ID: 516205
Cookbook: browseurl.jbs
Time: 08:43:12
Date: 05/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

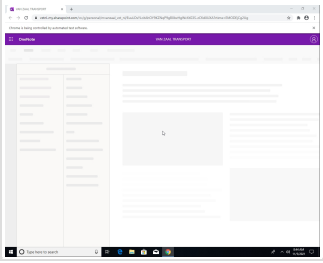
Windows Analysis Report https://vztnl-my.sharepoint.co…

Overview

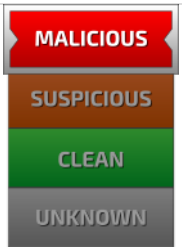
General Information

Sample URL:	http://https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?e=5%3ahV4RUj&at=9
Analysis ID:	516205
Infos:	

Most interesting Screenshot:



Detection



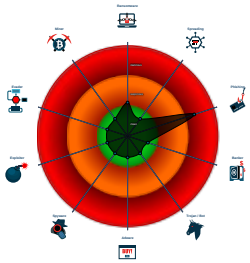
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish20
- Phishing site detected (based on im…
- Found iframes
- Suspicious form URL found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5924 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?e=5%3ahV4RUj&at=9 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2192 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,6233830419226784550,16524938468778052118,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /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:

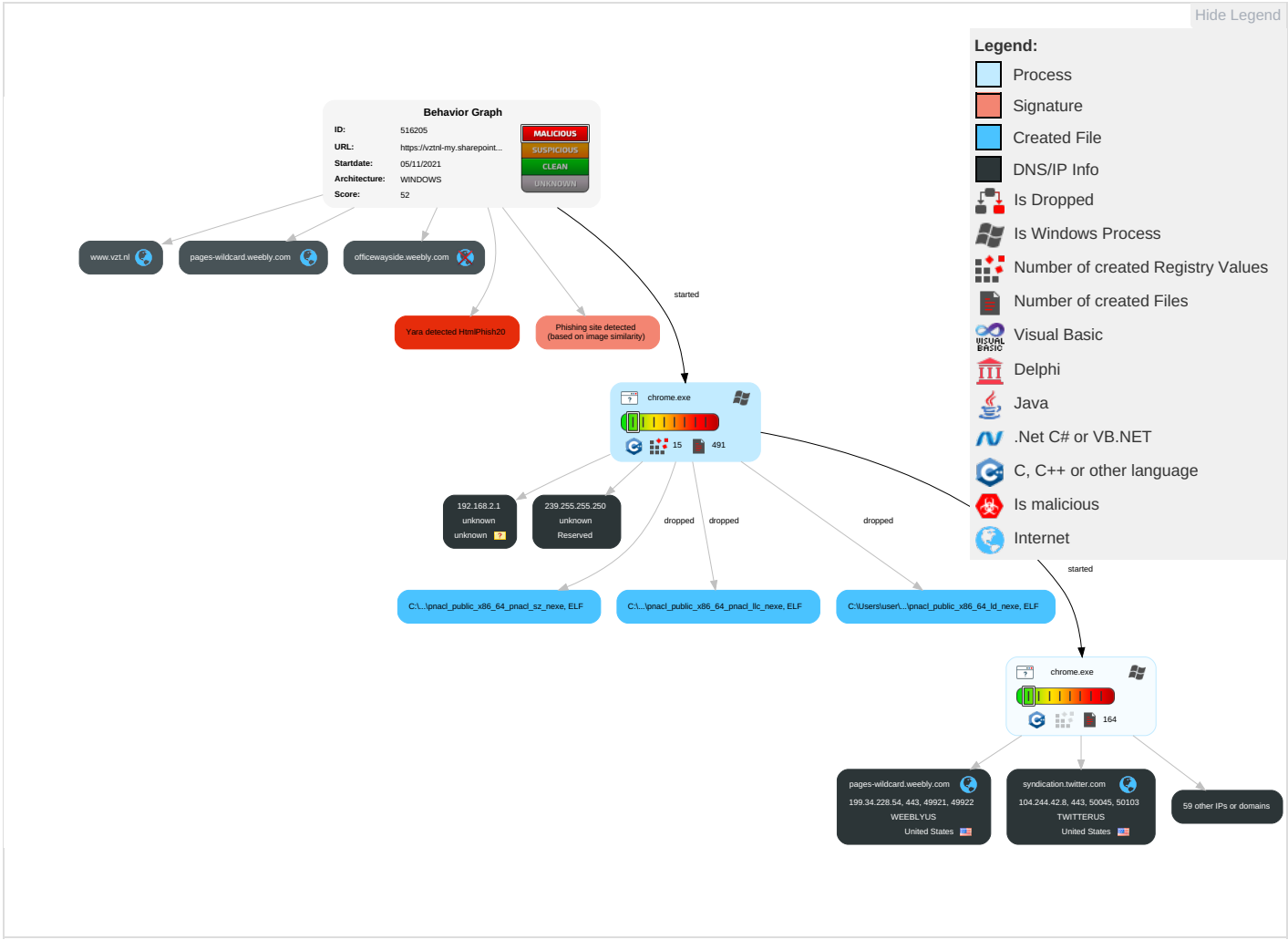
Yara detected HtmlPhish20

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

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

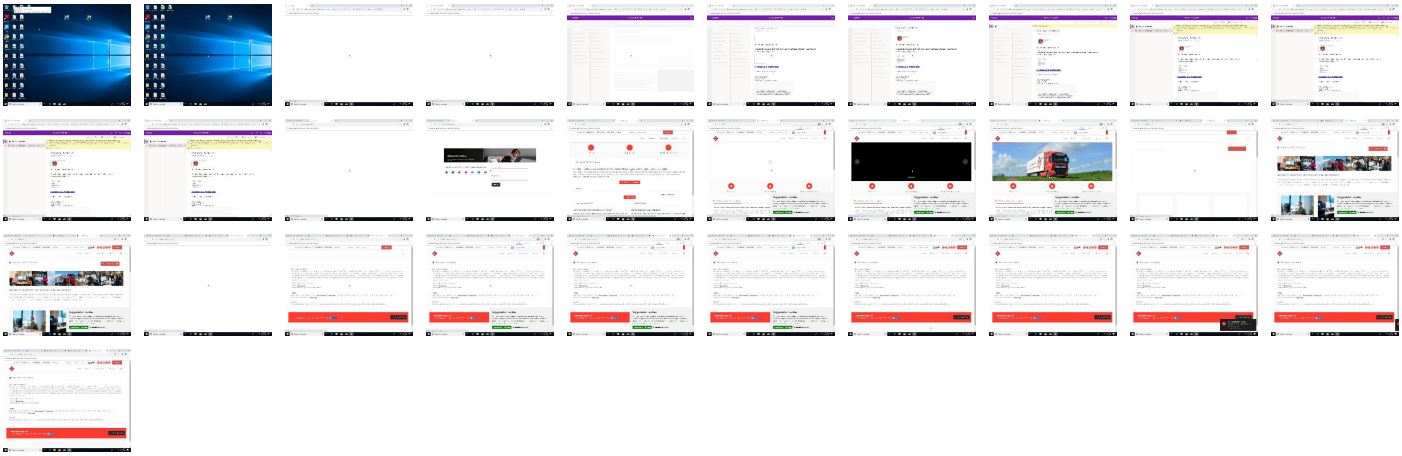
Behavior Graph

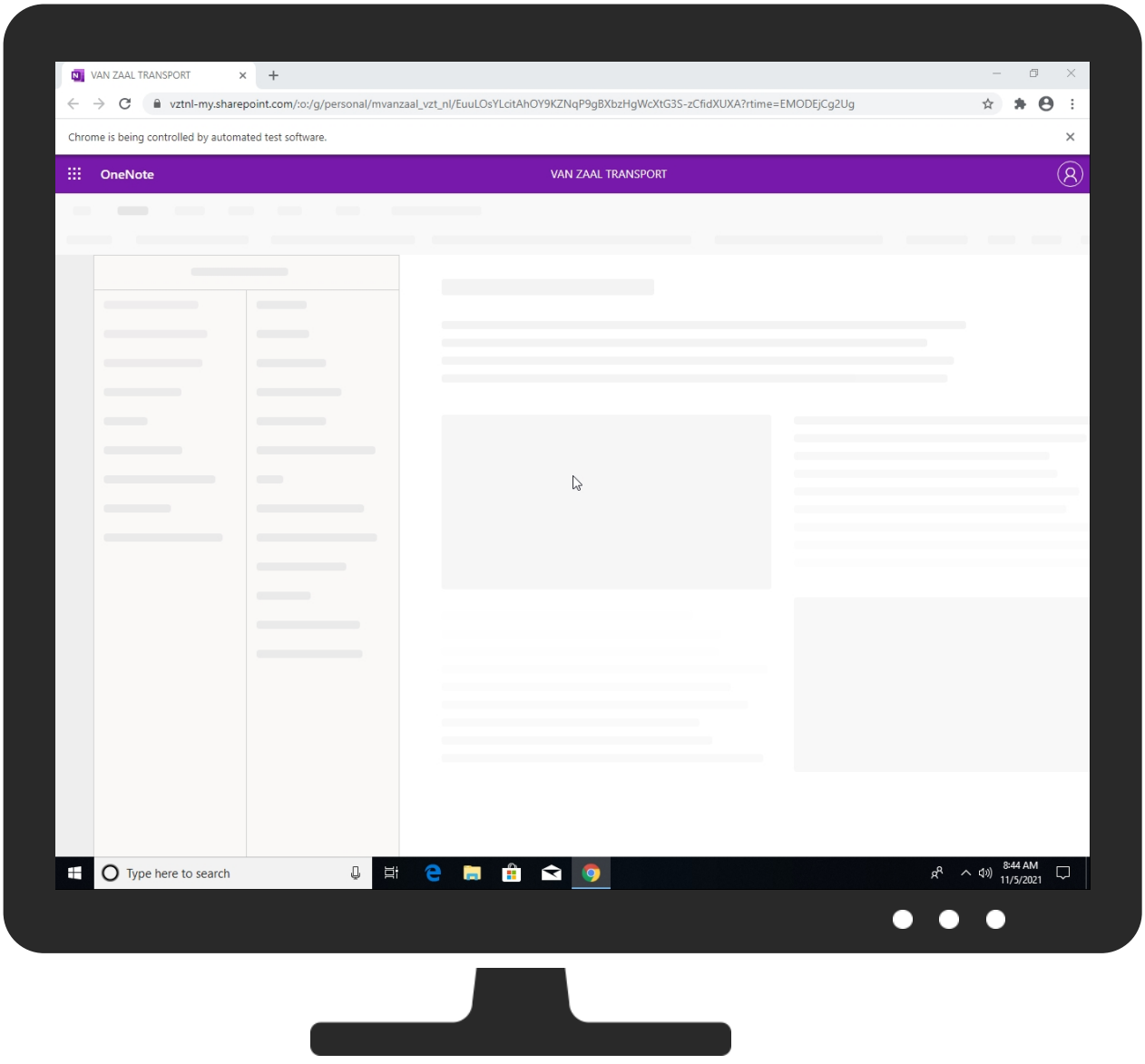


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?e=5%3ahV4RUj&at=9	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-	0%	Avira URL Cloud	safe	
http://https://www.vzt.nl/	0%	Virustotal		Browse
http://https://vztnl-my.sharepoint.com/personal/mvanzaal_vzt_nl/_layouts/15/Doc.aspx?sourcedoc=%7Bc63a8beb-	0%	Avira URL Cloud	safe	
http://https://vztnl-my.sharepoint.com/personal/mvanzaal_vzt_nl/_layouts/15/Doc.aspx?sourcedoc=	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.185.131	true	false		high
sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com	54.189.175.59	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false		unknown
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
i-db3p-cor005.api.p001.1drv.com	13.104.208.160	true	false		high
embed.tawk.to	104.22.25.131	true	false		high
va.tawk.to	104.22.24.131	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
ssl-google-analytics.l.google.com	142.250.186.168	true	false		high
www.google.com	142.250.185.196	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
accounts.google.com	142.250.184.237	true	false		high
www-google-analytics.l.google.com	142.250.186.142	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
pop-esv5.mix.linkedin.com	108.174.11.37	true	false		high
www-googletagmanager.l.google.com	142.250.186.168	true	false		high
www.freeprivacypolicy.com	104.26.7.220	true	false		high
syndication.twitter.com	104.244.42.8	true	false		high
187270-ipv4.farm.dprodmgd104.aa-rt.sharepoint.com	40.108.231.27	true	false		unknown
pages-wildcard.weebly.com	199.34.228.54	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.vzt.nl	185.159.242.66	true	false		unknown
cs511.wpc.edgecastcdn.net	152.199.21.140	true	false		high
cs672.wac.edgecastcdn.net	192.229.233.50	true	false		high
clients.l.google.com	216.58.212.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.161	true	false		high
officewayside.weebly.com	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
messaging.office.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
vztnl-my.sharepoint.com	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false		unknown
cdn.syndication.twimg.com	unknown	unknown	false		high
www.onenote.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
ton.twimg.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
ec.editmysite.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.vzt.nl/algemenevoorwaarden	true		unknown
http://https://vztnl-my.sharepoint.com/personal/mvanzaal_vzt_nl/_layouts/15/Doc.aspx?sourcedoc={c63a8beb-720b-402b-84e6-3d29936a3fd8}&action=view&wd=target%28VAN%20ZAAL%20TRANSPORT.one%7Cee96c080-a5a0-45b2-ab17-4c46e71e821a%2FVAN%20ZAAL%20TRANSPORT%7C8b790e4f-45a0-4569-b92d-4e687cda39f3%2F%29	true		unknown
http://https://www.vzt.nl/	true	• 0%, Virustotal, Browse	unknown
http://https://www.vzt.nl/vacatures	true		unknown
http://https://officewayside.weebly.com/	false		high
http://https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?rtime=EMODEjCg2Ug	true		unknown
http://https://platform.twitter.com/widgets/widget_iframe.a53eecb4584348a2ad32ec2ae21f6eae.html?origin=https%3A%2F%2Fwww.vzt.nl	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
192.229.233.50	cs672.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
74.125.140.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.196	www.google.com	United States		15169	GOOGLEUS	false
142.250.186.142	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
108.174.11.37	pop-esv5.mix.linkedin.com	United States		14413	LINKEDINUS	false
185.159.242.66	www.vzt.nl	Netherlands		48635	ASTRALUSNL	false
104.22.25.131	embed.tawk.to	United States		13335	CLOUDFLARENETUS	false
199.34.228.54	pages-wildcard.weebly.com	United States		27647	WEEBLYUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
104.26.7.220	www.freeprivacypolicy.com	United States		13335	CLOUDFLARENETUS	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
216.58.212.174	clients.l.google.com	United States		15169	GOOGLEUS	false
54.189.175.59	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.22.24.131	va.tawk.to	United States		13335	CLOUDFLARENETUS	false
13.104.208.160	i-db3p-cor005.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
152.199.21.140	cs511.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.8	syndication.twitter.com	United States		13414	TWITTERUS	false
40.108.231.27	187270-ipv4.farm.dprodmgd104.aa-rt.sharepoint.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.131	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
93.184.220.70	cs45.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
142.250.186.168	ssl-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	516205
Start date:	05.11.2021
Start time:	08:43:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?e=5%3ahV4RUj&at=9
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
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 • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.win@36/215@33/29
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://officewayside.weebly.com/ • Browse: https://www.vzt.nl/ • Browse: https://www.vzt.nl/vacatures • Browse: https://www.vzt.nl/algemenevoorwaarden
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0b4951b4-d0e4-4e71-9fc4-22dd46c3cf69.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):	380301
Entropy (8bit):	6.02771407872512
Encrypted:	false
SSDEEP:	6144:65qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:NfKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	4AA12560F6A03557F5E21845D8BD6ED8
SHA1:	FF83369942FE485E461AB12F7EAFC13FB7C173B7
SHA-256:	5B6ECDBB1CC3DE9D172D7C5F33CD2EFA56D5B6E7216CD362E4B38F824CE5061A
SHA-512:	1E9C38627DFD27AE399F5F60F5D5E19008500944603A0220505DD33AE9D62C0ADA0D9E37E4CED7F54A9D44802DE877855D7EF55D7DB450E99DB71DB0B345D6
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\0f15f81d-a2e2-434e-9a67-58ddd17ff18e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7512391398977583
Encrypted:	false
SSDEEP:	384:BrzQkmlnOhOYV9/EbNYrxvUw3bouTHOrG/CrtyEWxbS6uNrJQmtaBiowkLOmSoNj:h2Cl5m27TIeDK8GAfbaYKil01L
MD5:	94968980FCE87ED59EE57CCF86E80D2A
SHA1:	996650D95F6F0EEA9078B518F7496BB6378CA023
SHA-256:	7EC765660DA31615D53309EF84EFA4B2937E66C84AD347BB8AA752A460D3F9F9
SHA-512:	B2CBA79AAB5492E591FC63D90C085632D7119B877EAC3EEC3FAEB0CA9ED9812152BF09975D94BF650A0D8D97F019CA1A35E82E2DC7EDE91D729A341A463B9F3B
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.....*...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..._J8.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\121fd69f-b957-4895-a006-a33ff20a68aa.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):	388692
Entropy (8bit):	6.048450819661499
Encrypted:	false
SSDEEP:	6144:y5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:lfKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	59C93E5A6FD105CCBBCDBC94FF94FCB3
SHA1:	6D497DD864079B4CB08122D36FEC8403BB3CD0E1
SHA-256:	408C4A2260D37A3772FCA6F249111A537C908750074300E28C10C4B9FE0FE956

C:\Users\user\AppData\Local\Google\Chrome\User Data\121fd69f-b957-4895-a006-a33ff20a68aa.tmp	
SHA-512:	E51E188AAA0E294A802DEBB556210B88A93E23B611787B881AA80FC7C5FED8E3727DD27745AE22A9CF7F1BA28F6B6DC3D689AEC3BA21FC4F609A282B2DA47042
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4aa17048-b48a-4aa3-baf1-3b0bed51ffbe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7509136026305394
Encrypted:	false
SSDEEP:	384:nrzQkmlnKOJEbNYrxvUw3bouTHOrG/CrtyEWxbS6uNrJQmtaBiowkLOmSoNx1ohg:VCl5m27TIeDK8GAfbaYKiI01V
MD5:	5803E255B7CB1DFD9CC105D0A95F49A1
SHA1:	2D80608C4FE1817765BCB81801860B624BF2A503
SHA-256:	60D0F2A2C58BDC4F0E622C8EEDCEF0D7F8BC3D15011F6318A47D065969191BFE
SHA-512:	0D0A9F43F1572B4B55226E77650699003F67CA6CD65539DEB9F1A6F50E120976E167B784BE5FFDC4FD56C52C4D9493C6269F09104A5AF71FA0590B66138939E0
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..._J8.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\8fab66d0-c0c0-45ec-ab2f-9bf291b7af51.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7513041283196924
Encrypted:	false
SSDEEP:	384:xrzQkmlnOhOYV9/EbNYrxvUw3bouTHOrG/CrtyEWxbS6uNrJQmtBfBiowkLOmSow:x2Cl5m20TIeDK8GAfbaYKiI012
MD5:	4BA74987251F63ABCC50A16F504B0079
SHA1:	CDDF3C5313E2C214F5AE0A1384079853C6E0BC50
SHA-256:	16DE3ED6B6B53E01E21162DA7E2CBA90DB85E8DC9E70CC7612AA86ED91B58335
SHA-512:	07EB00D87EFB23EC2A9B3206B32C93EE4D6DC1ED1993747E0CFDBB85AC2AF4DF6FC2D033D56AAD6DFA3DC413850495DB8AABDC6CB0925705C1BB32E0B9E2C4E5
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..._J8.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\91e10707-f2fc-4de7-a82d-025d5e58dcf3.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):	380301
Entropy (8bit):	6.027714232218829
Encrypted:	false
SSDEEP:	6144:d5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:efKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	62E808A23902417D8A3930B7E5D63BD6
SHA1:	982E9563F0DF4BB61870F9BF2D50DB91890B54BA
SHA-256:	7BA7C368F120BC62036CB17CA80A86B79CBBCD952BDE9714219D4324EC55A57D
SHA-512:	8B84D3AC1B64A4EEE5FAD1A1AFB75B9BA4EA611CAAC5706E3C7C1C7DB751066B7DF706FDBB5478F50EA58A9E68B1A1745CCF099C0E2F74C9338D0B44F3BCDC38

C:\Users\user\AppData\Local\Google\Chrome\User Data\91e10707-f2fc-4de7-a82d-025d5e58dcf3.tmp

Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\986d42f7-8649-4b92-94b4-5d02b1873e4a.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):	388692
Entropy (8bit):	6.048451018491718
Encrypted:	false
SSDEEP:	6144:B5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:6fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	606664FD06CDED65700A21980D23129A
SHA1:	D71BB8ACE58D3BB558BE5282B8D1E604E3548A9C
SHA-256:	D883662A4C9CFB3754B98A097EA0C289941383F07304B313B8CB872E17733C53
SHA-512:	1C3389EB28115F48D614B6B867C55210468453F4DFF73B9A1888735936209466D0F91A1A2785854A4FFD1F6C50764905DB801F83A81DF0237B563FE6AD0CFFE6
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHn:+EwozZHn
MD5:	BEBB369FF4A565B19D5E0BC83CD176AE
SHA1:	A6F07666F8DDDF61E5AACE533129BFB541A8A769
SHA-256:	8018F98553432706436A31FFD1E743018C3B7F1AA8D34B2FA18F494A4CFCEB19
SHA-512:	5D2F9F6E9502517AFF4673C3157D57046D4E38D70B5E228F468FB820363E559087D1A2F2E4006B4589BF3F175A4507F1FA3D7BE5FC34F9FA39EB17757DAEC17F
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04c6cca4-0188-475f-ac99-d1ed562bc353.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):	3789
Entropy (8bit):	4.915213810953836
Encrypted:	false
SSDEEP:	96:HNOaXDHzQqp05HmC3rF56VSGiDGBoGwdGMGUGpYGafS:HNOaXDHzQqp05GC3j6VSrDKoF9vIYY
MD5:	273C43D21752C6647D7C070B46322DDD
SHA1:	4467D7874CB8666CD3C6A2DD3206D437740D1C7B
SHA-256:	77AEB51E3600BC400987AD9E48080B2B3946104EC395E021D88FECB152759ED6
SHA-512:	ACA24399C762940EC21FC8025834023D486558D39B07636F678639804EC3E10F8308807BC05A6CE04776C7A1A16133165B35C11A81553A7FBBC7AFAC7E246CB5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04c6cca4-0188-475f-ac99-d1ed562bc353.tmp

Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13283192657489347","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13283192657514167","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13283192657654724","port":44

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14aa6f6e-9895-4db4-9727-b671feffa61c.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):	5161
Entropy (8bit):	4.978369900353042
Encrypted:	false
SSDEEP:	96:nRXbCT/9paAKIkxk0JCKL8zkT1ffbOTQVuwn:nRXbU9p9O4KekTB7
MD5:	F002F8B4369585549CB0BC2F3D060166
SHA1:	27A3881B294E02C70683DDCB2D7300DBF3AFF112
SHA-256:	3D23E53B0485E8BB22D6538F7E3344DA4E843E51AABCBF0F967F15216F99E275
SHA-512:	52F18FA1251345F606226CE21AA902F23D87EA276D917B8D8A575DDDEF6CB1C57FA8FD2AB39C2FC69A559EE41EB27C74A523E583F39C55D055A80D8B360C3E 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1acbed87-8197-4359-9c2a-06279cf10548.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19182
Entropy (8bit):	5.569913927491441
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrUPHGEBvkhs4x:4Llnm1kXqKf/pUZNCgVLH2HfqrU/GRsG
MD5:	EB953263BAACE925EED19C3B1B7D8158
SHA1:	53FEC6B020D0DCA5F438B6CF1BA93F5A02654B58
SHA-256:	99BF89949E39AFA6030D21C799FD3A07FDB1C77C7E9CA5D24E148D4AF23835F3
SHA-512:	90A42FA422698187F81528A053D30A473EA8755CEDF155F8BBAAF56AB0CE8B6E0035BC659AE9F9D6516137ED524E4214A73981E2A3F0F37EA1DFFD592D720B6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\231ea2da-f740-431a-8097-6740c71b77fe.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):	5475
Entropy (8bit):	4.994312789290705
Encrypted:	false
SSDEEP:	96:nRXbt0L7/9paAKIVxk0JCKL8TkFjgrkBhjAbOTcSVuwn:nRXbi9p9V4KKkF8rkBBok
MD5:	110062AED86B9F6120F6D2613F912F38
SHA1:	4B3C9274D0906F68E346F2742B69C93CBA8E3DAA
SHA-256:	E58E081EB42D9F483200E3041E7BC6D73E7E91653D4EDE661D14B0D889F834A3
SHA-512:	C589D173651B9A3D678D3DF9DCC5FB1D80C5A811545D58F33C192865777674FDA35A9140255E8AEE37F9B9AEC632D609C11F8A49427C5CC1A51A627524FBD7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\231ea2da-f740-431a-8097-6740c71b77fe.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\258e079b-edbe-4112-b71f-7af796bb374c.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
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40e2a574-c4b4-4d2e-bc9e-b72ceb1bd68c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17092
Entropy (8bit):	5.582896832887841
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrU9Bvchs4f:4Llnm1kXqKf/pUZNCgVLH2HfqrU+sM
MD5:	6FC2F63CBEC1E76B48EAE52E37ED0140
SHA1:	FBA607248F47FEFFD391F2006847F9D2ACD26E3E
SHA-256:	79635E13361771D2402893604D47DF057831E309D71E734AF5339C3C9057AD24
SHA-512:	AD4A99B4AFC32CC3D0DAF49B1D215332F7AE3ACC33A147FB70F44A740780E5C878343586FC9E8047E1B5B090DA19BBD0E29592BB810AB4A90A5C4F7FB14281 0
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\425fe601-baa9-4cea-a0d8-b9cc59068067.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):	5502
Entropy (8bit):	4.999052606914048
Encrypted:	false
SSDEEP:	96:nRXbt0LZ/9paAKIVxk0JCKL8TkFjgrkBhjBbOTcSVuwn:nRXbG9p9V4KKkF8rkBBRk
MD5:	A4D12F4870AE317D1C81BDBC7D51667B
SHA1:	A1CCD07A3A7AD19ABD056F298366CE0B32AC6981
SHA-256:	7465AA3C9D8C352364CA391246C92F3D4CFA35FEA57B7D8BA3EB27B7FA3CACE4
SHA-512:	F3FE07A15EA4E356DD992E082716CD803CFBAAE9692402B6C757CED29041C3D306C7EE8E0D811604CDC17F0FAD44C11D7CBF52590A96B182E8B6787037BFF6 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\425fe601-baa9-4cea-a0d8-b9cc59068067.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\435de003-915b-44c8-b79d-0ce5c08395ae.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19181
Entropy (8bit):	5.569746020090754
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrUPHG1Bvchs4I:4Llnm1kXqKf/pUZNCgVLH2HfqrU/GWsn
MD5:	68BDC06A9D332EAB42A3E962B84911A0
SHA1:	FC8CB146A6FB122BF5D5B3012714137406E2BEF8
SHA-256:	E995B566FF9F369D58635DFDA66F3F5DC584E872CB3070C47FA4C83F2F3A5AA4
SHA-512:	371B816B77BD5F10DD8F71B0CB9C933204D7482C74B1BAC0F99FE04F97A9FBCA8BB72331DBF15F83840B0AB1CF0DDDC73F77E741F2C60AA80BBC2AD74A632 0D
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82313930-2534-4216-9555-736974a52c63.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535521318873734
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrUPHGAnT1Bvys4L:4Llnm1kXqKf/pUZNCgVLH2HfqrU/GAnk
MD5:	B2B80F82C22E5212E1688A82228A3BF2
SHA1:	8B078BC21BEF06218B09CC62110823ED6354D30C
SHA-256:	BD8F133AE32F673AB3196959662A69B258E7F6EE36184F8470AEC8E92DA58A27
SHA-512:	5E5FF0C9EB29A352E2A60CB950DF9AB935C7F9F50B49D8C4E32D2B84CF7D64CD4ABA7D19887D2D1530EE89D9564716D132FA194477D2F1F22F8A7DCD776063 9
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8550e2f8-0d6d-4c99-817b-61e6ba47022a.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8550e2f8-0d6d-4c99-817b-61e6ba47022a.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8683dfc9-5ae2-45e5-9c54-6836adc5dbce.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):	3724
Entropy (8bit):	4.915158679720832
Encrypted:	false
SSDEEP:	96:HQNOaXDHzQqp05HmC3rF56VSGdoxECdSoKkGAhS:HQNOaXDHzQqp05GC3j6VSqoxEuSonc
MD5:	9EF4595B7C260CF293ED92FCF1BC78E9
SHA1:	556728E5878B9EC7451ABF1E573215B1829FDB03
SHA-256:	5D3A8EF9D0DA1F9B292E4DC7ABEB4A96C0C1D18B4475774EEE6717366E4FC5AA
SHA-512:	6BF11537E1193AD82E674FDF85B020B62013D43060CD388D4C94F8CFCDBD4EDCF404335FE47384519850B5226DA569D7F14BCEE52AD39E9F50D9184EC9FBCDF
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13283192657489347","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13283192657514167","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a7b8998-c8de-47e6-af2b-4715a2fc6f31.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.229260785562624
Encrypted:	false
SSDEEP:	6:mH+/qM+q2PN723iKKdK25+Xqx8chI+IFUtQ+NZmw2+oMVkwON723iKKdK25+Xqx7:7qM+vVa5KkTXfchI3FUtz/cMV5Oa5KkI
MD5:	50248FDF9D8F46DBF5B11842F9C5E22C
SHA1:	A6FE66442B412B03EB3CDF7C0C07ECDC67FBC1D8
SHA-256:	EA532561466DBDA9AE4A9F489C829C7FD290F1A16FD973E37AF2A646EE6889BE
SHA-512:	3FE2E2323F5D83BB442FFE6B084CD0E9F8F4175FD11EC2DDDD466F24F010D7A3E031A373F605DB6FD9C98DAA665027E8EF68EDF8B495DF3A3AB029FF328945 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/11/05-08:44:32.702 bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/11/05-08:44:32.704 bfc Recovering log #3.2021/11/05-08:44:32.704 bfc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.229260785562624
Encrypted:	false
SSDEEP:	6:mH+/qM+q2PN723iKKdK25+Xqx8chI+IFUtQ+NZmw2+oMVkwON723iKKdK25+Xqx7:7qM+vVa5KkTXfchI3FUtz/cMV5Oa5KkI
MD5:	50248FDF9D8F46DBF5B11842F9C5E22C
SHA1:	A6FE66442B412B03EB3CDF7C0C07ECDC67FBC1D8
SHA-256:	EA532561466DBDA9AE4A9F489C829C7FD290F1A16FD973E37AF2A646EE6889BE
SHA-512:	3FE2E2323F5D83BB442FFE6B084CD0E9F8F4175FD11EC2DDDD466F24F010D7A3E031A373F605DB6FD9C98DAA665027E8EF68EDF8B495DF3A3AB029FF328945I 8
Malicious:	false
Reputation:	low
Preview:	2021/11/05-08:44:32.702 bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/11/05-08:44:32.704 bfc Recovering log #3.2021/11/05-08:44:32.704 bfc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4226
Entropy (8bit):	6.291640409116152
Encrypted:	false
SSDEEP:	96:E25HN4ciOl4cMWdYS2xBUSZ2fpS8lPlbtFpmUikeRN:n5vlS62kSKp/9ht3mUip
MD5:	7AAE72AECB035B7F4264332921482B21
SHA1:	F24C53C3E3029C5CB0A39BFD8A11B1D39BC6DBAF
SHA-256:	ADD7419DCE7DC43AACF43A49E0D9DF39C8832F1CF0E6F5373BA34633ECA6DA8A
SHA-512:	5F6B7DA354ACEC47088DCDF86EC05F98A0641CBB51F4878FFFB7CE29927C3EBE895D253AA3760EDAD51792447F17088E198DD60AF61B458753C95959287E614
Malicious:	false
Reputation:	low
Preview:	....."...?..15..3d29936a3fd8..402b..4569..45a0..45b2..4c46e71e821a..4e687cda39f3..720b..84e6..8b790e4f..a5a0..ab17..action..aspx..b92d..c63a8beb..com..doc..ee96c080..https..layouts..mvanzaal..my..nl..one..personal..sharepoint..sourcedoc..target..transport..van..view..vzt..vztnl..wd..zaal..emodejcg2ug.$euulosylcitahoy9kznqp9gbxbzhgwcxtg3s..g..o..rtime..zcfidxuxa..5..9..at..e..hv4ruj..3000..475f..5207..91852cc028a3..93a67f66..a18f...ahr0chm6ly92enrubc1tes5zagfyzxbvaw50lmnvbs86bzovzy9wzxjzb25hbc9tdmfuemfhbf92enrfbmwvrxv1te9zwuxjaxrbae9zoutatnfqowdcwgj6sgdxy1h0rzntlxpdzmlkwfvyqt9ydgltzt1ftu9erwpdzzjvzw..b01300a0..bc62..c0b6..cid..default..e3e44aeaa037..originalpath..slrid*...?....15.....3000.0....3d29936a3fd8.....402b.....4569.....45a0.....45b2.....475f.1....4c46e71e821a.....4e687cda39f3.....5.+....5207.2....720b.....84e6.....8b790e4f.....9.,....91852cc028a3.3....93a67f66.4....a18f.5....a5a0.....ab17.....action.....ahr0chm6ly92enrubc1tes5zagfyzxbvaw50lmnvbs86bzovzy9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\000003.log	
Size (bytes):	1051
Entropy (8bit):	3.700705179613882
Encrypted:	false
SSDEEP:	12:6XRMDj0dlkl5LMsbPXNNRq8lMAl05illvO1ajcyOTHMewsvH/IH7tB8FQ9flXVls:rn4lkzMsx7VMAYi/PjcyFeYF1Xs
MD5:	8E41B994F22AD340D10446AF09F7ABF9
SHA1:	129449110C1FA8E352764D25CCB6E27D72CCCBAC
SHA-256:	AEAF342A1F38CD1493329EC8D34248A82577664641485885C73BCA22F9E7B4E9
SHA-512:	D347E9508DB7D8BEEFC8B64EABF2961076257D5A8DE399BCADE4CEFA2038AC1D2ADA8A3443EF30864C5274930AA6B0B6DDBCD02FB0DCC7E345FB1E5EEEC2FDCB
Malicious:	false
Reputation:	low
Preview:	. .....2....(.o".....R.....i.....).h.t.t.p.s._.e.u.c.-.o.n.e.n.o.t.e...o.f.f.i.c.e.a.p.p.s...l.i.v.e...c.o.m._.0.@.1..h.e.a.l.t.h.D.b..... ...Of.jV.....2.....2.....2.....-.....2....h.e.a.l.t.h.E.v.e.n.t.s.....2.....2.....2.....2.....2.....2.....2..... .....h.e.a.l.t.h.E.v.e.n.t.s.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2..... .....2.....2.....2.....2.....2.....2.....". .....h.e.a.l.t.h.E.v.e.n.t.s..... .....2.....2.....2.....2.....2.....2.....2..... ....2.....2.....2.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\000005.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	850
Entropy (8bit):	5.3715204876864995
Encrypted:	false
SSDEEP:	24:DTn94IcnXf3n3bWofG2B5CrYuNThsA+e9Xeb9V+fSx0:DTnHcXTWovB5OYuLsc9XehXx0
MD5:	95F86A40B10993AE831C86FEA37376ED
SHA1:	92B6FCABA1AB0A625EA30C5BB75AC88C03CD287D
SHA-256:	06ABB653E715993543BA341698B2C23EC3242F6920DE54FE133D03AFE2EA3478
SHA-512:	53FCD376280F84AEE287129585CB2FA1EF3CA88EDFA3C579511AACD1EFFB3A2AE22FDFEC557332D4E0784A59B73F62C56A50CD9CE97C73E4916E80BF4D051DAC
Malicious:	false
Reputation:	low
Preview:	....(.....2...3$.....+.!..... ...."..... ...]|...h.e.a.l.t.h.E.v.e.n.t.s.....!.....9 2.....".."....."....."....#..".....".....$.....2.....2..... ..%...T.....T.....&..."....."....."....'..."....."....."....(..."....."....."....).....! .....*..... .....m..).h.t.t.p.s._.e.u.c.-.o.n%.@o.t.e...o.f.f.i.c%..p....l.i.!.<..c.o.m._.0.@.1.2...D.b.....A]... .....M5.....$....2.....Z5.....# .....i.....A.....".b....aA.M..,-.....7w".491.Lb.%.....!. .....$. .X$.....$l.....7.....2...".filter .leveldb.BuiltinBloomFilter2..@.....[b.Y.&.....h.e.a.l.t.h.E.v.e.n.t.s.....D!..0..4.....W...$uG.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	451
Entropy (8bit):	5.321625962264694
Encrypted:	false
SSDEEP:	12:W+vVa5KkKiSQcdiFUtSVWf00hfnJguerRoT:/Va5KkNLcdWgSVX0kuerk
MD5:	64A0964694CF9BAE22B921C9BDAFC07C
SHA1:	7D699B89560EB1D6D60913E316FDFB923BF9A9D6
SHA-256:	1F1ED458CE5EEEA5C1BE08DFEC35482898A5AD8A4CA210ECEB3E32F05A608615

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\LOG	
SHA-512:	2F54A3A8CC4C1EF9A401EAD18D5CB5F7E27A1F1A6FF942036C13E61F215A08E0FD2120D5605258A5EBF8921B7ABD0E3659F9E4BDA7976AF1AAEF93F7243D0E6
Malicious:	false
Reputation:	low
Preview:	2021/11/05-08:44:20.505 160c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb/MANIFEST-000001.2021/11/05-08:46:11.363 b7c Level-0 table #5: started.2021/11/05-08:46:12.169 b7c Level-0 table #5: 850 bytes OK.2021/11/05-08:46:12.172 b7c Delete type=0 #3.2021/11/05-08:46:12.173 b7c Manual compaction at level-0 from (begin) .. (end); will stop at (end).

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_euc-onenote.officeapps.live.com_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.086325104814544
Encrypted:	false
SSDEEP:	3:Fdb+4L8hunTOinyj4/llltpXaGDNlWaRw4X/:ZFnC94/ll3Eyzm4X/
MD5:	6C00A86CC4D64371324BADCB881FDD50
SHA1:	E07B1B011CB807FFA4EF9EB28B64E9EEDF6CF155
SHA-256:	888658E723E73097FE802E50F6DEE23A720B813747FF8C74394D5C6A5AA39402
SHA-512:	56F22E0B68B6E9A9C5DD991526D8BA0BF8131DA3EC6BCE489EB54B495371B5FAE6C8B79CCB4853A6BD2F6ACCA5AF0CAF6185848319E153C71C5A0DEA76FB34A8
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....B.....+.....&.....h.e.a.l.t.h.E.v.e.n.t.s.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2825
Entropy (8bit):	4.864734775786638
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9G:HQxGKWDS1i/5vYGmGqOGKJ03QshH
MD5:	4475D531A97CBC19BC6E1798BB10FF23
SHA1:	ACC646E47AFD877D4E7272A11BC34B3FE79E62FD
SHA-256:	89D7C4916871A486928BD9FA996D1FD613E6ADEDD2E10B1CAB2ADF20BBF47C33
SHA-512:	277EF14539AF646C3A5790B1BE427EA7A0900B5543611E5BA0CCE85D07216E0EF4FE747088E37C9185E18F4086EED4CBE7E3A31002D845E72B96E531D763C47D
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5475
Entropy (8bit):	4.994312789290705
Encrypted:	false
SSDEEP:	96:nRXbt0L7/9paAKIVxk0JCKL8TkFjgrkBhjAbOTcSVuwn:nRXbi9p9V4KKkF8rkBBok
MD5:	110062AED86B9F6120F6D2613F912F38
SHA1:	4B3C9274D0906F68E346F2742B69C93CBA8E3DAA
SHA-256:	E58E081EB42D9F483200E3041E7BC6D73E7E91653D4EDE661D14B0D889F834A3
SHA-512:	C589D173651B9A3D678D3DF9DCC5FB1D80C5A811545D58F33C192865777674FDA35A9140255E8AEE37F9B9AEC632D609C11F8A49427C5CC1A51A627524FBD7D
Malicious:	false
Reputation:	low

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

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5502
Entropy (8bit):	4.999052606914048
Encrypted:	false
SSDEEP:	96:nRXbt0LZ/9paAKIVxk0JCKL8TkFjgrkBhjBbOTcSVuwn:nRXbG9p9V4KKkF8rkBBRk
MD5:	A4D12F4870AE317D1C81BDBC7D51667B
SHA1:	A1CCD07A3A7AD19ABD056F298366CE0B32AC6981
SHA-256:	7465AA3C9D8C352364CA391246C92F3D4CFA35FEA57B7D8BA3EB27B7FA3CACE4
SHA-512:	F3FE07A15EA4E356DD992E082716CD803CFBAAE9692402B6C757CED29041C3D306C7EE8E0D811604CDC17F0FAD44C11D7CBF52590A96B182E8B6787037BFF64
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5260
Entropy (8bit):	4.978752904900634
Encrypted:	false
SSDEEP:	96:nRXbt0L7/9paAKIwxk0JCKL8TkFj1jbOTcnVuwn:nRXbi9p9e4KKkFZ3Z
MD5:	2E6AAA7D9AD0B73810F8FCAF7C74836E
SHA1:	8F1DA47294FE791F914549EC6085496D976905E4
SHA-256:	881AD4974F99442B41B6848A0509452ADF70619830C5800AE7439C7712AA53A2
SHA-512:	77A4D0C2C082C6599B59EEA86E02609249B029726CEF6B40D1CEF54A5567F6E35C633E78C533335267A67021E939D55BA3E83251DDB5347D93244D3B02A3A9E8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19181
Entropy (8bit):	5.569746020090754
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrUPHG1Bvchs4I:4Llnm1kXqKf/pUZNCgVLH2HfqrU/GWsn
MD5:	68BDC06A9D332EAB42A3E962B84911A0
SHA1:	FC8CB146A6FB122BF5D5B3012714137406E2BEF8
SHA-256:	E995B566FF9F369D58635DFDA66F3F5DC584E872CB3070C47FA4C83F2F3A5AA4
SHA-512:	371B816B77BD5F10DD8F71B0CB9C933204D7482C74B1BAC0F99FE04F97A9FBCA8BB72331DBF15F83840B0AB1CF0DDDC73F77E741F2C60AA80BBC2AD74A6322 0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19182
Entropy (8bit):	5.569913927491441
Encrypted:	false
SSDEEP:	384:9ewtgLl3HXm1kXqKf/pUZNCgVLH2HfDWrUPHGEBvkhs4x:4Llnm1kXqKf/pUZNCgVLH2HfqrU/GRsG
MD5:	EB953263BAACE925EED19C3B1B7D8158
SHA1:	53FEC6B020D0DCA5F438B6CF1BA93F5A02654B58
SHA-256:	99BF89949E39AFA6030D21C799FD3A07FDB1C77C7E9CA5D24E148D4AF23835F3
SHA-512:	90A42FA422698187F81528A053D30A473EA8755CEDF155F8BBAAF56AB0CE8B6E0035BC659AE9F9D6516137ED524E4214A73981E2A3F0F37EA1DFFD592D720B6(
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\be785a6f-ad71-4b15-a857-96ed2afe8d9a\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\be785a6f-ad71-4b15-a857-96ed2afe8d9a\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	3:TnGON00EPfc:S3Pk
MD5:	0B3654915C8F4A0F9400A686D00FDD44
SHA1:	C3695CF5C2690170A21F75A4D4DE6423FAB20711
SHA-256:	98FB1FF7E0B9631D34F7DE4F5E3F762EFC64B7695B4E479D441C843316584B1D
SHA-512:	F9A325405BA26F109291E260DDF9C167E8FDADE3CB0AE87860DC5E665F6ED4557B817153C56FA61B0CB5FB19638B6ECC5AB4CE3021937EB21FAE62CBA8404F98
Malicious:	false
Reputation:	low
Preview:	(.....+oy retne...../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\be785a6f-ad71-4b15-a857-96ed2afe8d9a\index-dir\the-real-indexP. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	3:TnGON00EPfc:S3Pk
MD5:	0B3654915C8F4A0F9400A686D00FDD44
SHA1:	C3695CF5C2690170A21F75A4D4DE6423FAB20711
SHA-256:	98FB1FF7E0B9631D34F7DE4F5E3F762EFC64B7695B4E479D441C843316584B1D
SHA-512:	F9A325405BA26F109291E260DDF9C167E8FDADE3CB0AE87860DC5E665F6ED4557B817153C56FA61B0CB5FB19638B6ECC5AB4CE3021937EB21FAE62CBA8404F98
Malicious:	false
Reputation:	low
Preview:	(.....+oy retne...../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\index.txt (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	118
Entropy (8bit):	5.524024142648763
Encrypted:	false
SSDEEP:	3:2NsJ0K0FSEwsp1BvcWPL3zOL3N35D7uSkGD8uTc:2Nxv3Hp1BEWPe3N17uSkPcc
MD5:	3FA33DB129427D47AEA5C85F411C3456
SHA1:	F036D128CB3BEE8965E5B6D5ED4578CEABAADB6B
SHA-256:	195F043A31A1694E04E6A43067B40B14DEE55E5CD8A4DBC53E639F1A19BCD02D
SHA-512:	7E23D4FFCE4A0BB3994461C5A6366CAC1A11A9415ACF9DA0C3620BFCCAA34F54E1BBD258C645062493EDB6B611A2C3DE86A136E7F64E578BD1864C066CD7B96
Malicious:	false
Reputation:	low
Preview:	.J..shelluxlog.$be785a6f-ad71-4b15-a857-96ed2afe8d9a..".....E...Ri..S.(.0..(https://euc-onenote.officeapps.live.com/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\index.txt. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	118
Entropy (8bit):	5.524024142648763
Encrypted:	false
SSDEEP:	3:2NsJ0K0FSEwsp1BvcWPL3zOL3N35D7uSkGD8uTc:2Nxv3Hp1BEWPe3N17uSkPcc
MD5:	3FA33DB129427D47AEA5C85F411C3456
SHA1:	F036D128CB3BEE8965E5B6D5ED4578CEABAADB6B
SHA-256:	195F043A31A1694E04E6A43067B40B14DEE55E5CD8A4DBC53E639F1A19BCD02D
SHA-512:	7E23D4FFCE4A0BB3994461C5A6366CAC1A11A9415ACF9DA0C3620BFCCAA34F54E1BBD258C645062493EDB6B611A2C3DE86A136E7F64E578BD1864C066CD7B96
Malicious:	false
Reputation:	low
Preview:	.J..shelluxlog.$be785a6f-ad71-4b15-a857-96ed2afe8d9a..".....E...Ri..S.(.0..(https://euc-onenote.officeapps.live.com/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\index.txt.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	118
Entropy (8bit):	5.524024142648763
Encrypted:	false
SSDEEP:	3:2NsJ0K0FSEwsp1BvcWPL3zOL3N35D7uSkGD8uTc:2Nxv3Hp1BEWPe3N17uSkPcc
MD5:	3FA33DB129427D47AEA5C85F411C3456
SHA1:	F036D128CB3BEE8965E5B6D5ED4578CEABAADB6B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\e6b36ac5f5cc9cbcdac0c08392db25625d539905\index.txt.tmp

SHA-256:	195F043A31A1694E04E6A43067B40B14DEE55E5CD8A4DBC53E639F1A19BCD02D
SHA-512:	7E23D4FFCE4A0BB3994461C5A6366CAC1A11A9415ACF9DA0C3620BFCCAA34F54E1BBD258C645062493EDB6B611A2C3DE86A136E7F64E578BD1864C066CD7B96
Malicious:	false
Reputation:	low
Preview:	.J..shelluxlog.$be785a6f-ad71-4b15-a857-96ed2afe8d9a..".....E...Ri..S.(.0..(https://euc-onenote.officeapps.live.com/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\3b57046a-a87c-4550-8d87-0760b8408cc0.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\6ae47188-9dea-4aa8-966c-f51e5997aee6.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957678621686452
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdSZsBdLJlyH7E4f3K3X
MD5:	93D2E0EFF548FC5E2DA9EC4E630D565B
SHA1:	3D0F4AF0C9516FB2FFE8690E7E932062BF2F147B
SHA-256:	D0044287A77347B99FB2FE2D4DE94B11EDE6659696A45D5874CA31312D2239FF
SHA-512:	3D9F2000B6F8B9DD108BFE62790E2A9E4D2742AFA0819464F7FB0C4E77B9A3DA860F326B985A6E37087141F5AA8DE959DC4218DD05EA3F6F90F1899B632CF13
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent StateMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\ab842098-936c-4d4d-8f14-db4c50a135a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957678621686452
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdSZsBdLJlyH7E4f3K3X
MD5:	93D2E0EFF548FC5E2DA9EC4E630D565B
SHA1:	3D0F4AF0C9516FB2FFE8690E7E932062BF2F147B
SHA-256:	D0044287A77347B99FB2FE2D4DE94B11EDE6659696A45D5874CA31312D2239FF
SHA-512:	3D9F2000B6F8B9DD108BFE62790E2A9E4D2742AFA0819464F7FB0C4E77B9A3DA860F326B985A6E37087141F5AA8DE959DC4218DD05EA3F6F90F1899B632CF13
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I 58
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E6 67
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.16113721736112
Encrypted:	false
SSDEEP:	12:sTvVa5KkkGHArAFUtaGm/En5Oa5KkkGHArfJ:OVa5KkkGgkgnOa5KkkGgV
MD5:	5151CE25743307A0173D00083E0E4404
SHA1:	67517D6C79F494B8EF1B8C973B88FEFDDB4043B1
SHA-256:	2C89AA6C31FD902FA075AFB5263755B712E9DBBDE617B1957D1C466939FEFF8D
SHA-512:	B4CF1DE109921603B61879967C879CDAF5ECFA220F4F08045B704239E559B7FC01B8C880808EBA39E25BE128450DA572A3B51251F0282D045AF4EC6D670CC465
Malicious:	false
Reputation:	low
Preview:	2021/11/05-08:45:45.822 b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/11/05-08:45:45.823 b50 Recovering log #3.2021/11/05-08:45:45.825 b50 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.16113721736112
Encrypted:	false
SSDEEP:	12:sTvVa5KkkGHArAFUtaGm/En5Oa5KkkGHArfJ:OVa5KkkGgkgnOa5KkkGgV
MD5:	5151CE25743307A0173D00083E0E4404
SHA1:	67517D6C79F494B8EF1B8C973B88FEFDDB4043B1
SHA-256:	2C89AA6C31FD902FA075AFB5263755B712E9DBBDE617B1957D1C466939FEFF8D
SHA-512:	B4CF1DE109921603B61879967C879CDAF5ECFA220F4F08045B704239E559B7FC01B8C880808EBA39E25BE128450DA572A3B51251F0282D045AF4EC6D670CC465
Malicious:	false
Reputation:	low
Preview:	2021/11/05-08:45:45.822 b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/11/05-08:45:45.823 b50 Recovering log #3.2021/11/05-08:45:45.825 b50 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\c9bf6c43-a4a6-46ab-a1d5-80529051edd3.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A 0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.274971768552856
Encrypted:	false
SSDEEP:	12:c/vVa5KkkOrsFUtS7Z/07z5Oa5KkkOrzJ:cHVa5Kk+gSS5Oa5Kkn
MD5:	662FBDEE20969CB3A4A04D8E3FEAF959
SHA1:	48CA48F8047EBC0503D13E57D98F8517E594D285
SHA-256:	BACECC80814533F1E867F5A6540D1D65A589A3ABE43F7ABDFFBA3F25D729C2C7
SHA-512:	886E5B7BBB412BC847B80ABCAC298A791C31FE82A9C1E3984A5C09BCA303F4398A3911ECDB0AB59D43E0B0E575D4F63A55FB0A3A6BF1AB0B691C94F3E5CBF 507
Malicious:	false
Reputation:	low
Preview:	2021/11/05-08:46:41.532 1e24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/11/05-08:46:41.533 1e24 Recovering log #3.2021/11/05-08:46:41.533 1e24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\af6a1fd2-43f2-4931-b5b4-f48bd962ea2f.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):	5260
Entropy (8bit):	4.978752904900634
Encrypted:	false
SSDEEP:	96:nRXbt0L7/9paAKIwxk0JCKL8TkFj1jbOTcnVuwn:nRXbi9p9e4KKkFZ3Z
MD5:	2E6AAA7D9AD0B73810F8FCAF7C74836E
SHA1:	8F1DA47294FE791F914549EC6085496D976905E4
SHA-256:	881AD4974F99442B41B6848A0509452ADF70619830C5800AE7439C7712AA53A2
SHA-512:	77A4D0C2C082C6599B59EEA86E02609249B029726CEF6B40D1CEF54A5567F6E35C633E78C533335267A67021E939D55BA3E83251DDB5347D93244D3B02A3A9E8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4697215-8a3c-4dbf-97cf-78e6637a8549.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):	371
Entropy (8bit):	5.4477143429126595
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4697215-8a3c-4dbf-97cf-78e6637a8549.tmp	
SSDEEP:	6:YAQNPaU69RfSHJR8wXwlmUUAnIMp5kc2UpJeKb/rNSTWhh4Dj8wXwlmUUAnIMOkw:YJaU69RAJ9+UAnInDUpAKb/rNgmh4r+y
MD5:	0530750EE3A802E83B8E1BDD2944F203
SHA1:	31124CCFCE67350FCB34D2914AF98FDB67DA1FF6
SHA-256:	01EBED8C7DAB95C66E68E4407FB390564D33DD57BDDDD0CA611280E5C6797243
SHA-512:	158AD8FB0D8DB1FDCB0925483D836E6CBFA4992E6BC6C84888FCC0637A9DC5557ED63B1D1272ACE9A7CE596A44E33414826175A1E8B81D2388D074C44585B95
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1667663092.710264,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1636127092.710269},{"expiry":1667663083.972226,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1636127083.972232}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c72f5f44-c458-45bf-9016-51e76d2c568c.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):	369
Entropy (8bit):	5.445505315502751
Encrypted:	false
SSDEEP:	6:YAQNPgH09RfSHJR8wXwlmUUAnIMp5kc6RGJeBKb/rNSTWhh4Dj8wXwlmUUAnIMOf:YJZ9RAJ9+UAnIn5QAKb/rNgmh4r+UAno
MD5:	3D305AAAC8287754EC9E2B61578A028E
SHA1:	276DFFF617A9C63A37A1D4E4E581214C42DBB201
SHA-256:	D28E1A0045D655C31BB29593777AE1CAABE487E5BC52315D50BC80C8722F1EF8
SHA-512:	B31E70F3287EBC29CA605A2C11411A1F8215C2649B1F78DA820D93D06E4454417372E2D6677EA3227522EF10DD0D6ECE76FEAB63D048F2856230B455F9C88340
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1667663099.8622,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1636127099.862206},{"expiry":1667663083.972226,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1636127083.972232}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c7e48424-f6e4-4ad7-8814-73af7ebf2f8b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577353973011821
Encrypted:	false
SSDEEP:	384:9ewt1Ll3HXm1kXqKf/pUZNCgVLH2HfDWrUd5vRs4p:tLlnm1kXqKf/pUZNCgVLH2HfqrUls6
MD5:	2E088412F874C48E92FDB1279E708C4E
SHA1:	98F02E550FB6DF7958E1B5BFE6096CA33E58E5F4
SHA-256:	87D2F494D122C42BBD07DCA79C26960E75502AF382750C4EF4532EDA474BFF90
SHA-512:	E88C27E66B0ED53D82D2181FAB76384718A30DB353F1E9F2C46ABB674554155387839F6C860F7D6F38141845FCC06869870FC1E86431CC82AF352018C2D65885
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280600654892956","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e7ad6b51-7857-44d3-b944-15f591433305.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):	6098
Entropy (8bit):	5.198519654875093
Encrypted:	false
SSDEEP:	96:nRXbt0LM/996GQaAKIVxk0JCKL8TkFjgjkNMkltbOTcSVuwn:nRXbr90X9V4KKkF8jkNhFk
MD5:	66BA6A1BE897F50B3BE467552B126F17
SHA1:	2BB8CC6A3726C33A5E3E7252CA2F1114B816BDE8
SHA-256:	1C07D7B0A2F7A4964BA135A35D6255995FB677B68AFB8699EA87B24B7C0015C2
SHA-512:	C82922CE14B62CD00539978BD9719138F6BA5A54CA91627C33059BD36197A4C55D6ACD7EAB74BB0D83D7CAA51EE4242BF6EB484FC016401FC66201B219A19BE A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280600655473246","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f17c999e-afa4-4050-9f49-f83a46622429.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):	2825
Entropy (8bit):	4.864734775786638
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9G:HQxGKWDS1i/5vYGmGqOGKJ03QshH
MD5:	4475D531A97CBC19BC6E1798BB10FF23
SHA1:	ACC646E47AFD877D4E7272A11BC34B3FE79E62FD
SHA-256:	89D7C4916871A486928BD9FA996D1FD613E6ADEDD2E10B1CAB2ADF20BBF47C33
SHA-512:	277EF14539AF646C3A5790B1BE427EA7A0900B5543611E5BA0CCE85D07216E0EF4FE747088E37C9185E18F4086EED4CBE7E3A31002D845E72B96E531D763C47D
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_ count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"132485449526 75493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"adve rtised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternati ve_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spd y":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4(
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	380207
Entropy (8bit):	6.02753972963522
Encrypted:	false
SSDEEP:	6144:95qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:+fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	982ED40D0C9058BB4FA659C7EB649ABC
SHA1:	346738F43B711B167DAD5109B6ACF7E418AA2242
SHA-256:	C2034715477E74CA1D18D9FDCBD274338CBB7711EFECB69215FE84E3EC1E172A
SHA-512:	761C1A9D2A6FA31F09735B2BAF95C404F87F7C549899C096CC7B28EE8C90F912FE16080A1BEF036C25A0B379A3E25C61C4CBBF68E7A77D1F405B58DF0F9BB721
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	380207
Entropy (8bit):	6.027539677091094
Encrypted:	false
SSDEEP:	6144:A5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:7fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	2D9FE24998333A2131720708A9F13CE2
SHA1:	EC7FF929BA0C59A3E900D6A3CC498323FB0C116F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
SHA-256:	9068CA360E03C6705CACA90A97F516B2E5D4D928654EF13214E944DA529095B9
SHA-512:	392E6EF9C846F99E473894A145B43C414BE34D76C731A5BBE447FD20A4F20E32F1DE5D5013BF94EFCA99C3039A73BDB85E5F9B5335442100DCA6552AEFE9B4AF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateQ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	388691
Entropy (8bit):	6.048451269918974
Encrypted:	false
SSDEEP:	6144:z5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:kfKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	0BA19538225CC0A52FFFDB5599C12283
SHA1:	E5C39C56068863FF5B203F8FF505BF9A0C79CF1C
SHA-256:	FA53A3D788A6894FAAB66D5974981DFF0854D1BAEDEA16C970C9426CA2D08D18
SHA-512:	12308651EA4D3783AE7383E382494063078D79F48B837CFE7DD2222B54A1A4EBF97632F5172856D961CBA8BC60CEA945459D2CA49EE1157DD1CF6334E6919912
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7513041283196924
Encrypted:	false
SSDEEP:	384:xrzQkmlnOhOYV9/EbNYrxvUw3bouTHOrG/CrtyEWxbS6uNrJQmtBfBiowkLOmSow:x2Cl5m20TIeDK8GAfbaYKiI012
MD5:	4BA74987251F63ABCC50A16F504B0079
SHA1:	CDDF3C5313E2C214F5AE0A1384079853C6E0BC50
SHA-256:	16DE3ED6B6B53E01E21162DA7E2CBA90DB85E8DC9E70CC7612AA86ED91B58335
SHA-512:	07EB00D87EFB23EC2A9B3206B32C93EE4D6DC1ED1993747E0CFDBB85AC2AF4DF6FC2D033D56AAD6DFA3DC413850495DB8AABDC6CB0925705C1BB32E0B9E2C4E5
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..._J8.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\Module Info Cacher (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7509136026305394
Encrypted:	false
SSDEEP:	384:nrzQkmlnKOJEbNYrxvUw3bouTHOrG/CrtyEWxbS6uNrJQmtaBiowkLOmSoNx1ohg:VCl5m27TIeDK8GAfbaYKiI01V
MD5:	5803E255B7CB1DFD9CC105D0A95F49A1
SHA1:	2D80608C4FE1817765BCB81801860B624BF2A503
SHA-256:	60D0F2A2C58BDC4F0E622C8EEDCEF0D7F8BC3D15011F6318A47D065969191BFE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cacher (copy)

SHA-512:	0D0A9F43F1572B4B55226E77650699003F67CA6CD65539DEB9F1A6F50E120976E167B784BE5FFDC4FD56C52C4D9493C6269F09104A5AF71FA0590B66138939E0
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..._J8.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\a5c34fb8-309e-4931-ae69-cfa882eddd75.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):	388691
Entropy (8bit):	6.048451269918974
Encrypted:	false
SSDEEP:	6144:z5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:kfKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	0BA19538225CC0A52FFFDB5599C12283
SHA1:	E5C39C56068863FF5B203F8FF505BF9A0C79CF1C
SHA-256:	FA53A3D788A6894FAAB66D5974981DFF0854D1BAEDEA16C970C9426CA2D08D18
SHA-512:	12308651EA4D3783AE7383E382494063078D79F48B837CFE7DD2222B54A1A4EBF97632F5172856D961CBA8BC60CEA945459D2CA49EE1157DD1CF6334E6919912
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\b9605b12-d85e-46f8-8653-deae86a7e2a4.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):	388691
Entropy (8bit):	6.048451068786157
Encrypted:	false
SSDEEP:	6144:a5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:tfKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	939879F42BE2F4815F711D8337DD7C36
SHA1:	E1C57AE9CF433CF161C5E6EAEEFC133CC846FA8C
SHA-256:	C44C3106A6A79E3D6BD88CA64E84E733BCB1A0D0121C510B6638C52F9C86D9B8
SHA-512:	A42504CD9DD5518ED6842F382A44EAD4835DE087D046937685B74ECAE74DF1A99C1EF9F221F0DAC78A969CDE7559FE5091C8D8EE42664B98ADC6CFBE989FC13
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\c3d5b237-92ef-42d6-b5eb-ba743b21ca1c.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):	380207
Entropy (8bit):	6.02753972963522
Encrypted:	false
SSDEEP:	6144:95qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:+fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	982ED40D0C9058BB4FA659C7EB649ABC
SHA1:	346738F43B711B167DAD5109B6ACF7E418AA2242
SHA-256:	C2034715477E74CA1D18D9FDCBD274338CBB7711EFECB69215FE84E3EC1E172A

C:\Users\user\AppData\Local\Google\Chrome\User Data\c3d5b237-92ef-42d6-b5eb-ba743b21ca1c.tmp	
SHA-512:	761C1A9D2A6FA31F09735B2BAF95C404F87F7C549899C096CC7B28EE8C90F912FE16080A1BEF036C25A0B379A3E25C61C4CBBF68E7A77D1F405B58DF0F9BB721
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e0f2f360-9c45-438f-ba54-faf1988f84f3.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):	380207
Entropy (8bit):	6.02753972963522
Encrypted:	false
SSDEEP:	6144:95qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:+fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	982ED40D0C9058BB4FA659C7EB649ABC
SHA1:	346738F43B711B167DAD5109B6ACF7E418AA2242
SHA-256:	C2034715477E74CA1D18D9FDCBD274338CBB7711EFECB69215FE84E3EC1E172A
SHA-512:	761C1A9D2A6FA31F09735B2BAF95C404F87F7C549899C096CC7B28EE8C90F912FE16080A1BEF036C25A0B379A3E25C61C4CBBF68E7A77D1F405B58DF0F9BB721
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\f886a1ca-f242-41a5-8a93-3157a719445a.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):	380207
Entropy (8bit):	6.027539677091094
Encrypted:	false
SSDEEP:	6144:A5qfA+gDZF5MZqDl0AG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinl:7fKZfMZqDRGNPUZ+w7wJHyEtAW0
MD5:	2D9FE24998333A2131720708A9F13CE2
SHA1:	EC7FF929BA0C59A3E900D6A3CC498323FB0C116F
SHA-256:	9068CA360E03C6705CACA90A97F516B2E5D4D928654EF13214E944DA529095B9
SHA-512:	392E6EF9C846F99E473894A145B43C414BE34D76C731A5BBE447FD20A4F20E32F1DE5D5013BF94EFCA99C3039A73BDB85E5F9B5335442100DCA6552AEFE9B4AF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.636127056949658e+12,"network":1.636098258e+12,"ticks":166908945.0,"uncertainty":3939152.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488019533"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\449dfbd3-9b61-4822-835a-d71f52895d15.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916

C:\Users\user\AppData\Local\Temp\449dfbd3-9b61-4822-835a-d71f52895d15.tmp	
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.l...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\5924_2024320734_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F52
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uliwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_pnacl_json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C3E
Malicious:	false
Reputation:	low
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A1580
Malicious:	false

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p .....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95F
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h.....fff..... .....J.$<[.,$J.l=....J.$<....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_ client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Preview:	.ELF.....>..... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@...`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A631E
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333EA
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `...;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:...D...K...T ...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt_abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E38B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Preview:	!<arch>./ 0 0 0 0 94 `....._pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62FC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `....._pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....!.....!.....'.....G..... .....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i..... ..0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."..".."..".....@.....`..... ...@...`..... ...@...`..... ...@...`..... ...@...`.....`... ...@...`.....`...`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870FE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

C:\Users\user\AppData\Local\Temp\5924_2024320734_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y..... .....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`... ...@... @.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..? .y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\5924_2024320734\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C 2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5924_2024320734\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",. "name": "PNaCl Translator Multi-CRX",. "manifest_version": 2,. "minimum_chrome_version": "30.0.0.0",. "version": "0.57.44.2492",. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\969b2941-83c6-4e0f-b25a-d6657478a755.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
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\a92e0b9c-ebcb-40c5-b235-69a3c02132c9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp\a92e0b9c-ebcb-40c5-b235-69a3c02132c9.tmp	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\cb6479d2-1770-4a55-919f-2f059e3f9a3b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(...>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\ca\messages.json	
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CE B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885 B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5924_1029456932\CRX_INSTALL_locales\de\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 5, 2021 08:44:17.359812021 CET	192.168.2.6	8.8.8.8	0x4970	Standard query (0)	vztnl-my.sharepoint.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:17.462770939 CET	192.168.2.6	8.8.8.8	0xfbb6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:17.467504978 CET	192.168.2.6	8.8.8.8	0x6719	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:19.132209063 CET	192.168.2.6	8.8.8.8	0xb5c0	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:28.858696938 CET	192.168.2.6	8.8.8.8	0xdfef	Standard query (0)	amcdn.msftauth.net	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:31.967278957 CET	192.168.2.6	8.8.8.8	0x22b1	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:32.153986931 CET	192.168.2.6	8.8.8.8	0x53bf	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:32.522413969 CET	192.168.2.6	8.8.8.8	0xed53	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:33.542860031 CET	192.168.2.6	8.8.8.8	0xc33c	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:39.199045897 CET	192.168.2.6	8.8.8.8	0xd17	Standard query (0)	officewayside.weebly.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:39.851694107 CET	192.168.2.6	8.8.8.8	0xa628	Standard query (0)	messaging.office.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:40.147746086 CET	192.168.2.6	8.8.8.8	0x52c5	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.287204981 CET	192.168.2.6	8.8.8.8	0x3b05	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.608175039 CET	192.168.2.6	8.8.8.8	0xfe81	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:43.058093071 CET	192.168.2.6	8.8.8.8	0x40b3	Standard query (0)	officewayside.weebly.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:43.225164890 CET	192.168.2.6	8.8.8.8	0x2574	Standard query (0)	www.vzt.nl	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.307845116 CET	192.168.2.6	8.8.8.8	0x1965	Standard query (0)	www.freeprivacypolicy.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.478915930 CET	192.168.2.6	8.8.8.8	0x9d56	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.702235937 CET	192.168.2.6	8.8.8.8	0xce29	Standard query (0)	embed.tawk.to	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:45.331959963 CET	192.168.2.6	8.8.8.8	0x3dc9	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:45.344944000 CET	192.168.2.6	8.8.8.8	0x7039	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 5, 2021 08:44:45.538989067 CET	192.168.2.6	8.8.8.8	0x34e8	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.738662004 CET	192.168.2.6	8.8.8.8	0x7a3	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.785864115 CET	192.168.2.6	8.8.8.8	0x7c5e	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.828006983 CET	192.168.2.6	8.8.8.8	0x1a79	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.104110003 CET	192.168.2.6	8.8.8.8	0xaf9f	Standard query (0)	www.vzt.nl	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.433672905 CET	192.168.2.6	8.8.8.8	0x1ff0	Standard query (0)	syndication.twitter.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.779333115 CET	192.168.2.6	8.8.8.8	0xbec9	Standard query (0)	va.tawk.to	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.959992886 CET	192.168.2.6	8.8.8.8	0x3bed	Standard query (0)	cdn.syndication.twimg.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.345818043 CET	192.168.2.6	8.8.8.8	0xbc10	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.496726990 CET	192.168.2.6	8.8.8.8	0x8500	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.654261112 CET	192.168.2.6	8.8.8.8	0x8e7	Standard query (0)	ton.twimg.com	A (IP address)	IN (0x0001)
Nov 5, 2021 08:45:35.344067097 CET	192.168.2.6	8.8.8.8	0xc9ad	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 5, 2021 08:44:17.484040976 CET	8.8.8.8	192.168.2.6	0x4970	No error (0)	vztnl-my.sharepoint.com	vztnl.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:17.484040976 CET	8.8.8.8	192.168.2.6	0x4970	No error (0)	vztnl.sharepoint.com	165-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:17.484040976 CET	8.8.8.8	192.168.2.6	0x4970	No error (0)	165-ipv4e.clump.dprodmgd104.aa-rt.sharepoint.com	187270-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:17.484040976 CET	8.8.8.8	192.168.2.6	0x4970	No error (0)	187270-ipv4e.farm.dprodmgd104.aa-rt.sharepoint.com	187270-ipv4e.farm.dprodmgd104.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:17.484040976 CET	8.8.8.8	192.168.2.6	0x4970	No error (0)	187270-ipv4.farm.dprodmgd104.aa-rt.sharepoint.com		40.108.231.27	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:17.490251064 CET	8.8.8.8	192.168.2.6	0xfbb6	No error (0)	accounts.google.com		142.250.184.237	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:17.493084908 CET	8.8.8.8	192.168.2.6	0x6719	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:17.493084908 CET	8.8.8.8	192.168.2.6	0x6719	No error (0)	clients.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:19.183444023 CET	8.8.8.8	192.168.2.6	0xb5c0	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:28.884706020 CET	8.8.8.8	192.168.2.6	0xdfef	No error (0)	amcdn.msftauth.net	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.002568007 CET	8.8.8.8	192.168.2.6	0x22b1	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.002568007 CET	8.8.8.8	192.168.2.6	0x22b1	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.002568007 CET	8.8.8.8	192.168.2.6	0x22b1	No error (0)	db3pcor005-com.be.1drv.com	i-db3p-cor005.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.002568007 CET	8.8.8.8	192.168.2.6	0x22b1	No error (0)	i-db3p-cor005.api.p001.1drv.com		13.104.208.160	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 5, 2021 08:44:32.187918901 CET	8.8.8.8	192.168.2.6	0x53bf	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.235301018 CET	8.8.8.8	192.168.2.6	0xf44	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:32.542152882 CET	8.8.8.8	192.168.2.6	0xed53	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:33.568207026 CET	8.8.8.8	192.168.2.6	0xc33c	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:33.568207026 CET	8.8.8.8	192.168.2.6	0xc33c	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.161	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:39.220592022 CET	8.8.8.8	192.168.2.6	0xd17	No error (0)	officewayside.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:39.220592022 CET	8.8.8.8	192.168.2.6	0xd17	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:39.220592022 CET	8.8.8.8	192.168.2.6	0xd17	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:39.872173071 CET	8.8.8.8	192.168.2.6	0xa628	No error (0)	messaging.office.com	omexmessaging.osi.office.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:40.166763067 CET	8.8.8.8	192.168.2.6	0x52c5	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:40.166763067 CET	8.8.8.8	192.168.2.6	0x52c5	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:40.166763067 CET	8.8.8.8	192.168.2.6	0x52c5	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:40.166763067 CET	8.8.8.8	192.168.2.6	0x52c5	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:40.166763067 CET	8.8.8.8	192.168.2.6	0x52c5	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:40.301398039 CET	8.8.8.8	192.168.2.6	0x997c	No error (0)	gstaticadssl.l.google.com		142.250.185.131	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.146219015 CET	8.8.8.8	192.168.2.6	0x1241	No error (0)	ssl-google-analytics.l.google.com		142.250.186.168	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.305080891 CET	8.8.8.8	192.168.2.6	0x3b05	No error (0)	ec.editmysite.com	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:41.305080891 CET	8.8.8.8	192.168.2.6	0x3b05	No error (0)	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com		54.189.175.59	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.305080891 CET	8.8.8.8	192.168.2.6	0x3b05	No error (0)	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com		54.149.0.4	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:41.627502918 CET	8.8.8.8	192.168.2.6	0xfe81	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:43.085256100 CET	8.8.8.8	192.168.2.6	0x40b3	No error (0)	officewayside.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:43.085256100 CET	8.8.8.8	192.168.2.6	0x40b3	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:43.085256100 CET	8.8.8.8	192.168.2.6	0x40b3	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 5, 2021 08:44:43.257169962 CET	8.8.8.8	192.168.2.6	0x2574	No error (0)	www.vzt.nl		185.159.242.66	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.329993963 CET	8.8.8.8	192.168.2.6	0x1965	No error (0)	www.freeprivacypolicy.com		104.26.7.220	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.329993963 CET	8.8.8.8	192.168.2.6	0x1965	No error (0)	www.freeprivacypolicy.com		104.26.6.220	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.329993963 CET	8.8.8.8	192.168.2.6	0x1965	No error (0)	www.freeprivacypolicy.com		172.67.73.152	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.407284021 CET	8.8.8.8	192.168.2.6	0x5df	No error (0)	www-google tagmanager.l.google.com		142.250.186.168	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.498380899 CET	8.8.8.8	192.168.2.6	0x9d56	No error (0)	platform.twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:44.498380899 CET	8.8.8.8	192.168.2.6	0x9d56	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.734512091 CET	8.8.8.8	192.168.2.6	0xce29	No error (0)	embed.tawk.to		104.22.25.131	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.734512091 CET	8.8.8.8	192.168.2.6	0xce29	No error (0)	embed.tawk.to		172.67.38.66	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:44.734512091 CET	8.8.8.8	192.168.2.6	0xce29	No error (0)	embed.tawk.to		104.22.24.131	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:45.353672981 CET	8.8.8.8	192.168.2.6	0x3dc9	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:45.366318941 CET	8.8.8.8	192.168.2.6	0x7039	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:45.366318941 CET	8.8.8.8	192.168.2.6	0x7039	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:45.560403109 CET	8.8.8.8	192.168.2.6	0x34e8	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:45.560403109 CET	8.8.8.8	192.168.2.6	0x34e8	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:45.560403109 CET	8.8.8.8	192.168.2.6	0x34e8	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:45.560403109 CET	8.8.8.8	192.168.2.6	0x34e8	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:45.789854050 CET	8.8.8.8	192.168.2.6	0xe025	No error (0)	www-google-analytics.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.760082960 CET	8.8.8.8	192.168.2.6	0x7a3	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:46.760082960 CET	8.8.8.8	192.168.2.6	0x7a3	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.804605007 CET	8.8.8.8	192.168.2.6	0x7c5e	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:46.856493950 CET	8.8.8.8	192.168.2.6	0x1a79	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:46.856493950 CET	8.8.8.8	192.168.2.6	0x1a79	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.856493950 CET	8.8.8.8	192.168.2.6	0x1a79	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.856493950 CET	8.8.8.8	192.168.2.6	0x1a79	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:46.856493950 CET	8.8.8.8	192.168.2.6	0x1a79	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 5, 2021 08:44:49.123449087 CET	8.8.8.8	192.168.2.6	0xaf9f	No error (0)	www.vzt.nl		185.159.242.66	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.452428102 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	syndication.twitter.com		104.244.42.8	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.452428102 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	syndication.twitter.com		104.244.42.72	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.452428102 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	syndication.twitter.com		104.244.42.200	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.452428102 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	syndication.twitter.com		104.244.42.136	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.801527977 CET	8.8.8.8	192.168.2.6	0xbec9	No error (0)	va.tawk.to		104.22.24.131	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.801527977 CET	8.8.8.8	192.168.2.6	0xbec9	No error (0)	va.tawk.to		104.22.25.131	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.801527977 CET	8.8.8.8	192.168.2.6	0xbec9	No error (0)	va.tawk.to		172.67.38.66	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:49.981242895 CET	8.8.8.8	192.168.2.6	0x3bed	No error (0)	cdn.syndication.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:49.981242895 CET	8.8.8.8	192.168.2.6	0x3bed	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:49.981242895 CET	8.8.8.8	192.168.2.6	0x3bed	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:49.981242895 CET	8.8.8.8	192.168.2.6	0x3bed	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.380640984 CET	8.8.8.8	192.168.2.6	0xbc10	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:50.380640984 CET	8.8.8.8	192.168.2.6	0xbc10	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.516022921 CET	8.8.8.8	192.168.2.6	0x8500	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:50.516022921 CET	8.8.8.8	192.168.2.6	0x8500	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:50.516022921 CET	8.8.8.8	192.168.2.6	0x8500	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:50.516022921 CET	8.8.8.8	192.168.2.6	0x8500	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Nov 5, 2021 08:44:50.676170111 CET	8.8.8.8	192.168.2.6	0x8e7	No error (0)	ton.twimg.com	cs511.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 5, 2021 08:44:50.676170111 CET	8.8.8.8	192.168.2.6	0x8e7	No error (0)	cs511.wpc.edgecastcdn.net		152.199.21.140	A (IP address)	IN (0x0001)
Nov 5, 2021 08:45:35.363662958 CET	8.8.8.8	192.168.2.6	0xc9ad	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5924 Parent PID: 3532

General

Start time:	08:44:13
Start date:	05/11/2021
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://vztnl-my.sharepoint.com/:o:/g/personal/mvanzaal_vzt_nl/EuuLOsYLcitAhOY9KZNqP9gBXbzHgWcXtG3S-zCfidXUXA?e=5%3ahV4RUj&at=9
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 2192 Parent PID: 5924

General

Start time:	08:44:14
Start date:	05/11/2021
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=1592,6233830419226784550,16524938468778052118,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis