ID: 532644
Cookbook: browseurl.jbs
Time: 15:30:24
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

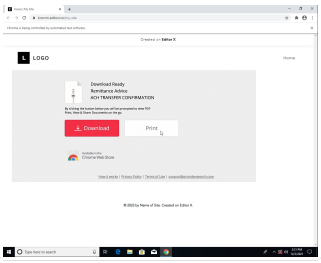
Windows Analysis Report https://knorrm.editorx.io/my-s…

Overview

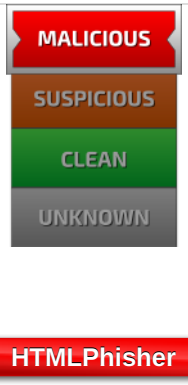
General Information

Sample URL:	http://https://knorrm.editorx.io/my-site
Analysis ID:	532644
Infos:	

Most interesting Screenshot:



Detection



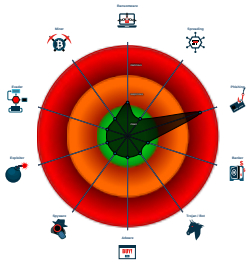
HTMLPhisher

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Phishing site detected (based on im…
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3532 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://knorrm.editorx.io/my-site MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4672 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,3209099605232646438,4037437087009067876,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 8856 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1552,3209099605232646438,4037437087009067876,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6680 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

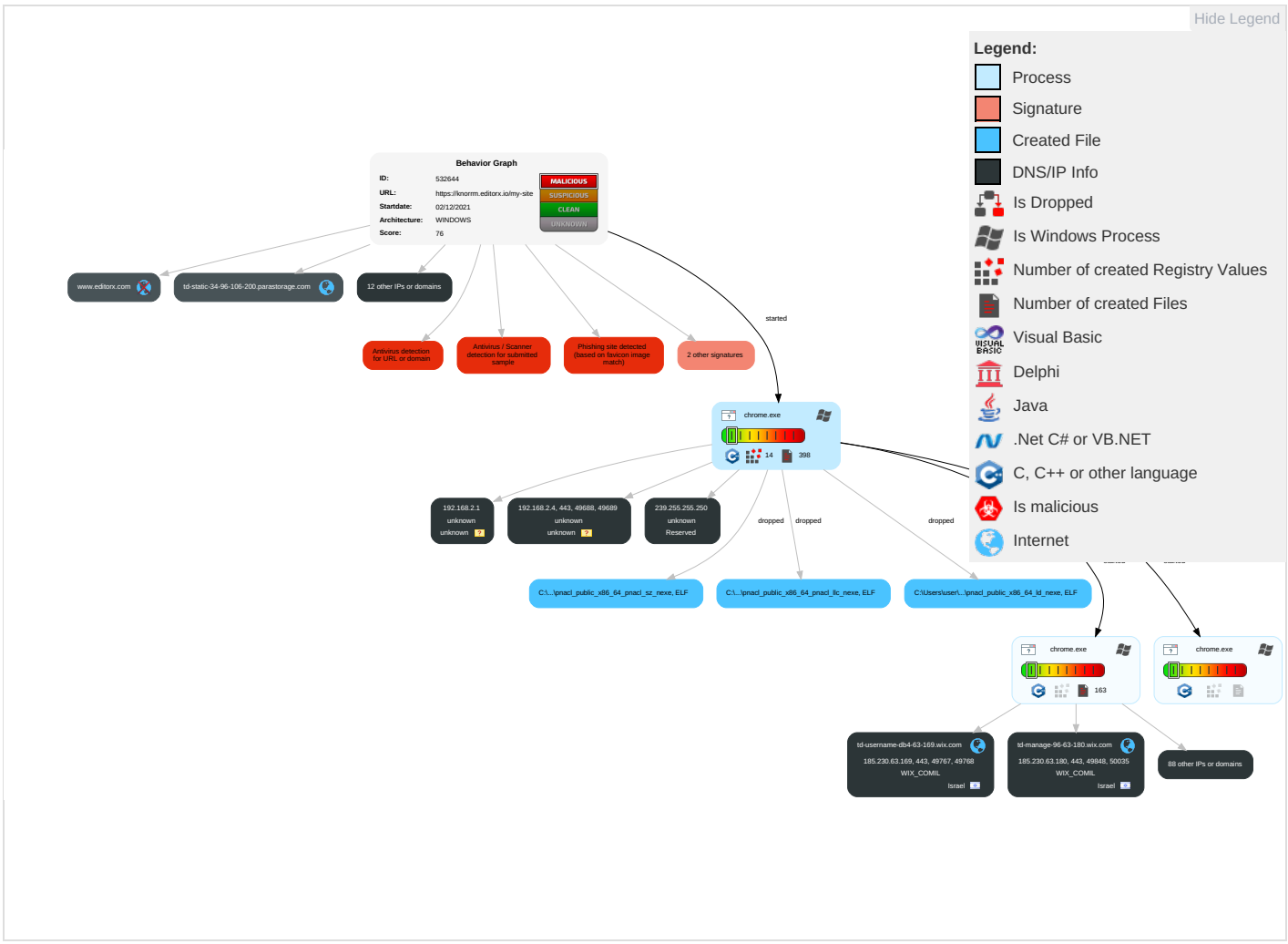
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

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

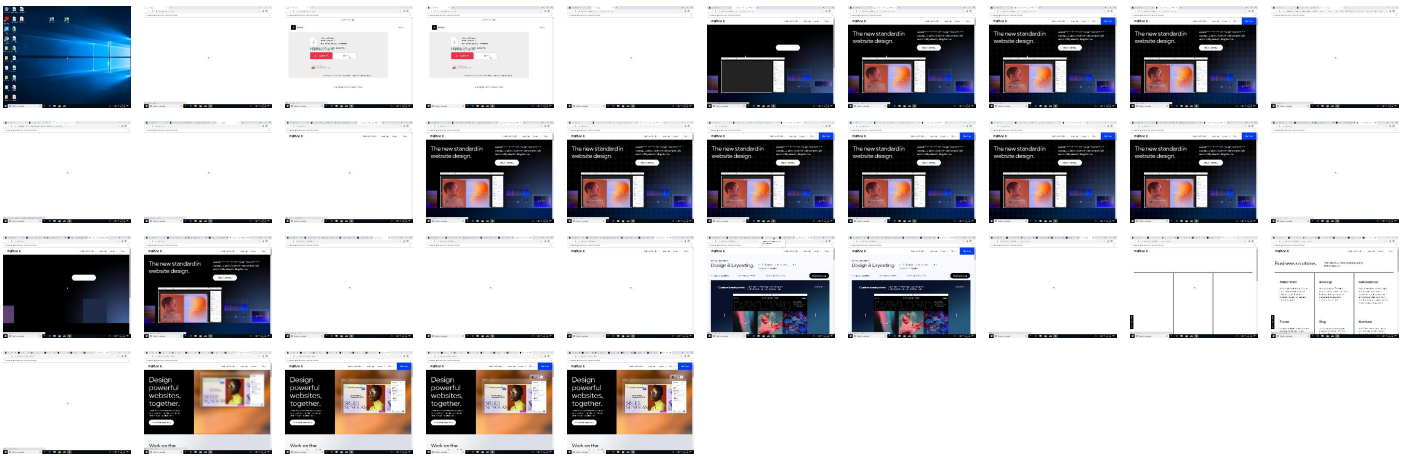
Behavior Graph

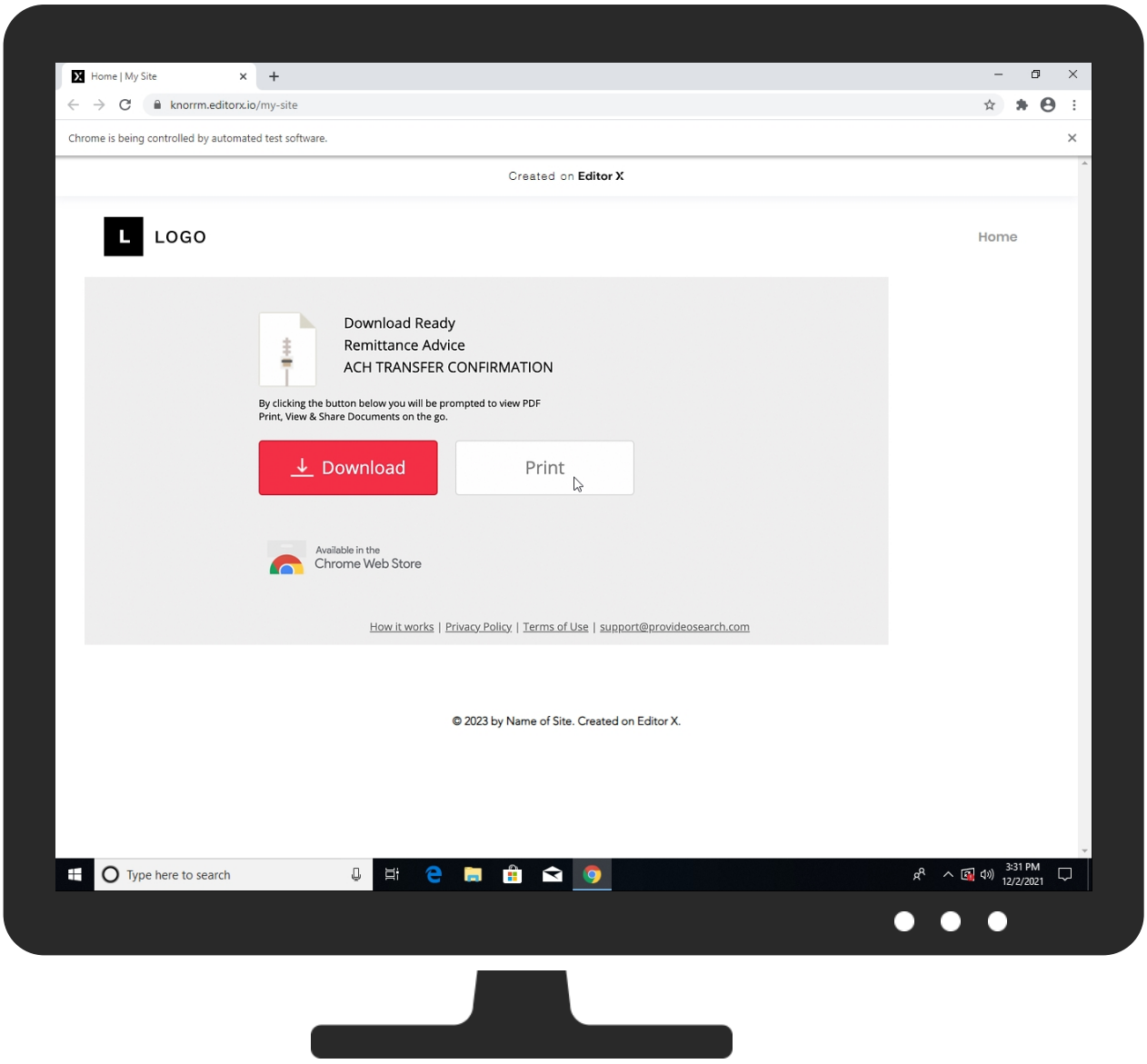


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://knorrm.editorx.io/my-site	0%	Virustotal		Browse
http://https://knorrm.editorx.io/my-site	0%	Avira URL Cloud	safe	
http://https://knorrm.editorx.io/my-site	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3532_1062995977_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://cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com/login.html?ktswdxfrcq=ETwfKm4EReiNE6Z44&mncam=6LTpYOijKxFoxy5xx&iws=dF38gbfCIMFvjQNn6s3Gguq	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://editorx.com/?utm_campaign=vir_editorx_wixad_live23Responsive	0%	Avira URL Cloud	safe	
http://https://knorrm.editorx.io/my-site2	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.editorx.com/?utm_campaign=vir_editorx_wixad_live23Responsive	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
td-balancer-db4-63-177.wixdns.net	185.230.63.177	true	false		unknown
coralsmtp.com	172.67.173.3	true	false		unknown
td-balancer-db4-63-96.wixdns.net	185.230.63.96	true	false		unknown
adservice.google.com	172.217.168.34	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
t.co	104.244.42.133	true	false		high
td-username-db4-63-169.wix.com	185.230.63.169	true	false		high
cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com	206.190.215.254	true	false		unknown
www.google.com	172.217.168.68	true	false		high
bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	52.201.184.93	true	false		high
q.quora.com	3.225.133.12	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
pagead46.l.doubleclick.net	172.217.168.2	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
stats.l.doubleclick.net	108.177.127.155	true	false		high
s.twitter.com	104.244.42.3	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
td-manage-96-63-180.wix.com	185.230.63.180	true	false		high
editorx.com	185.230.63.96	true	false		unknown
pop-lor1.mix.linkedin.com	144.2.14.5	true	false		high
dualstack.reddit.map.fastly.net	151.101.1.140	true	false		unknown
td-static-34-96-106-200.parastorage.com	34.96.106.200	true	false		high
prod.pinterest.global.map.fastly.net	151.101.0.84	true	false		unknown
www3.l.google.com	142.250.203.110	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
googleads.g.doubleclick.net	142.250.203.98	true	false		high
td-verticals-96-63-199.wix.com	185.230.63.199	true	false		high
sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	52.2.188.208	true	false		high
dualstack.pinterest.map.fastly.net	199.232.80.84	true	false		unknown
www.google.co.uk	172.217.168.3	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
d3ok6da481jyw8.cloudfront.net	18.66.180.97	true	false		high
www.google.ch	172.217.168.35	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3.eu-de.cloud-object-storage.appdomain.cloud	158.177.118.97	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
alb.reddit.com	unknown	unknown	false		high
4382365.fls.doubleclick.net	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
manage.editorx.com	unknown	unknown	false		unknown
v.pinimg.com	unknown	unknown	false		high
frog.editorx.com	unknown	unknown	false		unknown
bundler.wix-code.com	unknown	unknown	false		unknown
ct.pinterest.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.editorx.com	unknown	unknown	false		unknown
sentry.wixpress.com	unknown	unknown	false		high
static.parastorage.com	unknown	unknown	false		high
i.pinimg.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.redditstatic.com	unknown	unknown	false		high
video.wixstatic.com	unknown	unknown	false		high
siteassets.parastorage.com	unknown	unknown	false		high
static.wixstatic.com	unknown	unknown	false		high
knorrm.editorx.io	unknown	unknown	false		unknown
www.linkedin.com	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
apps.wix.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
frog.wix.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
analytics.google.com	unknown	unknown	false		high
www.pinterest.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com/login.html?ktswdxfrcq=ETwfKm4EReiNE6Z44&mncam=6LTpYOijKxFoxy5xx&iws=dF38gbfCIMFvjQNn6s3Gguq	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://4382365.fls.doubleclick.net/activityi;dc_pre=COy47cKqxfQCFY1FHQkd-RsB_g;src=4382365;type=count;cat=edxwebsi;ord=1;num=9815794333789;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2F?	false		high
http://https://4382365.fls.doubleclick.net/activityi;dc_pre=COCzkbKqxfQCFTSkhQodbSgJNw;src=4382365;type=count;cat=edxwebsi;ord=1;num=123899974432;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2F%3Futm_campaign%3Dvir_editorx_wixad_live?	false		high
http://https://www.editorx.com/?utm_campaign=vir_editorx_wixad_live	true		unknown
http://https://www.editorx.com/collaboration	true		unknown
http://https://www.editorx.com/features/design	true		unknown
http://https://4382365.fls.doubleclick.net/activityi;dc_pre=CJjCn7qqxfQCFalDHQkdrpMClw;src=4382365;type=count;cat=edxwebsi;ord=1;num=8457205604592;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2F?	false		high
http://https://www.editorx.com/features/business-ecommerce	true		unknown
http://https://4382365.fls.doubleclick.net/activityi;dc_pre=CICwpMqqxfQCFZKfhQodsIICeA;src=4382365;type=count;cat=edxwebsi;ord=1;num=3728117479370;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2Ffeatures%2Fbusiness-ecommerce?	false		high
http://https://knorrm.editorx.io/my-site	true		unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://adservice.google.com/ddm/fls/i/dc_pre=COCzkbKqxfQCFTSkhQodbSgJNw;src=4382365;type=count;cat=edxwebsi;ord=1;num=123899974432;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2F%3Futm_campaign%3Dvir_editorx_wixad_live	false		high
http://https://www.editorx.com/	true		unknown
http://https://4382365.fls.doubleclick.net/activityi;dc_pre=CPnGysaqxfQCFQSnGwodQd8NWg;src=4382365;type=count;cat=edxwebsi;ord=1;num=7806985237820;gtm=2wgba1;auiddc=856099019.1638455504;u1=c2fd7215-c2b3-410f-b718-e6cd2698f71b;u2=null-user-id;~oref=https%3A%2F%2Fwww.editorx.com%2Ffeatures%2Fdesign?	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.23.149.158	unknown	United States		14618	AMAZON-AESUS	false
144.2.14.5	pop-lor1.mix.linkedin.com	Netherlands		14413	LINKEDINUS	false
151.101.0.84	prod.pinterest.global.map.fastly.net	United States		54113	FASTLYUS	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
34.96.106.200	td-static-34-96-106-200.parastorage.com	United States		15169	GOOGLEUS	false
185.230.63.199	td-verticals-96-63-199.wix.com	Israel		58182	WIX_COMIL	false
216.58.215.230	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
3.231.113.219	unknown	United States		14618	AMAZON-AESUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
52.201.184.93	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
206.190.215.254	cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com	United States		32354	UNWIREDUS	false
3.225.133.12	q.quora.com	United States		14618	AMAZON-AESUS	false
108.177.127.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
172.217.168.2	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
52.2.188.208	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
185.230.63.96	td-balancer-db4-63-96.wixdns.net	Israel		58182	WIX_COMIL	false
142.250.203.110	www3.l.google.com	United States		15169	GOOGLEUS	false
172.67.173.3	coralsmtp.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
185.230.63.169	td-username-db4-63-169.wix.com	Israel		58182	WIX_COMIL	false
185.230.63.180	td-manage-96-63-180.wix.com	Israel		58182	WIX_COMIL	false
199.232.80.84	dualstack.pinterest.map.fastly.net	United States		54113	FASTLYUS	false
104.244.42.3	s.twitter.com	United States		13414	TWITTERUS	false
151.101.1.140	dualstack.reddit.map.fastly.net	United States		54113	FASTLYUS	false
172.217.168.35	www.google.ch	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.34	adservice.google.com	United States		15169	GOOGLEUS	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
18.66.180.97	d3ok6da481jyw8.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
158.177.118.97	s3.eu-de.cloud-object-storage.appdomain.cloud	United States		36351	SOFTLAYERUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532644
Start date:	02.12.2021
Start time:	15:30:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://knorrm.editorx.io/my-site
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:	11
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:	mal76.phis.win@45/209@54/40
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://editorx.com/?utm_campaign=vir_editorx_wixad_live • Browse: https://s3.eu-de.cloud-object-storage.appdomain.cloud/earlgrimes/diosmotic/index.html?key=68169122c1091c8e769a69a3729343e13c289555&url_01=https://confusable-historicopolitical-yarak.s3.us-west-002.backblazeb2.com/index.html&url_02=https://cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com/index.html&url_03=https://frontate-gauchely-unbroached.s3.us-west-002.backblazeb2.com/index.html&url_04=https://contestable-cryptographers-cuckold.s3.us-west-002.backblazeb2.com/index.html&url_05=https://bibliomane-cambio-emperil.s3.us-west-002.backblazeb2.com/index.html&redirect=https://www.amazon.com • Browse: https://editorx.com/ • Browse: https://www.editorx.com/ • Browse: https://www.editorx.com/features/design • Browse: https://www.editorx.com/features/business-ecommerce • Browse: https://www.editorx.com/collaboration
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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U....''<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.''.Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.''.g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.I..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N..._k...&.....$.....i.F.d.....D!e.....Y...,.E..m.;.1... $.F..O.F.o_}.uG.....,.%.>,.Zx.....o....c./.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.104060594129527
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SSDEEP:	6:kKLk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:T9kPlE99SNxAhUeYlUSA/t
MD5:	97EADE941340FF24A445CAE9406B8C08
SHA1:	50D23C1146345292FF32D34B1C0825BFF4131375
SHA-256:	28208560B10FB8D0495EF4838BD7D80E642BDE138212ABF0368090F46FDD2978
SHA-512:	AF9868B7DE223842DE9FE11E34D5656A54775AC0DE9BC4415925EF4700AFC0BE68D4AAF3B6D88A071453302838E6481A7DEF3361E2EBCA3007BE41B5C953EF85
Malicious:	false
Reputation:	low
Preview:	p..... .....d.WL....(..... .....q.\].....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\12691279-f8d8-428f-ab27-b75f6a4dd563.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):	196206
Entropy (8bit):	6.075089057103021
Encrypted:	false
SSDEEP:	3072:fZHYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:B4MWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	ADF6209702763A2DD8891E451304C2F0
SHA1:	E0D821B7ABB5EFA96BFA921957B13F3667F272EE
SHA-256:	206DF789916EB88FA84C9E8A174AD74045AB77B2C84050068A40AA6AF9063C62
SHA-512:	52432C54A23C2E8E27770BF7894ED8F7302072E1407E607B8840DCA879409F356787A6FACAF89117DBE69004B7A1AC7E9914BE107767AF452AB3201D84A6936D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\141ed95e-b8f7-4a6e-a9a2-6eb337d8e073.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7489226956225954
Encrypted:	false
SSDEEP:	384:Jr6V9jY2fAX3VEKZ8N5rSv9H3mpD+HveGKdro7Fdx23LzqrIhmgUaYXp1B6ODDta:xWyFl2/l+YezpDvcHbCjKZ/dlM
MD5:	E0A683E841A033F8150D0150536B52E9
SHA1:	ACF515388BE6B97672D0C1E3C1BD20E31C0DC758
SHA-256:	59485CF305D7F042FE23EE3B5F0D50B414C692FBFAA419F58693F0A5E8E5C6F8
SHA-512:	3DBA79042DEACFE7D1412154E5E73984A8903C6061F873EB7CE6101BBC284F74B6F9B645C1C9D3316EB245BE8A664079D23C02F44853A87EE38E1236054828E7
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....L.8.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\16724e3d-37d1-4fc0-88da-0ad4167ef841.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):	187916
Entropy (8bit):	6.046628063796689
Encrypted:	false
SSDEEP:	3072:6YMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:LMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	33A5527DA3F4A94F5E626EAD4EB2B966
SHA1:	D1637ADEDF723DC8B2D0D16BCC952FBC0AFE100D
SHA-256:	4E3BFED857623789BC48D99507023287695DBA0556C0124E75ACB6AC86549079
SHA-512:	FA09D47E34F5DF190981D4DBCCE3739341AD08C6C3EE3336003176349C2A821277E26120CCC585DCDA69C72740623918EC0770B60C2A23AD50E058A516F0286

C:\Users\user\AppData\Local\Google\Chrome\User Data\16724e3d-37d1-4fc0-88da-0ad4167ef841.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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\26533b5b-fc31-4d77-9f89-e38c9fecb520.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748589082357496
Encrypted:	false
SSDEEP:	384:Zr6V9jY2fAX3VEKZ8N5rSv9H3mpD+HveGKdro7Fdx23LzqrIhmgbYXp1B6ODDtNY:hWyFl2/6+YezpDvcHbCjKZ/dls
MD5:	223A1C2CA26E5DBA541697942424598B
SHA1:	D6D70D84AFE2FE28CF09EC7E7AD3EDC761C835D4
SHA-256:	A50005F43B721F469C91FA28A0765C25A452E481FC9423DA1827B0BB2A1A0EEA
SHA-512:	70C290867596C3A9B2776DB1E1AA52E0D192249712F96C924132437585915D587326FC99E47DFF2E7B9B2C5337425B001D2C3F22FA35FA184D209BD758384F1C
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....L.8.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\3539f6cf-62d6-43e1-b6c6-3e6f68806656.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):	196206
Entropy (8bit):	6.075090514965164
Encrypted:	false
SSDEEP:	3072:IgdYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:7CMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	022909A100183A8165B615BA2013BD68
SHA1:	E20E3412C5F97F7167515519D53602DFCD9D46FA
SHA-256:	E507401EF48074104D0BD2610075BF69304D63B067B8BA0969C7F06915FA6D88
SHA-512:	E835B8AF01833D9FB3594F809827F29445313E459E5143713A77C72A424A5E09D8A7318689FCAF95FBB6C0A812A0DEC27BB1B2AD3C53EB336E990AA1DAA11A3I
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\52698a96-deee-49f8-81f3-4dc86037610f.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):	187739
Entropy (8bit):	6.046199589829693
Encrypted:	false
SSDEEP:	3072:iYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:DMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	A546D120146D7F539F122C4B04F27BBB
SHA1:	7711C374AFD219EE883047B3A17A0D1088AA063C
SHA-256:	47809FD9C582FB6F4B9B87501EF08DB7E1B6631C0270930427C0D45B00E0C781
SHA-512:	1557795E70FC02F849FADD84E3D26B5858C3568A1162471845022C6E02BC1F983EDDBBA7182ED798C0E5DEC97B900262069C7294137BA6144F62D8B211E6DBDI
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\52698a96-deee-49f8-81f3-4dc86037610f.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\5bd851eb-cb42-48bc-b784-7fa20e6fc407.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):	187739
Entropy (8bit):	6.046200725671734
Encrypted:	false
SSDEEP:	3072:QYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:lMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	D7D7FC351E6A8175B31D4BD5F3EC3B3B
SHA1:	733475E5C43E639CE7341249C021F6B117EFFCBA
SHA-256:	BD612F750673D391BECD612810286300B26A1FAE40C97E63EBB001FCE8A1077A
SHA-512:	5865223831DC0698051F52F44B9CD8D828E3C2A682E4AC55F05D0F719695B2F4D03AED7AFACEFA95B3B34A234104CDAB5C00EE305411C9F3DF3D642EF6A7E8I9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\820821df-42d0-4414-a086-41540ac78849.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):	187822
Entropy (8bit):	6.046364912152096
Encrypted:	false
SSDEEP:	3072:1YMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:qMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	BA74EF8AB3F7E42A9EAA82E19C8CE75E
SHA1:	5D2142C238DF12D16C12E41FCE30733D4BC4B2D8
SHA-256:	EFA736EDEF7D99E13BCD6539E0607AF4985D7F31BCD6F79C09ADD9F37B622922
SHA-512:	B6DB70654F46FFA1F492CA1100527DB4BBDD6D67379CC3BBA078EB2761BCECC6E03AEDDB4FB4B1B958D2A6C7A964E778C0EBE274ABA04ABA1735A6FCB7F36A1C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\9e824f8c-3aa0-4206-a58e-21cea2b6e72b.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):	187822
Entropy (8bit):	6.046364912152096
Encrypted:	false
SSDEEP:	3072:1YMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:qMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	BA74EF8AB3F7E42A9EAA82E19C8CE75E
SHA1:	5D2142C238DF12D16C12E41FCE30733D4BC4B2D8
SHA-256:	EFA736EDEF7D99E13BCD6539E0607AF4985D7F31BCD6F79C09ADD9F37B622922
SHA-512:	B6DB70654F46FFA1F492CA1100527DB4BBDD6D67379CC3BBA078EB2761BCECC6E03AEDDB4FB4B1B958D2A6C7A964E778C0EBE274ABA04ABA1735A6FCB7F36A1C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\9e824f8c-3aa0-4206-a58e-21cea2b6e72b.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

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:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0c7a8252-0848-4d01-94ea-5a18e17ce2b6.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):	5126
Entropy (8bit):	4.886399088252022
Encrypted:	false
SSDEEP:	96:JzMaKxDHGXOKDEFEhT3EaGBGazKEb6hG7yC6V5rAK17GD1EwArGPmM:JzMaKxDHGXOKDzB3Ea47KEb6hayC6V5W
MD5:	EB05FE7322C96AF605D7C69C1B9F686E
SHA1:	25AD07BF51A013BA53AFBF655F4F118A082A1291
SHA-256:	B497538CA3806EB163887F8A8782D4C82B94002B47F3FA17458557E895F6F955
SHA-512:	9C89B40E254B7E459EA38BCBA7A9A0528CC1413255C8DAFDC09A3DCCDAD0161E29A17AB967178A06169F1F245A46C043ACE02D864DC36D5443F98E0C3957172
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285521089421332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285521106737013","port":443,

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\18c57c87-cb0b-47b1-8652-50cb163ac04d.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):	5203
Entropy (8bit):	4.960137598558945
Encrypted:	false
SSDEEP:	96:nuLC+9pIKIq5k0JCKL8jkt41MmbOTlVuHn:nuL59pI4h4KSkt4x
MD5:	ACA052B2F81AF8174280A6734DE03F94
SHA1:	0468C346DCFEEE56E075573E3FAC0DA69ECFD080
SHA-256:	20BCA6AE95311AC3913DEB46A4BC66FED25F6BA5162EED0FFA03914874F8431A
SHA-512:	D15CE47F7610FB605D164519381A9E988DE001E71BE90C47AA50CDFED214B465ADCA0D897ED0D12A7371F74F733C1CF1918C35B92ABE3126EDE2869F89EEB2D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\18c57c87-cb0b-47b1-8652-50cb163ac04d.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2fb8934d-3020-4958-810b-f21113cb57c7.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):	22602
Entropy (8bit):	5.536010246550904
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUIHG5nZbkb6D4+C:bLlfQ1kXqKf/pUZNCgVLH2HfzrU8G5nM
MD5:	BE1A8C78BCD07723BEC50FC8AFF15C95
SHA1:	78312562115CA4E60347768BAE46C1AC2C5274BC
SHA-256:	0FA7F0A585F48E1FE315C0F04D1FB81653B0CF031F9F7E8D8D2D24D3B9C373C0
SHA-512:	52EBC0A2330D525045E7BF5697643D62CCC3B5943B23FC27CDC32A3AB70381C55CC43C8AB9A01E56FCF4915CA670A4C777C1A6D240A459A401D4306EBAC2D0D
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":"13282929086920090","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\3da5997b-9bfd-4d8d-ac36-1eaaa60f240f.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):	5498
Entropy (8bit):	4.882887391870626
Encrypted:	false
SSDEEP:	96:JzMaKxDHGXOKDEFEhT3EaGwzdGiGdYGCEqG51GgZzGbV3GMwG8GeGtxGfG/GxXGE:JzMaKxDHGXOKDzB3EahdTD6qQtpAV3zK
MD5:	A86477BE5609FFC0D0690B04CC1B2ECA
SHA1:	18AD7484D1406B843B4E97BE988311E6E4763F16
SHA-256:	2F61DB428F690F258B9F42616EB15EF475C22500878C9DA62F5C6FF003BB0A0D
SHA-512:	088443FCC82BC2085304C90706515684595207B83F143D861EDA7C65049D3FF57D754566F2DAAF6DCBFD5D83A1E0E539582AA91F6153B2F4558BD8C6F8F9DDF2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285521089421332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285521106737013","port":443,

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41dc6e7c-fa84-4da8-afae-0dd4c3485945.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41dc6e7c-fa84-4da8-afae-0dd4c3485945.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d76698f-728a-4bac-8176-3e585282f264.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):	5.582815514035741
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUzkbiD4N:bLlfQ1kXqKf/pUZNCgVLH2HfzrU4GDS
MD5:	1C04F990271CB468FBC35B34B23FE1E7
SHA1:	78DBDE4DCE78D7AC2E0549FD1A4E466F4280198D
SHA-256:	555EDA1C67AD8341C17394240B2D5FBE1F6E4E54ADEB036DD155404B8987CE8B
SHA-512:	77EB3B6E14835710214B08090DA2C55A3E56DE00833DB13EF3BAEF8009BA5C0E044EF7744A8D6F1206AB6AD88E397D008F8459E0A2DF0AB85C5995944DAC7D5D
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":"13282929086920090","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\5fc73274-0bdb-4121-ac43-a2f654863cfd.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):	6057
Entropy (8bit):	5.185810798044416
Encrypted:	false
SSDEEP:	96:nuL9a+95p7orIKIN5k0JC8LRWL8jkt41MobOTlVuHn:nuL395VorI/h48LYSkt4X
MD5:	2DC60A9FB95F503301BB392B9F14F41F
SHA1:	BBEF735E85983270A0A99A420330068FB5A2A65E
SHA-256:	BB4AB6702BAF637E698FB86346E29126D0BE3D9588C12BE4D736EA633D9F0EE6
SHA-512:	9F32E91B779FDE41246E752CCBB7D69CFF463FB7E09180835E6DC359208B0AE3BC626FCE3DC870384032FD98A921E72C8852C451D406BE7DF43FA973C691F4C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91bff94e-c768-4032-acdd-68b90725c5ba.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):	19185
Entropy (8bit):	5.570169649882946
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUIHGYkb9D4c:bLlfQ1kXqKf/pUZNCgVLH2HfzrU8GpRT
MD5:	30B46B2D866F4040D5A6D0C434C119E9
SHA1:	7744519A94FC47D6247D26528D15930BDD986E7F
SHA-256:	4CEAA14469BA5F65BBB8B4E045D5DE8FF360C6E2FC1F79E5AFB531A7C14BF430
SHA-512:	729208A43A41308439AEA7C8B435A0386958C8AAEFF470688C6AEEE2821F828F50D6D3861D34D381758F07E1E87073DD6DF030C8A344B931F71B5840DFE54EEB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91bff94e-c768-4032-acdd-68b90725c5ba.tmp	
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":"13282929086920090","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\94e54ebb-77f4-4654-b6cd-a057d3dbf898.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):	5434
Entropy (8bit):	4.977589935855149
Encrypted:	false
SSDEEP:	96:nuL9C+9pIKIr5k0JC8LRWL8jkt41MobOTlVuHn:nuLj9pIhh48LYSkt4X
MD5:	6004B0D673E5D5ACF8A9E9E8F386830C
SHA1:	F2ED59122EFC1C34A81A2C39EE49BE0F46D4C2A5
SHA-256:	7BD3DA1A1763203CFA2F42D2CCDA9D7F377F96F3600AFF2A306C0EF8B672EE89
SHA-512:	307C9E52D02FE43D0B61F6CA5CE3221952201E0E8F698E1FF0DF47ADE974CFCBA4BE5CAED7B9F82A52528296FA39C6F13AD0B222F916F748C6D594D979E5289 1
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f43ece7-83ab-4e35-9ccc-a12078861420.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):	5.4820943119463745
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvmNp6KibT0KX8HD8wXwlmUUAnIMa:YhywcRE9RAJ9+UAnIimvmNH08n+UAnIr
MD5:	16508F8CEECFE2019D589F71F6990BED
SHA1:	F83B63406594248271830DBC62677D3F5C7E0660
SHA-256:	A7F792DB887D5F6BB548BD7B8DD494CA9D5EAF29D88AC095ED61932D1B97E641
SHA-512:	4A340A4C2EAAAD1F3D6FEFF892E950013139834B73285D1E28E8E21F91C1DE7E1C3AD0F6A82E238974BD7E5D43AA3D9A45BA4295BF490C19A30BAB9BB1EFC1 EB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477146.862353,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455546.862359}],"version":2}

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=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","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):	369
Entropy (8bit):	5.284117381321879
Encrypted:	false
SSDEEP:	6:mNJFON+q2Pwkn23iKKdK25+Xqx8chI+IFUtMJFY9XZmwKJFLHNVkwOwkn23iKKdP:iPOIvYf5KkTXfchI3FUtMPY9X/KPLT5S
MD5:	FB16979CE0027AB05E89C49905A257A4
SHA1:	679E5FF5BDF5C0B877ED018303F3726AEC309C1C
SHA-256:	9196B6F7AA8E5CF44AA8CD8AA846D0B161A2E69532B71FA5C5D34D5ED525AD84
SHA-512:	AD15003815E1A90C73F3E8F744B700A3267D82EE1896D28BE3073D1AACC0738A2262AA0D2F626917DCE5FA1E0D081FEC9A5F4354D15858D24B597F01989AE7E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/12/02-15:31:46.911 bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/02-15:31:46.915 bb8 Recovering log #3.2021/12/02-15:31:46.916 bb8 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):	369
Entropy (8bit):	5.284117381321879
Encrypted:	false
SSDEEP:	6:mNJFON+q2Pwkn23iKKdK25+Xqx8chI+IFUtMJFY9XZmwKJFLHNVkwOwkn23iKKdP:iPOIvYf5KkTXfchI3FUtMPY9X/KPLT5S
MD5:	FB16979CE0027AB05E89C49905A257A4
SHA1:	679E5FF5BDF5C0B877ED018303F3726AEC309C1C
SHA-256:	9196B6F7AA8E5CF44AA8CD8AA846D0B161A2E69532B71FA5C5D34D5ED525AD84
SHA-512:	AD15003815E1A90C73F3E8F744B700A3267D82EE1896D28BE3073D1AACC0738A2262AA0D2F626917DCE5FA1E0D081FEC9A5F4354D15858D24B597F01989AE7E
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:31:46.911 bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/02-15:31:46.915 bb8 Recovering log #3.2021/12/02-15:31:46.916 bb8 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):	1336
Entropy (8bit):	5.631268338833613
Encrypted:	false
SSDEEP:	24:/jZ85s/f3/3zOoZWs3/P9i1D/+Zgz+duyyWxzkr2PRN0kKEXUQyREAsuAu:v/fvT73k5+dryWFrW+UQWE+
MD5:	50960A3D9264645950BCAFEB7F409EC9
SHA1:	BFA5D2920D9A3DB0DB6BE54C93CF8ED511C36C51
SHA-256:	7D4728EAC04164B0BFB9ED32EF537094833AD3252A91D6FA6DFD1E0EC3C5A0CC
SHA-512:	AB6437AA0C247984AAAC8321CD76E1AB0F57B52A5FA69E18E29502869330FBC85935C64A37BE54C2539A09AAE73E3CD26CB0F9A06668CF239AC013A126DD7D 3
Malicious:	false
Reputation:	low
Preview:	.....".....campaign..com..creation..design..editor..editorx..https..live..responsive..utm..vir..web..website..wixad..x..www..home..io..knorrm..my..site*.....campaign... ...com.....creation.....design.....editor.....editorx.....home.....https.....io.....knorrm.....live.....my.....responsive.....site.....utm.....vir.....web.....website.....wixad.....w ww.....x..2.....a.....b.....c.....d.....e.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v... .....w.....x.....y...:.....B..... .....*8https://editorx.com/?utm_campaign=vir_editorx_wixad_live23Responsive Web Design | Website Creation |

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5461
Entropy (8bit):	4.98160730330291
Encrypted:	false
SSDEEP:	96:nuL90+9pIKIN5k0JC8LRWL8jkt41MobOTlVuHn:nuLJ9pI/h48LYSkt4X
MD5:	3D56791DC4F7A587704BE8EA80502271
SHA1:	3A3D93888C46E5E6549BCE08BA7369295FE5EEB8
SHA-256:	0C62486176EFDD10D97791538F28DB5640E68CB740B7C2714D462B57A7A1B54B
SHA-512:	AE1FB37D26E5DDD457039CDB60A04D2DBBD496A7F732759982C9B346CAE3C066B2D25481AC1DC698E244DE608243CF83F8521D3F6BCDEB9A0847699BAF846 D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (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):	5420
Entropy (8bit):	4.974828271470839
Encrypted:	false
SSDEEP:	96:nuLC+9pIKIZ5k0JC8LRWL8jkt41MmbOTlVuHn:nuL59pITh48LYSkt4x
MD5:	113EFD0FF7B3D30AAA8D0D91074A488A
SHA1:	516B4E099856A3AA05B681C2C046437A79F06F64
SHA-256:	E4704EEBCEFF142A13784125E61A7F29EE8C212D4679A45AC7519AE6AE569AD6
SHA-512:	88326DA468E352FF846A09653BCC7847D51BBD5A96E7D8C77FE813B610B161055FCC4162D271DB922EDE19BAE224D54850D6DBCDBEB4E21DC60F4BC57FC10 57
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	17092
Entropy (8bit):	5.582815514035741
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUzkbiD4N:bLlfQ1kXqKf/pUZNCgVLH2HfzrU4GDS
MD5:	1C04F990271CB468FBC35B34B23FE1E7
SHA1:	78DBDE4DCE78D7AC2E0549FD1A4E466F4280198D
SHA-256:	555EDA1C67AD8341C17394240B2D5FBE1F6E4E54ADEB036DD155404B8987CE8B
SHA-512:	77EB3B6E14835710214B08090DA2C55A3E56DE00833DB13EF3BAEF8009BA5C0E044EF7744A8D6F1206AB6AD88E397D008F8459E0A2DF0AB85C5995944DAC7D5 D
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":"13282929086920090","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\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

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

Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577469748337392
Encrypted:	false
SSDEEP:	384:NfxtwLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUTkCVD4t:qLlfQ1kXqKf/pUZNCgVLH2HfzrUY0D+
MD5:	9F018411CAB29455906DEBE2DBCB078D
SHA1:	0745665B02142BDD483DA8B7EF542E018D0001E3
SHA-256:	6A3DE4E8B3525DB9BAD621533DA329477DE2C2AF9B4FC6917C73327D9DA627B7
SHA-512:	CBC36046F2391B874A5A635055BB1AF234079F170758C9AB017AD951F7CEF6F61DA779C13E8586AF593C3DAC8E62D4690E1FE6B04E8A99FF908996499E5A9F3D
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":"13282929086920090","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 Preferences50 (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):	19184
Entropy (8bit):	5.5700242330433145
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUIHGnkbQD4i:bLlfQ1kXqKf/pUZNCgVLH2HfzrU8GksF
MD5:	24F800F4F210D620C7A40D959EFBBA81
SHA1:	175D8449F095580BE76ED83B6C9F03A96E012385
SHA-256:	B1E8DF0F2D3031782D53D6D363FB02BBB5254379521FF46A47724737C6569BEC
SHA-512:	EF6C6F0E2F004BBE75C0076C1B6CEEE098D39680A9E8C3B702A7AB469062F102CE7098E45FE8131C84F12E54472934669124B0AA607F1960E2A1DAEA93EAED5B
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":"13282929086920090","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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\073ccda8-2169-4248-9c37-e3993d1c3c2b.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):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 58
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):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\2cd2a388-0e62-49f5-9c69-6806c2d67d02.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2 F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 58
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\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):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
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):	418
Entropy (8bit):	5.154780658936791
Encrypted:	false
SSDEEP:	12:iSAvYf5KkkGHArAFUtMR/KCF5Jf5KkkGHArfJ:izYf5KkkGgkgMoYJf5KkkGgV
MD5:	E563207822F5257503211AB68B8FD118
SHA1:	941FC6DD00F1665A8769D46C52DB5FB1103DE48D
SHA-256:	FD59E059321F642444D3BC9201C18B6C9CEC39741224CEE982785B798F8F7C32
SHA-512:	487F2F57B728535BD75C648202E8E79E2738F9513F2F30FC03145DAED54FBE65513B12834DBC7E59C408D52C5EB6902BE55D5B60B0105FDF575A8332F4CED874
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:32:39.899 2080 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/12/02-15:32:39.902 2080 Recovering log #3.2021/12/02-15:32:39.903 2080 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old/ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old/ (copy)	
Entropy (8bit):	5.154780658936791
Encrypted:	false
SSDEEP:	12:iSAvYf5KkkGHArAFUtMR/KCF5Jf5KkkGHArfJ:izYf5KkkGgkgMoYJf5KkkGgV
MD5:	E563207822F5257503211AB68B8FD118
SHA1:	941FC6DD00F1665A8769D46C52DB5FB1103DE48D
SHA-256:	FD59E059321F642444D3BC9201C18B6C9CEC39741224CEE982785B798F8F7C32
SHA-512:	487F2F57B728535BD75C648202E8E79E2738F9513F2F30FC03145DAED54FBE65513B12834DBC7E59C408D52C5EB6902BE55D5B60B0105FDF575A8332F4CED874
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:32:39.899 2080 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/12/02-15:32:39.902 2080 Recovering log #3.2021/12/02-15:32:39.903 2080 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.338270273906305
Encrypted:	false
SSDEEP:	12:i+vYf5KkkOrsFUtM2V1/K2l5Jf5KkkOrzJ:icYf5Kk+gMWMiJf5Kkn
MD5:	346EF919C7B53B103702F8B393A1B4BA
SHA1:	36DF296F99BFB7A3A80E232C24FC6DDDD33613C8
SHA-256:	5306F7FA0B193497E8CA147E047E43615FC428F03BAA2640B1DF84BFF32CD12F
SHA-512:	9AD404DF3C8204BFBAD7B13A854752AA096A03A71E873B8DB1989FFA46B89A995E822E47802CDAF2A0E0E3F2F52DBE3606361B17C5F47538BC938FB5882AAD8C
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:33:46.426 1874 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/12/02-15:33:46.427 1874 Recovering log #3.2021/12/02-15:33:46.427 1874 Reusing old log C:\Users\user\AppData\Local\G oogle\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (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):	371
Entropy (8bit):	5.4820943119463745
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvmNp6KibT0KX8HD8wXwlmUUAnIMa:YhywcRE9RAJ9+UAnIimvmNH08n+UAnIr
MD5:	16508F8CEECFE2019D589F71F6990BED
SHA1:	F83B63406594248271830DBC62677D3F5C7E0660
SHA-256:	A7F792DB887D5F6BB548BD7B8DD494CA9D5EAF29D88AC095ED61932D1B97E641
SHA-512:	4A340A4C2EAAAD1F3D6FEFF892E950013139834B73285D1E28E8E21F91C1DE7E1C3AD0F6A82E238974BD7E5D43AA3D9A45BA4295BF490C19A30BAB9BB1EFC1EB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477146.862353,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455546.862359}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (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):	371
Entropy (8bit):	5.495904794867929
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvm+t6ibT0KX8HD8wXwlmUUAnIMOU:YhywcRE9RAJ9+UAnIimvmi608n+UAnIe
MD5:	E95E0ED5E8965BBC90EF45418531B56D
SHA1:	BA9C73BD9C004CC62E0E8D00AA5F03F93E300EE7
SHA-256:	0C72AFFD77BC539DED19783CBB00190A793F6D9B932E98AA144F7664423602E0
SHA-512:	0CBD67277CB7A6FBDF7A4969FA9BF47D94E44785D4E49067977DC8590F81EC14484BDCD725E101F974231436FFAEB4EF863640F1BEAD14A948CBF6B607BF7FDC
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477121.029759,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455521.029848}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity%L (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):	370
Entropy (8bit):	5.487055410708311
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvmzhnibT0KX8HD8wXwlmUUAnIMOk:YhywcRE9RAJ9+UAnIimvmt08n+UAnI/a
MD5:	463A998AF93EB0CCFFBE55F79852A4EC
SHA1:	3FAB4BFF4D4485F6939F06514C602D8D2328D77A
SHA-256:	85B57707F501EB4AB5878BECB76C2DB7EF9B31252FF893E3B6F76A884EE05668
SHA-512:	B5D23430023EC78124E54CEEB3AF38F2E2D95D960FA22985AA754958FC962397ED4DCD2ADDA7691E941DB576E20C589CC8890ABACBA783DA0094B5A2E0821FA
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477104.09912,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455504.099125}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b9a25a87-b2d7-4980-a6d1-228844d55ba2.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):	5.495904794867929
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvm+t6ibT0KX8HD8wXwlmUUAnIMOU:YhywcRE9RAJ9+UAnIimvmi608n+UAnIe
MD5:	E95E0ED5E8965BBC90EF45418531B56D
SHA1:	BA9C73BD9C004CC62E0E8D00AA5F03F93E300EE7
SHA-256:	0C72AFFD77BC539DED19783CBB00190A793F6D9B932E98AA144F7664423602E0
SHA-512:	0CBD67277CB7A6FBDF7A4969FA9BF47D94E44785D4E49067977DC8590F81EC14484BDCD725E101F974231436FFAEB4EF863640F1BEAD14A948CBF6B607BF7FDC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477121.029759,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455521.029848}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bca8f2e9-5768-4016-b6b4-6ac53e041f9b.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):	5.481217147635611
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvm4FpYWRKibT0KX8HD8wXwlmUUAX:YhywcRE9RAJ9+UAnIimvm4vYW808n+UY
MD5:	B504DE329D7F8A072FF971B9408D491C
SHA1:	F30736863595C5005BBC404F8EE4AF8D1DC493EA
SHA-256:	DBF4E64E3EAC9EEB7876CF559B444243266B7D3F0CF4625C854FD9C5E37D7B86
SHA-512:	16BA6902B3DEF58E89098E35CD88AF8DD4DF57C853C913C2D9F731064F023B87F1A976E9EE7F6BF9FE621D37BB4E1813064EE5E629B71373D6CE0FB60A2F4AFC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477154.669883,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455554.669891}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c1e58dab-7767-468e-a14f-c97258c2d25a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c1e58dab-7767-468e-a14f-c97258c2d25a.tmp	
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577469748337392
Encrypted:	false
SSDEEP:	384:NfxtwLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUTkCVD4t:qLlfQ1kXqKf/pUZNCgVLH2HfzrUY0D+
MD5:	9F018411CAB29455906DEBE2DBCB078D
SHA1:	0745665B02142BDD483DA8B7EF542E018D0001E3
SHA-256:	6A3DE4E8B3525DB9BAD621533DA329477DE2C2AF9B4FC6917C73327D9DA627B7
SHA-512:	CBC36046F2391B874A5A635055BB1AF234079F170758C9AB017AD951F7CEF6F61DA779C13E8586AF593C3DAC8E62D4690E1FE6B04E8A99FF908996499E5A9F3D
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13282929086920090","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c5225362-fee7-4efb-86ce-e57c906ac692.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):	5420
Entropy (8bit):	4.974828271470839
Encrypted:	false
SSDEEP:	96:nuLC+9pIKIZ5k0JC8LRWL8jkt41MmbOTlVuHn:nuL59pITh48LYSkt4x
MD5:	113EFD0FF7B3D30AAA8D0D91074A488A
SHA1:	516B4E099856A3AA05B681C2C046437A79F06F64
SHA-256:	E4704EEBCEFF142A13784125E61A7F29EE8C212D4679A45AC7519AE6AE569AD6
SHA-512:	88326DA468E352FF846A09653BCC7847D51BBD5A96E7D8C77FE813B610B161055FCC4162D271DB922EDE19BAE224D54850D6DBCDBEB4E21DC60F4BC57FC10 57
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_d efault_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_rig ht":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb9447f9-fde4-45f9-9118-79d6cfcbda1e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	5461
Entropy (8bit):	4.98160730330291
Encrypted:	false
SSDEEP:	96:nuL90+9pIKIN5k0JC8LRWL8jkt41MobOTlVuHn:nuLJ9pI/h48LYSkt4X
MD5:	3D56791DC4F7A587704BE8EA80502271
SHA1:	3A3D93888C46E5E6549BCE08BA7369295FE5EEB8
SHA-256:	0C62486176EFDD10D97791538F28DB5640E68CB740B7C2714D462B57A7A1B54B
SHA-512:	AE1FB37D26E5DDD457039CDB60A04D2DBBD496A7F732759982C9B346CAE3C066B2D25481AC1DC698E244DE608243CF83F8521D3F6BCDEB9A0847699BAF8468 D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_d efault_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_rig ht":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ced0446a-8514-4652-a3f4-9d26fc2e0376.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ced0446a-8514-4652-a3f4-9d26fc2e0376.tmp

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\d4fae92d-74be-47dc-a793-08dbb87b3429.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):	5168
Entropy (8bit):	4.963018536625875
Encrypted:	false
SSDEEP:	96:nuLDt9pIKIi5k0JCKL8jkt41MmbOTlVuHn:nuLR9pIgh4KSkt4x
MD5:	68DBB7A52346BF866C0DE18AC619D6A7
SHA1:	47183D1073365C0B73A0F2AA840E72519B84FA27
SHA-256:	3706D1832D03A6846521A88377EEA2BA4D5F51113887A536B00F61999BEAE1C8
SHA-512:	C20F3868E364F0BB92576CF883E6663FDC0888A049695DE9609128A695E108869D6B4A270A01092BE91F2A67028958CE3D597F6475F5065B27AA298C34C8F34D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282929087618440","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_d efault_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_rig ht":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ef6cd694-29b5-486a-994c-65fa045c71aa.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):	370
Entropy (8bit):	5.487055410708311
Encrypted:	false
SSDEEP:	6:YAQNzJVWwchDE9RfSHJR8wXwlmUUAnIMp51mvmzhnibT0KX8HD8wXwlmUUAnIMOk:YhywcRE9RAJ9+UAnIimvmt08n+UAnI/a
MD5:	463A998AF93EB0CCFFBE55F79852A4EC
SHA1:	3FAB4BFF4D4485F6939F06514C602D8D2328D77A
SHA-256:	85B57707F501EB4AB5878BECB76C2DB7EF9B31252FF893E3B6F76A884EE05668
SHA-512:	B5D23430023EC78124E54CEEB3AF38F2E2D95D960FA22985AA754958FC962397ED4DCD2ADDA7691E941DB576E20C589CC8890ABACBA783DA0094B5A2E0821FA
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1669991503.734598,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1638455503.734603},{"expiry":1638477104.09912,"host":"z4fu60utlCqc0SG7qX0Aly/C49LwuJujZm0cK2LqO+s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638455504.099125}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ef7c7abf-ae31-416c-a368-c060842b354a.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):	19184
Entropy (8bit):	5.5700242330433145
Encrypted:	false
SSDEEP:	384:NfxtRLlq+XQ1kXqKf/pUZNCgVLH2HfD3rUIHGnkbQD4i:bLlfQ1kXqKf/pUZNCgVLH2HfzrU8GksF
MD5:	24F800F4F210D620C7A40D959EFBBA81
SHA1:	175D8449F095580BE76ED83B6C9F03A96E012385
SHA-256:	B1E8DF0F2D3031782D53D6D363FB02BBB5254379521FF46A47724737C6569BEC
SHA-512:	EF6C6F0E2F004BBE75C0076C1B6CEEE098D39680A9E8C3B702A7AB469062F102CE7098E45FE8131C84F12E54472934669124B0AA607F1960E2A1DAEA93EAED5B
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":"13282929086920090","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl: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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
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):	196206
Entropy (8bit):	6.075089057103021
Encrypted:	false
SSDEEP:	3072:fZHYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:B4MWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	ADF6209702763A2DD8891E451304C2F0
SHA1:	E0D821B7ABB5EFA96BFA921957B13F3667F272EE
SHA-256:	206DF789916EB88FA84C9E8A174AD74045AB77B2C84050068A40AA6AF9063C62
SHA-512:	52432C54A23C2E8E27770BF7894ED8F7302072E1407E607B8840DCA879409F356787A6FACAF89117DBE69004B7A1AC7E9914BE107767AF452AB3201D84A6936D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local 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):	187739
Entropy (8bit):	6.046199589829693
Encrypted:	false
SSDEEP:	3072:iYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:DMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	A546D120146D7F539F122C4B04F27BBB
SHA1:	7711C374AFD219EE883047B3A17A0D1088AA063C
SHA-256:	47809FD9C582FB6F4B9B87501EF08DB7E1B6631C0270930427C0D45B00E0C781
SHA-512:	1557795E70FC02F849FADD84E3D26B5858C3568A1162471845022C6E02BC1F983EDDBBA7182ED798C0E5DEC97B900262069C7294137BA6144F62D8B211E6DBD
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748589082357496
Encrypted:	false
SSDEEP:	384:Zr6V9jY2fAX3VEKZ8N5rSv9H3mpD+HveGKdro7Fdx23LzqrIhmgbYXp1B6ODDtNY:hWyFl2/6+YezpDvcHbCjKZ/dls

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache.. (copy)	
MD5:	223A1C2CA26E5DBA541697942424598B
SHA1:	D6D70D84AFE2FE28CF09EC7E7AD3EDC761C835D4
SHA-256:	A50005F43B721F469C91FA28A0765C25A452E481FC9423DA1827B0BB2A1A0EEA
SHA-512:	70C290867596C3A9B2776DB1E1AA52E0D192249712F96C924132437585915D587326FC99E47DFF2E7B9B2C5337425B001D2C3F22FA35FA184D209BD758384F1C
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....L.8.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\b11cee56-abfb-40e1-99f1-c7c1a268a183.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):	196206
Entropy (8bit):	6.075088531676399
Encrypted:	false
SSDEEP:	3072:fJRYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:ReMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	887FBB91B975FA0098A4629F21481798
SHA1:	958FD64B57B9C88B50637A297648ED4B7D68299C
SHA-256:	76ACD57335271D9AF96577B7B6EC80C875BA7EB830F2C80DDC94F2B4B57349C8
SHA-512:	C1D75672CD97D87D3D276286148BBEEF8BB593CB241CF54C34C132941F9D2593F14AB3A8E31C05CD426D31D66A7BB4C6B758FFCB9D34F039E66D6BA1A520915
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\bc762102-bb72-45af-9747-1443aafcbc31.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):	196206
Entropy (8bit):	6.0750889694651455
Encrypted:	false
SSDEEP:	3072:ItcYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:u5MWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	6E19857DBB22F965E24F95F88F352C62
SHA1:	50D588F155FCF088FA06EDC79CD8126BFA739DB5
SHA-256:	DB60E1DDC05AF0FDF2676951A1DA436FF3861EC0B9A77534C9F626AFF1535AD0
SHA-512:	E67F3D4039198D7680C29313629EF097D5685FF316DAAB51D74D9DCE3045459D83CB3974B8388728B63DD082DADD8DE8DADB199B95F118CF2B9F73580F2C92C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\cc4494a5-7772-4fa5-9bac-619facb358fb.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):	196206
Entropy (8bit):	6.075089296519995
Encrypted:	false
SSDEEP:	3072:IldYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:mCMWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	8B242009B012F054CF27D35D90DE73CF

C:\Users\user\AppData\Local\Google\Chrome\User Data\cc4494a5-7772-4fa5-9bac-619facb358fb.tmp	
SHA1:	F2298BC71F2D41D8BF643DB6CA545DBABA2915A1
SHA-256:	A99E132CE9533F1217A6F03602802AFFA14F5464E4BA0E918642920D28A8D229
SHA-512:	DF2031BF6D94ECF76A3DA37CC0BB2D92112F094CFE4B6D75B1CC80EC277D8074A7C25DD1D8D6B01D6E25475A807851C2D2E6B5F4A5F61F4FC62BB5976C9FCDE
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\ddfe153b-efed-48ff-961d-ed8de781285d.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):	187916
Entropy (8bit):	6.04662856052348
Encrypted:	false
SSDEEP:	3072:FYMdQTSrjtujBL+S6bv4KHFd1vi197I7PfAlFcbXafIB0u1GOJmA3iuRp:6MWT5jsSyAiP5i3aQaqfIlUOoSiuRp
MD5:	3649048DC02D620794B057A46D53506F
SHA1:	2CBC9DB4D4C4042BAA706D41BE0202A9BB7358AD
SHA-256:	991D0CE82C8EC202BB94248705FA0F54B9D28B635458C3FF21C75AEB14326D99
SHA-512:	D8305E1E1447841D056F61E7C282BE012A8A09915FD96F2520BC7F341A07C5476F6EB496E2DCE400E5EE8F512A7D159408D47F4DE5445791EAB69C091E430CED
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638455489078511e+12,"network":1.638455489e+12,"ticks":317488115.0,"uncertainty":3939795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715110517"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Temp\3532_1062995977_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\3532_1062995977_platform_specific\x86_64\pnacl_public_pnacl_json	
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E
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 prev ent ", . "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\3532_1062995977_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:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 0
Malicious:	false
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\3532_1062995977_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:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
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\3532_1062995977_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

C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
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\3532_1062995977_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
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\3532_1062995977_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:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A631 E
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`..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.n acl_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_4 xi32_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\3532_1062995977_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:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a	
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.__div moddi4.__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\3532_1062995977_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:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Reputation:	low
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 ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (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\3532_1062995977_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:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62(FC
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\3532_1062995977_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:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DDF 00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

C:\Users\user\AppData\Local\Temp\3532_1062995977_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
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\3532_1062995977_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:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
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\3532_1062995977\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\3532_1062995977\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": "_plat form_specific/x86_32/".. },.. {.. "nacl_arch": "x86-64",.. "sub_package_path": "_platform_specific/x86_64/".. },.. {.. "nacl_arch": "arm",.. "sub_package_pa th": "_platform_specific/arm/".. }..].}.

C:\Users\user\AppData\Local\Temp\3532_1687868227_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):	1765
Entropy (8bit):	6.016932513650603
Encrypted:	false
SSDEEP:	48:p/hKAGj0FnAp7XgNGIaku9E5tPJXaWqkbszesM:R5Gj0FAlsaBmfPsRD3M
MD5:	6D1D175F88B64546105E3E7C31D1129A
SHA1:	75A1B56F55BB62B05365A0FDBFC7941DE77CBFAF
SHA-256:	A0BC246E8E160A9BB32FA60F4E7A04D148A17125F426509466031E07731FDF81
SHA-512:	5C80908331E30C7EAD67F7F6C5AB064B07626FD9C58925A0D2124D66B25C5AE2F218BDACFB68AFCB332E88EB297CFB7E0A7A9E5E1E54C9B7A510FEF095F9B54F
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiSUxrUllPSmhIVEZaclILRmN5UC12SkJrVjNWbWVLdHo4d1hEb2VPWjBZMCJ9LHsicGF0aCI6InNzbF9lcnJvcl9hc3Npc3RhbnQucGliLCJyb290X2hhc2giOiJyRFZLUnlPcXBQQnI3RGhkM2VTazBKZzYxUlJXOVNzeHFBYU95WDFiWHFjIn1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiZ2lla2NtbWxua2xlbmxhb21wcGtwaGtuam1ubnBuZWgiLCJpdGVtX3ZlcnNpb24iOiI3IiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"nBdNk-7bgnEftAs4hWaHwF1Lk9pt7Eh6pcqe2gyNsE7VnVRp-H27tm1RFAF4htCUlXNJxX6YY-MUiK2DqJpQ3c73KDaFV8DcnadQfcXO3Lbrw7jLYSUaSdzujPkTyhuFcq_BhK0KWiIJ0aJgh7nVOBfAa5AbE6oFlLKMB2Ls0gmzS1-a5hUIu4rw2h9r9jkr6gLYbein5Jk2hdwW3u-1GNjyki4dftG2iZNAI8VhUf5gnCiF4AHCnYSGJsM0RGkmO_HJIzgwpQpP3RDsG2ioeKgxL-kcHhjXWOj3uVGyxpp1FkyHGkeGuqpFZMAxx3CEBiOtFj7i3iQxkgEW-E3uMKI3yA

C:\Users\user\AppData\Local\Temp\3532_1687868227\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):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B56D
Malicious:	false
Reputation:	low
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\3532_1687868227\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.169145448714876
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFY8Wypv/KS1f:F6VlMQyBSS1f
MD5:	4AAA0ED8099ECC1DA778A9BC39393808
SHA1:	0E4A733A5AF337F101CFA6BEA5EBC153380F7B05
SHA-256:	20B91160E2611D3159AD82857323FEBC906457756678AB73F305C3A1E399D18D
SHA-512:	DFA942C35E1E5F62DD8840C97693CDBFD6D71A1FD2F42E26CB75B98BB6A1818395ECDF552D46F07DFF1E9C74F1493A39E05B14E3409963EFF1ADA8889715287
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "sslErrorAssistant",. "version": "7".}

C:\Users\user\AppData\Local\Temp\3532_1687868227\ssl_error_assistant.pb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2816
Entropy (8bit):	6.108955364911366
Encrypted:	false
SSDEEP:	48:jkbh6AW2Bfc3osI6Hc3+XgU+EVeY55J4gXM/QDH4yq2dxckdfmkM:jkbhM2a3pntgQVb8Ylq2di
MD5:	E2F792C9E2DD86F39E8286B2EAD2FC70

C:\Users\user\AppData\Local\Temp\3532_1687868227\ssl_error_assistant.pb	
SHA1:	8A32867614D2A23E473ED642056DED8E566687F9
SHA-256:	AC354A4723AAA4F06BEC385DDDE4A4D0983AD51456F52B31A8068EC97D5B5EA7
SHA-512:	6A7AF0CA1EFA65A89A9CA3B8DF0D2E24F21D91673C60CDFEEB02D33647442B01D535497249542F40E66E0D2DD3E9F8ED1F4A201FD97138D07A2B71366737E58
Malicious:	false
Reputation:	low
Preview:	...5.3sha256/fjZPHewEHTrMDX3l1ecEIeoy3WFxHyGplOLv28kIbtI=.5.3sha256/m/nBiLhSttu1YmOz7Y3D2u1iB1dV2CbIfFa3R2YW5M=.5.3sha256/8luf4xRbVCmCMQTJn 3rxlgllO1IOKoyuSUgmXyfaIKs=.5.3sha256/8IHdrS+r6IWzSMcRcD/GA6mBxk1ECX8tGRW0rtGWILE=.5.3sha256/k/2eeJTznE32mblA/du19wpVDSIReFX44M8wX a2JY30=.5.3sha256/urWd7jMwR6DJgvWhp6xfRHF5b/cba3iG0ggXtTR6AfM=.5.3sha256/IJPCDSE5tM9H3nuD5m6RU2i9KDdPXVn4qmC/ULlcZzc=.5.3sha256/0G y8RMdbxHNWR2GQJ62QKDXORYf5JmMmnr1FJFPYpzM=.5.3sha256/8tTICtyaxIQrdbYYDdgZhTN0OpM9kYndvoImtw1Ys5E=.5.3sha256/F7HIlsaG0bpJW8CzYekRbt FqLVTTGqwvuwPDqnlLct0=.5.3sha256/zaV2Aw1A742R1+WpXWvL5atsJbGmeSS6dzZOfe6f1Yw=.5.3sha256/UwOkRGMlP0K/mKNJdpQ0sTg2ean9Tje8UTOvFYzt1G E=.5.3sha256/w7KUXE4/BAo1YVZdO3mBsrMpu4IQuN0mhUXUI//agVU=.5.3sha256/JnPvGqEn36FjHQlBXtG1uWwNtdMj1o2ojR/asqyypNk=.5.3sha256/AUSXlKD Cf1X30WhWeAWbjToABfBkJrKWPL6KwEi5VH0=.5.3sha256/zSyVjjFJMIeXK0ktVTIjewwr6U5OePRqyY/nEXTI4P8=.5.3sha256/9dcHlrXN2WV/ehbEdMxMZ8lV4qv GejCtNC5r6nfTviM=.5.3sha256/E+0WZLGSIe5nddlVKZ5fYzaNHHCE3hNqi/OWZD3iKgA=.5.3sha2

C:\Users\user\AppData\Local\Temp\6138112f-9088-4fdb-bf01-af24b501d338.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\ecc51f6f-817c-4338-8909-a2d0446c4dcc.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
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.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\f9ffb12c-7f07-4f9f-a802-01af22007eab.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

C:\Users\user\AppData\Local\Temp\f9ffb12c-7f07-4f9f-a802-01af22007eab.tmp	
Preview:	.

C:\Users\user\AppData\Local\Temp\fa6beb42-6ead-494d-aef6-2be19783f1fe.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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir3532_1078712992\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_dir3532_1078712992\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
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
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": "Connecteu-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_dir3532_1078712992\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\cs\messages.json	
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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
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_dir3532_1078712992\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "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 completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\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:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
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.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\el\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):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\el\messages.json	
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "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_dir3532_1078712992\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\es\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):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\es\messages.json	
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\es_419\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):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3532_1078712992\CRX_INSTALL_locales\et\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):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

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
Dec 2, 2021 15:31:28.494987011 CET	192.168.2.4	8.8.8.8	0xdd76	Standard query (0)	knorrm.editorx.io	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:28.499826908 CET	192.168.2.4	8.8.8.8	0xadc4	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:28.526767015 CET	192.168.2.4	8.8.8.8	0x6c62	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.135010958 CET	192.168.2.4	8.8.8.8	0x8885	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.164729118 CET	192.168.2.4	8.8.8.8	0x2ffc	Standard query (0)	siteassets.parastorage.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.165180922 CET	192.168.2.4	8.8.8.8	0xa266	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.305258989 CET	192.168.2.4	8.8.8.8	0x451d	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.597935915 CET	192.168.2.4	8.8.8.8	0xd7d3	Standard query (0)	frog.editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:31.264803886 CET	192.168.2.4	8.8.8.8	0x6499	Standard query (0)	www.editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:33.330841064 CET	192.168.2.4	8.8.8.8	0xe469	Standard query (0)	www.editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:36.646153927 CET	192.168.2.4	8.8.8.8	0xe3fc	Standard query (0)	editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:38.083188057 CET	192.168.2.4	8.8.8.8	0x73d4	Standard query (0)	bundler.wix-code.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:39.974751949 CET	192.168.2.4	8.8.8.8	0x4798	Standard query (0)	apps.wix.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:42.241833925 CET	192.168.2.4	8.8.8.8	0x8612	Standard query (0)	manage.editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.386193991 CET	192.168.2.4	8.8.8.8	0xa6ef	Standard query (0)	4382365.fls.doubleclick.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.386708975 CET	192.168.2.4	8.8.8.8	0xb3cb	Standard query (0)	www.redditstatic.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.388910055 CET	192.168.2.4	8.8.8.8	0x4c1b	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.389070034 CET	192.168.2.4	8.8.8.8	0x2b	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.391455889 CET	192.168.2.4	8.8.8.8	0x3855	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.392137051 CET	192.168.2.4	8.8.8.8	0x5cbd	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.411147118 CET	192.168.2.4	8.8.8.8	0xe764	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.797694921 CET	192.168.2.4	8.8.8.8	0xb864	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.868822098 CET	192.168.2.4	8.8.8.8	0x5b95	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.869046926 CET	192.168.2.4	8.8.8.8	0xd7c6	Standard query (0)	analytics.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.869064093 CET	192.168.2.4	8.8.8.8	0xa5c3	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.969403982 CET	192.168.2.4	8.8.8.8	0xff6	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.972632885 CET	192.168.2.4	8.8.8.8	0x1633	Standard query (0)	alb.reddit.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.054625988 CET	192.168.2.4	8.8.8.8	0x8bc0	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.059519053 CET	192.168.2.4	8.8.8.8	0x50e7	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.435542107 CET	192.168.2.4	8.8.8.8	0xc35a	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.528137922 CET	192.168.2.4	8.8.8.8	0x245f	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.600878000 CET	192.168.2.4	8.8.8.8	0x76a2	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.604072094 CET	192.168.2.4	8.8.8.8	0xf1af	Standard query (0)	www.pinterest.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.826771975 CET	192.168.2.4	8.8.8.8	0xb69c	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.856472015 CET	192.168.2.4	8.8.8.8	0x4a01	Standard query (0)	sentry.wixpress.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.996741056 CET	192.168.2.4	8.8.8.8	0xdf0e	Standard query (0)	v.pinimg.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.999674082 CET	192.168.2.4	8.8.8.8	0x7775	Standard query (0)	i.pinimg.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:31:45.324417114 CET	192.168.2.4	8.8.8.8	0x4bd7	Standard query (0)	s3.eu-de.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.198987007 CET	192.168.2.4	8.8.8.8	0x5d30	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.348717928 CET	192.168.2.4	8.8.8.8	0x2e42	Standard query (0)	coralsmtp.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.480884075 CET	192.168.2.4	8.8.8.8	0x2b5f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.826684952 CET	192.168.2.4	8.8.8.8	0x5a64	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:47.544903994 CET	192.168.2.4	8.8.8.8	0x4ece	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:49.850537062 CET	192.168.2.4	8.8.8.8	0x6167	Standard query (0)	cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:52.667315006 CET	192.168.2.4	8.8.8.8	0x7269	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:10.996254921 CET	192.168.2.4	8.8.8.8	0x4fa	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:19.979546070 CET	192.168.2.4	8.8.8.8	0x9977	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:25.271975994 CET	192.168.2.4	8.8.8.8	0x950a	Standard query (0)	video.wixstatic.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:29.711469889 CET	192.168.2.4	8.8.8.8	0xe3c9	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:29.711812973 CET	192.168.2.4	8.8.8.8	0xb731	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.248157024 CET	192.168.2.4	8.8.8.8	0x32d	Standard query (0)	siteassets.parastorage.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.411386967 CET	192.168.2.4	8.8.8.8	0xdd65	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.629559040 CET	192.168.2.4	8.8.8.8	0x563a	Standard query (0)	www.editorx.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.814945936 CET	192.168.2.4	8.8.8.8	0xf1af	Standard query (0)	frog.editorx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:28.527400970 CET	8.8.8.8	192.168.2.4	0xadc4	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:28.527400970 CET	8.8.8.8	192.168.2.4	0xadc4	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:28.529973984 CET	8.8.8.8	192.168.2.4	0xdd76	No error (0)	knorrm.editorx.io	username.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:28.529973984 CET	8.8.8.8	192.168.2.4	0xdd76	No error (0)	username.wix.com	5f36b111-username.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:28.529973984 CET	8.8.8.8	192.168.2.4	0xdd76	No error (0)	5f36b111-username.wix.com	td-username-db4-63-169.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:28.529973984 CET	8.8.8.8	192.168.2.4	0xdd76	No error (0)	td-username-db4-63-169.wix.com		185.230.63.169	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:28.566329956 CET	8.8.8.8	192.168.2.4	0x6c62	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.153764963 CET	8.8.8.8	192.168.2.4	0xde1c	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.154088020 CET	8.8.8.8	192.168.2.4	0x8885	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:29.154088020 CET	8.8.8.8	192.168.2.4	0x8885	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.185719013 CET	8.8.8.8	192.168.2.4	0xa266	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:29.185719013 CET	8.8.8.8	192.168.2.4	0xa266	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.185920000 CET	8.8.8.8	192.168.2.4	0x2ffc	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:29.185920000 CET	8.8.8.8	192.168.2.4	0x2ffc	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:29.185920000 CET	8.8.8.8	192.168.2.4	0x2ffc	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	frog.wix.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.201.184.93	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.197.5.33	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.224.180.226	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.45.176.168	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		50.17.151.88	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		35.168.159.214	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.71.145.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:29.322844982 CET	8.8.8.8	192.168.2.4	0x451d	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.7.14.148	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	frog.editorx.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.23.149.158	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.201.180.67	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.45.176.168	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		18.211.17.184	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.224.180.226	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.88.78	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		100.25.184.182	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:30.622347116 CET	8.8.8.8	192.168.2.4	0xd7d3	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.201.184.93	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:31.288961887 CET	8.8.8.8	192.168.2.4	0x6499	No error (0)	www.editorx.com	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:31.288961887 CET	8.8.8.8	192.168.2.4	0x6499	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:31.288961887 CET	8.8.8.8	192.168.2.4	0x6499	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-db4-63-96.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:31.288961887 CET	8.8.8.8	192.168.2.4	0x6499	No error (0)	td-balancer-db4-63-96.wixdns.net		185.230.63.96	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:33.354065895 CET	8.8.8.8	192.168.2.4	0xe469	No error (0)	www.editorx.com	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:33.354065895 CET	8.8.8.8	192.168.2.4	0xe469	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:33.354065895 CET	8.8.8.8	192.168.2.4	0xe469	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-db4-63-177.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:33.354065895 CET	8.8.8.8	192.168.2.4	0xe469	No error (0)	td-balancer-db4-63-177.wixdns.net		185.230.63.177	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:36.667396069 CET	8.8.8.8	192.168.2.4	0xe3fc	No error (0)	editorx.com		185.230.63.96	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:38.106004000 CET	8.8.8.8	192.168.2.4	0x73d4	No error (0)	bundler.wix-code.com	d3ok6da481jyw8.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:38.106004000 CET	8.8.8.8	192.168.2.4	0x73d4	No error (0)	d3ok6da481jyw8.cloudfront.net		18.66.180.97	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:38.106004000 CET	8.8.8.8	192.168.2.4	0x73d4	No error (0)	d3ok6da481jyw8.cloudfront.net		18.66.180.110	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:38.106004000 CET	8.8.8.8	192.168.2.4	0x73d4	No error (0)	d3ok6da481jyw8.cloudfront.net		18.66.180.44	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:38.106004000 CET	8.8.8.8	192.168.2.4	0x73d4	No error (0)	d3ok6da481jyw8.cloudfront.net		18.66.180.74	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:39.996684074 CET	8.8.8.8	192.168.2.4	0x4798	No error (0)	apps.wix.com	verticals.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:39.996684074 CET	8.8.8.8	192.168.2.4	0x4798	No error (0)	verticals.wix.com	td-verticals-96-63-199.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:39.996684074 CET	8.8.8.8	192.168.2.4	0x4798	No error (0)	td-verticals-96-63-199.wix.com		185.230.63.199	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:42.264950991 CET	8.8.8.8	192.168.2.4	0x8612	No error (0)	manage.editorx.com	manageorigin.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:42.264950991 CET	8.8.8.8	192.168.2.4	0x8612	No error (0)	manageorigin.wix.com	td-manage-96-63-180.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:42.264950991 CET	8.8.8.8	192.168.2.4	0x8612	No error (0)	td-manage-96-63-180.wix.com		185.230.63.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:42.946055889 CET	8.8.8.8	192.168.2.4	0x59d2	No error (0)	www-google tagmanager .l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.196126938 CET	8.8.8.8	192.168.2.4	0x955e	No error (0)	www-google-analytics .l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.406018019 CET	8.8.8.8	192.168.2.4	0xb3cb	No error (0)	www.reddit static.com	dualstack.reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.406018019 CET	8.8.8.8	192.168.2.4	0xb3cb	No error (0)	dualstack. reddit.map .fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.406018019 CET	8.8.8.8	192.168.2.4	0xb3cb	No error (0)	dualstack. reddit.map .fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.406018019 CET	8.8.8.8	192.168.2.4	0xb3cb	No error (0)	dualstack. reddit.map .fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.406018019 CET	8.8.8.8	192.168.2.4	0xb3cb	No error (0)	dualstack. reddit.map .fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.410301924 CET	8.8.8.8	192.168.2.4	0x2b	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.411184072 CET	8.8.8.8	192.168.2.4	0x5cbd	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.411184072 CET	8.8.8.8	192.168.2.4	0x5cbd	No error (0)	platform.t witter.map .fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.412036896 CET	8.8.8.8	192.168.2.4	0xa6ef	No error (0)	4382365.fl s.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.412036896 CET	8.8.8.8	192.168.2.4	0xa6ef	No error (0)	dart.l.dou bleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.412060022 CET	8.8.8.8	192.168.2.4	0x4c1b	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.412060022 CET	8.8.8.8	192.168.2.4	0x4c1b	No error (0)	s-pinimg-c om.gslb.pi nterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.413538933 CET	8.8.8.8	192.168.2.4	0x3855	No error (0)	connect.fa cebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.413538933 CET	8.8.8.8	192.168.2.4	0x3855	No error (0)	scontent.x x.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		3.225.133.12	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		34.230.123.66	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		3.224.194.150	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		18.215.205.165	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		18.205.51.212	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.430721998 CET	8.8.8.8	192.168.2.4	0xe764	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.815243959 CET	8.8.8.8	192.168.2.4	0xb864	No error (0)	adservice. google.com		172.217.168.34	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.896258116 CET	8.8.8.8	192.168.2.4	0xd7c6	No error (0)	analytics. google.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.896258116 CET	8.8.8.8	192.168.2.4	0xd7c6	No error (0)	www3.l.goo gle.com		142.250.203.110	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:43.896583080 CET	8.8.8.8	192.168.2.4	0x5b95	No error (0)	www.google.co.uk		172.217.168.3	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.910459995 CET	8.8.8.8	192.168.2.4	0xa5c3	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.910459995 CET	8.8.8.8	192.168.2.4	0xa5c3	No error (0)	stats.l.doubleclick.net		108.177.127.155	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.910459995 CET	8.8.8.8	192.168.2.4	0xa5c3	No error (0)	stats.l.doubleclick.net		108.177.127.154	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.910459995 CET	8.8.8.8	192.168.2.4	0xa5c3	No error (0)	stats.l.doubleclick.net		108.177.127.156	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.910459995 CET	8.8.8.8	192.168.2.4	0xa5c3	No error (0)	stats.l.doubleclick.net		108.177.127.157	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.991214991 CET	8.8.8.8	192.168.2.4	0xff6	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.991214991 CET	8.8.8.8	192.168.2.4	0xff6	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.991214991 CET	8.8.8.8	192.168.2.4	0xff6	No error (0)	glb-na.mix.linkedin.com	pop-lor1.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.991214991 CET	8.8.8.8	192.168.2.4	0xff6	No error (0)	pop-lor1.mix.linkedin.com		144.2.14.5	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.991699934 CET	8.8.8.8	192.168.2.4	0x1633	No error (0)	alb.reddit.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:43.991699934 CET	8.8.8.8	192.168.2.4	0x1633	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.991699934 CET	8.8.8.8	192.168.2.4	0x1633	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.991699934 CET	8.8.8.8	192.168.2.4	0x1633	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:43.991699934 CET	8.8.8.8	192.168.2.4	0x1633	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.073863029 CET	8.8.8.8	192.168.2.4	0x8bc0	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.078627110 CET	8.8.8.8	192.168.2.4	0x50e7	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.078627110 CET	8.8.8.8	192.168.2.4	0x50e7	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.078627110 CET	8.8.8.8	192.168.2.4	0x50e7	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.078627110 CET	8.8.8.8	192.168.2.4	0x50e7	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.0.84	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.64.84	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.128.84	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.457211971 CET	8.8.8.8	192.168.2.4	0xc35a	No error (0)	prod.pinterest.global.map.fastly.net		151.101.192.84	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.555862904 CET	8.8.8.8	192.168.2.4	0x245f	No error (0)	googleads.g.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.622056961 CET	8.8.8.8	192.168.2.4	0x76a2	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.622056961 CET	8.8.8.8	192.168.2.4	0x76a2	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:44.630650997 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.630650997 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.846115112 CET	8.8.8.8	192.168.2.4	0xb69c	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.876331091 CET	8.8.8.8	192.168.2.4	0x4a01	No error (0)	sentry.wixpress.com	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:44.876331091 CET	8.8.8.8	192.168.2.4	0x4a01	No error (0)	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		52.2.188.208	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:45.036613941 CET	8.8.8.8	192.168.2.4	0xdf0e	No error (0)	v.pinimg.com	v.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:45.036613941 CET	8.8.8.8	192.168.2.4	0xdf0e	No error (0)	v.pinimg.com.gslb.pinterest.com	2-01-37d2-0007.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:45.048141956 CET	8.8.8.8	192.168.2.4	0x7775	No error (0)	i.pinimg.com	i.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:45.048141956 CET	8.8.8.8	192.168.2.4	0x7775	No error (0)	i.pinimg.com.gslb.pinterest.com	2-01-37d2-0004.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:45.048141956 CET	8.8.8.8	192.168.2.4	0x7775	No error (0)	dualstack.pinterest.map.fastly.net		199.232.80.84	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:45.346195936 CET	8.8.8.8	192.168.2.4	0x4bd7	No error (0)	s3.eu-de.cloud-object-storage.appdomain.cloud		158.177.118.97	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.224872112 CET	8.8.8.8	192.168.2.4	0x5d30	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:46.224872112 CET	8.8.8.8	192.168.2.4	0x5d30	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.383085012 CET	8.8.8.8	192.168.2.4	0x2e42	No error (0)	coralsmtp.com		172.67.173.3	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.383085012 CET	8.8.8.8	192.168.2.4	0x2e42	No error (0)	coralsmtp.com		104.21.96.46	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:31:46.500977993 CET	8.8.8.8	192.168.2.4	0x2b5f	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:46.853023052 CET	8.8.8.8	192.168.2.4	0x5a64	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:46.853023052 CET	8.8.8.8	192.168.2.4	0x5a64	No error (0)	pagead46.l.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:47.566567898 CET	8.8.8.8	192.168.2.4	0x4ece	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:47.566567898 CET	8.8.8.8	192.168.2.4	0x4ece	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:49.873186111 CET	8.8.8.8	192.168.2.4	0x6167	No error (0)	cineplasty-cystectomy-sheltering.s3.us-west-002.backblazeb2.com		206.190.215.254	A (IP address)	IN (0x0001)
Dec 2, 2021 15:31:52.701845884 CET	8.8.8.8	192.168.2.4	0x7269	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:31:52.707525015 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:11.046406031 CET	8.8.8.8	192.168.2.4	0x4fa	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:19.999150038 CET	8.8.8.8	192.168.2.4	0x9977	No error (0)	www.google.ch		172.217.168.35	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:25.293673992 CET	8.8.8.8	192.168.2.4	0x950a	No error (0)	video.wixstatic.com	media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:25.293673992 CET	8.8.8.8	192.168.2.4	0x950a	No error (0)	media-router.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:25.293673992 CET	8.8.8.8	192.168.2.4	0x950a	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:29.730581999 CET	8.8.8.8	192.168.2.4	0xe3c9	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:29.730581999 CET	8.8.8.8	192.168.2.4	0xe3c9	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:29.732580900 CET	8.8.8.8	192.168.2.4	0x560d	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:29.744545937 CET	8.8.8.8	192.168.2.4	0xb731	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:29.744545937 CET	8.8.8.8	192.168.2.4	0xb731	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.276257992 CET	8.8.8.8	192.168.2.4	0x32d	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:30.276257992 CET	8.8.8.8	192.168.2.4	0x32d	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:30.276257992 CET	8.8.8.8	192.168.2.4	0x32d	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	frog.wix.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.209.65.183	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		35.168.159.214	A (IP address)	IN (0x0001)

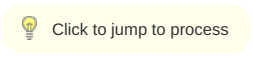
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.144.217.110	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.201.180.67	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.202.177.159	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.224.180.226	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.231.113.219	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:30.430394888 CET	8.8.8.8	192.168.2.4	0xdd65	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.45.176.168	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.649249077 CET	8.8.8.8	192.168.2.4	0x563a	No error (0)	www.editorx.com	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:32.649249077 CET	8.8.8.8	192.168.2.4	0x563a	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:32.649249077 CET	8.8.8.8	192.168.2.4	0x563a	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-db4-63-177.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:32.649249077 CET	8.8.8.8	192.168.2.4	0x563a	No error (0)	td-balancer-db4-63-177.wixdns.net		185.230.63.177	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	frog.editorx.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.231.113.219	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.204.209.24	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.88.78	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		52.45.176.168	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.144.217.110	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		50.17.151.88	A (IP address)	IN (0x0001)
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.164.30.7	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:32:32.843553066 CET	8.8.8.8	192.168.2.4	0xf1af	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.209.65.183	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3532 Parent PID: 3096

General

Start time:	15:31:25
Start date:	02/12/2021
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://knorrm.editorx.io/my-site
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 4672 Parent PID: 3532

General

Start time:	15:31:26
Start date:	02/12/2021
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=1552,320909960523264643840374 37087009067876,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8

Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 8856 Parent PID: 3532

General

Start time:	15:32:28
Start date:	02/12/2021
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=audio.mojom.AudioService --field-trial-handle=1552,3209099605232646438,4037437087009067876,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6680 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis