMlbeQxn4ZdZQB-OFmNbdIvk9f4X00Afp0hXBwXDa-unMy-xntb&typo=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs%21BKZQjSsteGBggQGWxWGDijKX	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://onedrive.live.comh	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://amcdn.msftauth.net/me?partner=OneNoteOnline&version=10.21153.1&market=EN-GB&wrapperId=suites	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.163	true	false		high
gabby-gratis-tarascosaurus.glitch.me	52.5.55.81	true	false		high
accounts.google.com	216.58.205.77	true	false		high
i-am3p-cor006.api.p001.1drv.com	13.104.158.180	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
linkprotect.cudasvc.com	18.196.58.60	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
1drv.ms	13.107.42.12	true	false		high
i-db3p-cor005.api.p001.1drv.com	13.104.208.160	true	false		high
i.ibb.co	145.239.131.60	true	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
messaging.office.com	unknown	unknown	false		high
c.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
skyapi.onedrive.live.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
p.sfx.ms	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false		unknown
spoprod-a.akamaihd.net	unknown	unknown	false		high
www.onenote.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/redir?resid=6060782D2B8D50A6%21129&authkey=%21ApbFYYOKMpcYgog&page=View&wd=target%28Quick%20Notes.one%7C9d63e26b-8e15-4b90-a730-077581269bde%2FEnvironmental%20Fluids%7C74fd9e3e-3791-42d6-9ff6-6a7ed758b675%2F%29	false		high
http://https://gabby-gratis-tarascosaurus.glitch.me/wein.html	false		high
http://https://onedrive.live.com/view.aspx?resid=6060782D2B8D50A6!129&ithint=onenote%2c&authkey=!ApbFYYOKMpcYgog	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.5.55.81	gabby-gratis-tarascosaurus.glitch.me	United States		14618	AMAZON-AESUS	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
145.239.131.60	i.ibb.co	France		16276	OVHFR	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
13.107.42.12	1drv.ms	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
13.104.158.180	i-am3p-cor006.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.104.208.160	i-db3p-cor005.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.163	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
18.196.58.60	linkprotect.cudasvc.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458823
Start date:	03.08.2021
Start time:	19:21:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs!BKZQjSsteGBggQGWxWGDijKXGIKI%3fe%3dYSYU1OrRbk-OgIBVwfjzEw%26at%3d9&c=E,1,kIuIGEH799izsJ8ZzgEzo4vQsPME7QtXgthIwQx0qxxoPwhTl2ujgDMlbeQxn4ZdZQB-OFmNbdIvk9f4X00Afp0hXBwXDa-unMy-xntb&typo=1
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:	17
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:	mal56.phis.win@33/293@27/17
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://gabby-gratis-tarascosaurus.glitch.me/wein.html

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:23:18	API Interceptor	2x 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:\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):	122040
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGm
MD5:	516136E560C1392A28EDFA1A957050D7
SHA1:	BBDF208E48EFC052D332255EF84184BFC946BF5F
SHA-256:	4F812F7C8163C50FE75F441AC6797E18D02B8B66895BC94D0E1153FE24FADEFE
SHA-512:	8F25750E9014F7576E5C81E1A3DE605BB29839A38F0E60D58AB79E034ED1847D9E88A427A834BCA95BF7C4627197AC1194D5A487E0D5E5F88B95E46C4574A425
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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.157610353092084
Encrypted:	false
SSDEEP:	12:I5kPlE99SNxAhUe0ew5kPlE99SNxAhUe0et:I5kPcUQUfew5kPcUQUfet
MD5:	DCA7DA942510315AD32D003D6282E191
SHA1:	A130CB2FD96793F509401D2039F967FD2A739E1E
SHA-256:	A2AAD0F0148909C6D2C319BE7E7E314338DBA0E57EF6ABB8EC9C3C33985FADB4
SHA-512:	F49B3820EEE8D20EAEDA0BD6C2C33446024B9BFD40EBB90DDB916B1E34DE605DC4D73F77745AAA421B61A97C7905AF76B362BFE1C2DDE0A2B675D6F7D6A6E308
Malicious:	false
Reputation:	low
Preview:	p..... .....qK.@....(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....R....(..... .....T'._.....$.....\...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\20bcb68b-3340-487f-a994-6e6013be61e8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7502012165145016
Encrypted:	false
SSDEEP:	384:NnWdlbAaTYNVDVMXCXRAN/JrXqv/Nv3uB/KHLGGXS1rQTp1xuvnXbWrEFmlyl1Qx:tKWBlqz6SgerJfj4nrWbKdDZJj
MD5:	7E24762D877A0A1B217345D68B6267D8
SHA1:	6D0A86D9F89CC7EE4B7E90194A68263E4579310C
SHA-256:	E0528956E206CEC9202FB9F62DE70D6D613D1133B7AB8D6F69EADA52EF8238EE
SHA-512:	9C3874641F84257CA250AC07BDD6BE320A96283D0C34FEBD2A1344EE55961E44448F6CA2CC3DF92CA9CCF024FB513F952053B30872837C354994440459F49BAA
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\5da72804-b830-4f10-ba4e-c2ca5b197a45.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):	174469
Entropy (8bit):	6.079656246861076
Encrypted:	false
SSDEEP:	3072:NK9GaYTJQE+mugy9+QV1T7IRwdfLSNPGFcbXafIB0u1GOJmA3iuR/:A4xaV+QfT7GSmhMaqfIlUOoSiuR/
MD5:	073FD0C2EB14F7565AF22BBD430C93F5
SHA1:	6892787F5DB318904484055ADAFC7AA6F2062421
SHA-256:	6C3EED2A1154F7F5692B89BFA51E42F781FCD60788A956190E76B48241074911
SHA-512:	01EEC71B6148BF0FBA28C9105773101D07BE479B7C3A76D11B14ACA831EFD1221C8AD8E9ACB2A61D85EB326DE3531B0126F9D11C1495589589DEB629DF320EI7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.6280113695865e+12,"network":1.628011371e+12,"ticks":5032300437.0,"uncertainty":4530891.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6811ed3f-5d46-464a-8a78-76faacf528bd.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):	174469
Entropy (8bit):	6.079656818900088

C:\Users\user\AppData\Local\Google\Chrome\User Data\6811ed3f-5d46-464a-8a78-76faacf528bd.tmp	
Encrypted:	false
SSDEEP:	3072:NuSGaYTJQE+mugy9+QV1T7IRwdfLSNPGFcbXafIB0u1GOJmA3iuR/:0HxaV+QfT7GSmhMaqfIlUOoSiuR/
MD5:	F9876DBD4D073D0D76AE9BCD519E6EEF
SHA1:	48682768D2C7F92BC7BAFE9C06482B486A034209
SHA-256:	EAC1885619AA8AD678E31EB5E255C5D2D23382A3E277543DAD591D671101D37F
SHA-512:	DE67FC88E5DC0FFF61C0ABDA490F1D29FA60D3342B28E29B52131AB5C5ABB8BF56FFD43DEF9DE59DDE6BE9D6EB7852D54AC3B440277D8CDF9823C33818B4A0D1
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.6280113695865e+12,"network":1.628011371e+12,"ticks":5032300437.0,"uncertainty":4530891.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d075f6d-1af8-4feb-89b6-470ecb72ceee.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):	166011
Entropy (8bit):	6.050195054947153
Encrypted:	false
SSDEEP:	3072:KYGaYTJQE+mugy9+QV1T7IRwdfLSNPGFcbXafIB0u1GOJmA3iuR/:OxaV+QfT7GSmhMaqfIlUOoSiuR/
MD5:	8AEF41020D42DCF014891D5763B1601B
SHA1:	C983E91675194087DC5E07B133D54F79635D90D2
SHA-256:	35809E7A1B35EFF6726C5F8773C1FD838F079931E8752EEB42D405EBB101D52E
SHA-512:	09AE658E667054225A3389E13EC683DE83B29BE373A4A1532F0C723FC349186044C6E645175B8CE0542AB6ECFFCAE049FE0C3634E6DAE8CB7C906B6A513EAEDA
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.6280113695865e+12,"network":1.628011371e+12,"ticks":5032300437.0,"uncertainty":4530891.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715955758"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\7702be74-bba3-48e6-8a44-8faf509af6fb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749551965972552
Encrypted:	false
SSDEEP:	384:DnWdlbAavNVlCXRAN/JrXqv/Nv3uB/KHLGGXS1rQTp1xuvnXbWrEFmlyl1QvRxp1:qWBlqz6SgerJfj4nrWbKdDZJd
MD5:	4A27E33BEE11C178D3332548350FD775
SHA1:	91C41C0683B85ECD264ACB767F5BAFCD7CD7903D
SHA-256:	F911DE7EC335FBCE44605169125DBB4F7D9F5AF253041052933D21ECE5E053F1
SHA-512:	2448AA9C89DD86A3AB0B6990235196785AFDAACC6CCCAB824D4C7351802C802F4D3641C41428A5D56AFEDA5CA47F428981575539C5CFEA292959F9552644DB9
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....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\77c8dfa8-68fb-4118-ac78-3e75947a034b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.749805335732858
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\77c8dfa8-68fb-4118-ac78-3e75947a034b.tmp

SSDEEP:	384:9nWdlbAaTYNVDVMXCXRAN/JrXqv/Nv3uB/KHLGGXS1rQTp1xuvnXbWrEFmlygS1i:9KWBlqzoSgerJfj4nrWbKdDZJv
MD5:	73890879BF7B96D4009BFE3C9544E5E0
SHA1:	8B199FE70CDAB6530E5E6E9F581A514C8E70F252
SHA-256:	62B85A96DD5E66DC6605158F1E4D9069CB5258FFE6630E85AB24EC87EE05E8D9
SHA-512:	1F7EAE06571DEF3DC77855167322A5B7F0BE8169460ABC84C370F31496AA8C2429E98067D5993F474B7C6840097A1D504FCABFDC0EE0BFA5F9B3DD6288950BB
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\89aa96a9-db20-48aa-9f45-a39e4c428029.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):	174469
Entropy (8bit):	6.079657826140563
Encrypted:	false
SSDEEP:	3072:gTeGaYTJQE+mugy9+QV1T7IRwdfLSNPGFcbXafIB0u1GOJmA3iuR/:YTxaV+QfT7GSmhMaqfIlUOoSiuR/
MD5:	0E4900927263A39F8155B24E3BA3837D
SHA1:	6978C33269317A3CA9FF7055F85E587703EF9E6F
SHA-256:	2402ACE199CE7145DA23DA31EE6B29895E14BB8007DC376DF3752FBDBBCBFE28
SHA-512:	909FB88A8233C173A57D0A5DC290377CB65ECB59EE0E132C12DD62AC7DB29E085904EB053126EBDAF2EC8388CE098CADD57A8B911A86EBC0931FA19EA7318CF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.6280113695865e+12,"network":1.628011371e+12,"ticks":5032300437.0,"uncertainty":4530891.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715955758"},"plugins":{"metadata":{"adobe-flash-player":{"di

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:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d3a3581-d5ef-44b4-8919-d3347e9209a7.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):	2878
Entropy (8bit):	5.595385191664325
Encrypted:	false
SSDEEP:	48:YBU9uUFUjKUVU5Im6UUhhUygM/U8JU0/U1KUeiw6UcYqPeUekUeaUhwUkvUeP:oU9uUFUjKUVUK7UUbU+/U8JU0/U1KUzy
MD5:	C153B1A084CF1CB668B266CD7E540882
SHA1:	765A4FFB219124434C9F87B1A14684AE177A7F43
SHA-256:	358E9A17A7CC8EDB3C1BAC38432FF1C5388E683565A61F4620FB44D4677A3949

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d3a3581-d5ef-44b4-8919-d3347e9209a7.tmp	
SHA-512:	5FAD3BEE347C2272DB613392C08A508FA8062611117489C529273515BC840798B426FB0BF8217CE97468007E921DF29DDF51F39952D56310222E928B9D1F6F05
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659547371.762355,"host":"CDbqhc2H3cirAeTI0h5kB8Yesl71fzdHWo+30538LcU=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.762364},{"expiry":1659547386.188435,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011386.188444},{"expiry":1659547385.434081,"host":"G7aWUbdedtpS5PKCyHhVr4JB2CPejwlLqcs6cy4CxdQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011385.434088},{"expiry":1643563385.859086,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011385.85909},{"expiry":1659547387.125457,"host":"NRbo+SJrMiydIRb8dNqQFXJu7cvIkr1nN8dDkqo4V0g=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011387.125465},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1cf82c7a-aa3f-4088-a7d0-3c4a63f4be82.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):	3212
Entropy (8bit):	5.5926789956348895
Encrypted:	false
SSDEEP:	96:oU9uUFUjKUVUK7UUbU+/U8eUmTUR/UzKUD6UcHPeU3U/UCUkOYUDUg:oU9uUFUmUVUEUUbUCU1UuUR/UzKUD6UM
MD5:	59170E79C1B3888655AC8D4975F34BFF
SHA1:	50905FF4FED72F81C3DD566AB5E4B1D5B818A8B8
SHA-256:	14D477FB15AB6670DC2F1CB4F9F249FC4D1489A56E0830F6FCC7FF3E63134300
SHA-512:	FC4034B95B555A46A96D628C8BEB206074EE7FB8D4206049A3CA9826EA5775B69B0D531B94B14BBDC092525180017FBCBDF4CA5ECE242A9092CEC540C740AAC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659547371.762355,"host":"CDbqhc2H3cirAeTI0h5kB8Yesl71fzdHWo+30538LcU=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.762364},{"expiry":1659547386.188435,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011386.188444},{"expiry":1659547385.434081,"host":"G7aWUbdedtpS5PKCyHhVr4JB2CPejwlLqcs6cy4CxdQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011385.434088},{"expiry":1643563385.859086,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011385.85909},{"expiry":1659547387.125457,"host":"NRbo+SJrMiydIRb8dNqQFXJu7cvIkr1nN8dDkqo4V0g=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011387.125465},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f9c4a1d-fd8d-4632-82d8-6476bc2a37b3.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):	3381
Entropy (8bit):	5.592944166888457
Encrypted:	false
SSDEEP:	96:oUPUjuUFUjKUVUK7UUbU+/U8eUmTU+/UZKUD6UcHPeU3U/UCUkHYU5Ug:oUPUjuUFUmUVUEUUbUCU1UuU+/UZKUDT
MD5:	C9386966815CED20D1F75900C2B3BFD9
SHA1:	921CA5460023FC3422AC4BFB027C41A32F72F2E6
SHA-256:	D0E2E68509AFF7AADE8F6C9D6EBCF0E12903D77F95811B0C238306FB1EEE5F59
SHA-512:	B025EDF0FE0B6F168395EFD3D246152CE6318E1DEB76BBCD2B72CF19234AD037FC5AE8252857E0BD2496421611EED31A2D45E30CE67849AC8D6837D937374B89
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659547371.762355,"host":"CDbqhc2H3cirAeTI0h5kB8Yesl71fzdHWo+30538LcU=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.762364},{"expiry":1643791459.304645,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011459.304649},{"expiry":1659547386.188435,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011386.188444},{"expiry":1659547385.434081,"host":"G7aWUbdedtpS5PKCyHhVr4JB2CPejwlLqcs6cy4CxdQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011385.434088},{"expiry":1643563385.859086,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011385.85909},{"expiry":1659547387.125457,"host":"NRbo+SJrMiydIRb8dNqQFXJu7cvIkr1nN8dDkqo4V0g=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\344f6f6c-7377-4fd2-b848-6fcd12d16364.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):	5155
Entropy (8bit):	4.964110660285545
Encrypted:	false
SSDEEP:	48:YcWkKSChkliLqAOqqTlYGlQKHoTw0xfrf4MqM8C1Nfct/9BhUJo3KhmeSnpdkCJC:neLkt9pIKIX5k0JCKL8dkC1CbOTlVuHn
MD5:	F5663805302F954FC66A0274C3729181
SHA1:	1890BDE70D02C6CD6DE750FD94DDF25EA258BD6A
SHA-256:	FB36BFE713E20C391B210ABA103F979F940D16FC4FF32648CF7C5DA23260B1B7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\344f6f6c-7377-4fd2-b848-6fcd12d16364.tmp	
SHA-512:	ED8DF89A2FC26BEDBEEE17FDA8D7E047CC1E3E1536A85B78CCC0656C8FD0110209C2D8BEE229096A61B339FBDE72E962E1447C03210246E27773A88E0052ED AC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272484965225921","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\369afe18-7081-438f-a949-13fa88a89e46.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):	3380
Entropy (8bit):	5.592424558401295
Encrypted:	false
SSDEEP:	96:oUPUjuUFUjKUVUK7UUbU+/U8eUmTUH/UpKUD6UcHPeU3U/UCUkHYU5Ug:oUPUjuUFUmUVUEUUbUCU1UuUH/UpKUDT
MD5:	56FC3AC42F910BBA6CC476A9884A25D2
SHA1:	EFCD6B0556DC63245075BFDFE2D4101AE29FE127
SHA-256:	5C11CE0F9760F34518E938CCCB3156F49233243C4503E4A0163C6BF26BF46AF3
SHA-512:	F0700169C73764409513DF05049825B5BA650B207101A7995B8D909F7C0A16059DE267ACEACE2710786833620E6C834B183FE313A906DAC352B6FE5806E7AD7E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659547371.762355,"host":"CDbqhc2H3cirAeTI0h5kB8Yesl71fzdHWo+30538LcU=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.762364},{"expiry":1643791459.304645,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011459.304649},{"expiry":1659547386.188435,"host":"GEcuSqu7rlPobX764M1CaiPUB2cMfcpAYaTr+jU1RL8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011386.188444},{"expiry":1659547385.434081,"host":"G7aWUbdedtpS5PKCyHhVr4JB2CPejwlLqcs6cy4CxdQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011385.434088},{"expiry":1643563385.859086,"host":"J1vb45Jgq2/qjkWZwNbKgaUpoBQP5P5rX+6N7h9uDfA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011385.85909},{"expiry":1659547387.125457,"host":"NRbo+SJrMiydIRb8dNqQFXJu7cvIkr1nN8dDkqo4V0g=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\479f65b0-35c4-43e7-8318-677ae5b8f6c3.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):	5182
Entropy (8bit):	4.968390924028951
Encrypted:	false
SSDEEP:	48:YcWkKSChkliGqAzqqTlYGlQKHoTw0xfrf4MqM8C1Nfct/9BhUJo3KhmeSnpdkCJC:neLRY9pIKIX5k0JCKL8dkC1CbOTlVuHn
MD5:	141947653DB362389494784C374C9470
SHA1:	3678FC8C6BA98EA3666E1155179238A4C64F80F1
SHA-256:	2F11D528A0B43145DF3FFF934BD874F77E906DA947B2BDB3968CEE29EC28984B
SHA-512:	35746145FCD6C80879FE3274FE75478165B3D7F56EFED80A44821BC9EDD529796BEC252B4C991834AC775C2129AE02F8D8E14DDC1BCDFACE014E54F18345291
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272484965225921","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ffd6cb0-83ee-4e3c-ac4e-e22d8f244003.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ffd6cb0-83ee-4e3c-ac4e-e22d8f244003.tmp	
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6626180b-7833-4d04-b249-920feee1c2eb.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):	2043
Entropy (8bit):	5.593424356383935
Encrypted:	false
SSDEEP:	48:YBUd6UUhXM/U8JUi/UIzKUeizUmqPeUekUez8UjwUkvUeP:oUUUm/U8JUi/U+KUzzUdPeU3UvUMUkV
MD5:	44E336168A5F0B456B29D8EE2BC35420
SHA1:	0A8C376A4DAA8E07EC620B0A5D764AF7E8C74F12
SHA-256:	8880940F853A8A9DC119BE53109ADE6C1044BE41855D5FD7F5FC53AD07380ACF
SHA-512:	7E2A7652FAFFC389FC08707571728DC34E4C40DCAF1C068581BB44043B4ED9C60A80CFE936AD0B09C7018F8C28DFF8D30F59BC6A447DBFF121A3D42485C6B83
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659547371.762355,"host":"CDbqhc2H3cirAeTI0h5kB8Yesl71fzdHWo+30538LcU=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.762364},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659547371.891539,"host":"PWduskw9l7J4Ttt+vSPfdOVvFQ7WN4xbyVQbOaNDDMo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628011371.891545},{"expiry":1659547375.826753,"host":"UC8KSSoxALrqlAJ4GA/7FO3WXVKBL6nRFgmbn2hJGnU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011375.826757},{"expiry":1659547379.210549,"host":"ZIz0zb+i5Se5XnPvjxPYwp2SBUcMbD6XG74Xe1kw2KE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628011379.210554},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c00b008-59f7-4fd7-b768-8e3c8817d41d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5778
Entropy (8bit):	5.177941497783885
Encrypted:	false
SSDEEP:	96:neLvY9iqCxJS4hIKIX5k0JCKL8dkC1CbOTlVuHn:neLA9iqC/vI5h4KckCk
MD5:	D8A14E78AE03CBDD21C012E9BBF445DC
SHA1:	F2EFB3E8B43FC151E3B9C0FD0127492F6982BF1D
SHA-256:	D2C985405C4110F9BA0D989D726E7FAE33ED15F8C54E852EC7D493CE23E08CCA
SHA-512:	8E85F9141538D96E812A12B73C5D0B18373FBCFAFE23E4457A81649F177D42E384BB08D8F4E28152AF1D68FE6529BEE4B313744C085690EB05247DBB3430A468
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272484965225921","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c732de1-07e4-4854-b33e-45925f7fd22d.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):	5839
Entropy (8bit):	5.177458470633795
Encrypted:	false
SSDEEP:	96:neL/3Y9iqCxJS4hIKI95k0JCKL8dkC1qbOTlVuHn:neL/o9iqC/vIXh4KckC4
MD5:	8744FBE48314A5F69C47DD719BA502C1
SHA1:	84FCCBDD24391A9A9618986077484FCD96D2DAF7
SHA-256:	4A27F2F76978362696E6673AF1079B357F38731C7109C0F50FB865EE14C7C1AD
SHA-512:	A5D7AA91BA8DCF81C67D1555928028B9FCFA64FABD717889B811FC40B24716FBA9409166DD1F59E1EF1E61DD864304E4BB66AD19B786F4D52066C3EC74D2EA6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c732de1-07e4-4854-b33e-45925f7fd22d.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272484965225921","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al
l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_d
efault_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_rig
ht":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"
,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\87973641-dfe5-478e-89b4-a47e807cb30c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low

Preview:

{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":
[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660
7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"adverti
sed_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","s
upports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{
"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9481541f-99ba-4ae2-aa24-b0f51ab7a260.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):	5814
Entropy (8bit):	5.175656797344366
Encrypted:	false
SSDEEP:	96:neL/gY9iqCxJS4hIKI95k0JCKL8dkC1CbOTlVuHn:neL/Z9iqC/vIXh4KckCk
MD5:	E127BCB415645CC9DD2EFD7EA59E5BE1
SHA1:	5C5D51E648C2FAD1389CD72EF5F32D9E363E5D62
SHA-256:	2B896AD265A04D73375E6098CB2FA5217CEA6C6A84894FE41A3917AE91F896C3
SHA-512:	00BE74A367DCBA9048FDAA475E04E77586B42222C3F599B11F315443130A15AB3698D55A91F4EAFC33387B8ED4EFF435F2094AD4B956EE40A173E822BA172087
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272484965225921","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al
l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_d
efault_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_rig
ht":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"
,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.192270129839362
Encrypted:	false
SSDEEP:	6:meTNIq2Pwkn23iKKdK9RXXTZIFUtpHTrAVFZZmwPHTVkwOwkn23iKKdK9RXX5LJ:XBIvYf5Kk7XT2FUtpHAX/PH55Jf5Kk73
MD5:	63DF85619E13AF185BF8BD0308E6C565
SHA1:	7B78CFF41A20AEAF52F49FEEC3051EA8B923E87F
SHA-256:	2207098AEDB0CE998262B7DAE753D0227A91B1C876ECC4EFA681318F4820DE6F
SHA-512:	1315CBB51B5E6F75E561BE7C36F5325A8CC5854BF37A76ACF8650C075D46A4DFE9A21DB40462485AA90FE6DDA5A84D985C1FAFFB8CFD5F944C85B9EC124239 5
Malicious:	false
Reputation:	low

Preview:

2021/08/03-19:23:06.890 15e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/
08/03-19:23:06.895 15e0 Recovering log #3.2021/08/03-19:23:06.898 15e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik
eDatabase/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.oldNT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.192270129839362
Encrypted:	false
SSDEEP:	6:meTNIq2Pwkn23iKKdK9RXXTZIFUtpHTrAVFZZmwPHTVkwOwkn23iKKdK9RXX5LJ:XBIvYf5Kk7XT2FUtpHAX/PH55Jf5Kk73
MD5:	63DF85619E13AF185BF8BD0308E6C565
SHA1:	7B78CFF41A20AEAF52F49FEEC3051EA8B923E87F
SHA-256:	2207098AEDB0CE998262B7DAE753D0227A91B1C876ECC4EFA681318F4820DE6F
SHA-512:	1315CBB51B5E6F75E561BE7C36F5325A8CC5854BF37A76ACF8650C075D46A4DFE9A21DB40462485AA90FE6DDA5A84D985C1FAFFB8CFD5F944C85B9EC1242395
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:23:06.890 15e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-19:23:06.895 15e0 Recovering log #3.2021/08/03-19:23:06.898 15e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.169307915817593
Encrypted:	false
SSDEEP:	6:meTLVq2Pwkn23iKKdKyDZIFUtpHTwU+gZmwPHTzSIkwOwkn23iKKdKyJLJ:XlvYf5Kk02FUtpHV/PH15Jf5KkWJ
MD5:	B3399DD1142E8269BA9D8F8AC9C0C2E8
SHA1:	E7A6D48D7403F1CA8BCB653F94BEC20EF80743DF
SHA-256:	16D1A57F93E24D99CF0699D94EC957B30A43FADD7BACB122323A4AEE82C5A978
SHA-512:	0B71900EE1BC1F06D55029663D4E2A9F4F3DC327E325574C596951FDAE636AAC1D5BE0D4DAE440A03AB928980047B34079649FC88D65AF63B2AB55D816A7F4A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:23:06.886 1860 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-19:23:06.889 1860 Recovering log #3.2021/08/03-19:23:06.890 1860 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.e (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.169307915817593
Encrypted:	false
SSDEEP:	6:meTLVq2Pwkn23iKKdKyDZIFUtpHTwU+gZmwPHTzSIkwOwkn23iKKdKyJLJ:XlvYf5Kk02FUtpHV/PH15Jf5KkWJ
MD5:	B3399DD1142E8269BA9D8F8AC9C0C2E8
SHA1:	E7A6D48D7403F1CA8BCB653F94BEC20EF80743DF
SHA-256:	16D1A57F93E24D99CF0699D94EC957B30A43FADD7BACB122323A4AEE82C5A978
SHA-512:	0B71900EE1BC1F06D55029663D4E2A9F4F3DC327E325574C596951FDAE636AAC1D5BE0D4DAE440A03AB928980047B34079649FC88D65AF63B2AB55D816A7F4A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:23:06.886 1860 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-19:23:06.889 1860 Recovering log #3.2021/08/03-19:23:06.890 1860 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\037a117947eadf82_0	
Entropy (8bit):	5.551521547648658
Encrypted:	false
SSDEEP:	6:mQnYEYpRlM9V6EzUiIaCuejamJv6gX382oE7Fk4jgDK6t:dDY/lOIiIaOjjFHoE7Fkp1
MD5:	C0279BF2463CCCA131F006A8C4C69C87
SHA1:	7B3B90930572F3DDDB4EEE9289AE6B3FB0937536
SHA-256:	991F37E7E58AD68540E71520374270F9E1B1452C3563F20CCF2F06647B1BEBCB
SHA-512:	01A76494E4F5CF8250C57BF59FE1A0B6DD2443818D0D30487D4FBDA618EA5C51467B2C0D721B8227BC58F87C586076873A0BF3DB45F3D851C7E6C9135E48780
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/..8A'/.....C0.....h!.0.f &e...M.$...;Y.U.A..Eo.....1.....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):	5.536782923100549
Encrypted:	false
SSDEEP:	6:mwPYEYpRlM9V6YWWWeueDFCKlAjl/eesi4AZK6t:1bY/lytjpSrPT
MD5:	0D17D14A7DD346ECFDBAF01EFD6944A4
SHA1:	502020C10A65B37BC004BB59EF510B02C0C9BCAF
SHA-256:	3556EB0152AB8A98801746C09FFDF0271173CB65AAB67409DEF25A7332E477AF
SHA-512:	09C26C3D3A0CF2E4194C9E71D7AB5B2BEE09F23470D60FA257DA1270C553E993BBE4EFBC414E645B6C378890E2C46C2BAC9B9D02E9BA092E33050E66F9FCB0 E4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....X,....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/LearningTools/LearningTools.js .https://onenote.com/x=.8A'/.....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):	5.581464609500177
Encrypted:	false
SSDEEP:	6:mUDPYxPEWg7450NdNbaXEmGhQv0u66nxnK6t:nIEWg7MUdJXrGv0Op
MD5:	81963F2F265F85738179485FAF8E5EF5
SHA1:	96C84918BD9EBD28C9494A62623339C2BA9423FB
SHA-256:	6B89E3004624153389AAAD8276CE531B6E3B06D7C8EBC0EB066D0D14CDD54889
SHA-512:	D4B662842B8F25418172E7566AEF943DF391EDFE1CD71C14C102A0B8A40523B47AD9800FC1D481DC82431FFDD1DE14AB71AE743E75A2A5121A63532B61E56F1
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/.~Q8A'/.....Y...8.a.kC..-@.....w.- |...p.A..Eo.....pa.....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):	5.542502625858814
Encrypted:	false
SSDEEP:	6:mpNYxPEP9NUAFndQ16wggulgvfqzrFcalhK6t:KiEPUAFndgxgguOvWKal7
MD5:	0C3E7213C8D066F467EF11DCA1755035
SHA1:	55722EC3227B76EA5C85B456124953332A79FF1C
SHA-256:	72F6323D80B4363DEC6C6E770E502436F785B5F59D3B3E749CC5ABBD6CF9DAEB
SHA-512:	2258B8244222C69CF2947E334F5F533E958F175E0FA00BBC462C2D591A8D159D6BC2A499D109FA95FCE9074D5ACD97230EE7DB4FECE7B72E9522CB7E9F3A913 B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bb91d310fc8f48c_0	
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/...8A'/.....-l..).=Cs_.... . ...A.....A..Eo.....x.C.....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):	5.663836821643476
Encrypted:	false
SSDEEP:	6:mkRPYxPEP9NQo0eAMdj6ZgIubRO6bsrGRK6t:4EPRdiURO6bsSr
MD5:	DACC85D4F44B3ED3FBDCAE9077E318B7
SHA1:	F8539D5D2B6C0190492B750D90127F115C95C801
SHA-256:	CB0764A9822E4C9FE07F44BFB478FD8C466AFFC5320AB2264002FFBE113CB774
SHA-512:	2B2ADC5583CA019317C34D71744C34CEC4C69F157AF524EB65C1DE85A2F60280CE4924BB511196061913EF738BBC1549F855989D38C3DF4EA06BD558902A87B
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/...8A'/.....;.....N0.. L.>..M.KDPHW.....&...A..Eo.....(C.d.....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):	5.566914516521525
Encrypted:	false
SSDEEP:	6:mYPYxPEP9NQo0ClJSnNdd6KlAuK5zmrWAkK6t:aEPoddzHKxtR
MD5:	0DB43E095E5DF7F7F8BF7BB1E50CFC1E
SHA1:	9B42F5CF545A672037311F9A212E040393D6B52D
SHA-256:	50FDE2979B4C8BE4C0BF4CF0717F681FE658C953185D00E16A46981662DA0C7E
SHA-512:	EA043955D90E59B6F25CF1A961C2F455D37EFFFC7639743B6378D2D465D9214BE0FC030FBAB292444458F528A73E83EF61A953B6231F4E5A28618C192146BE8B
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/J..8A'/..... .....e....Rh../.F.zoL...e..TgE..Y..u.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12be61d7f6fe1090_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.595981146392751
Encrypted:	false
SSDEEP:	6:mpnYxPEP9NYmFPMduDK+pE/5JJZBec2/F0K6t:ZEP1PMdaq/55Bec29G
MD5:	659CC6A140060B43BF5C3B2050D66F62
SHA1:	E1B908645E7A5E6BC4D279AE6662E2C8002BC8B6
SHA-256:	5394A6B61D0832C2777099DD79255B12D731EBD4176B2F6BD5DC158A1F43E6EA
SHA-512:	249447BB5178E4006601FD29069AE68BF2594A57866946F7278461D7FA5493541783A589C6B7E76554FCCBD300F909D8BD3FB56FBFAEFDCD96CC1CDD6426D15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/uiSlice20.min.js .https://live.com/...8A'/.....xa.#.\.;.P*V.i.&..?..M*.....A. .Eo.....8wC.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\161fd244fa689573_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	5.596985346063187
Encrypted:	false
SSDEEP:	6:m/EYgcOEo0wUZAoz8pMdlr1UgtTcMYYzK4bfBDK6t:VcVwmJdlrmFMYYz/
MD5:	F65E7265995E6523064BD96AA4B5F103

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\161fd244fa689573_0	
SHA1:	E7BC54C45E8102AABEDDF5DA53F0C90DCF9199EC
SHA-256:	63A3FC6E8A81B98AE7695A160F1972382BA1309526DF406979E4E8991613DE7A
SHA-512:	87185E792CD18F43BC0BFB88B12769BA837F1CE4EA3BC56C46F7983D0FD93C3708A6BCCE33C6D9511B98F1FA0EEF8594DE01BD5F67BF9621228EFD8A00C2343
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~....e.&...._keyhttps://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20210614.002/wac1-cdc297b4.js .https://live.com/...8A'/.....NU{.n.f...C').....CN.'..Y.c...A..Eo.....iA.X.....A..Eo.....

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):	5.640608638910603
Encrypted:	false
SSDEEP:	6:mayYxPESQ4dedtA3Qe8okr56N9hnBohZK6t:PnEH4dedCFuYQp
MD5:	A2E49D4C068091EC78AF8F856C9B80BD
SHA1:	ECA094F73CD1B9340D1DA908BBEF2E3AEF1FA575
SHA-256:	786838346C392DBC7A0A07B56263250A6EF321644288D9374E7365A0F656989B
SHA-512:	677323826A8F467D251497990293FCB7C3997C93B0295AE5A1787A991399315F7C484754B0A8E5A3C8CBCE74466C241BE2141BA9559147F859D924380BFC657B
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/._Q8A'/.....u..*\...A.<U..0z4E..F...'$b.A..Eo.....(,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a7750ff440fe8cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.623450106378633
Encrypted:	false
SSDEEP:	3:m+lnZK8RzYFLlpELpDc9zuVHFZSRzTJjgVlHCG/PmpHlir3KGu9hm5mfA/lpK5kt:mQYxPELpD6aHFsNdj1GGLir14fAbK6t
MD5:	486F740AA29E15E1A5646CA4BA3A55AE
SHA1:	295F6501A317C522D2D69B278F2BBB16B208F0EB
SHA-256:	312B5291F44917127EC9F04BA1CC060BC3DDEA6ACF2DAF3E108EB3B32122105B
SHA-512:	C453839545B23B5A9C70FD5B820F32E130CE5580B97B31453D1E0F5BC39EE4F00F7735348D65ED0B9F628C91EA13A1D1CE63189D57E2BB6ACB5C65E789238CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o.....z...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h47F4322F99F46093_App_Scripts/2057/WoncaIntl.js .https://live.com/.EQ8A'/.....W.....m...CpM..T.@..]..{.X.s@~.:*/cT..A..Eo.....N.0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b3e5202d92bd1be_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.573590923283803
Encrypted:	false
SSDEEP:	6:m/YxPEP9N5HYnJbx/UdtfptOYUaypK4HHXZK6t:LEPCPsdtXOYUak
MD5:	D181B373CDC6BDCBDC2F6B862628CF3D
SHA1:	40A6945932EBAFA259E976DEED6582BE0D7E393A
SHA-256:	F417F2F23F6F6A8A2BE4490AAF1414D8AB3D82DB78BB48128F6CEB1BFFD8D3DE
SHA-512:	2C11CB6012022A63313CD3BE28906FDBD570D3C437EF089848A6628348F9181C1E8A313F54FA98260E14424E1F75046B0CFDFBE30A55954D88359DB3B65DCC99
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/onenote-intl-mlr.min.js .https://live.com/..x8A'/.....1m.....R...l...v...g.{...i.`.A..Eo.....i.bT.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\205ef0c584d89ac9_0	
Category:	dropped
Size (bytes):	267
Entropy (8bit):	5.629485972225043
Encrypted:	false
SSDEEP:	6:mF6YxPEP9N/+6MXqNdTJ6VClM0aPm4KthK6t:K/EP23qNd9+ClM3K1
MD5:	D3B0E29ED45F2E905C7A705DEC37EFEB
SHA1:	649637AC1912A01153E1B4B58A875C9B9AAC35B6
SHA-256:	89167145AD5724D621259B32100FDCAB31E9A8CB5D1193FC4A15F881E73EE0F4
SHA-512:	C70C7635822DD90732FE939648933E5FDA53B861F0E7B6E9B052AB995116EBFBA961C7E7C565961D14C67CB500FD0DD8755B8FD303B2A18D00D550638D990D6
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/.".8A'/.... .....:.p..Z3...m....^F..XG8.....es`..A..Eo.....A..Eo.....

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):	5.5680782055369615
Encrypted:	false
SSDEEP:	6:meWNXYxPEP9NiGvtdWNdI6qgdHJnBP/yP43hK6t:JWSEPhMdI4dj+U
MD5:	19EA2D8609B313D4255C82020BD67A5C
SHA1:	45612B88EF4A4090F86DB3339F3A3EB3BA29CA85
SHA-256:	82649549F4EED66FAF26436E20A5611C8C0B05F744E90CEF1C9C7F3214B7F0CC
SHA-512:	2413AAE369AE2FF52E9F54627C4DFAD0D8525B4667D7E360F6D49145964E048A488FF0A3C80EE23FC8E3BE00BC8C7D78130B996541A0DC38A1D7E40E41E4121
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/...8A'/.....FHO'...V.. ./.Rr.....B...'b..U....A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37c3c5f79988b064_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.770290677607059
Encrypted:	false
SSDEEP:	1536:K/duTT0Ps1dzkajN7KzWYj4xkAAd1sYohWOxt5VX58rjQ8p9G1qvSPf:zT0UQQ7vZk51s42t5l58AJ1qo
MD5:	0504585004D45DC52BC33066F83DB8BB
SHA1:	F3DFAC96E3D1F547B901A5E7A029B44B44FBB3A9
SHA-256:	CF0F245A6C94DE7599FA6ED4ACBEA5D03D219B9B2FF53BF63471CA17778D23EA
SHA-512:	703D6EEC3AF646B0BA1E622CC895B4E59277D14AA78DCECC929987D8F9FB9959D63553035E076AC1F461DE4C6CB1C55A05B71E40E588758BE4C4885B1D2B88 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...`.f.....4F0061FCE064B45CA8D32BFE49AB070E58A8808F491B78EED509DA584A35DA6A.....'.JN....O ....n..%.,[.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@zM.....module....Q.@.|t.....exports...Qc.....docume nt.(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.....QbBX.....d.....Qb.....e.....Qb..l|....f.....Qb...H....h.....S...QbR.....j.....Qb.....k.....Qb .Y.i....l.....Qb.|.....n.....Qb..^.....o.....QbVe,o....p.....Qb.....q.....Qb.`.....r.....Qbv.:B....s.....R....Qb.....v.....Qb.p.t....w.....Qb...5....x.....Qb.}.....y....

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):	5.536738732913596
Encrypted:	false
SSDEEP:	6:mRYxPEP9NQo0g0fdn6olW8XxDGx9hyANEJhK6t:9EPhUdMWFGx9kXJ7
MD5:	E04142294AEE961A9479196FD9BDEAF3
SHA1:	348D92A17512C21BC509876B836CC39670D76103
SHA-256:	558D3E946FC5D47EFB6E0A7020E0ADBA5D5C2584B2676BD553C5E0D99D74D352

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e2045da28285ce5_0	
SHA-512:	EEA913C9AC4AB67E9D5ADC8CF402CB32A7ADAE1690A5EF0BC05A62050BEBD3696328E1312DD133A3B6299F01E4ADCAE2D81706DA5146388C1F55201ED5E91E8C
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/..8A'/.....H. ...nO.>'.}.>..}k/.Mp.l.-.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\45de7baa1e70f6fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.612760618112615
Encrypted:	false
SSDEEP:	6:m+SYxPEP9N5HYxEEXodHMdUK62z/kjVmsXYB4G/lbK6t:9EPCCE4dsdUM/Umsorr
MD5:	4E61098B7FB71B16A3B9A2DE606F88C2
SHA1:	6BCC99F21A1B7C2890F46E33F393EF1F92B4F4C6
SHA-256:	D4A5F8F84DD6D544EF33E7C4836371CA27AEB3A86244AA1CC13E09E450C4CBA5
SHA-512:	2910366C68A2392F97B1A0264620CFEEDEC0AAEE81F249A15058A0C4D46592A7F21C731578509307D32D9437F81D3943183C6B9DA3482A73C487D04E7FE4511B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....AQ...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/onenote-navpane-strings.min.js .https://live.com/.8A'/.....I.K.,C. ..w...c.. ..T&Slj...D.[.<.A..Eo.....R.....A..Eo.....

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):	5.597812383556646
Encrypted:	false
SSDEEP:	3:m+lsoV6A8RzYFLlpEPw0XdfqaR2FvDzTJAOkjlHC8cWSfd9/Om2ZxtpK5kt:mUSYxPEP9NCaRsdzySF9J+1K6t
MD5:	6536EC28901E80EB2A6659A0721FD864
SHA1:	1B9757EB768220AE2CE51A9EDA6F7C9ADB531CF9
SHA-256:	A31499F9766195788CEF2EFE17DD0A018E71EA9A4B0C86AF4CC75276DE680ADC
SHA-512:	FB0EE3C387DB82FBF5554C8346C78CB46F0391075450034EF37DFE6BFDAD02A6C68CF59176A17A49E40A2F8A017EE80A0DFA9DED53CA7FA4D835E6D3C5DCC90
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/...8A'/.....[ZJ.b.G.WJ.3G.C..8.].....|d..L.A..Eo..... ..P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\509916821a0fc2da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.517334878294109
Encrypted:	false
SSDEEP:	6:myqlnYxPEP9N5H2A4MIfdL15oltIznFOwzrahK6t:XqKEPUuAdLzoX0Fw
MD5:	8EC76E8E9727CC43EEBCA63B02FAAB96
SHA1:	7732D6344F109408B8E6B5318FD2BB2C916FB3BF
SHA-256:	FD1E6FBEEAB975876690F816E9AFED637F08140950877F9D243A551879BE17AC
SHA-512:	CB36407FE5642D2AA29C2DD8E355F47DD5A8E25FD6A9AD7DB260A20ABC5B5542790BA61B2A15FBC6C6270F61CF26A9095C05B2055179BE2D98514311193BDCF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....@...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/osfruntime_strings.js .https://live.com/.:.8A'/.....8...9...S.. n.....^w8P.c...5Z .A..Eo.....e.G.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\511f06892f5a721b_0	
Size (bytes):	229
Entropy (8bit):	5.378908129231829
Encrypted:	false
SSDEEP:	6:mz4PnYyeDM+uDCn6JoFVueIpoX2zqr4tbK6t:RPsM+uDG6JoF/l/XN
MD5:	18785F0C53980E760121E05C2AAE38C4
SHA1:	9FDBD18133B50C30287F559635B2D4190AFFEFAF
SHA-256:	AEC78ACFD691F84321B2BD9F49FD9F6D7C45B79C84216C8DFBF2136A60975525
SHA-512:	67D44E603708F34411575F33ECAC17B27EC413376978BEE86047CEA0E009E440E358B5820DCE19295DA2BDA3DACD12495A3E1AA1B9DA427212102740E2BC05C A
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/.t.8A'/.....^..... .....=i....}.Yo.F.....t.A..Eo..... k$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52f8f953e4a5a9ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.462357717140378
Encrypted:	false
SSDEEP:	3:m+ly0DlgOA8RzY6zKLEkKc3WRXEUXUgKWXET/uFvDOzqPCGLGo15lHCm/llhsbAc:m2DyEY68E9xEEUgLErksilubAt4jK6t
MD5:	AC2BF6063DEDCA9C3E8507CD3083FF66
SHA1:	FF62CF493FB5A8C917F1167C06EFAAC6749856F1
SHA-256:	38C92B3852E9758D2647FED026FF6E8C612FC05C6BB20C80D7C79D76DFDEA729
SHA-512:	678D7BB67ACE43D6AA426E19089F975E95307D3A353998961074FB799DF3C3499DCC58FAD6E38C10909ADD4433EAA7D3365530FAF95F9E2397D58C940C860E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://gabby-gratis-tarascosaurus.glitch.me/..@=A'/.....;.....}$=D./.:.. .6J...+tM.C.]..A0w....A..Eo.....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):	5.62434488263108
Encrypted:	false
SSDEEP:	3:m+lq0bs8RzYFLlpE/QAPklQIdFvDzTJpg1mh1lHCxhl/lN4yFGI3m2mJlXlpK5kt:mCb9YxPEYlrdpwmh6l/lWU/mBJlDK6t
MD5:	F12D4A51601B721DFAC0606BC93B9820
SHA1:	9877C2F3978FCF8FE1E1AD870AA5DEA6A50BFC85
SHA-256:	A9C1C0339E7A2BF21CC48406522DFA369927D406A67FEF617E3ABA1C7F56F9DD
SHA-512:	EE738F04AECA35B1BBD4514A3E26EADE8B842AA5750746FB155A4E22BAD8149755A825B04E260EB9CBEF1A643C2631F1ECA92B3A79582CBD2D7E7D9C092FD5 D5
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/.P8A'/.....2...7). ...a.F.s.]..?..h.3.....A..Eo.....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):	5.580809440544859
Encrypted:	false
SSDEEP:	6:m+hY5TYpQyCEP9NFBUKm2ndCcrywokAeK6t:JBpQLEPFfdbH
MD5:	30DE973626402D1F3C4A4010CAAC2940
SHA1:	BE34367F9A0FA588A481E8B41924865C763DE2ED
SHA-256:	C2D23C2AD1290FE66011D0FD65B4A1A04F90A98BC2F55A2270EC1FFBDD21F172
SHA-512:	663FD0E119A270556A30D43D5EE9A51D2E22120925C3AF4BFC46C5F3A590C79F5B6A0234DB6D6552525360DC646D543DCC8DB3FBE74CC1CBE8CE4495E80130 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\617f78aaa544a720_0	
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/X1.8A'/...../.}!)a...pgr....^a.=.q\.....A..Eo.....7.<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\69d491139461ce46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.587756711517315
Encrypted:	false
SSDEEP:	6:mq/VYxPEP9N5HYLKLxTLxMdDc/AQUdC//W4C//hK6t:16EPCLKdHxMddphT
MD5:	7D26A2D50EE2BB6450523A357D460E5F
SHA1:	04C0391CA1ACF02AC5CFB777DAB8E3CE47925E55
SHA-256:	3E236FF8497601871C1E33C02C83218DC993891555ED0B29D6B0C02BF8689DBA
SHA-512:	E8698373648E5FAAD1DFF687063D59779B09B2FB38C56BA88842DE2970791B17FEC53AE23467AA9903B0C20F2F92AE759AF1BFE47772EDB9A44BE0F8A48FFF2D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...}....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/onenote-ribbon-intl.min.js .https://live.com/..x8A'/...../....:...3.x.v.....1 ;.A..Eo.....z.....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):	5.594597419654928
Encrypted:	false
SSDEEP:	6:mxYxPEP9NaP6Vfdkl16OgltyttEvqArT4K6t:5EPnNdkl1cyttuzS
MD5:	C194046033B71BCBC02E211D2067B14D
SHA1:	F2C9793924E6DF6FD6F57FC2882A258629F0C35F
SHA-256:	39638BE414FE773460B3B195ABE21C8958FCEA58D8D1D001621F4E3959E59413
SHA-512:	C158EBB539CF80133999067C77E3F3C3D292F1E04A0743CD9B6F8222F38B4E96ABE0524EFEE6C9A2740478B5AE93C45CA35981FC72F844CDDB082DF939D92AE
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/E].8A'/.....<.....+.....!.....@...Z..W4.f.A..Eo.....a.....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):	5.4855485236550035
Encrypted:	false
SSDEEP:	6:m63zYEYpRlM9V60OZ8xCuepLJv6qX0onPUp06ZXlhK6t:hY/l5moRnvG02l7
MD5:	82E3D1AE4EC45443229F42BD176EB524
SHA1:	558A686C7FF26AC0D429AFF4B520C927F9A593DC
SHA-256:	1CC8C96699F0A3F5AA7A7F70C5B785A23D2B5A9E5C82E063928D016E5404DDCE
SHA-512:	17494CF12D900CCB4C7CE4FA5D102894FA933017EA6F98130C5F13D31068AC24AB5203FF5731E163EC1E7D647AA8494D8B20EB355F7FF4BCDDCF615F0D3F9C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/pickadate.min.js .https://onenote.com/..8A'/.....M.....K.Z..'.%.xQ.....VhA.g`..t.A..Eo.....H.Q.....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):	5.505273589302107
Encrypted:	false
SSDEEP:	6:m3kVYEYpRlM9V6ydueJe6XYrwX3w0+m4j7lZK6t:bNY/lGYg3B+mC71
MD5:	C3BDF51B333B1526AC5C3BAB1E2FC630

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6daa52f36522edb6_0	
SHA1:	7E1C2D11EDC0FB11F75A0C3F9333EA8826F919CD
SHA-256:	CDC25E78BC06669305E6E72DA6D8761CF6C696DE2800A03009CA2FA0E04D74AA
SHA-512:	D88967F174B5027E04CB14F939D0CD48DA28AC6293A241B948204D54668F2DD9FA3363BC1F34A0718D367DCB2435F84674F337B13BFA883BC5FCCD0F6B2F649
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...S....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/CommonDiagnostics.js .https://onenote.com/{..8A'/.....2.....:.....DZ.....V ..U....A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6fe11d08e6f3391d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.588951641155005
Encrypted:	false
SSDEEP:	6:mnYxPEP9N5HYLKLrMPlHdJYaA4z/iNa5+tRK6t:vEPCLKsPKdPz/iNayr
MD5:	F5BB34FC3F4A23425950A477C14EEDD6
SHA1:	C8AE5C3363960412DBD804C6795AADC9E23E855D
SHA-256:	A631277ABCC08A763BE12FC56CA25AD62AF6F931ABC706CD55880D9A7C8A1122
SHA-512:	CC1F0B1982C874F1866B35E62E9884BE7CBE8D0239B49C700239082A3AA8850285DABFD716C0C4BF581EB680F2B250CFBE3BBB5C428319B03DD32FCBEE4264 3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/onenote-ribbon-sprite-lazy.min.js .https://live.com/{.8A'/..... ..1~}^I....E../.{~...."....d.A..Eo.....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):	5.4626456886818415
Encrypted:	false
SSDEEP:	3:m+lUdGXa8RzYJb9yKIf8QPKxoULMIM/uFvDpueTJvkC+flHC6hf/zANqaRSeM9hz:mMYyK08fz1ueFvkrAnBR7M9hnJlDK6t
MD5:	A3EC00AC004460C30F24D84542EBE4E8
SHA1:	14682DD10C63F2592427E99727C725C40413161F
SHA-256:	6F03F21F42E281644C8408AAC5D6191EAD8B868D7500B4F86A4BC756ABD2696C
SHA-512:	AC9A00686B19C7759232AAC25A04CAFBABD2F638427B6CEEE12E65B4C97DEBD51AA6C1BC0C40F4643EA72344F64E2709768A6F74F36109CA91324781C4720BD 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....%...._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js .https://onenote.com/w..8A'/.....I.....Z.e...3]OO....B../...e..!.A..Eo.....<..X.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7531fee981b72877_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	5.910224750770822
Encrypted:	false
SSDEEP:	6:mOnYSHT8NWQAlKPUQydm11O9ySM+4V/bK6tRX2nzP+sZqSM+4/l:XFz8NWQCUUXmK5tk1r2yGti
MD5:	09ED298F13FD3E9E7D944E4FC59634FB
SHA1:	B336D6C3021AF2D9C73F50C33CF7A7934D728456
SHA-256:	F60381A85786A71A9A55638DE472BBB801BB6E2C123064048B8A42B3BC479E36
SHA-512:	5E27726DCFFB54484BF521B989E036FA901E05E301DDD0FAADACB11315016983FB1C176667F8FCB4CBC45FFFA988335028699FE6B689032B758C07FD19D6C97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....r....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://gabby-gratis-tarascosaurus.glitch.me/...9A'/....._6.....X.)....'.z.(..... .....r.Mm.A..Eo.....~.....A..Eo.....9A'/.Po..4F0061FCE064B45CA8D32BFE49AB070E58A8808F491B78EED509DA584A35DA6A....X.)....'.z.(.....r.Mm.A..E o.....t..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78bedd258028e0c4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78bedd258028e0c4_0	
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.581803579224367
Encrypted:	false
SSDEEP:	3:m+lsZ1T/gv8RzYFLlpEPw0XdGMGk6x/uFvDzTJHd+1lHCKgzEXkeUb8DGlj4K5mJ:m0EYxPEP9NGMGKdHQ6KH/rGlz43RK6t
MD5:	DF07F62A99F86E955DD1303EFC1FC2E0
SHA1:	B29D36631459D8B4476115415012A4FB29170857
SHA-256:	4EE727FC4CBE9A4AC3A1623EF58FC9E9C8EA4169FB13FF1C7624713F15A3CBB3
SHA-512:	FD9F49D53EEF9E55B7FE3747DDAD8387C857AE8BB5EEE42BDFDC893DB9A079F7AA56DA26AD026727FE63908292BD1EF54CFB6B1443D8B461E0BCC104A3119F6
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/...8A'/.....po...u"...O.8...h.. ....m;.@_..A..Eo.....g.l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7972073d97ac6a72_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.5987042622516086
Encrypted:	false
SSDEEP:	6:m8DEY5TYpQyCEP9NFmbyK4nGIfdX1UYNPhCK6t:0pQLEPFmbZBAdXKoy
MD5:	5CB4621FB10D913B04639187FF2289DD
SHA1:	BBE779866AEE5DDFEEFCF020F50970FD6D16534A
SHA-256:	6DA5D784ED4AAC17022A41B57C4DFED13FA88B50DDEE68735F8569C951422A7E
SHA-512:	5AC0A84E10EEB507F34153532561F68D22160C71466832529CC4BC3793AF2C8ED6D0629416F66EAA3D826DD956EBB84CB2FCA3E0C2F16B09C037A25EC52B9CE4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/161432541018_App_Scripts/Feedback/latest/Intl/en-gb/officebrowserfeedbackstrings.js .https://live.com/>t.8A'/.....o..r.wX.|.Q4z...K.%`7k.?...A..Eo.....k.....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):	5.590979927868593
Encrypted:	false
SSDEEP:	6:mjYxPEVP9YGVQB4L0NdH6ncnts+tZK6t:3EFFL0Nd2qtJtT
MD5:	321D08F3EA86B73A02F975F5AC2E7D03
SHA1:	2943505AD6C583289908BD02FC8F6667B86F051F
SHA-256:	36CA59BDCA3045DD9F55F116BE546441C7917676F7410AAC3A7C8F174DADE47D
SHA-512:	7E0065F0A14BCA4B7600035D72B70403A9900CD238F3C88211DD31DCFD2ABBF413C02456A0725068059BB33732CB92457B4FC9507D482C53D2E04639CC3444CE
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/.XP8A'/.....%.....3..n....c..."...s.&.. }..Q...A..Eo.....c.&.....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):	5.434437792487881
Encrypted:	false
SSDEEP:	6:mSEYyeDM+uDCnHAO7OrNNueLlG+ydLqZL2Si3uDs41VbK6t:NpM+uDGpiLlGzWZC3Mnj
MD5:	137702CE68022E15293A87FEEAF1CE13
SHA1:	DC596C97CEFF8394E3BDC1124FA11A12BCA11589
SHA-256:	EC226A7013875D8B8192C4DFDF964BD4C518120D0297F5B25B045D75646CBDB8
SHA-512:	A35AA983D0A213E25BD34F4A5C3D26F3FC91F9328036997E0218F8B66770D76A1B97780F1061961ADE825C8E4F6656C0BF401FD5513003C99E61661748E90DA9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\810e53cf61aed9ba_0	
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://appsforoffice.microsoft.com/lib/1.1/hosted/telemetry/oteljs_agave.js .https://onenote.com/y..9A'/.....8.....<..W.).....,..J|.Yr[)....C...A..Eo.....3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ec4cb91ffcb0ae0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	5.657735395793046
Encrypted:	false
SSDEEP:	6:mlXYgcOEo0wUZAoh0Ndi38qz2YRUPK4uRK6t:o3cVwmONdiz2X6
MD5:	E162AABE0535ED8BC18CB1C73CF13F88
SHA1:	C5FB6001C83E15A00579CAF43F21B1AC55397466
SHA-256:	45E134C9CAECD59DA18DA571C873B5CEBDA002DD08B431DE89707827C48EB007
SHA-512:	418FF4F61FCD17EDC2083C11A73CAB12BA22BF164937545E23259041A082E351D43FD6870A9C5DD0945F443D730884D0E12A619094B81934553C281FCAF38BBF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~...Y..]...._keyhttps://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20210614.002/wac0-efa56458.js .https://live.com/...8A'/.....k...V.G.....\....@J.qq..Xe..A..Eo.....|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fb80b44416c605e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.5625895893241655
Encrypted:	false
SSDEEP:	3:m+lUJta8RzYRtMxANIhpSV+nROzqPCGLGoF/1lHCuSglB2nqXmx56I8cndDWm1XX:mTtXYlNYpSVkbFCfhf6I8cvpK6t
MD5:	61F5C432AB572073F444ADE99555D3D2
SHA1:	73C135AD3F179F8715412F4AC1C22FD0EDF1E7D5
SHA-256:	9E2C537B7972D5D32522E6280C0E58EF483A30E8A326CCB50372849C71576A6A
SHA-512:	AB1CF3D0118C0F5FDD5016F0836F147BC4F6157A681BEB841530E8AF33E9D017A989C43DD3B1F7158020813CFC1D69F5F7A0C9D0DD89F24D5880269A2CE1112
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....._keyhttps://kit.fontawesome.com/585b051251.js .https://gabby-gratis-tarascosaurus.glitch.me/..9A'/.....7.....R:..."2.]T@.....f.....[C.A..Eo.....BP8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\936ea5f25b0204ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.689787037117347
Encrypted:	false
SSDEEP:	6:m6UtXYxPEP9N5HSx+6R2cNd5qh6NSBIdot14yK6t:NEEEPEgk2cNdghmSBXt1z
MD5:	B771439C10E045945DB5C9DBCC39B103
SHA1:	952AA53176C71B3C52B724AE89F93AB2B843DE6F
SHA-256:	ABF5D97802A497C23DDB4F9B89B91F9D8064376DA82CEDB1232D9EB8EA8A1C19
SHA-512:	1CACEF98A8BAC600B232EB04ABEB8C41C0144368B452E9EA1EE20A9B0F2111E676E02772C58FCF74EA626E56B167B33140C3D1592F5DAA8C154AE9FDA22A4155
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/2057/OneNoteSimplified.Wac.TellMeModel.js .https://live.com/...8A'/.....Ep...Kh"...)3.....xi<zq..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\93a3fa42e61c139b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.49510272901747
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\93a3fa42e61c139b_0	
SSDEEP:	3:m+lZEl6v8RzYJb9yKIf8QPKxQBHWFvDzTJjwlPDr/il/YLmV6gK5muXpK5kt:mxVYyK08fUHMdjY//i1mVLK4uZK6t
MD5:	3FE439296F4EC92F2E1168069DB4164D
SHA1:	49A72F69AAF29C8BEA127876D7E5003638BD8D54
SHA-256:	E08AE8DE0E1CB013F334E82BA0740E357E93DF8C83D6227A3CF6072B80601E43
SHA-512:	4E42ECAD6E38EDBC0012B6F8ED5BE1A3D9CBDF42B39D4ACC34FAB43E0C5B93C85745410D91D6347672297E7274872F95C615DF4E6F79256A63E12E05A227F8 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...."PG..._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://live.com/T/.8A'/.....b.....bC;.....Kn.fo...3...^.".A..Eo.....:..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9895df97930d526d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	5.59759667118365
Encrypted:	false
SSDEEP:	6:mktXYgcOEo0wUZAolOfdJlDeALuNrpCj3JhK6t:BcVwmlOfdJliC9
MD5:	22D299A717635440A79F08464E06218E
SHA1:	6BE00369C191AB1258465B24A3C1D737D3CFCDAA
SHA-256:	7586A49C64E49C44DFD31E600A7894C181D132617303D8C128B7C5C4904D412F
SHA-512:	D46A06D9987E708225EBBFE208AD470A347D370D6C367E10B38D5FD0AAEF8729ED35A054503454316422E6422F18CC9BD6B852C2F238480433F1C4DB777477A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~...a....._keyhttps://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20210614.002/wac2-bf8b3319.js .https://live.com/...8A'/.....o.. H~eW.$.6[f.....;..CH.5....g.3.A..Eo.....g.....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):	5.566871786444301
Encrypted:	false
SSDEEP:	6:mR/VYxPEP9NmZMdFdDZ/laqVglc7K3/bK6t:PEPmZMdFdNAqKcE1
MD5:	DC2F296DCD721D8266E53BCBAFFDCC7B
SHA1:	1EBA5EC4AAE72A479EC88B5960AE538DF5D4B3D0
SHA-256:	EF839A38B510D20DE24A59224E489E01AD22C05D14DDD1B202CEA4A43E33AA80
SHA-512:	EFB7DEDDF047B9942E4DBBDDAB43C3EF60CFBD1C216AA48B3407D048B6B1D36949C8A6C346929A2B4F14516E02C8C95541FEF734EC1849D8A60DDAF025140 13
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/..x8A'/.....ZX.a...j.~T.....]...=M. 1....A..Eo.....;MT.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5534787ec2d07e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.380101097696778
Encrypted:	false
SSDEEP:	6:m0tVYPCGdL7Mdl+Kl16CxPKhE1dB4TeK6t:kCGdHMdlv1IhE1/7
MD5:	DA1B570E45E04E81835385D2A36428A4
SHA1:	ECA775457003A372D52DA7D22355C763560C0861
SHA-256:	40AFB11609FE27E9D694D3F5F8B6DE5C3C28D600C89C072A58CD6EDC69A1CF4D
SHA-512:	CDB17F591BBEB54D66D60863D07A23F5A43A929AB19F8841A3BC72AA044CD42822708ADAFD0E7F45E44424765FA3962A7FA064EBB7A4A9A23644D5C3B9F9691 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....._keyhttps://p.sfx.ms//storage/aria-2.5.0.min.js .https://live.com/j.?8A'/.....F..E/....G8pL.c\..].Ep.).t.y.=.A..Eo.....je.....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):	5.649198719541895
Encrypted:	false
SSDEEP:	3:m+liAls8RzYFLlpEfjTQndJyV8sRzTJJKl11lHCVzllllPOCGiJ0rLgUoMmX/tlB:mWnYxPEwdUhNdEv6R/lJ32vGnX/ZK6t
MD5:	C06C125A4DA66331C0E1E09CDE772580
SHA1:	A51FAB42BCA07A3E869BCA2F8867B7C467B9612D
SHA-256:	6689929EE4DDE81002A557030044ED8EA4A435B92AE1BA7C3ABF21EADABD9AAB
SHA-512:	FDD6015C5E6D8E3E06A5A71A8DA830F47782586947F1BDB15D4A1268130D3FAFE013A795319A7640F673EAFC9AD4DCA06BD5A83BA97F4B8F715A25DEF83A5B 7
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/.k.8A'/.....V...aN#U..m.. ....{.\.....r8...A..Eo.....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):	5.598129963210775
Encrypted:	false
SSDEEP:	6:mr+XY5TYpQyCEP9NL+nNdvy1VbtmU4RxH0+kK6t:LpQLEPwdvqtsi
MD5:	36EADCAFDA413D7C6A148BDB0156B17F
SHA1:	C75F93879E873D53771C4B178C4975B06E632A11
SHA-256:	8DC38DF8E26169A099478BD593F35C4A93AC8B6FA1BD6FD13E7C9BF5911B1858
SHA-512:	5A193B4124494BDD71C3DB472FD0DD88A5CD86DEB085432B73F3B51B4ADDCF4D7AD359F6F5961A12458832DBB811E44168E62040D66C20CAF6385D6D6301D8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/161432541018_App_Scripts/wacairspaceanimationlibrary.js .https://live.com/..z8A'/.....(.-P... .''..u.uc.....]....7..3.A..Eo.....4.v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b63c1cd7c7087090_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.648863141585669
Encrypted:	false
SSDEEP:	6:mxh/VY5TYpQyCEg9f6aHwcNdB1pqBBPOhbMRK6t:s9pQLEW6F+dcXPOtMr
MD5:	C5236919B7A56FAB7C4923AD6AA9DBC4
SHA1:	0C4A8758E82F4D09CA21BE2C4E74C40A99AA7FA0
SHA-256:	1FC3292F345BA8A86A7F0FD15AA8EF482418AF5DE0CC0540366FFFEE01E7BA51
SHA-512:	0B557FB315B4E0F04BAFD97AD89A75178FBD1DD96430F708F308625D84CBE115EB214828D8BC28410F0EDD9AB122845840C2CEB8E1BB9D1B4B4CC4AA0B8677 B6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/h1E2EA8A7D7D7DBF1_App_Scripts/2057/CommonIntl.js .https://live.com/,LQ8A'/.....:..... ....l..q....`.a.._o.A..Eo.....0>t3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf789c709f3fbb5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.673893127526506
Encrypted:	false
SSDEEP:	6:m+lVYmr/jFbXEAI7Nd//C1cg1axaddxPB5lDK6t:Bf/9XEAIpd3COKd1p
MD5:	869FF217F7864DDEA5445DC215554020
SHA1:	F87F866698DE04D1B5CFE97B84FEBB0FD64B6DB8
SHA-256:	A1958A13B9ADC955F1D398303C1B9F83E3E8527CD1AB2CED885A901862D0FF6C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf789c709f3fbb5b_0	
SHA-512:	AAF979F9E918B48694AE63176220FCD53F1A7C9A5BB1E854FE649A4B78DDCE5CF671EFCF7B478500C2E18278ADB87A5DD203E4D590E7AA61FEFE50D6C02E365C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....%...._keyhttps://amcdn.msftauth.net/me?partner=OneNoteOnline&version=10.21153.1&market=EN-GB&wrapperId=suiteshell .https://live.com/.m.8A'/.. .....T.Gm....<.^...u.^...R...@..}..A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c28cce5b128f8326_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.562999612004603
Encrypted:	false
SSDEEP:	6:m/nYET08NaYWbVOqZkMEwzhbW3lSm4jihK6t:eg8NaY8ZkIzc3kmZ7
MD5:	489326B9554965801578F0A397D02970
SHA1:	57C50D6B491AD409C19B2D20307E0653A2FA1262
SHA-256:	1781E43B6D0F7932831530576197A0F377904839D2CF2E94A00D085F35504424
SHA-512:	ABB0E0DF112AC60AC780F51F1CCB33048B75EB19400DB7CDC0ED9BDFAA1F4181F0DC4924EAD5CB95657A3E9281CE6CA1227F458754A1AD3DA1EB3C0E59E5661
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://gabby-gratis-tarascosaurus.glitch.me/P.>=A'/.....;.....T. ?.|.....\.. ...Q...r....I...A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3c2b2f548f3ba44_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.551555075491867
Encrypted:	false
SSDEEP:	6:mG/VYxPEP9NmMFPMd2pN8SqbyhN4JLK6t:xyEPmM1MdPK09
MD5:	A886E8623B9743E0D284EA04DE571B3B
SHA1:	9AC5100FF0D80D7FB56E7A9187B5F3A5D911AB03
SHA-256:	C3B1D83127C312D1D59EC58A393A424936FEEF9BD50CFE7CFD147BF532D9AA93
SHA-512:	8F235CB5A525AB366C731E62694288355C513D8AFF0C90E49B4C4CC1F623FFCB47DE9B52A1988BE0EC59DBA5184FBA05AC3787A4D761F0C0DDB4FEFC14FD03AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....`....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/common50.min.js .https://live.com/H(.8A'/.....A.....8.Rn.x.....|.....~*.[... .`\...=.A..Eo.....q.g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c578d2a2ae09a113_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.60922634193517
Encrypted:	false
SSDEEP:	6:mflXYxPElqNH5RqcNdR6kk19jS6AiK6t:dEQRvdo5S6v
MD5:	55CA4B70ACBD15EE11FC47304BBE76D1
SHA1:	E41423EB2B7490BEB209080D971A240BC11333AA
SHA-256:	A9B0DBA35079C136D23F9F146B3DB6E601B63435EC2B4823C4FF6094E6AD91D0
SHA-512:	D0E1C86FD16BEF7819ACAF54668F2D6811F1B29FA32A57AD5C652348FFDB037A26A97991ACB266CA5A6E1481B3872595A85C96784730B11E096C5380FB21C7E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...n....._keyhttps://c1-onenote-15.cdn.office.net/o/s/h6A90C95AE995BE75_App_Scripts/2057/Box4Intl.js .https://live.com/.P8A'/.....Q.....]....~]'wA....:{.[.K.....-.A..Eo.....s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cae36ae7fa4d6ce2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cae36ae7fa4d6ce2_0	
Size (bytes):	231
Entropy (8bit):	5.592018321303949
Encrypted:	false
SSDEEP:	3:m+l7Ea08RzYP2FycyGYWCULLuFvDOzqPCGLGo++v1lHCr//tF8IuOAk7OFyP5mlJ:mgVYerCUM9yr/1YW7h4ldbK6t
MD5:	4D85365DC47DF0C1DB8B5353F14FB54B
SHA1:	2F0C20A89F51199BBC8D60C4B6DD811BB96D2B94
SHA-256:	C88CA8CA504E18B5039646DC6FF72866A7D7F66914E812565C9399FB1F7A9EEF
SHA-512:	702EB72BB8BAE07C19FC9CA5C8AEDAC61EF8E1E716143204F8199120C088EE212E298EBEF5FF7F25F2C35C42B2E3E15023A8765992412004B068700C5DE7E85A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...L.%....._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://gabby-gratis-tarascosaurus.glitch.me/.>=A'/.....;..... Mf..+....5.S.....T{@...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cff45f8378caad97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.643040520941119
Encrypted:	false
SSDEEP:	6:mnIEYxPEQT+WdMKOsd36Wl8eZ8NoE/VH4nbK6t:UyEcdLddpwNBI
MD5:	774AE979CCC1CA2E0859B78B140BED3B
SHA1:	CA0F34D9650A60FFD848E8AF4C69827C7DE93652
SHA-256:	F09955B2794E63AAAB3D7B0D783D4C040317C4B22F8192E3777734E167FFAF87
SHA-512:	357B7F48255A9EDD11FAE701135807753D671477E520910459A6094272D2088EFCF43F838312229B948815C1ADB1CDDD5548A7A37980437AFB121B1BFDC64CE7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l.....V...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h8882E6B1B66D0BB7_App_Scripts/wacBoot.min.js .https://live.com/.WP8A'/.....U..|k.....|.=.+2..Z...j.!...`..A..Eo.....!.$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d1b76a59a9e3f660_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.54697088011956
Encrypted:	false
SSDEEP:	6:mFYEYpRlM9V6iym18queVCK6VlXYZ84TJhK6t:sY/lkBZVwXY6Op
MD5:	AD962A852D8980BE5821AF0A23F99325
SHA1:	F5B05D1EA66A4184C1E0354F96ECDC17CA0CF2EE
SHA-256:	87FC0B7A65ED8E566E1E777964D4CF22221D6749D511ECDD724DFBBAFF8F174D
SHA-512:	237AB456B9D2AA28F056B769957898C6BD59D0AA775F7145651A6D81CD1E151A5F9A83D26AA2F7DAC925745F244A4FB5F1BD6BAA42942B4B4DA9293F3874E565
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/ExternalResources/js-cookie.js .https://onenote.com/_..8A'/.....J.....(....M..*K.l..e.<.....(k.w.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d598c76bdc491128_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.603228746244778
Encrypted:	false
SSDEEP:	6:mIYgcOEo0wUZAoxyAYxdPAv6O/lwdqv8nUygrsbK6t:xcVwmxyAqdSCqv8UygM
MD5:	75B2F1CF13957BEA0B364645A5D7327B
SHA1:	5D2839B4DC5B7C3A228367C8B259B941E6173FDA
SHA-256:	6540D905D1B2E4A249A275B2A06B6853B2D3E738D5C4F9AC07BB875952335E5C
SHA-512:	34B4994BCDBE9106C7223BC48544EE4557BEE5F71C54BF2429D0376369A03D0C0E07E35CF847D5349C340A7511121DF49115A065A07AD30889C0F47783FD4CB3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....-..1...._keyhttps://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20210614.002/jquery-1.7.2-39eeb07e.js .https://live.com/R..8A'/.....5.....].IG.W.V.v...xYpK....w....2...ct.A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d5b6ea09967e5c42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.575496956636322
Encrypted:	false
SSDEEP:	3:m+lxkA8RzYFLlpEPw0XdO1WFvDzTJ0VddkjlHC+960ZET9NrR2k3F9WmmFt/pK5M:mFYxPEP9NO1MdMpFSE51R2+HhmxK6t
MD5:	C9CFA904ACFB328F51C7B9656C8DBF0D
SHA1:	6DB1D5F1146E004B488AE34A5CDB8B6E5ECD46F6
SHA-256:	7744ECC26D1B6437CFCC54590320F2FB1D9D4FF6BCD00D5B80ADDABBA759032E
SHA-512:	B598760ADB1BDF36F75B0C021760D14783F1E3770B8C9720E6C4557C8B531E86D1651E69559F0B87F605090EC5CCB30A21D027E18699F21C2643A1F5D6203A98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/appChrome.min.js .https://live.com/..x8A'/.....!.a.Q.R~.%j....[...0... .R....A..Eo.....U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6c9ff9f20c21023_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	5.707979482176224
Encrypted:	false
SSDEEP:	6:maYqkSTVeKZZpMzNgXSur3dDh6t+Otv6AthK6t:ygPsJ43dNfOtvvt7
MD5:	AB713091B74D3DC5E53D483E4C91CF43
SHA1:	8A61DA5C4E11606CC442E7B2BD382A1FD096C13F
SHA-256:	6B60735CFCA52FBDD85C4FD6F2FE61208C3B431075E5BF6C4EE779D9BE23BD1F
SHA-512:	29AE19E9A223A1A480A0EC1D028F81026B0AAE91557A2DB500A19E28CD48D8B683AE9F4D2C264AD9C9AC9B096E6EDA0BB67ED56769341FD8B2777F06621FE6B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://onedrive.live.com/handlers/clientstring.mvc?mkt=en-GB&group=GroupFolders&v=19.710.0628.2003&useRequiresJs=False .https://live.com/.?8A'/.....67l+T..7a;.y...}....<..=...2.\..A..Eo.....c1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de272f24ef9bbe31_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.399903374021273
Encrypted:	false
SSDEEP:	3:m+l1sC8RzYFLlpEk/WvLQFvDzTJvY+v1lHC+m810oo3VARnyRq76P5m3YhltpK5M:mYsPYxPEUdvY+6+mxomVQCl4MbK6t
MD5:	82008ED0E0BB1D56CE028CBD5CB992C6
SHA1:	957EAFEA785462FDA64F67330850955C5733BB51
SHA-256:	86A30C2BD2BCCD5F247AE35E0263022D44956135CCFFCAAD7AE72286C9B7C705
SHA-512:	BBCF888967B1CE3D3ECFCBCE557EF0500F23C9CCCC0070C3D1AAFEAB5E0B2B0271C72220EEECB04A93155231B95A163333D10990687DF21490FFB9BF861352A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....8.n...._keyhttps://c1-onenote-15.cdn.office.net/o/s/App_Scripts/onenote-boot.min.js .https://live.com/..I8A'/.....[.....(.P~v...A.....4.....`jT.A..Eo..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\df616072ed05fe37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.590962575922801
Encrypted:	false
SSDEEP:	3:m+l4El08RzYFLlpEPw0XdOT/uFvDzTJCBN1KlflHCP/Uzgz4hTjipCNW/yRmJqtX:m/ElVYxPEP9NOgdMP8MznpCCnJqZK6t
MD5:	BD91FEF2C2623FDCC81DACEE50BAD1D9
SHA1:	6469828EC3F068324FE97A0434B20C4E4669F6F4
SHA-256:	8077C1AFB5222116208BFB88099DE29102E79423B28B966A694452A48FE51F41
SHA-512:	BC9B23C89ADCBB6FA859ED8FB7D84283136D782BF11D9DC3177E3450ABB000500DA92C0758E583AA51862546D650FEF6FE38D83F7394261E94D9895DAD5283C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\df616072ed05fe37_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/appChromeLazy.min.js .https://live.com/p$.8A'/.....|.....).u.]...|..F.F.D..[i.S.D..A..Eo.....j?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e0ac675daa08938b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.6125038523670785
Encrypted:	false
SSDEEP:	6:maGYxPEP9NI12TdJcxsSNls0I6/nzhK6t:f7EPa2TdJssS3r5
MD5:	7162B52AE65069DCB88266240234F9D6
SHA1:	3FC033CE00DA183A6A4550E41EE938CA0C893997
SHA-256:	69C8470F8671451EC2386E497DF35E09D6D6E73AA1B6D4CC2C22B78A67FB1682
SHA-512:	1325A8751F68DAFF462E5F53F5C3FC93C74461DB7F12C558FDEF82342A27D45BE3AA667BB71FEE321E603278C93E903A015375F5A49B0A7FE003AAB45BBD58F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....b_...._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/appIconsLazy.min.js .https://live.com/...8A'/.....;}.!A..R..H...R._..<4.wb..)..*.A..Eo.....:W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e1f7ecb6fc0a528f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.475820780212903
Encrypted:	false
SSDEEP:	6:mMYEYpRlM9V6fMYueF6qXgyWO4164qh/hK6t:5Y/lVH7DWO41uJ7
MD5:	9E431D84E29C3ED3484897EF6B382621
SHA1:	B24ACEF82BC743B429EB62E412D11FB5CA044E4A
SHA-256:	64894AFE949FFAA2F5DCAB084368BE917DFEE6C895AEF64FAE046788B03D49D0
SHA-512:	0AFEC649D3110AB55F697837801D21EF6EFD48BC48734ECA541671E256BD131A9DA6B8954F708EA1E8D8716CC57D8EB817C98DE38D7542EDE2BC72DC0FB66DCB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...9....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/Instrumentation.js .https://onenote.com/..8A'/.....M.....ShL.@.Ef...Hk.V..T....f..V....A..Eo.....}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2fa7340d4950923_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.412843722301016
Encrypted:	false
SSDEEP:	6:mk6XXYyeDM+uDCnJQuM6WGINuey62tmBKpY/dk4EDK6t:T6sM+uDGJQuSGyy9tm82/ev
MD5:	3268F8BFC1FC1D7478E7A96322A27A6A
SHA1:	78068269FFF363DCD869DAC4E8CA8594D8DAB4A7
SHA-256:	4A739404713A92297A108C2184016DCF20FACDCE7830D48827E93F4DFBDB11A9
SHA-512:	99DA1D05B50926D3EE586B60374A15F1B5FA33307B2276ADF62260747E20F274C0934267F501F932B90A6C7A2D8D3FEDCB044645DB7A5BF128F43AF4975881BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...G....._keyhttps://appsforoffice.microsoft.com/lib/1.1/hosted/en-us/office_strings.js .https://onenote.com/.Y.8A'/.....[.D..|.../\....21./.=.b.....A..Eo.....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e96383cd4fdf8308_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.383675894757497

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e96383cd4fdf8308_0	
Encrypted:	false
SSDEEP:	6:mbPYyeDM+uDCnyTASVNuev1+Aoyy9EK6t:6UM+uDGyN3vAo
MD5:	102DB22C1A901C2D87C4094A2DF09A9B
SHA1:	9FFCDE69F081E2AE14D81FDA56691228A6C2700F
SHA-256:	EC338C36C72A38D9ABB007CBA5B7D2C56ABCB7851F4FF2723EDB55C66899ED45
SHA-512:	5287DCC65C3CF4D23DC027C3780CD0EA103DA8B30A8F7F071F246587E4F28EB0BC12BD3EEF76FFFA16DF099EE89B424CA0A594733AFDFF15DC01A10E5ACB543
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...5..o...._keyhttps://appsforoffice.microsoft.com/lib/1.1/hosted/office.js .https://onenote.com/...8A'/.....h....'G.n..-..`...*V.....Q.A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ee2d74af9fde7e01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.546225198407955
Encrypted:	false
SSDEEP:	6:mylPYEYpRlM9V6iWAMbVue9mJv6fDQEvF/r3CK6t:fY/l0WAMj1BFLU
MD5:	147BA9FE7C4481E1388EB59A03784F81
SHA1:	93ECE9E2FA93C864825CC536EB7AB001225A8432
SHA-256:	B34314197FE336D8246F0A60BA6E2BC30F886F1AE91F4096AC2857798A78AE4A
SHA-512:	E38F9B2DAC2FE51334E94D384C1551863F11749EF3602AB5F32FC9D10F8AAF75A34E4418D38667B119326ADA52BA15089DFFA7D1DADA0C9382289D5298B29CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....s....._keyhttps://cdn.onenote.net/officeaddins/161432640454_Scripts/BrowserUls.js .https://onenote.com/...8A'/.....3.....gi?[J'..ug.S....;%...}s.....F{.A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f1c8f28f7b9cefec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.549693789375302
Encrypted:	false
SSDEEP:	3:m+l0h6/lLA8RzYFLlpEPw0XdcTdKpWFvDzTJrK1lHCuQlllroSZPMGwm7l1lpK5M:mQPYxPEP9NrMde6X/sSZPz7CK6t
MD5:	027021CE0A5F5E105BEF1E618976EAAC
SHA1:	7B69F7FC07BAD1716508C49A244620BAADFB0603
SHA-256:	61A5C666EA750785AF6FD903516D01981871A2829AB52FC04F4207CFF0501F95
SHA-512:	069152711A5644FC2D9D52144FBCB268CBE7311396802A185B3AD9142328AF1C5C8A1CB6214DE8B0AFF7ED80DD07E5A912B8022122F5B401A3D7D964F1933BE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....]....._keyhttps://c1-onenote-15.cdn.office.net/o/s/161432541018_App_Scripts/navigation.min.js .https://live.com/...8A'/.....8#....^.Xo.u...vKv'1.m..#...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f251984d116eca5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	268
Entropy (8bit):	5.7512125800776115
Encrypted:	false
SSDEEP:	6:mcpYqkSTVeKZZ0RFDgXSur3dEA9gaH1BqDK6t:rEgPmRN43dEyu
MD5:	8E8A0D1F7886BAEB5A0033C3364A5D8C
SHA1:	F865FEF63A3FC828B7093A4406E0934A6497D0BE
SHA-256:	465973491FB96A510A0A099FA202BDD234A9B0447EF6DF4BDB5526C436B0D1DA
SHA-512:	7C4A07D234E734E68E46DCF59418526A9AAB570453AEAA1F84A32E2107971C39F08BAAF60B65EE91ADCE77A2BDF8244D91EAA7D960A930419CA82655D963CAB1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Sa....._keyhttps://onedrive.live.com/handlers/clientstring.mvc?mkt=en-GB&group=Office&v=19.710.0628.2003&useRequiresJs=False .https://live.com/.TE8A'/.....mg..[...A|r2.@...&a.....[H^....A..Eo.....X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f3b70381e0b52174_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.671542811727805
Encrypted:	false
SSDEEP:	6:mi6PYxPEymh6cj5HSdNd8K/VPfjCbYYlbK6t:GMEymhyHdV/VPfWTlN
MD5:	8738955D6B8C44AA1A971C64F878F80E
SHA1:	F85142FB5BD74D48D8853B15A892A63CE227FC1A
SHA-256:	EC649A1E872D71FB14153F545B53FAD59644525E2C13A9CC5B6AE9A6A5AC5270
SHA-512:	8569FE0F8AC562483AFF437B608929692F7E86354F69E1D73F263985B2652BD78A7B8B8D4CF988705C8ADE5AB7C664410DBE45AD55728F72A890450BE960396B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....Rx...._keyhttps://c1-onenote-15.cdn.office.net/o/s/h83B1CF4978D4D8AD_App_Scripts/2057/OneNoteIntl.js .https://live.com/$WQ8A'/.....[.....^$T.y ..v\..X...<.?....9...W..0..A..Eo.....]t.y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fa1d01002fa990ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.636878306098589
Encrypted:	false
SSDEEP:	6:miWY5TYpQyCEv/aNG+CFdyaAjE6whqUVhi/RK6t:cpQLEv/aNG+AdyaETj5D
MD5:	4F69A409660262D021049842B74778E1
SHA1:	AF7EA4C03F0FC5609E0CBFE8B7D318140908EF1D
SHA-256:	3FBC2929DAB506C008A248F58E7261E2DB417FF8117AA86A3CBDBEC98702B932
SHA-512:	E0E3F7037461AC9503FE1AA3E37BBCF7AEBD826CB6C77DA12483EFD2E8A819D2E1667D343F6BCCCD0D15C04E1B8D8E49FB6AF290A9326B198EFCEC5D9E6AI 191
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.../....._keyhttps://c1-officeapps-15.cdn.office.net/o/s/h4DDC354F0F9CEFBE_App_Scripts/MicrosoftAjax.js .https://live.com/.FQ8A'/.....qs.,I;.....6 ..f.*.{=}.'f..A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fbfdce35af9204d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.628359034793947
Encrypted:	false
SSDEEP:	6:mHYgcOEo0wUZAoXXEEdjK6Fo0UZreraOtbK6t:+cVwmHdjPo0URefr
MD5:	84AB96CFA7B6180C1C98279BC5E7CA6B
SHA1:	ADB0E1D5E1E484D3184AE705F5C3C0AF6219CC1A
SHA-256:	83CCD7DAA1D499594B930421D11044C073301B61FA9739557A719FF6C531099D
SHA-512:	A382A7E2804BE3F52F6C895FD2D07098646522D9BCB26097105EE08BC950D5853D3F24F79E98622EBE481D6FE87A3AE28C3EBF6A908D8180751E8F9655693513
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://spoprod-a.akamaihd.net/files/onedrive-website-release-prod_master_20210614.002/wac_s_office-b64f5dcf.js .https://live.com/=..8A'/..... .....B.....(.../....D...."....J.&6.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	5.419425864985361
Encrypted:	false
SSDEEP:	24:fd/xT+/HwE8qBYEzmoI0tlPfkvmr4TJywuk8gHTiv2lpXNSZI:fbVE7YECfulPumr4FGk5fleW
MD5:	C717495354EB566206BDC2DA67E8A841
SHA1:	FDBDEEDE72749206E07043D60CFFD684B4128360
SHA-256:	9D28393139B20F720472668B14E54B5E1C07682E7497447E6CB5417FFB2D62AB
SHA-512:	5738AEDA5057E09667CB52B23FD566A35B6CBC2C835BE7C40D56C2B6A41BDF2C6E8FBAEA4F8BB5E8FD8E179B52CEF641434AB5EF54DE7DE42B4C95403C720 CA8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Malicious:	false
Reputation:	low
Preview:	....I..1oy retne....J.....d.....7..9A'/..q.....S..R..9A'/.....&...[....9A'/.....lM..j....9A'/.....^`lAD.....9A'/.....w(....1u...9A'/.....a.S.....8A'/.....#...@s.....8A'/... .....rZ/...Q...8A'/.....a'.N.....8A'/.....O.c....8A'/.....Gy.z....8A'/.....R.....8A'/.....j.uz;Ojm...8A'/.....`..Yj.....8A'/.....|1.-.Dt...8A'/.....~..t-....8A'/..... ."e.R.m...8A'/.....(.%.x...8A'/.....\((.E >...8A'/.....B.....8A'/.....1.....8A'/.....a.....8A'/.....K...vL@P.8A'/.....g.JM...@P.8A'/.....-I.Q.7..@P.8A'/..... [Y9...0@P.8A'/.....=z<..s.l@P.8A'/.....^ @P.8A'/.....[.n.@P.8A'/.....rj..=.ry@P.8A'/.....mR.....@P.8A'/.....[.?.p.x....8A'/.....s.h.D...@P.8A'/.....@ P.8A'/.....K..|L....8A'/.....5.....8A'/..... .D..x.a..8A'/.....D..H.....8A'/.....7...r`a...8A'/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	5.419425864985361
Encrypted:	false
SSDEEP:	24:fd/xT+/HwE8qBYEzmoI0tlPfkvmr4TJywuk8gHTiv2lpXNSZI:fbVE7YECfulPumr4FGk5fleW
MD5:	C717495354EB566206BDC2DA67E8A841
SHA1:	FDBDEEDE72749206E07043D60CFFD684B4128360
SHA-256:	9D28393139B20F720472668B14E54B5E1C07682E7497447E6CB5417FFB2D62AB
SHA-512:	5738AEDA5057E09667CB52B23FD566A35B6CBC2C835BE7C40D56C2B6A41BDF2C6E8FBAEA4F8BB5E8FD8E179B52CEF641434AB5EF54DE7DE42B4C95403C720CA8
Malicious:	false
Reputation:	low
Preview:	....I..1oy retne....J.....d.....7..9A'/..q.....S..R..9A'/.....&...[....9A'/.....lM..j....9A'/.....^`lAD.....9A'/.....w(....1u...9A'/.....a.S.....8A'/.....#...@s.....8A'/... .....rZ/...Q...8A'/.....a'.N.....8A'/.....O.c....8A'/.....Gy.z....8A'/.....R.....8A'/.....j.uz;Ojm...8A'/.....`..Yj.....8A'/.....|1.-.Dt...8A'/.....~..t-....8A'/..... ."e.R.m...8A'/.....(.%.x...8A'/.....\((.E >...8A'/.....B.....8A'/.....1.....8A'/.....a.....8A'/.....K...vL@P.8A'/.....g.JM...@P.8A'/.....-I.Q.7..@P.8A'/..... [Y9...0@P.8A'/.....=z<..s.l@P.8A'/.....^ @P.8A'/.....[.n.@P.8A'/.....rj..=.ry@P.8A'/.....mR.....@P.8A'/.....[.?.p.x....8A'/.....s.h.D...@P.8A'/.....@ P.8A'/.....K..|L....8A'/.....5.....8A'/..... .D..x.a..8A'/.....D..H.....8A'/.....7...r`a...8A'/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.263687494554813
Encrypted:	false
SSDEEP:	192:duP2SxzSQ1TM2FV56VMMTuwlSxz9Q1TB29W56VMj:OxzH1TxiPuza1Tsbw
MD5:	91F71ABEFF8D090709BB742BBB8F44ED
SHA1:	103DAEDCBBDB08101F2D1801ACD8BB22FDDCDA19
SHA-256:	57547AE0EF505CADCC597911804E420E30DDB40632A241644BF6A165395AB9E2
SHA-512:	9EBD163A75F3C1805874EA895C588270EE406469C7B47F5A331E1C5E19F785E08FC0002DAC12A90E3DF557FCAE21AB70C51FD8A029761FD67E890452BEDEB12
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	21568
Entropy (8bit):	2.5985870388387022
Encrypted:	false
SSDEEP:	96:6NCcNwmcG3bOTKrErxzR/AISrQ1TcB/eFkJm5HaVixwMNw3:6NCcuD2SxzSQ1TM2FV56VMwMu3
MD5:	01CA6EF1FDB0298216E1910BCE87255A
SHA1:	3C00257E6275981EF995290473C77197B1AC88BD
SHA-256:	6D8E11C976C6E8CFD0941E7E44CE15E62963F018983A49498163AE08AFDE22BE
SHA-512:	4D38FE5CBC292DDE9D2FF6A47A87A2772752146EB3D5EE2BB2922741B4B520A4D7BA5C0E9ED066F0ECA2F354842A6CA72539E5F74E9FEC7D90B2573E96ACD6FA
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18816
Entropy (8bit):	4.501113742364894
Encrypted:	false
SSDEEP:	192:31I/IlkUBuxw8q1kyMCkUBuxw8q1kyMN7Lq7ckUBuxw8q1kyM/FRTE:lOOBum86Bum8RLekBum89RQ
MD5:	27AF5BB824508C6D613E76808598E53C
SHA1:	CE683F98BB6FBAD8D2BFEE51A5643E14FAA37D43
SHA-256:	64BC7118C128693795385925B403EC8BDD9F5D4D915E1D84996888F57DA13EC1
SHA-512:	FC4E2FF828D9A9DBD7727868D324CC213E3D7F8198A390794DB6A738426DCF85A5A88D5BFDC888E00671F4576F160DB3E80FD8CC3EEB1D233ADF911683E64CE
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...73b9a08c_7944_4936_8028_73498cc6ba6b.....!:.+..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....e..`.....https://onedrive.live.com/redir?resid=6060782D2B8D50A6!129&authkey=!ApbFYYOKMpcYgog&ithint=onenote%2c&page=view&e=YSYU1OrRbk-OgIBVwfjzEw&at=9.....l...h.....`.....h.. .....`.....".....h.t.t.p.s.:././/.o.n.e.d.r.i.v.e...l.i.v.e...c.o.m./.r.e.d.i.r.?.r.e.s.i.d.=.6.0.6.0.7.8.2.D.2.B.8.D.5.0.A.6.!.1.2.9.&.a.u.t.h.k.e.y.=.!.A.p.b.F.Y.Y.O.K.M.p.c.Y.g.o.g.&.i.t.h.i.n.t.=.o.n.e.n.o.t.e.%.2.c.&.p.a.g.e.=.v.i.e.w.&.e.=.Y.S.Y.U.1.O.r.R.b.k.-.O.g.I.B.V.w.f.j.z.E.w.&.a.t.=.9..... .....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Size (bytes):	317
Entropy (8bit):	5.207922331875926
Encrypted:	false
SSDEEP:	6:m4F+q2Pwkn23iKKdK8aPrqIFUtp/fZmwP/fVkwOwkn23iKKdK8amLJ:PF+vYf5KkL3FUtp/f/P/fV5Jf5KkQJ
MD5:	241A3E2FC1143362ACBBFC92D2862F3E
SHA1:	072B59A44CAD665B5400B2A91A8D7F89CB88B1E8
SHA-256:	4BD253F15EA3C37DA47089D505CA1A564C1DF80D3FD4056ED6DF5FAD7DC8B864
SHA-512:	9E18D0E2083C6CF6E2FA691DD7B187C3B5E989F46485AE092364949896D206592A66B987C693A4706A3FA6FB864C7ED555F659EF539D412F6B00658A2B99116E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:22:45.231 72c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-19:22:45.233 72c Recovering log #3.2021/08/03-19:22:45.233 72c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.207922331875926
Encrypted:	false
SSDEEP:	6:m4F+q2Pwkn23iKKdK8aPrqIFUtp/fZmwP/fVkwOwkn23iKKdK8amLJ:PF+vYf5KkL3FUtp/f/P/fV5Jf5KkQJ
MD5:	241A3E2FC1143362ACBBFC92D2862F3E
SHA1:	072B59A44CAD665B5400B2A91A8D7F89CB88B1E8
SHA-256:	4BD253F15EA3C37DA47089D505CA1A564C1DF80D3FD4056ED6DF5FAD7DC8B864
SHA-512:	9E18D0E2083C6CF6E2FA691DD7B187C3B5E989F46485AE092364949896D206592A66B987C693A4706A3FA6FB864C7ED555F659EF539D412F6B00658A2B99116E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:22:45.231 72c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-19:22:45.233 72c Recovering log #3.2021/08/03-19:22:45.233 72c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:22:49.562542915 CEST	192.168.2.4	8.8.8.8	0x137f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:49.565059900 CEST	192.168.2.4	8.8.8.8	0xd1d5	Standard query (0)	linkprotect.cudasvc.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:49.575762987 CEST	192.168.2.4	8.8.8.8	0x34c5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:52.220829010 CEST	192.168.2.4	8.8.8.8	0x35ca	Standard query (0)	1drv.ms	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:22:52.342185020 CEST	192.168.2.4	8.8.8.8	0xa92c	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:55.735773087 CEST	192.168.2.4	8.8.8.8	0x9051	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:55.738262892 CEST	192.168.2.4	8.8.8.8	0xbb7b	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:57.281760931 CEST	192.168.2.4	8.8.8.8	0x771b	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:02.593763113 CEST	192.168.2.4	8.8.8.8	0x908d	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:05.700953007 CEST	192.168.2.4	8.8.8.8	0x4c88	Standard query (0)	skyapi.onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:05.952295065 CEST	192.168.2.4	8.8.8.8	0x435d	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:06.049063921 CEST	192.168.2.4	8.8.8.8	0xd12d	Standard query (0)	c.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:06.489257097 CEST	192.168.2.4	8.8.8.8	0xe95b	Standard query (0)	amcdn.msftauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:06.516297102 CEST	192.168.2.4	8.8.8.8	0x402f	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:07.331485987 CEST	192.168.2.4	8.8.8.8	0xe35a	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:07.510154009 CEST	192.168.2.4	8.8.8.8	0x4c5c	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:17.658849001 CEST	192.168.2.4	8.8.8.8	0x442e	Standard query (0)	gabby-gratis-tarascosaurus.glitch.me	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:18.285257101 CEST	192.168.2.4	8.8.8.8	0x9aa2	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:18.375216961 CEST	192.168.2.4	8.8.8.8	0x22af	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:18.375720978 CEST	192.168.2.4	8.8.8.8	0x4444	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.008569956 CEST	192.168.2.4	8.8.8.8	0x9714	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.166809082 CEST	192.168.2.4	8.8.8.8	0xb6a1	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.166829109 CEST	192.168.2.4	8.8.8.8	0x5e1c	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.292967081 CEST	192.168.2.4	8.8.8.8	0x2a07	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.828808069 CEST	192.168.2.4	8.8.8.8	0xb0eb	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.829443932 CEST	192.168.2.4	8.8.8.8	0x35f8	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.831367970 CEST	192.168.2.4	8.8.8.8	0x9025	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:22:49.600193024 CEST	8.8.8.8	192.168.2.4	0xd1d5	No error (0)	linkprotect.cudasvc.com		18.196.58.60	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:49.600193024 CEST	8.8.8.8	192.168.2.4	0xd1d5	No error (0)	linkprotect.cudasvc.com		35.158.39.45	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:49.607980013 CEST	8.8.8.8	192.168.2.4	0x34c5	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:49.618745089 CEST	8.8.8.8	192.168.2.4	0x137f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:22:49.618745089 CEST	8.8.8.8	192.168.2.4	0x137f	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:52.263890028 CEST	8.8.8.8	192.168.2.4	0x35ca	No error (0)	1drv.ms		13.107.42.12	A (IP address)	IN (0x0001)
Aug 3, 2021 19:22:52.392946005 CEST	8.8.8.8	192.168.2.4	0xa92c	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:22:55.772907019 CEST	8.8.8.8	192.168.2.4	0x9051	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:22:55.778660059 CEST	8.8.8.8	192.168.2.4	0xbb7b	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:22:57.346340895 CEST	8.8.8.8	192.168.2.4	0x771b	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:02.627269030 CEST	8.8.8.8	192.168.2.4	0x908d	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:02.627269030 CEST	8.8.8.8	192.168.2.4	0x908d	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:05.741522074 CEST	8.8.8.8	192.168.2.4	0x4c88	No error (0)	skyapi.onedrive.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:05.741522074 CEST	8.8.8.8	192.168.2.4	0x4c88	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:05.741522074 CEST	8.8.8.8	192.168.2.4	0x4c88	No error (0)	am3pcor006-com.be.1drv.com	i-am3p-cor006.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:05.741522074 CEST	8.8.8.8	192.168.2.4	0x4c88	No error (0)	i-am3p-cor006.api.p001.1drv.com		13.104.158.180	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:05.986565113 CEST	8.8.8.8	192.168.2.4	0x435d	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:06.098705053 CEST	8.8.8.8	192.168.2.4	0xd12d	No error (0)	c.live.com	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:06.098705053 CEST	8.8.8.8	192.168.2.4	0xd12d	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:06.532730103 CEST	8.8.8.8	192.168.2.4	0xe95b	No error (0)	amcdn.msftauth.net	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:06.552073002 CEST	8.8.8.8	192.168.2.4	0x402f	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:07.387085915 CEST	8.8.8.8	192.168.2.4	0xe35a	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:07.387085915 CEST	8.8.8.8	192.168.2.4	0xe35a	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:07.387085915 CEST	8.8.8.8	192.168.2.4	0xe35a	No error (0)	db3pcor005-com.be.1drv.com	i-db3p-cor005.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:07.387085915 CEST	8.8.8.8	192.168.2.4	0xe35a	No error (0)	i-db3p-cor005.api.p001.1drv.com		13.104.208.160	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:07.553994894 CEST	8.8.8.8	192.168.2.4	0x4c5c	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:07.633908033 CEST	8.8.8.8	192.168.2.4	0xb18f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:17.694015980 CEST	8.8.8.8	192.168.2.4	0x442e	No error (0)	gabby-gratis-tarascosaurus.glitch.me		52.5.55.81	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:17.694015980 CEST	8.8.8.8	192.168.2.4	0x442e	No error (0)	gabby-gratis-tarascosaurus.glitch.me		52.86.228.72	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:17.694015980 CEST	8.8.8.8	192.168.2.4	0x442e	No error (0)	gabby-gratis-tarascosaurus.glitch.me		107.23.110.216	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:17.694015980 CEST	8.8.8.8	192.168.2.4	0x442e	No error (0)	gabby-gratis-tarascosaurus.glitch.me		52.20.88.154	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:18.313596010 CEST	8.8.8.8	192.168.2.4	0x9aa2	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:18.408606052 CEST	8.8.8.8	192.168.2.4	0x22af	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:23:18.408606052 CEST	8.8.8.8	192.168.2.4	0x22af	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:18.412728071 CEST	8.8.8.8	192.168.2.4	0x4444	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:18.645167112 CEST	8.8.8.8	192.168.2.4	0x4a5c	No error (0)	gstaticadssl.l.google.com		142.250.186.163	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.048410892 CEST	8.8.8.8	192.168.2.4	0x9714	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.200683117 CEST	8.8.8.8	192.168.2.4	0xb6a1	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.202297926 CEST	8.8.8.8	192.168.2.4	0x5e1c	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.202297926 CEST	8.8.8.8	192.168.2.4	0x5e1c	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.320674896 CEST	8.8.8.8	192.168.2.4	0x2a07	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:23:19.862055063 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.862055063 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.863989115 CEST	8.8.8.8	192.168.2.4	0xb0eb	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.866821051 CEST	8.8.8.8	192.168.2.4	0x9025	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:23:19.866821051 CEST	8.8.8.8	192.168.2.4	0x9025	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 19:22:49.649696112 CEST	18.196.58.60	443	192.168.2.4	49731	CN=*.linkprotect.cudasvc.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Aug 3, 2021 19:22:49.649780035 CEST	18.196.58.60	443	192.168.2.4	49733	CN=*.linkprotect.cudasvc.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 19:23:17.972537041 CEST	52.5.55.81	443	192.168.2.4	49844	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Aug 3, 2021 19:23:17.972606897 CEST	52.5.55.81	443	192.168.2.4	49843	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4808 Parent PID: 4944

General

Start time:	19:22:43
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://linkprotect.cudasvc.com/url?a=https%3a%2f%2f1drv.ms%3a443%2fo%2fs%21BKZQjSsteGBggQGWxWGDijKXGIKI%3fe%3dYSYU1OrRbk-OgIBVwfjzEw%26at%3d9&c=E,1,kIuIGEH799izsJ8ZzgEzo4vQsPME7QtXgthIwQx0qxxoPwhTl2ujgDMlbeQxn4ZdZQB-OFmNbdIvk9f4X00Afp0hXBwXDa-unMy-xntb&typo=1'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 5940 Parent PID: 4808

General

Start time:	19:22:45
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=1576,16837710322178850958,12009668449574082098,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly