ID: 635386
Cookbook: browseurl.jbs
Time: 20:52:38
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

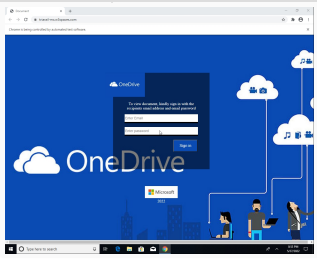
Windows Analysis Report

https://triarail-mx.w3spaces.com/

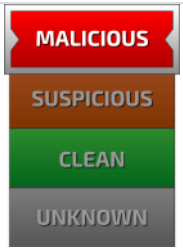
Overview

General Information

Sample URL:	http://https://triarail-mx.w3spaces.com/
Analysis ID:	635386
Infos:	



Detection



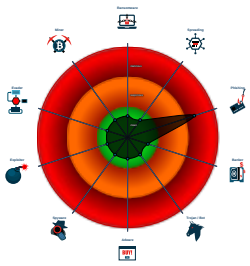
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- No HTML title found
- Form action URLs do not match ma…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2344 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://triarail-mx.w3spaces.com/ MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2740 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,4377966081719049101,2550601486194537045,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1964 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
28740.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Phishing

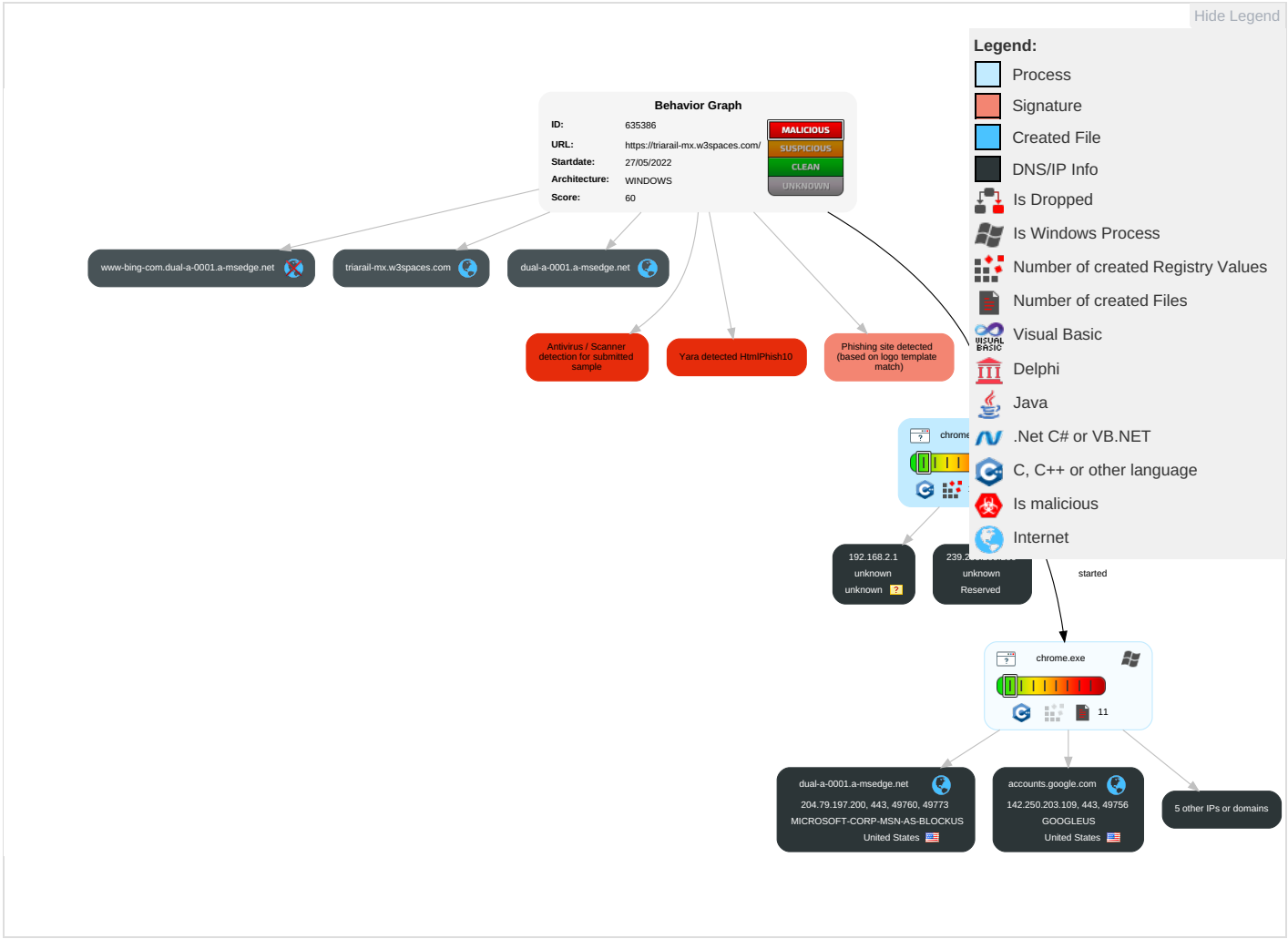
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

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	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	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	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

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://triarail-mx.w3spaces.com/	0%	Virustotal		Browse
http://https://triarail-mx.w3spaces.com/	0%	Avira URL Cloud	safe	
http://https://triarail-mx.w3spaces.com/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://triarail-mx.w3spaces.com/2	0%	Avira URL Cloud	safe	
http://https://triarail-mx.w3spaces.com/styles.css	0%	Avira URL Cloud	safe	
http://https://triarail-mx.w3spaces.com/	0%	Virustotal		Browse
http://https://triarail-mx.w3spaces.com/background.jpg	0%	Avira URL Cloud	safe	
http://https://triarail-mx.w3spaces.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
dual-a-0001.a-msedge.net	204.79.197.200	true	false		unknown
triarail-mx.w3spaces.com	13.226.244.95	true	false		unknown
clients.l.google.com	216.58.215.238	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

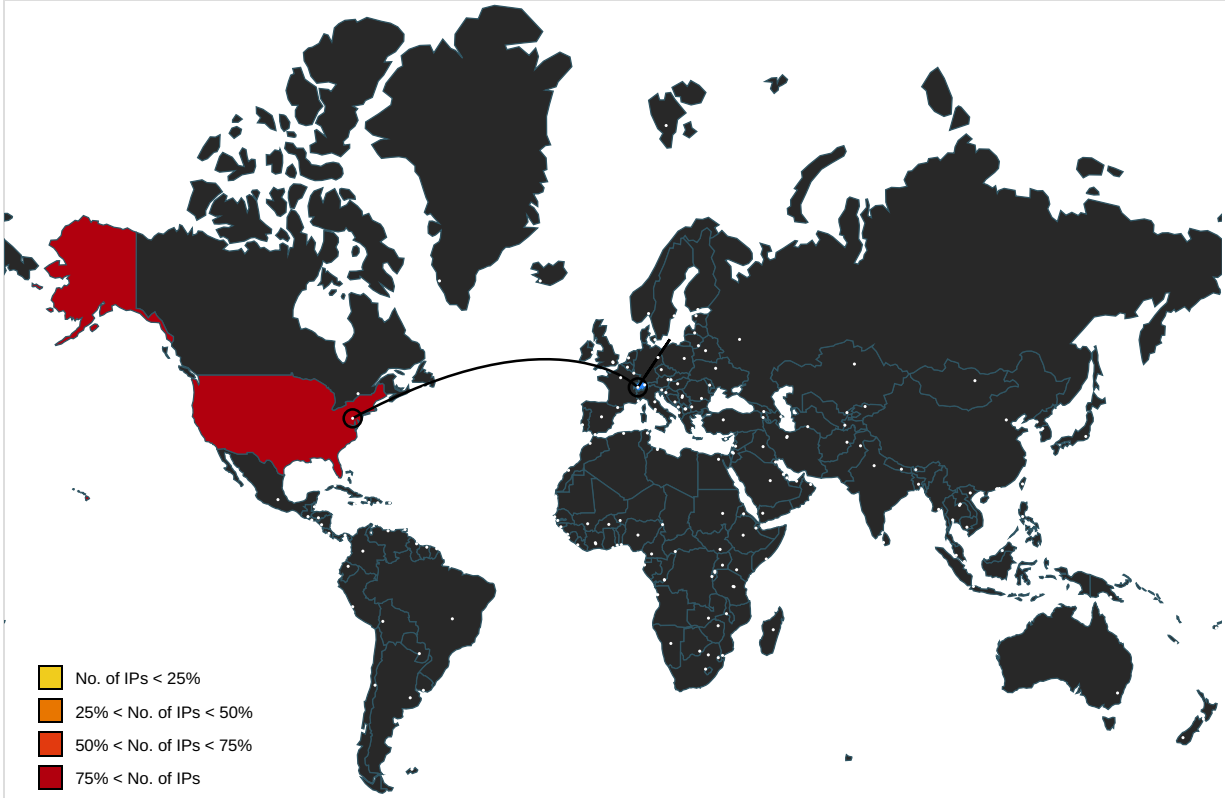
Name	Malicious	Antivirus Detection	Reputation
http://https://triarail-mx.w3spaces.com/	true	• 0%, Virustotal, Browse	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://triarail-mx.w3spaces.com/styles.css	true	• Avira URL Cloud: safe	unknown
http://https://triarail-mx.w3spaces.com/	true	• 0%, Virustotal, Browse	unknown
http://https://triarail-mx.w3spaces.com/background.jpg	true	• Avira URL Cloud: safe	unknown
http://https://triarail-mx.w3spaces.com/favicon.ico	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	91d06acf-3832-4b89-bc28-f4b352fe1e57.tmp.1.dr, ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://triarail-mx.w3spaces.com/2	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://https://www.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://apis.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://clients2.google.com	ea53a193-5322-422c-8027-1ba8d9ca8c76.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.79.197.200	dual-a-0001.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
13.226.244.95	triarail-mx.w3spaces.com	United States		16509	AMAZON-02US	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635386
Start date and time: 27/05/202220:52:38	2022-05-27 20:52:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 48s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://triarail-mx.w3spaces.com/
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:	15
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:	mal60.phis.win@20/85@4/7
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

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 142.250.203.99, 34.104.35.123, 172.217.168.42
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, content-autofill.googleapis.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, arc.msn.com, e12564.dspb.akamaiedge.net, a-0001.a-afdentry.net.trafficmanager.net, edgedl.me.gvt1.com, login.live.com, store-images.s-microsoft.com, update.googleapis.com, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\01950c6a-9bae-4205-b867-4ee29d881e82.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	modified
Size (bytes):	94708
Entropy (8bit):	3.75227194173807
Encrypted:	false
SSDEEP:	384:RzLIw69/mZKcV1XcnNgrJvcI3zQm3HCPGnarF6AaxDOeWBrNYm5uJqgUcHOiGUNk:ley156ujLke3msuEPXekKSEsJo
MD5:	CC86213D8C7D7C421A0443CF96EC2DCC
SHA1:	D5B2DBA9BADF1F520BE70EBBD54DCE29D8A6E916
SHA-256:	2FD597088F3EA16E31DFD7B2FFFBFF124A2210556B5A51FB16305198A2FBF22E
SHA-512:	1C77E52B64E19F02893F658A435FD3D05DC84DCA0A491F55B5ED5C1D597057CF495D1C9532921393782744B3A6526FA3267EE2CF2419F7AC0DE3FCF44BBBE51
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...j]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\2c53fa43-cc8a-48d9-ae59-31233bcff072.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751589421234318
Encrypted:	false
SSDEEP:	384:PzLIw69/SKlcnNgrJvcI3zQm3HCPGnarF6AaxDOeWBrNYm5uJqgUcHOiGUNt1A5e:By156ujLke3msuEPXekKSEsJP
MD5:	3BCA8119F9AEC9B863F3212B9424D200
SHA1:	26D0F8A836C4AA42238E51C06B416EA34334EB98
SHA-256:	5106E0C2948C1E891FEA1ECFDAC35EBF228A17827C56F5EA6EC4102C82BA2F32
SHA-512:	92F6C72A4AB279780CEF7FF347DD690E18EAF5ADBC6D31C46FC0F3450CE769E81FAD50AB937ED90CD1C1094D17B53ECDD246204A8523BF7DBBE8149616DEE 1C5
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j]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\6e0f9dbb-32ed-41f0-964c-f7f33a72c8ee.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):	207030
Entropy (8bit):	6.073096467903333
Encrypted:	false
SSDEEP:	3072:Eo3W0HdCqcBsM9ciOXlmrq3kxy44RdFcbXafIB0u1GOJmA3iuRw:j3WXfsUMVJ44daqfIlUOoSiuRw
MD5:	34CC04AAD80F307FF6106EF3968EFFD6
SHA1:	47CB31E11D9D731779D613238BC58331DBD8FDCC
SHA-256:	2669C99141A1E9A75A74A064F62AAFB87BCC708FAF522E5FF744969ED380EFAA
SHA-512:	51CC37DB7CC4E6B8FCF9E9DDAA0672AEF75A388D854E6231C1E3126F3B6CE15260294E010AA01D36F90572685156A7D8D1D4EFA8263CE8201EFBE1EACE42B C3

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":1.653677629963104e+12,"network":1.653677632e+12,"ticks":117938342.0,"uncertainty":4061019.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129523682"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\92bf1dda-6637-4421-830a-13f0ced0b57d.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):	207030
Entropy (8bit):	6.073096683446631
Encrypted:	false
SSDEEP:	3072:jo3W0HdCqcBsM9ciOXlmrq3kxy44RdFcbXafIB0u1GOJmA3iuRw:03WXfsUMVJ44daqfllUOoSiuRw
MD5:	B02B3AA32063DB5CA693B6636447E956
SHA1:	8C6E40C8DBE6768048298639B4CB355F55210C02
SHA-256:	0F52648635EAD5924A7EB376486592BA8A148DF33CFBA5A44E159C758ACD059F
SHA-512:	16D819FC47238D48A40455F78C30871E06DC8B9DE6D126AF475427DED02B10CF958F45E94073DE5213F973FFFF6C536DAF41ADB258BE70BFACB9B5153330C19C
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":1.653677629963104e+12,"network":1.653677632e+12,"ticks":117938342.0,"uncertainty":4061019.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\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\5c39f848-7c0d-4611-9b26-8531453c9001.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):	5197
Entropy (8bit):	4.968822877839025
Encrypted:	false
SSDEEP:	96:nXLl5T1pIKIJk5k0JCKL8JpkC12bOTlVuHn:nXLl51pIXkh4KYkCQ
MD5:	A9132BFAB5E1BE07A2FFF8DE096665CB
SHA1:	308CA345BCB460F92189C2749250C091A2A75282
SHA-256:	3DF0F14490ECD5A875D044FD38DEC5AB12860FC9F6C981207CC7A875FCEB7A72
SHA-512:	21E867D83ADA2D46A9B9465E74F26ABD5E3B44A766CADA1F044B0C2951EF2640632347C1D4A51217B005692F97E7E7BC2246EB46870D1C0D117B5B289DBE43AB

Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298151228425138","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\68ebcfcd-08d0-4ca4-b847-6c6110d1be25.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):	17703
Entropy (8bit):	5.576976459263201
Encrypted:	false
SSDEEP:	384:2qVtQLl+kXv1kXqKf/pUZNCgVLH2HfDPrUh5HUN4q:QLlVv1kXqKf/pUZNCgVLH2HfzrUrkt
MD5:	D70210EB2A4E3AE425A296F3B6D9AC5A
SHA1:	EEFC13986E02BFE532C7B59A517C56040F264CB0
SHA-256:	EC42D0A5AC2CFE42AD3D1901798CAB1ECA889A76D904EAC249ECDEE96AAD6F18
SHA-512:	20CED1C130961749F8A8BDBC0B49433107E1E6A6029216CFC079F221F2C7BF967E3D6AB0297C16E4A24C403A04D496598675CDCE743DF7211E685102ED276EC
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298151227299948","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_i

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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
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):	5.225120237885486
Encrypted:	false
SSDEEP:	6:AX2EI+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVfX2SSmWZmwYVfX2wVkwOwkn23iKG:AX2H+vYf5KkTXfchI3FUtiX2B/IX2wVo
MD5:	03EC3BAAD93020F53BFECEC770855C9A
SHA1:	5E3B8CCE88A77931A01F5CED492C70F54B2F69A7
SHA-256:	CAAFB83F7EEF1E98B1AB1C8D9FA8CEEC8AB3C9DE96C39873402293DA2E2738CC
SHA-512:	E362E13C87EBB7C0D13812FEA1830A145DCC6B5345358CC47DAB71046749D07C1642BF53B67663ED47556BC6D7FDD8B3A31F7DC09D80FA1E0BE42D2F5620B(55
Malicious:	false
Reputation:	low

Preview:	2022/05/27-20:54:09.150 d0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-20:54:09.152 d0c Recovering log #3.2022/05/27-20:54:09.153 d0c 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):	5.225120237885486
Encrypted:	false
SSDEEP:	6:AX2EI+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVfX2SSmWZmwYVfX2wVkwOwkn23iKG:AX2H+vYf5KkTXfchI3FUtiX2B/IX2wVo
MD5:	03EC3BAAD93020F53BFECEC770855C9A
SHA1:	5E3B8CCE88A77931A01F5CED492C70F54B2F69A7
SHA-256:	CAAFB83F7EEF1E98B1AB1C8D9FA8CEEC8AB3C9DE96C39873402293DA2E2738CC
SHA-512:	E362E13C87EBB7C0D13812FEA1830A145DCC6B5345358CC47DAB71046749D07C1642BF53B67663ED47556BC6D7FDD8B3A31F7DC09D80FA1E0BE42D2F5620B055
Malicious:	false
Reputation:	low
Preview:	2022/05/27-20:54:09.150 d0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-20:54:09.152 d0c Recovering log #3.2022/05/27-20:54:09.153 d0c 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):	474
Entropy (8bit):	5.0939866596444014
Encrypted:	false
SSDEEP:	12:JxSMSjIEYixuP1pdVBwhS9uhsiylYJBk778B/xgsj19RROUG2f9:KMO3xI1p/hiy+vY78BJgsz339
MD5:	3D0B8FCFC224D26256AE532ACED955A4
SHA1:	06365D05CC640DEBA3AEEC4B7C208DC5A481334D
SHA-256:	62253CFBF8BD484CD38B3AC81E13471F5AEAA20FB5B9FC7B06FFB45DB6525F29
SHA-512:	71899CB41948C368206903EE02E11ECC1DDF71695C3D91DD9CB3E06B688FE77FED8A23B0FCA14C06D71E592B5D229B5A8973B4AA6CA0EB685655DBA2E3111B3E
Malicious:	false
Reputation:	low
Preview:	.....".0....com..document..https..mx..triarail..w3spaces*H.....com.....document.....https.....mx.....triarail.....w3spaces..2.....3.....a.....c.....d.....e.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w.....x...:8.....BQ...M..... .....*!https://triarail-mx.w3spaces.com/2.Document:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhlGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1C
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
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5197
Entropy (8bit):	4.968822877839025
Encrypted:	false
SSDEEP:	96:nXLl5T1pIKIJk5k0JCKL8JpkC12bOTlVuHn:nXLl51pIXkh4KYkCQ
MD5:	A9132BFAB5E1BE07A2FFF8DE096665CB
SHA1:	308CA345BCB460F92189C2749250C091A2A75282
SHA-256:	3DF0F14490ECD5A875D044FD38DEC5AB12860FC9F6C981207CC7A875FCEB7A72
SHA-512:	21E867D83ADA2D46A9B9465E74F26ABD5E3B44A766CADA1F044B0C2951EF2640632347C1D4A51217B005692F97E7E7BC2246EB46870D1C0D117B5B289DBE43A B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298151228425138","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","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):	17703
Entropy (8bit):	5.576976459263201
Encrypted:	false
SSDEEP:	384:2qVtQLl+kXv1kXqKf/pUZNCgVLH2HfDPrUh5HUN4q:QLlVv1kXqKf/pUZNCgVLH2HfzrUrkt
MD5:	D70210EB2A4E3AE425A296F3B6D9AC5A
SHA1:	EEFC13986E02BFE532C7B59A517C56040F264CB0
SHA-256:	EC42D0A5AC2CFE42AD3D1901798CAB1ECA889A76D904EAC249ECDEE96AAD6F18
SHA-512:	20CED1C130961749F8A8BDBC0B49433107E1E6A6029216CFC079F221F2C7BF967E3D6AB0297C16E4A24C403A04D496598675CDCE743DF7211E685102ED276EC
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298151227299948","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\91d06acf-3832-4b89-bc28-f4b352fe1e57.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:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
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
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
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:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
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\afa8159d-b345-4b63-9808-7fa3a009cb14.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):	5197
Entropy (8bit):	4.968984821654305
Encrypted:	false
SSDEEP:	96:nXLlAt1pIKIJk5k0JCKL8JpkC12bOTlVuHn:nXLls1pIXkh4KYkCQ
MD5:	AE27B99113E51806E8089BD7FA382DE6
SHA1:	8D90F960011EC3C05D8888E3F258D5064432C24B
SHA-256:	D678A929E05E99FE9A265964D0C27FB3BDA8BE5B7A4FF85519486D06DC1B03E4
SHA-512:	E8A7845E1B1A5344FBEBE3BADF4FD27DA129AFE0F238B7233DCD5F1E683BA8F1214CB94FA7E93FBE081785E6E98A2AB218F6D3474D6B85BD823605EFAB47F4FA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298151228425138","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c8f96c6b-8060-46ad-8edf-8ff7a7c0a15c.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):	17356
Entropy (8bit):	5.571179285143444
Encrypted:	false
SSDEEP:	384:2qVtdLl+kXv1kXqKf/pUZNCgVLH2HfDPrUrvUN4h:dLlVv1kXqKf/pUZNCgVLH2HfzrUTky
MD5:	2C2BD349E3B2169666511EACF0F3AF59
SHA1:	B2EB4DD4D1A6C2B8E900EC5224E346AA9D40A09F
SHA-256:	401D07C835964E2B3155945CE2F7CBF8A1584407362A85EC8F87D5702D569794
SHA-512:	8EE6A83A463A224D678DDD9D9311186484523E89052E3BD72596C867624708F9614B1AE3596C4437DFA2369B6F6FC35CC5E6B1F7D1017411439CF57B86A877D2
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298151227299948","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_i

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dcbeb972-e93a-466b-aff7-c0da6c5412d0.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea53a193-5322-422c-8027-1ba8d9ca8c76.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:	96:6FGX0G70GhlGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1C
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"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\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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59

SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	207030
Entropy (8bit):	6.073096467903333
Encrypted:	false
SSDEEP:	3072:Eo3W0HdCqcBsM9ciOXlmrq3kxy44RdFcbXafIB0u1GOJmA3iuRw:j3WXfsUMVJ44daqfIlUOoSiuRw
MD5:	34CC04AAD80F307FF6106EF3968EFFD6
SHA1:	47CB31E11D9D731779D613238BC58331DBD8FDCC
SHA-256:	2669C99141A1E9A75A74A064F62AAFB87BCC708FAF522E5FF744969ED380EFAA
SHA-512:	51CC37DB7CC4E6B8FCF9E9DDAA0672AEF75A388D854E6231C1E3126F3B6CE15260294E010AA01D36F90572685156A7D8D1D4EFA8263CE8201EFBE1EACE42B2C3
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":1.653677629963104e+12,"network":1.653677632e+12,"ticks":117938342.0,"uncertainty":4061019.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129523682"},"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):	3.75227194173807
Encrypted:	false
SSDEEP:	384:RzLIw69/mZKcV1XcnNgrJvcI3zQm3HCPGnarF6AaxDOeWBrNYm5uJqgUcHOiGUNk:ley156ujLke3msuEPXekKSEsJo
MD5:	CC86213D8C7D7C421A0443CF96EC2DCC
SHA1:	D5B2DBA9BADF1F520BE70EBBD54DCE29D8A6E916
SHA-256:	2FD597088F3EA16E31DFD7B2FFFBFF124A2210556B5A51FB16305198A2FBF22E
SHA-512:	1C77E52B64E19F02893F658A435FD3D05DC84DCA0A491F55B5ED5C1D597057CF495D1C9532921393782744B3A6526FA3267EE2CF2419F7AC0DE3FCF44BBBE51
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...j]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\b44ac866-1f95-461d-86fc-26aa7415faa1.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):	207030
Entropy (8bit):	6.073096683446631
Encrypted:	false
SSDEEP:	3072:jo3W0HdCqcBsM9ciOXlmrq3kxy44RdFcbXafIB0u1GOJmA3iuRw:03WXfsUMVJ44daqfIlUOoSiuRw
MD5:	B02B3AA32063DB5CA693B6636447E956
SHA1:	8C6E40C8DBE6768048298639B4CB355F55210C02
SHA-256:	0F52648635EAD5924A7EB376486592BA8A148DF33CFBA5A44E159C758ACD059F
SHA-512:	16D819FC47238D48A40455F78C30871E06DC8B9DE6D126AF475427DED02B10CF958F45E94073DE5213F973FFFF6C536DAF41ADB258BE70BFACB9B5153330C19C
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":1.653677629963104e+12,"network":1.653677632e+12,"ticks":117938342.0,"uncertainty":4061019.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Temp\3aa381a4-acac-40ad-8878-f4141b69ec2f.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\ac7c5c8d-1f42-4e97-b6dd-c44eef909149.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\3aa381a4-acac-40ad-8878-f4141b69ec2f.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	4.132566655778463
Encrypted:	false
SSDEEP:	24:YHYpcyllEQVFc0Bh0GQVQQVEM0bRLzRd0bRLzRRpcyllNQVb26RQ0bR60L0ZWOFY:YHYpZaQLH1QKQ6xxzcxzvpZzQA6z2nhQ
MD5:	D7A97183BCBD5FB677AA84D464F0C564
SHA1:	CDBB279B864E2C0A51E0892B8714131802586506
SHA-256:	76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02
SHA-512:	36F0310DD06319E4A51F77E4C3D64F6276891CE6410FE2571324BB71F2FBCDA368EAC4267FF8268086BE6912E41787D0F70771755E3D49E3E8C26648EAC6EFC9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u04 42\u044a\u043f \u0434\u043e \u043f\u0440\u043b\u043e\u0436\u0435\u043d\u0438\u0435\u0442\u043e."},"craw_connect_to_network":{"message":"\u041c\u 043e\u043b\u044f, \u0441\u0432\u044a\u0440\u0436\u0435\u0442\u0435 \u0441 \u0441\u0435 \u043c\u0440\u0435\u0436\u0430."},"app_name":{"message":"\u041f \u043b\u0430\u0449\u0438\u0442\u043d\u043e\u044f \u0432 \u0443\u0435\u0431 \u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 Chrome"},"app_descr iption":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431 \u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 \u043d \u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e \u0441\u0442\u044a\u043f \u0434\u043e \u0432\u0433\u0440\u0430\u0436\u0434\u0430\u043d\u0435 \u0442\u0430\u0437\u0438 \

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	556
Entropy (8bit):	4.768628082639434
Encrypted:	false
SSDEEP:	12:YGGYp73YbYHOLBiGF14gevg7p6ixuYHOPBBVC9WO/NrnLAOK:YHYp73vuLBVV17pRunVC9WOFvAOK
MD5:	58BA5F65ED971591D1F9D81848EE31D0
SHA1:	BDA3C8B74653334FC8F060CAFBCEA58DF0113AB7
SHA-256:	CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885
SHA-512:	BA2A6BAA3011A54E6B07E29DFD133009D66B6CFFF525DEC0024BDE55A9BED463AD130307EE64BFB4A983A11FFD6B44BD53ED38EB144083A2CBEFA8D85C4D 5D41
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Ara mateix aquesta aplicaci\u00f3 no est\u00e0 disponible."},"craw_connect_to_network":{"message":"Connecteu-vos a una xarxa .'},"app_name":{"message":"Sistema de pagaments de Chrome Web Store"},"app_description":{"message":"Sistema de pagaments de Chrome Web Store"},"iap_un available":{"message":"La funci\u00f3 Pagaments a l'aplicaci\u00f3 no est\u00e0 disponible actualment."},"please_sign_in":{"message":"Inicieu la sessi\u00f3 a C hrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	550
Entropy (8bit):	4.905634822460801
Encrypted:	false
SSDEEP:	12:YGGYpTPklW+g5Q7wvAvPJE7ZEWJE7ZRpmJEWN20GN5Q9O/NrnLAOK:YHYpbt5SwvGJE7ZfJE7ZRpmJEEGN5WOi
MD5:	43161EFFA28A0DBFC67B8F7DBE1B5184
SHA1:	FE0A9235A59B51B7F564F14FF564344927F035B8
SHA-256:	3A04421DF5218E8ABD3B0E2AFE11E8338D7BDCBCD1ADB122416944B102BC9696
SHA-512:	FC6A391A4B37FFEE2182F29C1590E32766A1820DC58D0A70A8DD96D7ABE74B47181B24AFFF8ADAE12686CCB1B898DCDDB882EFD205C3387B5B6F3CFBE6E5E A78
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Aplikace v sou\u010dasn\u00e9 dob\u011b nen\u00ed dostupn\u00e1."},"craw_connect_to_network":{"message":"P\u0159ipojte se pros\u00edm k s\u00edti."},"app_name":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message":"Platby v aplikaci aktu\u00e1ln\u011b nejsou k dispozici."},"please_sign_in":{"message":"P\u0159ihlaste se do Chromu."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.795529861403324
Encrypted:	false
SSDEEP:	12:YGGYpB/wHlHE3qKWEMqKWRp8KW/wU0HWO/NrnLAOK:YHYpN4lGqKAqKgp8FiHWOFvAOK
MD5:	31264DDBF251A95DE82D0A67FA47DB3A
SHA1:	3A48DC7AF26A153594C7849E1D92AAC31296459B
SHA-256:	EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23
SHA-512:	B97D61BD71E3F0A91FF1048D2ACAD4BC092CCAF157B7A96029B6AB5AF1812B01814E3153CD894307CB13DC132523EAC22B19CADA6B97F4B81B0D1132562317B5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"craw_connect_to_network":{"message":"Opret forbindelse til et netv\u00e6rk."},"app_name":{"message":"Betalinger i Chrome Webshop"},"app_description":{"message":"Betalinger i Chrome Webshop"},"iap_unavailable":{"message":"Betaling i appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"please_sign_in":{"message":"Log ind p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	516
Entropy (8bit):	4.809852395188501
Encrypted:	false
SSDEEP:	12:YGGYpyBCEl9ljMRE1RRpUT6+ZMUO/NrnLAOK:YHYpQDbPpUTvTOFvAOK
MD5:	7639B300B40DDAF95318D2177D3265F9
SHA1:	BF9EFDF073231CB3FCFCA5CCCA25B079ECFC45BD
SHA-256:	356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0
SHA-512:	70593318C6626B5D25729E8D8109D5611B95283266621BE60ADD7E60C0DD5BC43848E956C767251B7B3CCDF5A0929922DE38F90CC8632CCD0C1CCFC7D6DEFE9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Die App ist momentan nicht verf\u00fcgbar."},"craw_connect_to_network":{"message":"Bitte stellen Sie eine Verbindung zu einem Netzwerk her."},"app_name":{"message":"Chrome Web Store-Zahlungen"},"app_description":{"message":"Chrome Web Store-Zahlungen"},"iap_unavailable":{"message":"In-App-Zahlungen sind momentan nicht m\u00f6glich."},"please_sign_in":{"message":"Bitte melden Sie sich in Chrome an."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	4.338644812557597
Encrypted:	false
SSDEEP:	24:YHYpgFMjXrNW1DWgHle+T2dAplFcTpW1auWgtes9WOFvAOK:YHYpkMj7yxHw+CdAplFcifIs9nhQ
MD5:	3026E922B17DBEE2674FDAEE960DF584
SHA1:	76602B1E3449F1B67DE42FD31A581B0821BFEFF0
SHA-256:	876845B5A061FAB3CF2A1466E01015DC40DF8449F1CB4205F575CEBED8717BAD
SHA-512:	0C4DCB2589553F9F75534E6C702EBF9095665C93D213564265E39220A99B61BB112A3B20980CE0377C7E98878E3240EB87312B5ECE874382B7E9CA90A0016992
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u0397 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ae \u03c0\u03c1\u03bf\u03c2 \u03c4\u03bf \u03c0\u03b1\u03c1\u03cc\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b4\u03b9\u03b1\u03b8\u03ad\u03c3\u03b9\u03bc\u03b7.","craw_connect_to_network":{"message":"\u03a3\u03c5\u03bd\u03b4\u03b5\u03b8\u03b5\u03af\u03c4\u03b5 \u03c3\u03b5 \u03ad\u03bd\u03b1 \u03b4\u03af\u03ba\u03c4\u03c5\u03bf.","app_name":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"app_description":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"iap_unavailable":{"message":"\u039f\u03b9 \u03c0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03b5\u03bd\u03c4\u03cc\u03c2 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ce\u03bd \u03b4\u03b5\u03bd \u03b4\u03b5\u03af\u03bd\u03b1\u03b9 \u03b1\u03c5\u03c4\u03ae\u03bd \u03c4\u03b7 \u03c3\u03c4\u03b9\u03b3\u03bc\u03ae \u03b4\u03b9\u03b1\u03b8

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	450
Entropy (8bit):	4.679939707243892
Encrypted:	false
SSDEEP:	12:YGGYp4Fp0JAvpErBpUwEGFpfJAKWO/NrnLAOK:YHYpAp0J3pURKpfJzWOFvAOK
MD5:	DBEDF86FA9AFB3A23DBB126674F166D2
SHA1:	5628AFFBCF6F897B9D7FD9C17DEB9AA75036F1CC
SHA-256:	C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE
SHA-512:	931D7BA6DA84D4BB073815540F35126F2F035A71BFE460F3CCAED25AD7C1B1792AB36CD7207B99FDDF5EAF8872250B54A8958CF5827608F0640E8AAFE11E0071
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App currently unavailable."},"craw_connect_to_network":{"message":"Please connect to a network."},"app_name":{"message":"Chrome Web Store Payments"},"app_description":{"message":"Chrome Web Store Payments"},"iap_unavailable":{"message":"In-App Payments is currently unavailable."},"please_sign_in":{"message":"Please sign into Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	450
Entropy (8bit):	4.679939707243892
Encrypted:	false
SSDEEP:	12:YGGYp4Fp0JAvpErBpUwEGFpfJAKWO/NrnLAOK:YHYpAp0J3pURKpfJzWOFvAOK
MD5:	DBEDF86FA9AFB3A23DBB126674F166D2
SHA1:	5628AFFBCF6F897B9D7FD9C17DEB9AA75036F1CC
SHA-256:	C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE
SHA-512:	931D7BA6DA84D4BB073815540F35126F2F035A71BFE460F3CCAED25AD7C1B1792AB36CD7207B99FDDF5EAF8872250B54A8958CF5827608F0640E8AAFE11E0071
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App currently unavailable."},"craw_connect_to_network":{"message":"Please connect to a network."},"app_name":{"message":"Chrome Web Store Payments"},"app_description":{"message":"Chrome Web Store Payments"},"iap_unavailable":{"message":"In-App Payments is currently unavailable."},"please_sign_in":{"message":"Please sign into Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	542
Entropy (8bit):	4.704430479150276
Encrypted:	false
SSDEEP:	12:YGGYpDbKEzebFcjwWtp6FPbF3QVcqHWO/NrnLAOK:YHYpqEzoFmpQymaWOFvAOK
MD5:	3F4B0F56C2839839FC3E3270ED4CB7B6
SHA1:	0D74EA655EAE3990E95BD26F6E1467EDF3EB3478
SHA-256:	1912EA5E0A62BBC669DC14AB5A5BD5514B0502C483EE1F27C3F8834384187079
SHA-512:	4E6A828FE73FC4AB03F0EE966CE7BD8061575A059E90709F908D8D91C5F4EB6A8D25BBFA100E48AD7AC94E76D3BCD3547C277B4150D515222757CC9906AD202
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"Los pagos en la aplicaci\u00f3n no est\u00e1n disponibles en este momento."},"please_sign_in":{"message":"Inicia sesi\u00f3n en Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	510
Entropy (8bit):	4.719977015734499
Encrypted:	false
SSDEEP:	12:YGGYpDbKEzebFcjwWtpML4c9WO/NrnLAOK:YHYpqEzoFmpMLBWOFvAOK
MD5:	1FD5DAF46C4D7C4F571C263EC37B943B
SHA1:	A57EE5EF6861F88005C2230EA3D633A1B4CA105A
SHA-256:	BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417
SHA-512:	79C3104F1DC51B17B062803209029C8165DBD391FBE0B69BB406D7B4F92FE1898CAC30E20C2E5CFB65D643B978095626C68EAA0CFCA064354D52D52D16BF21A9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	460
Entropy (8bit):	4.679279844668757
Encrypted:	false
SSDEEP:	6:YGGYpkeVeVfCb53Q67PZV6pPQpkjA5DeY68AoLRcZplNgCnGcPxYA8KoOK:YGGYpv2A77PrQPQpT/AoLRO/NrnLAOK
MD5:	0293A7BAE6EEE62C4067A80E262D6A2D
SHA1:	E76B07BD49FFBBFB6841B7335CBE7A9620714402
SHA-256:	D06F20D4D68D1DBB89EF7D8E405D9499CB2EB2560217CD5B4A51AB1DD50CAB44
SHA-512:	8BF97DA4038A9C4426A285D5FEF0953F4E7E6D0667091A39DE4D4C5B4C35FC7B6A804425DBB4B82356A93950738E4F0937DE1AD777AE75AAC9BFB97D63F771E0
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Rakendus pole praegu saadaval."},"craw_connect_to_network":{"message":"Looge \u00fchendus v\u00f5rguga."},"app_name":{"message":"Chrome'i veebipoe maksed"},"app_description":{"message":"Chrome'i veebipoe maksed"},"iap_unavailable":{"message":"Rakendusesisesed maksed ei ole praegu saadaval."},"please_sign_in":{"message":"Logige Chrome'i sisse."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	568
Entropy (8bit):	4.768364810051887
Encrypted:	false
SSDEEP:	12:YGGYpQTajDRdes6KUVJ8epQTNuflRdes6K27lO/NrnLAOK:YHYpQ67esNMpQJufI7esN27lOFvAOK
MD5:	E5BBE7DBBE75F45BDCD49DB8C797106E
SHA1:	0F069D7D19768180945F0D8B67DC71262FD586A2
SHA-256:	BFFB2248B4C66306133FA6ECBB1541F44B3BE22CC8D9A338D690E0B1D0C85532
SHA-512:	F6FE20B7A3B99BDBBF6F4737C8C63FE3098F060E6791BC40ED0E95FA5F93AA55C2643766EA2BE099E42EC378CB6E4B6FE7B5F2DA56C03A6A990B94A1F872B825
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Sovellus ei ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"craw_connect_to_network":{"message":"Muodosta verkkoyhteys."},"app_name":{"message":"Chrome Web Storen maksut"},"app_description":{"message":"Chrome Web Storen maksut"},"iap_unavailable":{"message":"Sovelluksen sis\u00e4iset maksut eiv\u00e4t ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"please_sign_in":{"message":"Kirjaudu sis\u00e4n Chromeen."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	515
Entropy (8bit):	4.699741311937528
Encrypted:	false
SSDEEP:	12:YGGYpsiwZALE0Dw9DtpsjzAvX2xSWO/NrnLAOK:YHYpsBvpsiX2xSWOFvAOK
MD5:	658DAD2AF2DC3AC1567D84E8B95F68B0
SHA1:	EE1121215960EC5ED5F7B6BDB8E4680731EBF83D
SHA-256:	978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29
SHA-512:	F2FB93245D80E2CB2CA1BB2B0654FE92AD9041A558850D78AF4031CB83D2AD3BF5ABCFE6BC32160D028CA3914FA69A64784858A34FA56389C08D52B316346A0 5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Kasalukuyang hindi available ang app."},"craw_connect_to_network":{"message":"Mangyaring kumonekta sa isang network."},"app_ name":{"message":"Mga Pagbabayad sa Chrome Web Store"},"app_description":{"message":"Mga Pagbabayad sa Chrome Web Store"},"iap_unavailable":{"message" :"Kasalukuyang hindi available ang Mga Pagbabayad na In-App."},"please_sign_in":{"message":"Mangyaring mag-sign in sa Chrome."},"jwt_retrieve_failed":{"message" :"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	562
Entropy (8bit):	4.717150188929866
Encrypted:	false
SSDEEP:	12:YGGYpKdgbfUSPcLf0E1UDWcLf0E1Uop6oTQpGnbgWWO/NrnLAOK:YHYpagI26Qq6QopRTQwnFWOFvAOK
MD5:	1E32A78526E3AC8108E73D384F17450B
SHA1:	BFE2E47D888BA530A27DD1BDE25C46433C2A545C
SHA-256:	80F6EE69F1E022812BCCC1DE1CDC53772CDF90F4E93224161B23FA607D45136A
SHA-512:	5504F6D440779BC96571863D60B1E175EEDDC2E65B1ABBCFCFD19123F329F2E025FBA4D49BD23E33B77FFB6061BA6645132E04D4A7DEDE77F514B2151CDDF8 96
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Application indisponible pour le moment."},"craw_connect_to_network":{"message":"Veuillez vous connecter \u00e0 un r\u00e9se au."},"app_name":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"},"app_description":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"} ,"iap_unavailable":{"message":"Les paiements via l'application ne sont pas disponibles pour le moment."},"please_sign_in":{"message":"Veuillez vous connecter \u00e0 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.454461505283053
Encrypted:	false
SSDEEP:	24:YHYpINcVc0KgcNZvCjK7jK6pVi8/pBKgcNkQVcRynX6XjOFvAOK:YHYpIcQvCjIjRpVVBXPsqihQ
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1A0 C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0910\u092a\u094d\u0932\u093f\u0915\u0947\u0936\u0928 \u0907\u0938 \u0938\u092e\u092f \u0909\u092a\u0932\u092c\u0 94d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"craw_connect_to_network":{"message":"\u0915\u0943\u092a\u092f\u093e \u0928\u0947\u091f\u0935\u0930\u094d\u0915 \u0938\u0947 \u0915\u0928\u0947\u0915\u094d\u091f \u0915\u0930\u0947\u0902."},"app_name":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940 \u0909\u092a\u0932\u092c\u094d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"please_sign_in":{"message":"\u0915\u0943\u092a\u092f\u093e Chrome \u092e\u0947\u0902 \u0938\u093e\u0907\u0928 \u0907\u0928 \u0915\u0930\u0947\u0902."},"jwt_retrieve_failed":

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.819520019697578
Encrypted:	false
SSDEEP:	12:YGGYpTOEu5TfIJPFJEPJEsxmfEWJEsxmfRpmJEzrMrQp5TfnHV5/WIWO/NrnLAOK:YHYpq7EJPkJExfJExRpmJE/LXzHV5/ji
MD5:	9CF848209FF50DBF68F5292B3421831C
SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD
SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333EDF5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenuta\u010dno nije dostupna."},"craw_connect_to_network":{"message":"Pove\u017eite se s mre\u017eom."},"app_name":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	612
Entropy (8bit):	4.865151680865773
Encrypted:	false
SSDEEP:	12:YGGYpiKQhMDCJNYygdGs61gdGs3piKQChMDZAYRO/NrnLAOK:YHYpzQhsiPgdG1gdGcpzQChsZAYOFvAD
MD5:	4AD92AFDE3408FBBE43B0C3C71677650
SHA1:	3488901077F336A3196F9AE116E36DF1674E1ACA
SHA-256:	61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E
SHA-512:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD09
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Az alkalmaz\u00e1s jelenleg nem \u00e9rhet\u0151 el."},"craw_connect_to_network":{"message":"K\u00e9rj\u00fck, csatlakozzon egy h\u00e1l\u00f3zathoz."},"app_name":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"app_description":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"iap_unavailable":{"message":"Az alkalmaz\u00e1son bel\u00fcli fizet\u00e9s jelenleg nem \u00e9rhet\u0151 el."},"please_sign_in":{"message":"Jelentkezzen be a Chrome-ba."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	461
Entropy (8bit):	4.642271834875684
Encrypted:	false
SSDEEP:	12:YGGYpDBHAeSnLPo2sWo25pmo22C/SzFAAh+M9WO/NrnLAOK:YHYplHcFTpmzOptWOFvAOK
MD5:	9008516AA1D8F8C2B8ECE70B7E4963AD
SHA1:	EA7AD4BE77A80A4B9FB1E59A340010830E494747
SHA-256:	89CAB0AF2B53C6ABEB93C8C628DDCBDD286A7A2672FE03440411BB654E3A0675
SHA-512:	46534829417CAD54310BA90AD4545918A2E934508E0CC3467E367944E52315B1BC6500119214EABD40D641DD167C077935436135AF1C0DB1D1007AE98E6175FC
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikasi tidak tersedia saat ini."},"craw_connect_to_network":{"message":"Sambungkan ke jaringan."},"app_name":{"message":"Pembayaran Chrome Webstore"},"app_description":{"message":"Pembayaran Chrome Webstore"},"iap_unavailable":{"message":"Pembayaran Dalam Aplikasi saat ini tidak tersedia."},"please_sign_in":{"message":"Harap masuk ke Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped

Size (bytes):	464
Entropy (8bit):	4.701550173628233
Encrypted:	false
SSDEEP:	12:YGGYpmXXHEva6Plqd6Wlqd3p6PqTX2zaWO/NrnLAOK:YHYpmnkvNtdRtd3pX6+WOFvAOK
MD5:	BB9C32BA62DDA02F9471C64B5F9CF916
SHA1:	9825037D5D9185C58456CDD887C77B10A41D8C84
SHA-256:	43A0B113D3773BA78F82BB9E42DDC46F6892D0FBBB351F94A7C105E4A146E9C1
SHA-512:	4D3DB91A6251F2DD9CBF97D29805A7AC23F49988966E9B686D486B4A8CEBEA33F5502E3891D5231674061127C282C745FB87FDA7467A6172851BF6925506C8CA
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App al momento non disponibile."},"craw_connect_to_network":{"message":"Collegati a una rete."},"app_name":{"message":"Pagamenti Chrome Web Store"},"app_description":{"message":"Pagamenti Chrome Web Store"},"iap_unavailable":{"message":"La funzione Pagamenti In-App non \u00e8 al momento disponibile."},"please_sign_in":{"message":"Accedi a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	806
Entropy (8bit):	4.671841695172103
Encrypted:	false
SSDEEP:	12:YGGYpqbrR5IYstMNcXh82q8b0kOoZ46ToZ43pqbtVD2CR5IYstR0O8b0KhO/Nrnk:YHYpcFiLRMACqNpctVPieOAhOFvAOK
MD5:	96C8CBD161D3CE9CB1A46CB2CD0C6583
SHA1:	78BBFCF035B5B620E353C8E520653ADD3F4E7DB8
SHA-256:	81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A
SHA-512:	692468B7B44D961D8248BBC30CC11DE9F3F7E89D01A609E6CB71CAF653D8212C15DFA834C5FB6E8261FD21A25E9616861C0A3FC01DB27CBBE79C3FDE2C654 DD
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u30a2\u30d7\u30ea\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"craw_connect_to_network":{"message":"\u30cd\u30c3\u30c8\u30ef\u30fc\u30af\u306b\u63a5\u7d9a\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"app_name":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"app_description":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"iap_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"please_sign_in":{"message":"Chrome \u306b\u30ed\u30b0\u30a4\u30f3\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	656
Entropy (8bit):	4.88216622785951
Encrypted:	false
SSDEEP:	12:YGGYpqHZMskkrcaw6cT/pb8pqHkrskeQV7wUO/NrnLAOK:YHYpsrkYcawwps5kdwUOFvAOK
MD5:	3CAF23A8EA2332D78B725B6C99EC3202
SHA1:	95C3504F55A929449EF2E3AB92014562AACD39AD
SHA-256:	BFE72BBC492B9018A599CB6575366696E431E6A38400E4B2ED06EAE3340D3AE5
SHA-512:	C000FCCB567D3590D4C401005E78C539961455BB13686296EC4FF7018BB0A4DAB2DA96FBDAA33D999C1409B5796932370219B3FF8490B671586DEBD6145519D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\ud604\uc7ac \uc571\uc744 \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"craw_connect_to_network":{"message":"\ub124\ud2b8\uc6cc\ud06c\uc5d0 \uc5f0\uacb0\ud558\uc138\uc694."},"app_name":{"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"app_description":{"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"iap_unavailable":{"message":"\ud604\uc7ac \uc778\uc571 \uacb0\uc81c\ub97c \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"please_sign_in":{"message":"Chrome\uc5d0 \ub85c\uadf8\uc778\ud558\uc138\uc694."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	576

Entropy (8bit):	4.846810495221701
Encrypted:	false
SSDEEP:	12:YGGYpmEOnxwkD9AMoAYQa9AMoAYNpALveYAyO/NrnLAOK:YHYpmznayAMHcAMHQpAzeYAyOFvAOK
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC68644E
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Programa \u0161iuo metu negalima."},"craw_connect_to_network":{"message":"Prisijunkite prie tinklo."},"app_name":{"message":"\u201eChrome\u201c internetin\u0117s parduotuv\u0117s mok\u0117jimo sistema"},"app_description":{"message":"\u201eChrome\u201c internetin\u0117s pard uotuv\u0117s mok\u0117jimo sistema"},"iap_unavailable":{"message":"Mok\u0117jimai programoje \u0161iuo metu negalimi."},"please_sign_in":{"message":"Prisijunkite prie \u201eChrome\u201c."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	584
Entropy (8bit):	4.856464171821628
Encrypted:	false
SSDEEP:	12:YGGYp6nQ11155y9k5hInf6whInf3pRKbqk0R5VR8WO/NrnLAOK:YHYpp11dy9iIdIvpc2ZgWOFvAOK
MD5:	1D21ED2D46338636E24401F6E56E326F
SHA1:	24497EDB25724BC4A57823C5CD06F50DB9647DD4
SHA-256:	434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606
SHA-512:	10A870718CC6281EE09DE01900D303B06589D9281C5849D6105C6FCF58BFFA3855F29C6ECA3689FFE6EF304BABCF41C5700EE2D8AFE711D57CB711194366FA6A
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Lietotne pagaid\u0101m nav pieejama."},"craw_connect_to_network":{"message":"L\u016bdzu, izveidojiet savienojumu ar t\u012bklu."},"app_name":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"app_description":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"iap_unavailable":{"message":"Maks\u0101jumi lietotn\u0113s pa\u0161laik nav pieejami."},"please_sign_in":{"message":"L\u016bdzu, pierakstieties p\u0101rl\u016bk\u0101 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	501
Entropy (8bit):	4.804937629013952
Encrypted:	false
SSDEEP:	12:YGGYpB928UZjdyE9iDCiop8682fURHWO/NrnLAOK:YHYpXK/iOiop8NFHWOFvAOK
MD5:	8F0168B9A546D5A99FD8A262C975C80E
SHA1:	B0718071BD0B7251D4459E9C87DF50C14622FBD6
SHA-256:	F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F
SHA-512:	A1191CDC496DDD7470BDCFAF186BB9488767159E0CA6A6242D195FA3351704DC8F8BBD03DBEE57D37BBD897C9E8D14B7325FB37D58AC80DEC0F972FF89375B8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er utilgjengelig for \u00f8yeblikket."},"craw_connect_to_network":{"message":"Du m\u00e5 koble til et nettverk."},"app_name":{"message":"Chrome Nettmarked-betalinger"},"app_description":{"message":"Chrome Nettmarked-betalinger"},"iap_unavailable":{"message":"Betaling i app er ikke tilgjengelig for \u00f8yeblikket."},"please_sign_in":{"message":"Du m\u00e5 logge p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	472
Entropy (8bit):	4.651254944398292
Encrypted:	false

SSDEEP:	12:YGGYpqK5XUoE32GFM2GapUEn7v0WO/NrnLAOK:YHYp/XaLeLapUEgWOFvAOK
MD5:	E7F74DCE7B6411E4E0D95E9252CF74FA
SHA1:	33CC6C73C5F8D0144C0260C2E5A9BD0DB3EF6477
SHA-256:	3564AEF46C01602B19CC29FD8A79676C543427EDE98206D0C91B33AF0CCF3977
SHA-512:	B0987002F8BC4F0B0AC41A87E90BA729464BF2F34D1CC413DD3837019F5F37FD46EB9E9FDABB97F5BDCB50768ABF808AF6E7C531CD7BCA477C71990D2F1333 5B
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App momenteel niet beschikbaar."},"craw_connect_to_network":{"message":"Maak verbinding met een netwerk."},"app_name": {"message":"Betalingen via Chrome Web Store"},"app_description":{"message":"Betalingen via Chrome Web Store"},"iap_unavailable":{"message":"In-app-betalingen is momenteel niet beschikbaar."},"please_sign_in":{"message":"Log in bij Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	549
Entropy (8bit):	4.978056737225237
Encrypted:	false
SSDEEP:	12:YGGYpTHlBqHdqcUP5Qp0mAW5Qp0mdpm5Qp0p9JqD2WO/NrnLAOK:YHYpRMdO5bmj5bmdpm5bLJBWOFvAOK
MD5:	E16649D87E4CA6462192CF78EBE543EC
SHA1:	53097D592B13F3C1370366B25024EA72208B136A
SHA-256:	EB435F7460A63576CA1ECB51948E7A3AD5168D2F175AE2B5836D469672923D84
SHA-512:	6EC702CEC6E312CAC6F33109A57F7D83A3F073F2F9A9BD42DB0F91A36F87D800EEB978C69023B6A0E00B86ECE3E1024C269F89D038F0926619F40D075F6689D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacja jest obecnie niedost\u0119pna."},"craw_connect_to_network":{"message":"Po\u0142\u0105cz si\u0119 z sieci\u0105."}, "app_name":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"app_description":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"} ,"iap_unavailable":{"message":"P\u0142atno\u015bci w ramach aplikacji s\u0105 teraz niedost\u0119pne."},"please_sign_in":{"message":"Zaloguj si\u0119 w Chrome." },"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	513
Entropy (8bit):	4.734605177119403
Encrypted:	false
SSDEEP:	12:YGGYpGAV9hv3/1PIc6WIc3paIBMMAV+KcIWO/NrnLAOK:YHYpGwLvt5R53pacHw1pWOFvAOK
MD5:	1F4BC8A5EFD59D61127ABEECD4B6CAE3
SHA1:	8647B4D2D643AE4F784ABDDC50D87A39AD02971A
SHA-256:	E1950CBBF056F068EA56160DDB318F3E6232BFBBE096D221C7CA6FCAACE2A8B9
SHA-512:	B58A95BBBC0A16B06826684198B481D2E15A7C760956721C3B538C62C902873A7856F328506457EE66311E45D7A16A4AAAC85B12853AA7EF09780189D28EB3DE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplicativo indispon\u00edvel no momento."},"craw_connect_to_network":{"message":"Conecte-se a uma rede."},"app_name": {"message":"Pagamentos da Chrome Web Store"},"app_description":{"message":"Pagamentos da Chrome Web Store"},"iap_unavailable":{"message":"No momento, os Pagamentos no aplicativo n\u00e3o est\u00e3o dispon\u00edveis."},"please_sign_in":{"message":"Fa\u00e7a login no Google Chrome."},"jwt_retrieve_failed":{" message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.742240430473613
Encrypted:	false
SSDEEP:	12:YGGYpmvMAV9BKx1PIZUFWIZUapITEpBqMAVCWWO/NrnLAOK:YHYpmvMwOxtEUIEUapIITqMwCWWOFvAD
MD5:	D80ECE7E4B3741CD9CD29B89D006B864
SHA1:	8F0D587B78E36861ED00524ABF886FA20E14CAE4
SHA-256:	C8FF9ACAEA1D3B6F8483339CB40F66BC563CCA8DD87F2337F813C492B20F451B

SHA-512:	8A53D9618BBD1A62CD48501E5620932631C1B045612082D99429628D2BF4409AEE3FA695107E82037B5CB332111C456CF3A74235C66B61380CF1E382914F1088
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplica\u00e7\u00e3o atualmente indispon\u00edvel."},"craw_connect_to_network":{"message":"Ligue-se a uma rede."},"app_name":{"message":"Pagamentos via Chrome Web Store"},"app_description":{"message":"Pagamentos via Chrome Web Store"},"iap_unavailable":{"message":"Os Pagamentos na app est\u00e3o atualmente indispon\u00edveis."},"please_sign_in":{"message":"Inicie sess\u00e3o no Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	554
Entropy (8bit):	4.8596885592394505
Encrypted:	false
SSDEEP:	12:YGGYpqOHHEG7PMeH8EPJWb2r9EWJWb2r9RpmJW9FjkUhI3C7PMdWO/NrnLAOK:YHYpbnEG7PjlJBfJBRpmJmBh57PEWOFY
MD5:	D63E66B94A4EA2085D80E76209582FB1
SHA1:	4ECAC3EB64DD6253310A0776E6D42257FC290D77
SHA-256:	91A5AAD210C3E0241106E8821B3897EDEFEC9D85033C94DB2324FF3A5FDE5AC7
SHA-512:	09AC34CF286FD0730EED4F6DB3E2FD00A026D0F42DCC75AE49B045DDAD38DFA38B0FB7823ECAC8B0A9BC2A89F4EAF4BCE081779F2ECDF6CC39286045577DC5C9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u00cen prezent, aplica\u021bia nu este disponibil\u0103."},"craw_connect_to_network":{"message":"Conecteaz\u0103-te la o re\u021bea."},"app_name":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome"},"app_description":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome "},"iap_unavailable":{"message":"Pl\u0103\u021bile \u00een aplica\u021bie nu sunt disponibile momentan."},"please_sign_in":{"message":"Conecteaz\u0103-te la Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1165
Entropy (8bit):	4.224419823550506
Encrypted:	false
SSDEEP:	24:YHYpNQVFc0BHlbZ0JRiKUG0L6RqQV9zJd0L6RqQV9zJRp00EQVqaQVFc0BRTlPzU:YHYpNQLHFQYKA6wQTz+6wQTz3paQAaQ8
MD5:	22F9E62ABAD82C2190A839851245A495
SHA1:	E7F79BD875918F0D0799DB5F45FAC6297FB66AF7
SHA-256:	9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F
SHA-512:	F577F2F0C344C4E4050AF025A9FB9AC78CADF7FE177F63AB9863826A9808B7FBF5D3363E3B61D7A6DB083EF5EBAC5474D710347B701640AB9C229A3E5D1F0A48
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u043e."},"craw_connect_to_network":{"message":"\u041f\u043e\u0434\u043a\u043b\u044e\u0447\u0438\u0442\u0435\u0441\u044c \u043a \u0441\u0435\u0442\u0438."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044f \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u043e."},"please_sign_in":{"message":"\u041f\u043e\u0436\u0430\u043b\u0443\u0439\u0441\u0442\u0430 \u0432\u043e\u0439\u0434\u0438\u0442\u0435 \u0432 Chrome."},"jwt_retrieve_failed":{"message":"\u041f\u0440\u043e\u0438\u0437\u043e\u0448\u043b\u0430 \u043e\u0448\u0438\u0431\u043a\u0430 \u043f\u0440\u0438 \u043f\u043e\u043f\u044b\u0442\u043a\u0435 \u0432\u044b\u043f\u043e\u043b\u043d\u0438\u0442\u044c \u0442\u0440\u0430\u043d\u0437\u0430\u043a\u0446\u0438\u044e."},""

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	548
Entropy (8bit):	4.850036636276313
Encrypted:	false
SSDEEP:	12:YGGYprMpsgCmIkPJE7ZEWJE7ZRpmJEtMxfAVADJ4ZAvIWO/NrnLAOK:YHYprMFCmvJE7ZfJE7ZRpmJEtMSVGKZo
MD5:	4BBAA10FD00AADBBA3EF6E805E8E1A62
SHA1:	1991901BD6A20C4A7977F09DF30C0CFF0524C504
SHA-256:	906C4F7FDDE15DE4C841E7910BBF14D9175E894BCB244B56E8447A5ADFA5B7AB
SHA-512:	3490F8826E3DB0C8B4FE7B1866DA27F6585ADF52E74392A592A60A916E8A784FF7B92B3DE8985084546D663588369D9BB03FCB25196B7F9C6DF607BEB7DEF010

Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplik\u00e1cia moment\u00e1lne nie je dostupn\u00e1."},"craw_connect_to_network":{"message":"Pripojte sa k sieti."},"app_name":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message":"Platby v aplik\u00e1cii moment\u00e1lne nie s\u00fa k dispoz\u00edcii."},"please_sign_in":{"message":"Prihl\u00e1ste sa do prehliada\u010da Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.7695148367588285
Encrypted:	false
SSDEEP:	12:YGGYpTOEtyPFTEPJEsvmfEWJEsvmfRpmJEiArERfH5/4WO/NrnLAOK:YHYpqoyPRAJEs4fJEs4RpmJEi6AfH5/x
MD5:	F45DE58765A37FD095319D7DEB0F2FB6
SHA1:	B585A485C9BC1982EDF7AE0B9AC73A8E91D41CB5
SHA-256:	8366774AA582035BC7D949F4E28FAEC371C305D01404DF56FFF5A78B4F6ECDB7
SHA-512:	F86334E6E6F90961AD9C8E7DD1A4E923476249469180AC69D9DE59746FE26FAECB585898FC50310380F20CEB0971CA1EB7B55046DA75276840AEA6BAFF574E6
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenutno ni na voljo."},"craw_connect_to_network":{"message":"Pove\u017eite se z omre\u017ejem."},"app_name":{"message":"Pla\u010dila v spletni trgovini Chrome"},"app_description":{"message":"Pla\u010dila v spletni trgovini Chrome"},"iap_unavailable":{"message":"Pla\u010dila v aplikacijah trenutno niso na voljo."},"please_sign_in":{"message":"Prijavite se v Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1152
Entropy (8bit):	4.2078334514915685
Encrypted:	false
SSDEEP:	24:YHYpY0f7BxQVnRl5LRO1QV1J0V8aQVEeORbo0V8aQVEeORbIp00V4i0f7BXR2QVj:YHYpV9xQVP5LyQHQQc/QcGpcH9XR2QVj
MD5:	92C1FAC62EB7F92EC3794D4A141BEF32
SHA1:	2AFA41BF51BF9A1089B0B92A9D2DC74299B79813
SHA-256:	9DF154C93B02695AF1CC39F085D9D178EC6AF131A62C2AFC65F125F8F9A5B7AC
SHA-512:	D0709E4F586EAC03548A47D72156CF48D9B4EB9AF9ED8335DF75F541AE1B4172541647EC8BA081965647A9EAE10DB342F87558977BE6075B2D3CC5C3995ED6EE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0410\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0430 \u0458\u0435 \u0442\u0440\u0435\u043d\u0443\u0442\u043d\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u043e\u0432\u0435\u0436\u0438\u0442\u0435 \u0441\u0430 \u0441\u0438\u0441\u0442\u0435\u043c\u043e\u043c."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0438 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0440\u0435\u0434\u0438\u0432\u043d\u043e\u043c \u043f\u0440\u043e\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0438 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0435\u0434\u0438\u0432\u043d\u043e\u043c \u043f\u0440\u043e\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0438 \u0443 \u0430\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0430\u043c\u0430 \u043d\u0438\u0441\u0443 \u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0435 \u043d\u0430 \u0432\u0435\u043e\u043c\u0430."},"please_sign_in":{"message":"\u041f\u04

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	523
Entropy (8bit):	4.788896709100935
Encrypted:	false
SSDEEP:	12:YGGYpg6hVGZE3aFMaap8Sp5b6hwUwrdIWO/NrnLAOK:YHYpg6hPaeaap8Sr6hwXIWOFvAOK
MD5:	6E1BE9CEE29818E54E3D1C7D483DD6F7
SHA1:	B9DD926B60E225C5BE8A1DBB7EF3ACE422A204A9
SHA-256:	E348583D8C53F4A5DEC4551DA93785C17108466E427E06F84708AA383EA0E326
SHA-512:	3ADB32C0F098E064B774E7E7F615F54C44ADFB3BFC554B06A17048C6077C5885D42BD89F6733D64D65EA1785033B36B386EF0B6661FD539855484EA5A2900BB7
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Appen \u00e4r inte tillg\u00e4nglig f\u00f6r tillf\u00e4llet."},"craw_connect_to_network":{"message":"Anslut till ett n\u00e4tverk."},"app_name":{"message":"Betalning via Chrome Web Store"},"app_description":{"message":"Betalning via Chrome Web Store"},"iap_unavailable":{"message":"Betalning i appen \u00e4r inte tillg\u00e4ngligt f\u00f6r n\u00e4rvarande."},"please_sign_in":{"message":"Logga in i Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	4.09652661599029
Encrypted:	false
SSDEEP:	24:YHYpqQV8k6Nvgnd0BQV3d0BQV5pWdPiWdBy7MIoWOFvAOK:YHYpqQ+k6NUaBQlaBQXpW3dBUMIehQ
MD5:	283D5177FB2FC7082967988E2683EC7C
SHA1:	DEDE43967F3CEF9D9325F140872A63BFCE2AA8C5
SHA-256:	E8D5820BDE31B66A7641068FDEDD1A5F20C1A783460B98887A670F38422099CF
SHA-512:	74413C00C58B7136038D4C41D5C7C79EC02A9830779ABB719D72536B74C5E338B1548A20290559FB3F4E2A938B728CF99041050DD1970848EE9A6590EB0AB3E4
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0e44\u0e21\u0e48\u0e2a\u0e32\u0e21\u0e32\u0e23\u0e16\u0e43\u0e0a\u0e49\u0e07\u0e32\u0e19\u0e41\u0e2d\u0e1b\u0e44\u0e14\u0e49\u0e43\u0e19\u0e02\u0e13\u0e30\u0e19\u0e35\u0e49"},"craw_connect_to_network":{"message":"\u0e42\u0e1b\u0e23\u0e14\u0e40\u0e0a\u0e37\u0e48\u0e2d\u0e21\u0e15\u0e48\u0e2d\u0e01\u0e31\u0e1a\u0e40\u0e04\u0e23\u0e37\u0e2d\u0e02\u0e48\u0e32\u0e22"},"app_name":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"app_description":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"iap_unavailable":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e43\u0e19\u0e41\u0e2d\u0e1b\u0e1e\u0e25\u0e34\u0e40\u0e04\u0e0a\u0e31\u0e19\u0e44\u0e21\u0e48\u0e1e\u0e23\u0e49\u0e2d\u0e21\u0e4

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	572
Entropy (8bit):	4.93347615778905
Encrypted:	false
SSDEEP:	12:YGGYpFh852XmYG45SfVVh5SX8pFBkw452kK/O/NrnLAOK:YHYpFhJ2Y95AJ5l8pFhlkwOFvAOK
MD5:	1BF2AA4BB904B406C9C2B7DF769BB540
SHA1:	8D29C4B7A79AB0657747CA194D1934292A46D2A8
SHA-256:	0F2E8285BA3E2BDBA6B16435FB941B07159AACFAC80196AD5941B79AB52B712A
SHA-512:	0DF48AE0A518A940489E91D8A0D6E7E47A3153747358E06CD792BFA3D826F47FA1502268F602E7D7EDFC1C111AEB3FAF0E67F845986DDA77E2FC4B3336BCF46C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Uygulama \u015fu anda kullan\u0131lam\u0131yor."},"craw_connect_to_network":{"message":"L\u00fctfen bir a\u011fa ba\u011flan\u0131n."},"app_name":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"app_description":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"iap_unavailable":{"message":"Uygulama \u0130\u00e7i \u00d6demeler \u015fu anda kullan\u0131lamaz."},"please_sign_in":{"message":"L\u00fctfen Chrome'da oturum a\u00e7\u0131n."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	4.268588181103308
Encrypted:	false
SSDEEP:	24:YHYpNQVVQVrll5eN7jAQVF0Zz0id0Zz0iRp00AQVqaQVVQVSMQVvjlkYHA1RnWOi:YHYpNQPQZ75exkQAz0/z00p2QAaQPQQN
MD5:	FD1C9890679036E1AD914218753B1E8E
SHA1:	58160F7A0FC94110A2876223E406A517C8E2660B
SHA-256:	39D19CC3387FFCE13A8F11DAD72E2FCBB7CD1A4367EC699AD7C40D6F52ECE717
SHA-512:	03E81C398EE6A5DC65A40CA07E1A4CBEC2662D2C151A76C9ECB813587D672AC71311C39C5C5DA8A1AE78A3A6CE3938609D1365F7819424FC34289C7743DF002
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u043e\u0433\u0440\u0430\u043c\u0430 \u0442\u0438\u043c\u0447\u0430\u0441\u043e\u0432\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u0456\u0434\u2019\u0454\u0434\u043d\u0430\u0439\u0442\u0435\u0441\u044f \u0434\u043e \u043c\u0435\u0440\u0435\u0436\u0456."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0443 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0443 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430 \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u043e\u0433\u0440\u0430\u043c\u0443 \u0437\u0430\u0440\u0430\u0437 \u043d\u0435 \u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"please_sign_in":{"message":"\u0423\u0432\u0456\u0439\u0434\u0456\u0442\u044c \u0443

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\vi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.846531831162704
Encrypted:	false
SSDEEP:	12:YGGYpqp80NORWLNiNI2k8yypSNiNI2k8yy+piNiNI2miI80NO5WO/NrnLAOK:YHYpmvNcCgWgUpudiIvN6WOFvAOK
MD5:	7D52E9357AB847B4CC8DBC8CC4DA93F5
SHA1:	AF877F3992D8056C8F08462BD575595BF79FE5B0
SHA-256:	313F71F3FFDCEFC76FC746FF2029FBF8FBE38BD83DCF952FC3DDCD8AA96D5CFB
SHA-512:	E66E7FACDF35A0F72AC61DEAAEC43A2DAC976CADEA146EBE3E90E739178F173E32ADCF909F05F2657F2AD66E2ECB6015F6733CEA4B9E42337246469F89D3A12F
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u1ee8ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"craw_connect_to_network":{"message":"Vui l\u00f2ng k\u1ebft n\u1ed1i v\u1edbi m\u1ea1ng."},"app_name":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"app_description":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"iap_unavailable":{"message":"Thanh to\u00e1n trong \u1ee9ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"please_sign_in":{"message":"Vui l\u00f2ng \u0111\u0103ng nh\u1eadp v\u00e0o Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\zh_CN\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	602
Entropy (8bit):	4.917339139635893
Encrypted:	false
SSDEEP:	12:YGGYpqrL0MdI1i1kovbdKD/vbdKopqIQfvJ19KhO/NrnLAOK:YHYpMLfjvsTvsop3QPAOFvAOK
MD5:	393680A09DEE0CB9046A62BDC0750B74
SHA1:	54E7F8215061A4AB241B87AE4E81C8F860EB2C2B
SHA-256:	D5FB52C2897FD5C294784DB63C933AC77C609D10AC91431CCB295D87452CBEE6
SHA-512:	14C214CAEFC69B085E918F492C75E2A48BC6A9C2D347D29403B26E69A474825E302A3E106710E5C04E047BD57EE684A67846A5DE956705FFBF41BB0614B8CEB2
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u5e94\u7528\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u3002"},"craw_connect_to_network":{"message":"\u8bf7\u8fde\u63a5\u5230\u7f51\u7edc\u3002"},"app_name":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"app_description":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"iap_unavailable":{"message":"\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u5e94\u7528\u5185\u4ed8\u6b3e\u3002"},"please_sign_in":{"message":"\u8bf7\u767b\u5f55 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_locales\zh_TW\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	680
Entropy (8bit):	4.916281462386558
Encrypted:	false
SSDEEP:	12:YGGYpqI8ROuDWMg0kP2uD/vbd8Em2uD/vbd8RpqI8RauDRsXwvC/KhO/NrnLAOK:YHYp38suDUSuD/v2OuD/v2Rp38cuDGbq
MD5:	CD30D132A7213FC1B7E03C6D0A49CCF7
SHA1:	1141DED39023B821FE9BB4682E0D1EB5469DAF76
SHA-256:	5717F13D10E63255947F750C79CBB6BD04A6D97A08261E8D5764AF5EB0561A28
SHA-512:	0DCD3CEB93AB58655551B00D7AD4FE4A6F1F6B24EDD31244FF9B57AE529BF1A9E0220A6258C64790F9CC9F026AB9DA3AEE1575809CC94DC4F8754194C958FD19
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u9019\u500b\u61c9\u7528\u7a0b\u5f0f\u3002"},"craw_connect_to_network":{"message":"\u8acb\u9023\u4e0a\u7db2\u8def\u3002"},"app_name":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"app_description":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"iap_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u61c9\u7528\u7a0b\u5f0f\u5167\u4ed8\u6b3e\u529f\u80fd\u3002"},"please_sign_in":{"message":"\u8acb\u767b\u5165 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL_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):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	192:RktDNJ2UzsL5KcASyoH+CouKP/iNGRo/oRHMIT:AZQflcsU
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGInZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwYXRoIjoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6Ik9nUkNIZlVoam9xOU93NHFfaEhvTTQxNzNMelJyYkVpUVdsRXNRSzhscFkifSx7InBhdGgiOiJfbG9jYWxlcy9kYS9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6Il9sb2NhbGVzL2RlL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoIjoiX2xvY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jYWxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\craw_background.js

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	544643
Entropy (8bit):	5.385396177420207
Encrypted:	false
SSDEEP:	6144:abyfBNC2FRdjiRXqbe5Dq31IVlMqX+wd5/CcMMJcRULt0NjyTOEzZQ+h72W3GB0n:Ft/g
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=e||{};e.scope={};e.arrayIteratorImpl=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};e.arrayIterator=function(a){return{next:e.arrayIteratorImpl(a)}};e.ASSUME_ES5=!1;e.ASSUME_NO_NATIVE_MAP=!1;e.ASSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");};e.global=e.getGlobal(this);.e.IS_SYMBOL_NATIVE="func

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\craw_window.js

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	261316
Entropy (8bit):	5.444466092380538
Encrypted:	false
SSDEEP:	3072:I5vU7I6s2M9duIWFCbmYJ4tnFWdqpMad2vywhIp81QFv9F9nNsZgiDdOFlV/mZmc:I5vqFCb2p8Gx9FNNsZ9Dd/ceR
MD5:	1709B6F00A136241185161AA3DF46A06
SHA1:	33DA7D262FFED1A5C2D85B7390E9DBC830CBE494
SHA-256:	5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8

SHA-512:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D19CB
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b,k=k||{};k.scope={};k.createTemplateTagFirstArg=function(a){return a.raw=a};k.createTemplateTagFirstArgWithRaw=function(a,c){a.raw=c;return a};k.arrayIteratorImpl=function(a){var c=0;return function(){return c<a.length?{done:!1,value:a[c++]}:{done:!0}}};k.arrayIterator=function(a){return{next:k.arrayIteratorImpl(a)}};k.makeIterator=function(a){var c="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return c?c.call(a):k.arrayIterator(a)};.k.arrayFromIterator=function(a){for(var c,d=[];!(c=a.next()).done;)d.push(c.value);return d};k.arrayFromIterable=function(a){return a instanceof Array?a:k.arrayFromIterator(k.makeIterator(a))};k.ASSUME_ES5=!1;k.ASSUME_NO_NATIVE_MAP=!1;k.ASSUME_NO_NATIVE_SET=!1;k.SIMPLE_FROUND_POLYFILL=!1;k.ISOLATE_POLYFILLS=!1;k.FORCE_POLYFILL_PROMISE=!1;k.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.k.objectCreate=k.ASSUME_ES5||"function"==typeof Object.cre

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\css\craw_window.css

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1741
Entropy (8bit):	4.912380256743454
Encrypted:	false
SSDEEP:	24:LalZ74H+rMwJHwIodHRmxt3jiu1iu1RDpfeWlMl548wJHwDwCapt/VMYXj8Eq27K:Z+rMm71le88S1tWYXmrVZFH
MD5:	67BF9AABE17541852F9DDFF8245096CD
SHA1:	A4AC74DD258E8E0689034FAA1B15A5C7C56DC3BB
SHA-256:	10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC
SHA-512:	298FA132C6F122798FDB9BC6DE8024915147ADC20355B56A92F0ED9ACCE4549BE6E7F42212E07DCA166E31624D4E66E299565845D4BA1C51CA935050641B61F
Malicious:	false
Reputation:	low
Preview:	html, body {. margin: 0;. overflow: hidden;.}..webview {. width: 100%;. height: 100%;. min-height: 100%;. position: absolute;.}...craw_overlay {. position: absolute;.. left: 0;. top: 0;. right: 0;. bottom: 0;.. background-color: white;.. -webkit-transition: opacity 250ms linear;.. display: -webkit-flex;. -webkit-flex-direction: column;. -webkit-flex: 1 0%;. -webkit-align-items: center;. -webkit-justify-content: center;.. -webkit-app-region: drag;.}...craw_overlay img {. margin: 16px;.}..#loading_overlay {. opacity: 1;.}..#offline_overlay {. opacity: 0;. display: none;.}..#offline_overlay > img {. -webkit-filter: saturate(0%);.}..#offline_overlay > span {. font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif;. font-size: 15px;. line-height: 21px;. color: #8d8d8d;. display: block;.}..#loading_splash {. width: 128px;. height: 128px;.}..#drag_overlay {. position: absolute;. left: 0;. top: 0;. right: 0;. bottom: 0;. pointer-events: none;. -webkit

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\html\craw_window.html

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	810
Entropy (8bit):	4.723481385335562
Encrypted:	false
SSDEEP:	12:hYenuEJIig5fRpvV4AEdN2sAAuzg/7RwQuLYpUH9KfRnQBGgZKy3QGgjPSWZDQL:hYeLJKTVNEuLAuzg/twQucpS9bj3
MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281BFF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/craw_window.css" rel="stylesheet">. <script src="/craw_window.js"></script>. </head>. <body>. <webview></webview>. . . . . </body>.</html>.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\flapper.gif

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	dropped
Size (bytes):	70364
Entropy (8bit):	7.119902236613185
Encrypted:	false
SSDEEP:	768:g5TXOSBAqNIPmA8NcjCWdM0VFMJEwavTeElfWupav5TXg7wV+irIPny9MTVQHydi:g5KSmiIPmAhZWiMsDfWug7DmqM6HybkF
MD5:	398ABB308EEBC355DA70BCE907B22E29
SHA1:	CFFB77B8A1724B8F81D98C6D6AD0071D10162252

SHA-256:	2B73533F47A99FFEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040
SHA-512:	FC7A56FC8A61A582161874B54ADBAD30A84840190008EDB0B6FBF84F91393CA58E988E3FE446F11A0C3C691C18249B93AEC2904B3D0C4F0857D79034F662385A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....!..NETSCAPE2.0.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:..B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.Ny Q.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:..B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m 4..7..!.....,.....'..w=.....\.)._6.k..OF...n.#\~"....2b3..I.)..eu.Q.`.e.....gr.?>.s.I0.....@.~.Tr.[8.+.,.;..EE....S.*f.....,.....B8/D..;.9.q.....ukC...r.I.....j.....BGY...o2J....+O4....X4.....cH%7....I.....0H!.!.....!.,..... .....p8.a$....hh@.4....X,A.0L..(....JX.j...,.....z.X.Q....jB.d....B..

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	3313
Entropy (8bit):	7.846746884883354
Encrypted:	false
SSDEEP:	48:ClSxMJp0X8Fza3CmwVb5+JsxBBMjxCyLilm+OjEXP8WmSP4O1yxB+lK8BeAJhmS:mtkMJWgG3u55ArM3UE/Hjj26K8tzF
MD5:	30899B6C4E4A757B8EC6DD2208ACDFB4
SHA1:	F2C5880A724C6D75CCE1B5191E0D82C3BC7DE768
SHA-256:	4F17EFBD974A41D88CB36567AAB6BF4586579E78780F00B1826676819E14BFF4
SHA-512:	58539E3F0AD7FEF30792EFCDBBD955599E11E4261C9946E7C3DFF6267E01747354EA3B901C46FC8329F81C68AFBEB2D05FE3FCB266BC5948DE8BEFA5B8D040 EE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a....IDATx.....S.d.....x{g..T...9..:.3...a.9..J.V....a...(.,.,...P@..)..d.\.)...D..i.f.yI..e{m..|.~...}.MC_oRz.....}.7...^o.,...I...V.....Z.....]... ...>.(..._..r_Z... .....4x.....|>`A../.x<..n.{..@....@../.X#.....D..X..@....c."..+^. ..>!H.....6..,.KJ...u.j..$I".L.....n.O.{0.<D0p.!.N...l6."..@.K.>A0d...?...."...\....H0d.d.'.l.;".>...`.&$I...P..6.!.xO... EQ...Y.F~BE..ea.e".~[.F.![..?..f.....,..... m.....$I....`..8.....@f>.....".Fw.....<...7.k.l!p.(..p...v...E.....|...@.P,...D.B..@. ...E."..../.....|...@. ...|...@. ...|../.....|.....\..^..,.n... ..8o.....ib>....zc.....|h .5.<..+...`...._.....,.....p....EK.a.X0...9)...QO.a.4....k...>.A.....`y{.4L....W>M.....^.N..<.[...w]..>.FK.O~...`...K.][...eY...H.+..z9...A..O3.)r;..c.u.B.....`^2...}.i. ^}.\.....w.u0....x~.u.....>.....~../_..2....;6..`(....MKE...f0.".I>."99.....y....Q.W$I.8]J0..AC(.*.....9_...g..#.....%....8.c.h..0..?\e..

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	531
Entropy (8bit):	7.465541280375791
Encrypted:	false
SSDEEP:	12:6v/7Qz6wYoewKPcggCPhFURX51KKpxDGvEVKvkjnqvRwHoHc:h6wLTK6chFUtKKpxC5XmV
MD5:	344554D96E418120BD80EF5DE5194697
SHA1:	23E141C3A6CE368ACC1C299F062AB85914BCB17E
SHA-256:	0A4BD08DB6422F8E7A8A218EF39C1B99A5A675F12697F26BE88F9AFC2E1F9378
SHA-512:	7AE38853E5ACCA479D7FD81D48BB88C671CF4DCE63342209BCFF045AC581A04B7B0ED48F6C58253DB950935C0522CAAA4FBC6CF5A25151A8960BA56FC80456 9E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx....k.a..?.]...Z5.P...`G77.....Q'q.....u..E...%.$].\...P.m5.....$M...K...#..p.....|.{.-*...Z....=.._.Dc<.J.R...A.@....I)...Lb..s&.q.T_..|a.....z ..0..m[.+ ..T.R9.7.`0..$~.....H.Q|.wg..r...E6n_.Y.E..x.(.....?{H.Z3;..="X.F.w.:.h...Z..V.S.|..V.....{T-.y....*..>.>.fQ...a.I.<;I..yr.....Un....7w.....S.3.Fg|.O..\.~{...S....d.....R .%.A...$.g.y..f.IW/..JC.z.H..)#....A+. .k.wb...p.m:a.?D.1GD.&..N.....?..\..n....W.O...j.%.`.*H.s.Fxt.\.....Yv.?.....f....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\topbar_floating_button.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.475799237015411
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/RPJDmV7bScsP4a9zln94FptVp:6v/lhPKM4nDspnAkZJNmgPdln2TTp
MD5:	8803665A6328D23CC1014A7B0E9BE295
SHA1:	9DA6EE729D5A6E9F30658B8EC954710F107A641F
SHA-256:	D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C
SHA-512:	ECD9E71B8BA1ED8BD4CA5A0936CB66A83611C4ABCBDA76C250F4CDF4AD80320212E8F5EEB79A38910718F8346ECC1AD580A3FA835EC2B22BE497F36899FB5 930

Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...Q..0.....2...(p...~Z.}'.>I%O...V!s...../...`.<..`.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\topbar_floating_button_close.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	252
Entropy (8bit):	6.512071394066515
Encrypted:	false
SSDEEP:	6:6v/lhPKM4nDsp7q1hKVlomsj9rxKNgtmN0VZ+GFYep:6v/7iMXVq1ylxemNgtmKVnYM
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D77A64
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..... ..Pp.X....H...b@...|.^LC_.E.BP+.....X.P.....q..~..p/. ..s.....%D^...$.....@.!...<...).? .4{.k.G3...4..[cH..0..l.8.!r..m.R..{.....`.f...#.x.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\topbar_floating_button_hover.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.423186859407619
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEHxrPLyN+ltNPhv/l2up:6v/lhPKM4nDspnAkZHVtERrPLygltNPn
MD5:	7CB6B9DC1A30F63B8BD976924B75AD96
SHA1:	0C40B0C496D2F2B5F2021C117EC8610AC03AB469
SHA-256:	721B7AAA9A42A54A349881615A12E3A26983ACA48E173FD2F66E66AA0D725735
SHA-512:	4764937364E355956B242B84010AC56102536D2AACBE4227F0E88E4DE7AB468571957EA6C33012539156E5349AE4F777115615AE3361F60ADDF9CD227424F76A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B.z.s...*.....$.<u..[.....h.....C.CA).....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\topbar_floating_button_maximize.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.8155898293424775
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZttd//HmnFz1P/ZjXlUTqyCIc30ItK1p:6v/lhPKM4nDsptF/HOP/ZjXlUeyCo/p
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A8654
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...HIDATx.....0.CQS.....~..".....m.v+Sq....<!...M8m..'...@$..0....E.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\images\topbar_floating_button_pressed.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped

Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEXIyN+ltN1/lsg1p:6v/lhPKM4nDspnAkZHVtEZgltN1eup
MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....$.<u..[.....h.....M..x(....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2344_888219420\CRX_INSTALL\manifest.json

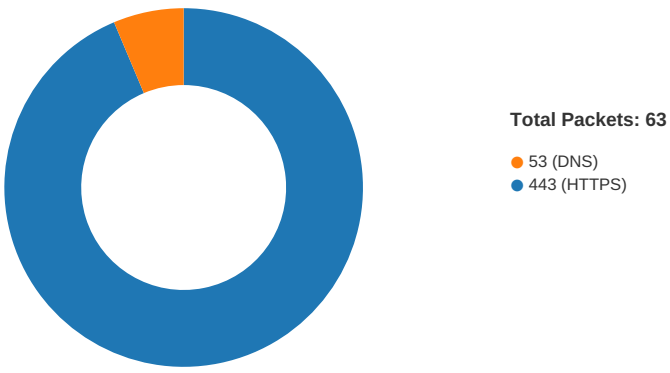
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1098
Entropy (8bit):	4.919185521409901
Encrypted:	false
SSDEEP:	24:BeVvlH141v5GFqeq7x7S4dudxNfN3IFKrGQZDN4:QVNVgvLecJSR1Y8r5ZW
MD5:	6CA25F3EF585B63F01BCDF8635120704
SHA1:	00C063811E31EA5F9A00F175A71EA25E7821F621
SHA-256:	49D9DE983F7436BA786E6E04A5A20C10F41687AE06B266B1B6553F696719563D
SHA-512:	566BFD9BADBD8951EE52E5911EB68B51E86286989096D32DE6E32A2523761B0E0AFCA251EF3BEA36B5D51FB8354A5FCA567772A02C3F3B9D8DFE529609FA043 0
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "name": "__MSG_APP_NAME__",. "description": "__MSG_APP_DESCRIPTION__",. "manifest_versio n": 2,. "version": "1.0.0.6",. "minimum_chrome_version": "29",. "default_locale": "en",. "app": {. "background": {. "scripts": [. "craw_background.js".]. }. },. "permissions": [. "identity",. "webview",. "https://www.google.com/",. "https://www.googleapis.com/*",. "https://payments.google.com/payments/v4/js/integr ator.js",. "https://sandbox.google.com/payments/v4/js/integrator.js".],. "oauth2": {. "auto_approve": true,. "scopes": [. "https://www.googleapis.com/auth/sierra",. "https://www.googleapis.com/auth/sierrasandbox",. "https://www.googleapis.com/auth/chromewebstore",. "https://www.googleapis.com/auth/chromewebstore.read only".],. "client_id": "203784468217.apps.googleusercontent.com". },. "icons": {. "16": "images/icon_16.png",. "128

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:53:50.957983017 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:50.958019018 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:50.958103895 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:50.958430052 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:50.958477974 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:50.958558083 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:50.959305048 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.959355116 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:50.959877968 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:50.959891081 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:50.960140944 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:50.960164070 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:50.960205078 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.960679054 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.960702896 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:50.960786104 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.961303949 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.961325884 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:50.961980104 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:50.962002039 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.016319036 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.017158031 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.021400928 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.021428108 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.021883011 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.021905899 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.021933079 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.022032976 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.022726059 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.022797108 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.023834944 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.023967981 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.039024115 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.049983025 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.077322960 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.077363014 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.078651905 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.078751087 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.078774929 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.078789949 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.080789089 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.081280947 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.379272938 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.379421949 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.379478931 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.379650116 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.379683018 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.379856110 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.380048037 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.380326986 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.386837959 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.386862040 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.386998892 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.387029886 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.387232065 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.387268066 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.426562071 CEST	443	49757	216.58.215.238	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:53:51.426652908 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.426673889 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.426704884 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.426774979 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.430464029 CEST	49757	443	192.168.2.4	216.58.215.238
May 27, 2022 20:53:51.430489063 CEST	443	49757	216.58.215.238	192.168.2.4
May 27, 2022 20:53:51.440413952 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.440526009 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.440540075 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.440555096 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.440632105 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.464500904 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.464517117 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.464624882 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.464903116 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.464916945 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.510561943 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.510596991 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.528254032 CEST	49756	443	192.168.2.4	142.250.203.109
May 27, 2022 20:53:51.528280020 CEST	443	49756	142.250.203.109	192.168.2.4
May 27, 2022 20:53:51.590887070 CEST	49758	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:51.590915918 CEST	443	49758	13.226.244.95	192.168.2.4
May 27, 2022 20:53:51.610539913 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:52.122714043 CEST	49759	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:52.164494991 CEST	443	49759	13.226.244.95	192.168.2.4
May 27, 2022 20:53:52.207392931 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.207431078 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.210503101 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.210525036 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.210530996 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.230003119 CEST	49762	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:52.230031013 CEST	443	49762	13.226.244.95	192.168.2.4
May 27, 2022 20:53:52.230129957 CEST	49762	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:52.230441093 CEST	49762	443	192.168.2.4	13.226.244.95
May 27, 2022 20:53:52.230456114 CEST	443	49762	13.226.244.95	192.168.2.4
May 27, 2022 20:53:52.274699926 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.276525021 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.276540041 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.276946068 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.277687073 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.277832031 CEST	443	49760	204.79.197.200	192.168.2.4
May 27, 2022 20:53:52.280498981 CEST	49760	443	192.168.2.4	204.79.197.200
May 27, 2022 20:53:52.287873983 CEST	49760	443	192.168.2.4	204.79.197.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:53:50.918502092 CEST	64277	53	192.168.2.4	8.8.8.8
May 27, 2022 20:53:50.920331001 CEST	56076	53	192.168.2.4	8.8.8.8
May 27, 2022 20:53:50.922497988 CEST	60758	53	192.168.2.4	8.8.8.8
May 27, 2022 20:53:50.942790031 CEST	53	64277	8.8.8.8	192.168.2.4
May 27, 2022 20:53:50.947736025 CEST	53	56076	8.8.8.8	192.168.2.4
May 27, 2022 20:53:50.948343992 CEST	53	60758	8.8.8.8	192.168.2.4
May 27, 2022 20:53:53.890722036 CEST	54069	53	192.168.2.4	8.8.8.8
May 27, 2022 20:53:53.910057068 CEST	53	54069	8.8.8.8	192.168.2.4
May 27, 2022 20:54:03.756653070 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:03.785171986 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:03.971071959 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.001032114 CEST	443	52474	216.58.215.238	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:54:04.001082897 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.001121044 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.001156092 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.009016991 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.013586998 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.059020042 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.060300112 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.087960005 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.089359999 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.102520943 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.107148886 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.107188940 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.107223034 CEST	443	52474	216.58.215.238	192.168.2.4
May 27, 2022 20:54:04.113746881 CEST	52474	443	192.168.2.4	216.58.215.238
May 27, 2022 20:54:04.162892103 CEST	52474	443	192.168.2.4	216.58.215.238

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:53:50.918502092 CEST	192.168.2.4	8.8.8.8	0x4692	Standard query (0)	triarail-mx.w3spaces.com	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.920331001 CEST	192.168.2.4	8.8.8.8	0xfea3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.922497988 CEST	192.168.2.4	8.8.8.8	0x2b99	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.890722036 CEST	192.168.2.4	8.8.8.8	0xf957	Standard query (0)	triarail-mx.w3spaces.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 20:53:50.942790031 CEST	8.8.8.8	192.168.2.4	0x4692	No error (0)	triarail-mx.w3spaces.com		13.226.244.95	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.942790031 CEST	8.8.8.8	192.168.2.4	0x4692	No error (0)	triarail-mx.w3spaces.com		13.226.244.54	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.942790031 CEST	8.8.8.8	192.168.2.4	0x4692	No error (0)	triarail-mx.w3spaces.com		13.226.244.59	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.942790031 CEST	8.8.8.8	192.168.2.4	0x4692	No error (0)	triarail-mx.w3spaces.com		13.226.244.90	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.947736025 CEST	8.8.8.8	192.168.2.4	0xfea3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:53:50.947736025 CEST	8.8.8.8	192.168.2.4	0xfea3	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
May 27, 2022 20:53:50.948343992 CEST	8.8.8.8	192.168.2.4	0x2b99	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
May 27, 2022 20:53:52.150535107 CEST	8.8.8.8	192.168.2.4	0x26f6	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:53:52.150535107 CEST	8.8.8.8	192.168.2.4	0x26f6	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)
May 27, 2022 20:53:52.150535107 CEST	8.8.8.8	192.168.2.4	0x26f6	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.910057068 CEST	8.8.8.8	192.168.2.4	0xf957	No error (0)	triarail-mx.w3spaces.com		13.226.244.95	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.910057068 CEST	8.8.8.8	192.168.2.4	0xf957	No error (0)	triarail-mx.w3spaces.com		13.226.244.54	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.910057068 CEST	8.8.8.8	192.168.2.4	0xf957	No error (0)	triarail-mx.w3spaces.com		13.226.244.59	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.910057068 CEST	8.8.8.8	192.168.2.4	0xf957	No error (0)	triarail-mx.w3spaces.com		13.226.244.90	A (IP address)	IN (0x0001)
May 27, 2022 20:53:53.919043064 CEST	8.8.8.8	192.168.2.4	0x6b78	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:53:53.919043064 CEST	8.8.8.8	192.168.2.4	0x6b78	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 20:53:53.919043064 CEST	8.8.8.8	192.168.2.4	0x6b78	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)
May 27, 2022 20:54:01.115206003 CEST	8.8.8.8	192.168.2.4	0xaace	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:54:01.115206003 CEST	8.8.8.8	192.168.2.4	0xaace	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)
May 27, 2022 20:54:01.115206003 CEST	8.8.8.8	192.168.2.4	0xaace	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- triarail-mx.w3spaces.com
- accounts.google.com
- clients2.google.com
- https:
  - www.bing.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49758	13.226.244.95	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:51 UTC	0	OUT	GET / HTTP/1.1 Host: triarail-mx.w3spaces.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-27 18:53:51 UTC	5	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 8319 Connection: close x-amz-id-2: cWGFs2/EZI+WZ5Y/6swnRjBulzriUxY/VxTXdA/jXMF5+zSLc5Ao3NsdaRoFRehss6rCHchiQgc= x-amz-request-id: X8SRMJ14AJ5FH1GC Last-Modified: Wed, 25 May 2022 13:49:03 GMT Accept-Ranges: bytes Server: AmazonS3 Date: Fri, 27 May 2022 18:49:06 GMT ETag: "13be996f3cdf309061b26fe6f4cb2d8b" Vary: Accept-Encoding X-Cache: Hit from cloudfront Via: 1.1 a285e962df0dcad9d1e7b1ac618b4c4c.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: DOGxbl4YMWlyVMg6jHqTQmakO8OH10djGXncW0y5K3gs6arExGlPOw== Age: 285
2022-05-27 18:53:51 UTC	5	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 73 74 79 6c 65 73 2e 63 73 73 22 3e 0a 09 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 20 35 30 30 70 78 3b 0a 09 77 69 64 74 68 3a 20 31 30 30 Data Ascii: <!DOCTYPE html><html><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="stylesheet" type="text/css" href="styles.css"><title>Document</title></head><body style="height: 500px;width: 100

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49756	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:51 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-27 18:53:51 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-05-27 18:53:51 UTC	3	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 18:53:51 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-EF8kcu_XV0X0inIR8lJPSw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-EF8kcu_XV0X0inIR8lJPSw' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 18:53:51 UTC	5	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-05-27 18:53:51 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49783	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:54:02 UTC	265	OUT	POST /threshold/xls.aspx HTTP/1.1 Origin: https://www.bing.com Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init X-PositionerType: Desktop X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage X-Search-SafeSearch: Moderate X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8} X-UserAgeClass: Unknown X-BM-Market: US X-BM-DateFormat: M/d/yyyy X-CortanaAccessAboveLock: false X-Device-OSSKU: 48 X-BM-DTZ: 60 X-BM-FirstEnabledTime: 132061327679472806 X-DeviceID: 0100748C0900D485 X-BM-DeviceScale: 100 X-Search-TimeZone: Bias=-60; StandardBias=0; TimeZoneKeyName=W. Europe Standard Time X-BM-Theme: 000000;0078d7 X-BM-DeviceDimensionsLogical: 1232x1024 X-BM-DeviceDimensions: 1232x1024 X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJPQDsAAcrCUQHVmc1QWYMPz0DXFqeRx8wamoowmwbwUSyNYpjtyJpJRDfEtLg1rKS4/zxABCoKsuMFRUBIP7PFid4xD2qKyI0URDzKuBMFjFkKzlG3Ps9MGF%2BBZXTdKnpAzZrlgOtRPCtamchXz28q0CRmPxXD6ZHI2rcMOvnUBLbt1zkoTBTKYibaVaGygpAEYQDTKkpAamKV8eOep8EnHN50LiR92MCKiQtLylSx/qTDVfvmE81bne2UzPZEbqlm/DPuKdzajAWp%2BXa91MUXk%2BgPu95uggy8QPGrNOWbn7lkTjFjqBdAhJ5m/BiU45rQu3ck%2B6RC%2BU%2BEalYU42PwbfQmsDwDZgAACHBtXI8rJNLaqAG5bveMLq14sdqoo9yPGDTdHxA7OjsAOmIxUTUXgi%2B44zK9rStYOMPMq4e6et15tJFBbG2jKGVdJMY3ZkTFu%2BHWNopmckOWLVgFNq79y3hmsdxc1wOedU50wO01k4tR95v4Imjx%2BJujGLa9TWHvuxeDQi9Y4ybY/y9vY1LteXSo0kKHbGazTsLNxyFfmSDOcn8ClbW9bmk0c4jHKD1yRpmMUoJ6GMEDPMqNOCkwrk63Ab7wPb/Ik//Xt/R1gr%2Bom7Tc2OeYYcdyru5UC/xxsJOAvl6NlTvqnrrwv3tNwIcpsdUqBF6TuxWSlAQvZrc4R0FfqAmC1gmCnHgcn6LOJmRb0NP4X2cysqVe7yMirSTCCMByWMIyPaVuut%2BME7E/g1i7%2BF6GOmOb4jaw5esWXZltZITutJph%2B%2BiB5Jhj5m5K8KwagRMAS5gWCtioSFd8CezxoiPqJxEvqdn2z7PYPJa2IEPLnuo8hgVRtHuU8/aTQiACqk%2BA7ilNPbpjD1XsiVE35rwQalWYecZgjOX1bVhMm1bTSpRC5s14qea2UC8ENIkJSR9nRsud1AE%3D%26p%3D X-Agent-DeviceId: 0100748C0900D485 X-BM-CBT: 1646732532 X-Device-isOptin: true X-Device-Touch: false X-Device-ClientSession: B3FD0EB2977A44E390C07B484049F516 X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI X-BM-ClientFeatures: pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader X-MSEdge-ExternalExpType: JointCoord X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40 Content-Type: text/plain;charset=UTF-8 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: www.bing.com Content-Length: 429 Connection: Keep-Alive Cache-Control: no-cache Cookie: MUID=BEEBF15262804E24A8DF6781500AB975; _SS=CPID=1653677609279&AC=1&CPH=4ef661f2
2022-05-27 18:54:02 UTC	268	OUT	Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 49 51 75 65 75 65 45 72 72 6f 72 3c 2f 54 3e 3c 49 47 3e 43 30 34 30 39 45 38 34 43 37 45 43 34 44 31 36 41 32 43 44 44 41 34 38 30 35 45 32 44 33 43 34 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 65 72 72 6f 72 54 79 70 65 22 3a 22 51 75 65 75 65 4f 76 65 72 66 6c 6f 77 22 2c 22 66 61 69 6c 43 6f 75 6e 74 22 3a 31 2c 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.CIQueueError</T><IG>C0409E84C7EC4D16A2CDDA4805E2D3C4</IG><D><![CDATA[{"errorType":"QueueOverflow","failCount":1,"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/I
2022-05-27 18:54:02 UTC	268	IN	HTTP/1.1 204 No Content Access-Control-Allow-Origin: * X-Cache: CONFIG_NOCACHE Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: BA390EC1FBF8480E87BBAC00DFD082F4 Ref B: FRA31EDGE0205 Ref C: 2022-05-27T18:54:02Z Date: Fri, 27 May 2022 18:54:01 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49789	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:54:05 UTC	268	OUT	POST /threshold/xls.aspx HTTP/1.1 Origin: https://www.bing.com Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init Content-type: text/xml X-MSEdge-ExternalExpType: JointCoord X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40 X-PositionerType: Desktop X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage X-Search-SafeSearch: Moderate X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8} X-UserAgeClass: Unknown X-BM-Market: US X-BM-DateFormat: M/d/yyyy X-CortanaAccessAboveLock: false X-Device-OSSKU: 48 X-BM-DTZ: 60 X-BM-FirstEnabledTime: 132061327679472806 X-DeviceID: 0100748C0900D485 X-BM-DeviceScale: 100 X-Search-TimeZone: Bias=-60; StandardBias=0; TimeZoneKeyName=W. Europe Standard Time X-BM-Theme: 000000;0078d7 X-BM-DeviceDimensionsLogical: 1232x1024 X-BM-DeviceDimensions: 1232x1024 X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJPQDsAAcrCUQHVmc1QWYMPz0DXFqeRx8wamoowmwbwUSyNYpjtyJpJRDfEtLg1rKS4/zxABCoKsuMFRUBIP7PFid4xD2qKyI0URDzKuBMFjFkKzlG3Ps9MGF%2BBZXTdKnpAzZrlgOtRPCtamchXz28q0CRmPxXD6ZHI2rcMOvnUBLbt1zkoTBTKYibaVaGygpAEYQDTKkpAamKV8eOep8EnHN50LiR92MCKiQtLyISx/qTDVfvmE81bne2UzPZEbqlm/DPuKdzajAWp%2BXa91MUXk%2BgPu95uggy8QPGrNOWbn7IkTjFjqBdAhJ5m/BiU45rQu3ck%2B6RC%2BU%2BEalYU42PwbfQmsDwDZgAACHBtXI8rJNLaqAG5bveMLq14sdqoo9yPGDTdHxA7OjsAOmIxUTUXgi%2B44zK9rStYOMPMq4e6et15tJFBbG2jKGVdJMY3ZkTFu%2BHWNopmckOWLVgFNq79y3hmsdxc1wOedU50wO01k4tR95v4Imjx%2BJujGLa9TWHvuxeDQi9Y4ybY/y9vY1LteXSo0kKHbGazTsLNxyFfmSDOcn8ClbW9bmk0c4jHKD1yRpmMUoJ6GMEDPMqNOCkwrk63Ab7wPb/Ik//Xt/R1gr%2Bom7Tc2OeYYcdyru5UC/xxsJOAvl6NlTvqnrrwv3tNwIcpsdUqBF6TuxWSlAQvZrc4R0FfqAmC1gmCnHgcn6LOJmRb0NP4X2cysqVe7yMirSTCCMByWMIyPaVuut%2BME7E/g1i7%2BF6GOmOb4jaw5esWXZItZITutJph%2B%2BiB5Jhj5m5K8KwagRMAS5gWCtioSFd8CezxoiPqJxEvqdn2z7PYPJa2IEPLnuo8hgVRtHuU8/aTQiACqk%2BA7ilNPbpjD1XsiVE35rwQalWYecZgjOX1bVhMm1bTSpRC5s14qea2UC8ENIkJSR9nRsud1AE%3D%26p%3D X-Agent-DeviceId: 0100748C0900D485 X-BM-CBT: 1646732532 X-Device-isOptin: true X-Device-Touch: false X-Device-ClientSession: B3FD0EB2977A44E390C07B484049F516 X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI X-BM-ClientFeatures: pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: www.bing.com Content-Length: 88754 Connection: Keep-Alive Cache-Control: no-cache Cookie: MUID=BEEBF15262804E24A8DF6781500AB975; _SS=CPID=1653677609279&AC=1&CPH=4ef661f2
2022-05-27 18:54:05 UTC	271	OUT	Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 43 30 34 30 39 45 38 34 43 37 45 43 34 44 31 36 41 32 43 44 44 41 34 38 30 35 45 32 44 33 43 34 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.ClientInst</T><IG>C0409E84C7EC4D16A2CDDA4805E2D3C4</IG><D><![CDATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,Ambie
2022-05-27 18:54:05 UTC	287	OUT	Data Raw: 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 54 65 78 74 22 3a 22 5b 63 6f 6e 73 74 72 61 69 6e 74 49 6e 64 65 78 44 6f 77 6e 6c 6f 61 64 65 72 2e 74 72 79 44 6f 77 6e 6c 6f 61 64 46 72 6f 6d 55 72 6c 41 73 79 6e 63 5d 20 44 6f 77 6e 6c 6f 61 64 20 66 61 69 6c 65 64 22 2c 22 53 74 61 63 6b 22 3a 22 5b 63 6f 6e 73 74 72 61 69 6e 74 49 6e 64 65 78 44 6f 77 6e 6c 6f 61 64 65 72 2e 74 72 79 44 6f 77 6e 6c 6f 61 64 46 72 6f 6d 55 72 6c 41 73 79 6e 63 5d 20 44 6f 77 6e 6c 6f 61 64 20 66 61 69 6c 65 64 5c 6e 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f Data Ascii: "QF","CF":"pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader","Text":"[constraintIndexDownloader.tryDownloadFromUrlAsync] Download failed","Stack":"[constraintIndexDownloader.tryDownloadFromUrlAsync] Download failed\nhttps://www.bing.com/
2022-05-27 18:54:05 UTC	303	OUT	Data Raw: 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 65 72 72 6f 72 54 79 70 65 22 3a 22 53 65 6e 64 54 69 6d 65 64 4f 75 74 22 2c 22 66 61 69 6c 43 6f 75 6e 74 22 3a 31 2c 22 54 53 22 3a 31 35 39 35 34 39 39 39 32 34 39 31 36 2c 22 52 54 53 22 3a 35 35 36 39 2c 22 53 45 51 22 3a 32 2c 22 55 54 53 22 3a 31 36 35 33 36 37 37 36 34 34 38 38 36 7d 5d 5d 3e 3c 2f 44 3e 3c 54 53 3e 31 35 39 35 34 39 39 39 32 34 39 31 36 3c 2f 54 53 3e 3c 2f 45 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 43 30 34 30 39 45 38 34 43 37 45 43 34 44 31 36 41 32 43 44 44 41 34 38 30 35 45 32 44 33 43 34 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 Data Ascii: cprod,CortanaSPAXamlHeader","errorType":"SendTimedOut","failCount":1,"TS":1595499924916,"RTS":5569,"SEQ":2,"UTS":1653677644886}...</D><TS>1595499924916</TS></E><E><T>Event.ClientInst</T><IG>C0409E84C7EC4D16A2CDDA4805E2D3C4</IG><D><![CDATA[{"CurUrl":"https

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:54:05 UTC	319	OUT	Data Raw: 74 6f 53 75 67 67 65 73 74 22 2c 22 53 63 65 6e 61 72 69 6f 22 3a 22 4d 50 50 22 2c 22 53 43 22 3a 31 2c 22 44 53 22 3a 5b 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 33 2c 22 51 22 3a 22 54 61 73 6b 20 4d 61 6e 61 67 65 72 22 2c 22 56 61 6c 22 3a 22 50 50 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 30 2c 22 48 53 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 30 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 41 75 74 6f 47 65 6e 65 72 61 74 65 64 2e 7b 39 32 33 44 44 34 37 37 2d 35 38 34 36 2d 36 38 36 42 2d 41 36 35 39 2d 30 46 43 43 44 37 33 38 35 31 41 38 7d 22 2c 22 44 4e 61 6d 65 22 3a 22 54 61 73 6b 20 4d 61 Data Ascii: toSuggest","Scenario":"MPP","SC":1,"DS":[{"T":"D.Url","K":1003,"Q":"Task Manager","Val":"PP","Ho":2,"Gr":0,"HS":1,"DeviceSignals":{"Rank":0,"PHits":"System.ParsingName","Id":"Microsoft.AutoGenerated.{923DD477-5846-686B-A659-0FCCD73851A8}","DName":"Task Ma
2022-05-27 18:54:05 UTC	335	OUT	Data Raw: 66 6f 22 3a 7b 22 4d 55 49 44 22 3a 22 42 45 45 42 46 31 35 32 36 32 38 30 34 45 32 34 41 38 44 46 36 37 38 31 35 30 30 41 42 39 37 35 22 2c 22 41 43 56 65 72 22 3a 22 34 65 66 36 36 31 66 32 22 2c 22 46 44 50 61 72 74 6e 65 72 45 6e 74 72 79 22 3a 22 61 75 74 6f 73 75 67 67 65 73 74 22 2c 22 69 73 4f 66 66 6c 69 6e 65 22 3a 30 2c 22 77 65 62 52 65 71 75 65 73 74 65 64 22 3a 31 2c 22 65 6e 74 72 79 50 6f 69 6e 74 22 3a 22 57 4e 53 53 54 42 22 2c 22 70 72 65 76 69 6f 75 73 45 78 70 65 72 69 65 6e 63 65 22 3a 22 53 65 61 72 63 68 42 6f 78 22 2c 22 64 65 76 69 63 65 48 69 73 74 6f 72 79 45 6e 61 62 6c 65 64 22 3a 31 2c 22 77 69 6e 64 6f 77 73 41 63 63 6f 75 6e 74 22 3a 22 33 22 2c 22 63 6f 72 74 61 6e 61 41 63 63 6f 75 6e 74 22 3a 22 33 22 2c 22 73 65 61 72 Data Ascii: fo":{"MUID":"BEEBF15262804E24A8DF6781500AB975","ACVer":"4ef661f2","FDPartnerEntry":"autosuggest","isOffline":0,"webRequested":1,"entryPoint":"WNSSTB","previousExperience":"SearchBox","deviceHistoryEnabled":1,"windowsAccount":"3","cortanaAccount":"3","sear
2022-05-27 18:54:05 UTC	351	OUT	Data Raw: 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 30 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 41 75 74 6f 47 65 6e 65 72 61 74 65 64 2e 7b 39 32 33 44 44 34 37 37 2d 35 38 34 36 2d 36 38 36 42 2d 41 36 35 39 2d 30 46 43 43 44 37 33 38 35 31 41 38 7d 22 2c 22 44 4e 61 6d 65 22 3a 22 54 61 73 6b 20 4d 61 6e 61 67 65 72 22 2c 22 41 70 70 4c 6e 63 68 22 3a 30 2c 22 41 72 67 73 22 3a 30 2c 22 4d 44 4e 22 3a 30 2c 22 45 78 74 22 3a 22 2e 65 78 65 22 7d 7d 5d 7d 2c 7b 22 54 22 3a 22 44 2e 50 50 22 2c 22 41 70 70 4e 53 22 3a 22 53 6d 61 72 74 53 65 61 72 63 68 22 2c 22 53 65 72 76 69 63 65 22 3a 22 41 75 74 6f 53 75 67 67 65 73 74 22 2c 22 53 63 65 6e 61 72 Data Ascii: iceSignals":{"Rank":0,"PHits":"System.ParsingName","Id":"Microsoft.AutoGenerated.{923DD477-5846-686B-A659-0FCCD73851A8}","DName":"Task Manager","AppLnch":0,"Args":0,"MDN":0,"Ext":".exe"}}]},{"T":"D.PP","AppNS":"SmartSearch","Service":"AutoSuggest","Scenar
2022-05-27 18:54:06 UTC	358	IN	HTTP/1.1 204 No Content Access-Control-Allow-Origin: * X-Cache: CONFIG_NOCACHE Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: 2E899C2B0D044AF1B0BDF76D3C2B8A62 Ref B: FRA31EDGE0620 Ref C: 2022-05-27T18:54:05Z Date: Fri, 27 May 2022 18:54:05 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49757	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:51 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:51 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-XxQIMdwom16mLkjX_tQn_g' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 18:53:51 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5625 X-Daystart: 42831 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 18:53:51 UTC	2	IN	Data Raw: 33 36 64 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 32 35 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 32 38 33 31 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5625" elapsed_seconds="42831"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-27 18:53:51 UTC	3	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-05-27 18:53:51 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49759	13.226.244.95	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:52 UTC	13	OUT	GET /styles.css HTTP/1.1 Host: triarail-mx.w3spaces.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://triarail-mx.w3spaces.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-27 18:53:52 UTC	23	IN	HTTP/1.1 200 OK Content-Type: text/css Content-Length: 699 Connection: close x-amz-id-2: bw8m+wUjF9bXle2mg35M1rBxLWSJ+5cvhNOHPoPnJZfS5mqMJRxlTVSY3s3XX6oc3HEHr75Kbc8= x-amz-request-id: KMFR7KTWB7KSBC7S Last-Modified: Wed, 25 May 2022 13:49:59 GMT Accept-Ranges: bytes Server: AmazonS3 Date: Fri, 27 May 2022 18:53:53 GMT ETag: "992a289300a1fdba1def12f8ae9b2c39" X-Cache: RefreshHit from cloudfront Via: 1.1 d2e5a3e85f972a4c5b9add94dea2057a.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: -mA1yAdoPmXgRJbFqJCRPM-BmNrf51gqh0nuaOrJoFUvAv1-GAArVg==

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:52 UTC	24	IN	Data Raw: 2a 62 6f 64 79 20 7b 0a 09 70 61 64 64 69 6e 67 3a 20 30 3b 0a 09 6d 61 72 67 69 6e 3a 20 30 3b 0a 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 20 75 72 6c 28 29 3b 0a 7d 0a 2e 66 6f 72 6d 20 7b 0a 09 68 65 69 67 68 74 3a 20 34 30 30 70 78 3b 0a 09 77 69 64 74 68 3a 20 34 30 30 70 78 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 35 29 3b 0a 0a 32 35 35 0a 09 7d 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 09 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 35 30 70 78 3b 0a 7d 0a 2e 6f 6e 65 20 7b 0a 09 68 65 69 67 68 74 3a 20 31 30 30 70 78 3b 0a 09 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 33 30 30 70 78 3b 0a 7d 0a 2e 69 6e 70 75 Data Ascii: *body {padding: 0;margin: 0;font-family: sans-serif;background-image: url();}.form {height: 400px;width: 400 px;background: rgba(0, 0, 0, 0.5);255}.container {padding-top: 150px;}.one {height: 100px;margin-left: -300px;}.inpu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49760	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:52 UTC	14	OUT	GET /th?id=OIP.g-qzb46-Ic0JYI6nPZVSOgHaCu&w=350&h=128&c=8&rs=1&qlt=90&o=6&dpr=1.25&pid=3.1&rm=2 HTTP /1.1 Host: www.bing.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://triarail-mx.w3spaces.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-27 18:53:52 UTC	15	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=1209600 Content-Length: 7692 Content-Type: image/jpeg X-Cache: TCP_MISS Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Timing-Allow-Origin: * Report-To: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://aefd.nelreports.net/api/report?cat=bi ngth"}]} NEL: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: 76DEA7DA105D43218B5B2338E90B5D8D Ref B: FRA31EDGE0610 Ref C: 2022-05-27T18:53:5 2Z Date: Fri, 27 May 2022 18:53:51 GMT Connection: close
2022-05-27 18:53:52 UTC	16	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 11 08 00 a0 01 b5 03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 01 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 01 02 08 06 07 09 05 03 04 ff da 00 08 01 01 00 00 00 00 f5 42 e2 2c 58 b1 65 8b 06 52 65 21 61 60 05 4b 2d b8 5c 45 8b 16 2c b1 60 ca 08 58 58 01 52 97 2c 2e 22 c5 8b 16 58 b0 65 Data Ascii: JFIF&""&0-0>>T&""&0-0>>T"B,XeRe!a`K-\E,`XXR,."Xe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49762	13.226.244.95	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:52 UTC	14	OUT	GET /background.jpg HTTP/1.1 Host: triarail-mx.w3spaces.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://triarail-mx.w3spaces.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>24</td><td>IN</td><td>HTTP/1.1 200 OK
Content-Type: image/jpeg
Content-Length: 65984
Connection: close
x-amz-id-2: LgxM1N9jD7yFg8dWHcBwNykciUQJcEfrhuDn0Ddy2Q/B0suiDyxaUitONt5iFzA56FaCLRWKCs8=
x-amz-request-id: 56TGGQQXVG3NGSCM
Last-Modified: Wed, 25 May 2022 13:48:32 GMT
Accept-Ranges: bytes
Server: AmazonS3
Date: Fri, 27 May 2022 18:53:53 GMT
ETag: "a8b29493b06270972eb5790a58537e94"
X-Cache: RefreshHit from cloudfront
Via: 1.1 ae1ca410ec705f1f12b416d7672bb01a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: FCO50-C1
X-Amz-Cf-Id: JDHScm-uiMhUB-kmBQuekzVj8iwp0LZGqCXpzKCzYDHDsLmU5gKc4Q==</td></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>25</td><td>IN</td><td>Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0a 10 0a 0a 09 09 0a 14 0e 0f 0c 10 17 14 18 18 17 14 16 16 1a 1d 25 1f 1a 1b 23 1c 16 16 20 2c 20 23 26 27 29 2a 29 19 1f 2d 30 2d 28 30 25 28 29 28 ff db 00 43 01 07 07 07 0a 08 0a 13 0a 0a 13 28 1a 16 1a 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 ff c2 00 11 08 04 1a 05 78 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 01 06 02 05 07 03 04 08 ff c4 00 1a 01 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 01 03 04 02 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 01 ab 0f a4 f1 c0 00
Data Ascii: JFIFC%# , #&')*)-0-(0%()(C(((x"</td></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>41</td><td>IN</td><td>Data Raw: 0a 78 f0 54 2c ce 40 b9 8e f9 03 ce 45 72 cc c5 87 1e 60 f1 c0 8b d5 7d ef f5 02 9b d4 78 fb b8 d0 d9 44 99 47 46 84 47 2a 97 11 b3 3a 34 22 3a 85 32 2c 78 85 85 fc 09 d9 40 92 eb a3 64 70 1c 57 06 93 ad 1d 25 a5 4f 76 a9 2e c2 80 bd 54 ac cd 5b 6e 50 c8 b5 cf ce f9 50 f0 12 0f 1c c7 8f 05 58 7d b9 92 3e e3 be 40 f3 a6 e2 41 82 c2 e9 16 92 8e 14 81 b1 c8 1b 1c 81 b1 48 1b 14 81 b1 c8 1b 1c 81 b1 c8 0a 88 f2 11 33 0f 1c 08 bd 57 de ff 00 50 29 bd 47 8f bb 8d 4a ee 27 8c f3 ff 00 b8 be 6a e1 ff 00 d2 e0 3e e9 ba a6 63 92 4b 3b 6d 9c 85 ce 75 34 ca 7c 57 ad 33 b5 26 c2 b4 e3 f9 7a b1 16 0b aa 94 99 0f ef b7 f3 9e 6f 9e 37 4e e1 e1 70 b1 3b e4 0c 59 70 b3 16 fc c5 85 e4 4f 79 29 f5 07 87 a8 cd b7 d4 26 84 55 a5 2d 4e 55 a5 36 a4 d6 9e b7 d6 d4 1f aa 9b c4 b5
Data Ascii: xT,@Er`}xDGFG*:4":2,x@dpW%Ov.T[nPPX}>@AH3WP)GJ'j>cK;mu4|W3&zo7Np;YpOy)&U-NU6</td></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>57</td><td>IN</td><td>Data Raw: a2 8e 1a 08 6b da a4 c1 0b 28 91 0c 99 02 3e 43 83 2a fd b2 39 54 ae 10 bf 22 ae e1 74 2a 0e fd 16 8c 80 d3 86 d8 11 0d 80 b6 66 6d 5f 91 ee 9e 21 c2 18 69 31 0a d9 09 8b 95 4b 31 a4 6b 81 9a 8a 95 c3 3e f0 c1 08 9f 6c 77 16 07 63 91 1b 86 6c a4 a7 81 17 b1 b1 44 e8 2a 27 4a 4f ca 24 c8 6a 23 72 ee 66 be 45 1c c4 2c 39 82 f6 e8 b4 8d 17 df 20 cd a3 9f 91 e6 be 21 c2 18 68 9b b7 51 da 45 1d 0c 42 79 c2 68 26 26 2b 63 d0 d6 22 8f fd 9b 1a 31 57 d5 86 28 68 95 5a 44 f6 ad 82 e2 ef 84 b5 7b bd 1d 8b 59 04 94 91 d7 a0 ae aa 54 43 36 e6 ae 74 5d 0c a5 0b 3e 4c 3f 91 d1 f1 0e 10 c3 45 b8 b5 c3 4a 4d 67 a5 dd 46 5d 31 25 7d a4 88 20 8d 20 4a 34 89 a7 d8 86 8d 84 46 90 41 04 11 d1 24 8b 5a ba b0 84 82 61 7c 8f 75 f1 0e 10 56 69 90 c8 99 2f 14 5e e1 31 66 d6 96 c3
Data Ascii: k(>C*9T"t*fm_!i1K1k>lwclD*'JO$j#rfE,9 !hQEByh&&+c"1W(hZD{YTC6t]>L?EJMgF]1%} J4FA$Za|uVi/^1f</td></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>73</td><td>IN</td><td>Data Raw: 49 a8 21 f3 76 e8 8d 65 1c f7 1f 88 4a 34 69 6a 97 cc ce 9c 3f 9d ba 2b 69 1e f9 4d 58 7d 1d 0b 73 7c a5 6b 33 58 89 b9 4d a0 0a 8d 84 02 ef 48 88 95 61 b1 e0 88 8e ee 59 22 55 a6 fb 72 df 01 ce a5 24 cc df 23 d1 97 de 3d 6f ce 90 60 d9 a3 e5 68 c1 5c 48 8e b2 3b 2f 43 f0 1f f7 6e 58 ef 5d 84 0a e4 fc c7 6c 56 c3 4d 75 71 ea ef 9f 10 d0 b0 6d e0 34 b2 8d fa 9f b2 a0 75 9d 2b 79 cf f5 88 44 83 82 94 72 b7 2f 4d 3f 9d ba 26 60 55 5c 1d d0 c7 d1 6e d8 02 e6 f8 d0 2a 50 ea 8e 61 17 58 0d 19 ba 99 9d 25 de 76 a3 13 5c 1f 7f d4 4a a7 6e f7 8b 1f b4 f1 e8 c8 99 7a f8 41 83 62 15 6c 43 d3 52 2d 37 45 e9 77 9a 9a a4 4d d5 ef d0 df 11 ff 00 84 30 1c 0a da a9 46 0f 37 61 f1 96 bc ef 48 70 c0 4a 37 b9 b1 fb 6f 85 01 a9 ae fe 8d f2 fa 1c 59 ab a7 46 05 50 00 74 52 e2
Data Ascii: I!veJ4ij?+iMX}s|k3XMHaY"Ur$#=o`h\H;/CnX]lVMuqm4u+yDr/M?&`U\n*PaX%v\JnzAblCR-7EwM0F7aHpJ7oYFPtR</td></tr>
<tr><td>2022-05-27 18:53:52 UTC</td><td>89</td><td>IN</td><td>Data Raw: d0 87 86 3c 2f a4 7c 36 99 97 d2 5f 49 7d 25 f4 97 d2 5f 49 7d 25 f4 97 d2 5f 49 8e 27 da 57 a9 2f ef 3a 64 26 85 1a 47 01 16 a2 8b 75 31 c4 fb 4b e9 3e d3 ed 3e d3 ed 0e 2a ba c2 c4 6a ca e7 3d 63 96 25 67 25 9c 33 5d a8 e2 3b 51 41 b4 2a dc 62 62 59 2f a4 be 93 1c 4c 71 fd c5 68 88 d5 4c f1 2b 84 ae 12 b8 4a e1 2a 2a 2a 2a 2b 84 ae 12 b8 4a e1 2a 2a 2b 84 ae 12 b8 4a e1 2b 84 ae 12 b8 4a e1 2a 2a 2a 2b 84 ae 12 b8 4a e1 2a 2a 2a 2a 2b 84 ae 12 a2 a2 a2 a2 a2 a2 a2 a2 b8 4a e1 2b 84 ae 12 b8 4a e1 2b 84 ae 12 b8 4a e1 2b 84 ae 12 a2 a2 a2 a2 b8 4a e1 2a 2a 2a 2a 2a 2a 2a 2b 84 ae 12 a2 a2 a2 a2 a2 a2 b8 4a e1 2b 84 ae 12 a2 a2 a2 a2 a2 a2 a2 a2 b8 4a e1 2b 84 ae 12 a2 a2 b8 4a e1 2b 84 ae 12 a2 a2 a2 a2 a2 b8 4a e1 2b 84 ae 12 b8 4a e1 2a 2a 2a 2a 2a 2a
Data Ascii: </|6_I}%_I}%_I'W/:d&Gu1K>>*j=c%g%3];QA*bbY/LqhL+J****+J**+J+J***+J****+J+J+J+J*******+J+J+J+J+J******</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49769	13.226.244.95	443	C:\Program Files\Google\Chrome\Application\chrome.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-05-27 18:53:53 UTC</td><td>89</td><td>OUT</td><td>GET /favicon.ico HTTP/1.1
Host: triarail-mx.w3spaces.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://triarail-mx.w3spaces.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:53 UTC	90	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 12984 Connection: close Last-Modified: Mon, 20 Dec 2021 10:29:18 GMT Accept-Ranges: bytes Server: AmazonS3 Date: Fri, 27 May 2022 18:53:53 GMT ETag: "577e7a60c9d61bb8273e7f376521983a" Vary: Accept-Encoding X-Cache: Error from cloudfront Via: 1.1 02c600d8206154a45f6cf88b24f1bda2.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: 7bN6rxmewKASyLzXOBsG2kKP6aoaUT779Y15R0oTP1Bv-3ci5fsRgA== Age: 160
2022-05-27 18:53:53 UTC	90	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6 b 0a 20 20 20 20 20 20 72 65 6c 3d 22 69 63 6f 6e 22 0a 20 20 20 20 20 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 77 33 73 63 68 6f 6f 6c 73 2e 63 6f 6d 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 0a 20 20 20 20 20 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 0a 20 20 20 20 2f 3e Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8" /> <meta name="viewport" conte nt="width=device-width,initial-scale=1" /> <link rel="icon" href="https://www.w3schools.com/favicon.ico" type="image/x-icon" />
2022-05-27 18:53:53 UTC	96	IN	Data Raw: 34 2e 36 31 30 37 20 34 2e 34 37 39 32 33 20 33 35 2e 33 36 39 32 20 34 2e 34 37 39 32 33 20 33 35 2e 38 36 34 32 43 34 2e 34 37 39 32 33 20 33 36 2e 39 35 38 20 33 2e 33 38 35 34 31 20 33 37 2e 35 35 36 38 20 32 2e 32 39 31 36 20 33 37 2e 35 35 36 38 43 31 2e 32 32 39 37 33 20 33 37 2e 35 35 36 38 20 30 2e 31 35 31 38 38 32 20 33 36 2e 39 31 30 31 20 30 2e 31 32 37 39 33 20 33 35 2e 37 36 30 34 5a 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 69 6c 6c 3d 22 23 30 34 41 41 36 44 22 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 70 61 74 68 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 3d 22 4d 35 2e 35 38 38 38 37 20 33 34 2e 37 32 32 35 43 35 2e 35 38 38 38 37 20 33 33 2e 30 31 33 39 Data Ascii: 4.6107 4.47923 35.3692 4.47923 35.8642C4.47923 36.958 3.38541 37.5568 2.2916 37.5568C1.22973 37.55 68 0.151882 36.9101 0.12793 35.7604Z" fill="#04AA6D" /> <path d="M5.58887 34.7225C5.58887 33.0139

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49773	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:54 UTC	103	OUT	GET /th?id=OIP.g-qzb46-Ic0JYI6nPZVSOgHaCu&w=350&h=128&c=8&rs=1&qlt=90&o=6&dpr=1.25&pid=3.1&rm=2 HTTP /1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: www.bing.com Cookie: SRCHUID=V=2&GUID=B298896C7AD4481EABB8EDC8003DB882&dmnchg=1; SRCHD=AF=IESS4A; SRCHU SR=DOB=20200930
2022-05-27 18:53:54 UTC	104	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=1209600 Content-Length: 7692 Content-Type: image/jpeg X-Cache: TCP_HIT Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Timing-Allow-Origin: * Report-To: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://aefd.nelreports.net/api/report?cat=bingth"}]} NEL: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: EA89F2F98FD0496699CEE3D5023818CC Ref B: FRA31EDGE0210 Ref C: 2022-05-27T18:53:54Z Date: Fri, 27 May 2022 18:53:53 GMT Connection: close
2022-05-27 18:53:54 UTC	104	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 11 08 00 a0 01 b5 03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 01 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 01 02 08 06 07 09 05 03 04 ff da 00 08 01 01 00 00 00 00 f5 42 e2 2c 58 b1 65 8b 06 52 65 21 61 60 05 4b 2d b8 5c 45 8b 16 2c b1 60 ca 08 58 58 01 52 97 2c 2e 22 c5 8b 16 58 b0 65 Data Ascii: JFIF&""&0-0>>T&""&0-0>>T"B,XeRe!a`K-\E,`XXR,."Xe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49772	13.226.244.95	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:53:54 UTC	103	OUT	GET /background.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: triarail-mx.w3spaces.com
2022-05-27 18:53:54 UTC	112	IN	HTTP/1.1 200 OK Content-Type: image/jpeg Content-Length: 65984 Connection: close x-amz-id-2: LgxM1N9jD7yFg8dWHcBwNykciUQJcEfrhuDn0Ddy2Q/B0suiDyxaUitONt5iFzA56FaCLRWKCs8= x-amz-request-id: 56TGGQQXVG3NGSCM Last-Modified: Wed, 25 May 2022 13:48:32 GMT Accept-Ranges: bytes Server: AmazonS3 Date: Fri, 27 May 2022 18:53:53 GMT ETag: "a8b29493b06270972eb5790a58537e94" X-Cache: Hit from cloudfront Via: 1.1 04011eeb624765f661211e7fdf697f0e.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: 31fQEfp4-k4cHAT3fHv63rxzc_VaIiOHfWliRe1hTnsmLUjSLrhY9g== Age: 2
2022-05-27 18:53:54 UTC	112	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 06 04 05 06 05 04 06 06 05 06 07 07 06 08 0a 10 0a 0a 09 09 0a 14 0e 0f 0c 10 17 14 18 18 17 14 16 16 1a 1d 25 1f 1a 1b 23 1c 16 16 20 2c 20 23 26 27 29 2a 29 19 1f 2d 30 2d 28 30 25 28 29 28 ff db 00 43 01 07 07 07 0a 08 0a 13 0a 0a 13 28 1a 16 1a 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 ff c2 00 11 08 04 1a 05 78 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 01 06 02 05 07 03 04 08 ff c4 00 1a 01 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 03 04 02 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 01 ab 0f a4 f1 c0 00 Data Ascii: JFIFC%# , #&')*)-0-(0%()(C((x"
2022-05-27 18:53:54 UTC	128	IN	Data Raw: 7a 29 be ae 6f 02 37 d4 ac 70 0f 08 dd 1d 7f 92 eb 4e 2d 95 95 5e 40 f5 79 00 ea f2 2c 71 c5 ba be 04 76 56 f8 7a 33 ed 36 bc 73 64 e7 73 ab 76 c2 7d dd 4f 14 f9 85 0e 7a 23 16 d3 1c 6d 11 c1 48 60 c6 b9 91 af 60 8f f3 9e 55 99 38 10 3c 6f 19 de 31 68 b4 5a 2d 05 89 e6 f2 ab 84 0c 24 79 4d e2 c3 3a cb 49 b6 4f 49 ab c7 89 21 6b 41 b4 e8 8d cf 5a 51 20 92 a4 ac af 1e 11 93 ff 00 4a b2 8d 35 9c 16 ed d8 50 36 14 0d 85 03 60 6c 7d dc 4a 33 c9 6a 5d 75 d7 08 6d 2a 21 b5 28 6d 4a 11 ea 2f 47 71 55 a9 8f 96 1c 53 0c 12 0e 36 8a 06 8b 76 68 a4 68 24 32 94 58 94 a3 4a 45 25 e7 5f fc e7 9e 09 9f 01 42 cc d6 66 2c 4e f9 03 ba 45 98 8b 31 61 9c b1 67 fa bd 79 43 27 4f ff 00 1f 20 ff 00 ea 42 e6 ca 3e 48 49 32 3b e5 b4 e8 ff 00 cb ac 56 36 0b 0c 58 08 7d fc 57 9e 71 Data Ascii: z)o7pN-^@y,qvVz36sdsv}Oz#mH``U8<o1hZ-$yM:IOI!kAZQ J5P6`l}J3j]um*!(mJ/GqUS6vhh$2XJE%_Bf,NE1agyC'O B>HI2;V6X}Wq
2022-05-27 18:53:54 UTC	137	IN	Data Raw: ca 72 f2 9c a1 78 d6 88 8b cf 2f b0 ee 50 f7 7a 23 da a6 ee d0 31 71 8f 46 d3 a3 04 ab e2 6a f2 9a a8 c1 40 ac cc cb 41 6a 55 89 ad fe a2 95 fb 18 e5 0f 77 a2 3d aa 6e ed 01 2b 6f 6f c4 10 92 23 56 9f b2 ce 50 f7 7a 23 da a6 ee d1 ac 27 53 fa 95 ed 81 6b 97 9a 17 9a 17 9a 17 9a 17 9a 17 9a 15 a6 1a b7 9a a4 8f b2 bc d0 bc d0 bc d0 bc d0 bc d0 bc d1 f6 1d ca 1e ef 44 7b 54 dd da 78 2c 16 0b 05 82 c1 3f 27 3b c2 f0 b5 2f 6b 2e 58 2c 16 0b 05 82 c3 ec 3b 94 3d de 87 14 7b 54 dd db 53 da 54 dd 7e c6 b9 43 dd b6 a3 41 73 fe 8a af 3e 13 7e ab da 17 38 ad c7 7e d1 92 1b 40 d2 89 f2 42 e0 fa df 65 59 91 b6 1f c8 ed 0f 69 53 75 fb 1a e5 0f 76 d6 c4 3b a3 79 c8 58 6d 5d fd 8e 91 6c ad fc aa 3f 5a 23 83 b6 67 b4 a9 ba fd 8d 72 87 bb 68 d8 63 e3 89 4d 8e 31 86 c0 c7 Data Ascii: rx/Pz#1qFj@AjUw=n+oo#VPz#'SkD{Tx,?';/k.X,;={TST~CAs>~8~@BeYiSuv;yXm]l?Z#grhcM1
2022-05-27 18:53:54 UTC	153	IN	Data Raw: 07 df 7d f7 d8 3c 88 2f 3c f3 cf 3c b3 41 6d a5 5f 69 ea 82 d5 ac 8c 8e 73 d8 3d f4 4b fc 4a 9a d4 9a c0 a1 38 89 3d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 68 5f df 7d f7 df 69 5c 30 fd f7 df 6b 07 df 7d f7 dd 7c 76 2f 3c f3 cf 3c f2 c5 e9 01 e0 27 ac 28 55 bc fe c3 0a 0c c6 65 4c 5c ae 9a fd 90 34 1a be eb 3d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 68 5f df 7d f7 df 69 5c 30 fd f7 df 6b 07 df 7d f7 dc 79 ac b1 bf ff 00 ff 00 ff 00 ef 45 7d a5 41 78 5f ca 95 8d 49 80 c6 35 3c 43 df 7f a6 9d f9 56 fa 41 f5 a5 bd f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 68 5f dc 75 f7 df 69 4c 71 fd f7 da 41 57 df 7d f7 df 7d f7 d7 c1 04 10 41 04 6f 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 7d f7 df 68 Data Ascii: }</<<Am_is=KJ8=}}}}h_}i\0k}|v/<<'(UeL\4=}}}}h_}i\0k}yE}Ax_I5<CVA}}}}h_uiLqAW}}Ao}}}}}}}}}}}}}h
2022-05-27 18:53:54 UTC	169	IN	Data Raw: f0 60 15 6d 8b eb 10 49 5b 1e 23 b3 f6 f6 47 26 ba b8 f0 0a 06 b6 7b c6 62 c4 d9 36 21 85 e1 95 d7 86 76 d6 53 3c 13 9d c9 41 14 aa 6c 65 af 28 52 dc 69 8d 8f f2 5f 05 aa 63 b6 45 0d 46 56 f9 59 d3 d7 c4 b0 a8 e1 0c 51 75 6a 15 35 40 0b 18 ef 07 2f 5d 80 fe 09 7b 45 72 2b fa a7 75 f0 97 61 fc 0e 67 7f f6 9f 2b cc 7b 4c f9 fd 67 68 f6 fa 0c d5 3e 43 89 dc fd fe 9d 80 b2 c6 64 aa 34 98 05 5a ee 35 50 75 59 ca c4 0f 50 f5 45 00 70 8a 8c 70 0d 63 bc 66 10 00 a7 dd 5d a1 a5 2b 28 32 dd e0 f4 4f d7 27 eb 93 f5 c9 fa e4 fd 72 7e b9 3f 5c 9f ae 4f d7 27 eb 93 f5 c9 fa e4 ae a0 dd 21 08 1b 55 77 66 f7 1d 6a ed 6e f9 42 ad 1d 50 4b 62 f7 ad 60 e1 7c 88 e1 32 3b 90 80 57 cd 12 ac 41 48 62 0d c4 65 2e fb c5 ba 0d 0d ff 00 e7 89 95 45 54 d1 7f c0 b1 06 26 50 ab 85 dd Data Ascii: `mI[#G&{b6!vS<Ale(Ri_cEFVYQuj5@/]{Er+uag+{Lgh>Cd4Z5PuYPEppcf]+(2O'r~?\O'!UwfjnBPKb`|2;WAHbe.ET&P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49782	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

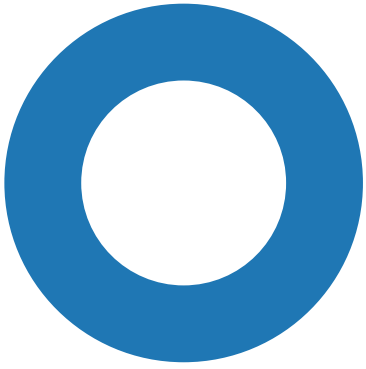
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:54:02 UTC	177	OUT	POST /threshold/xls.aspx HTTP/1.1 Origin: https://www.bing.com Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init Content-type: text/xml X-MSEdge-ExternalExpType: JointCoord X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40 X-PositionerType: Desktop X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage X-Search-SafeSearch: Moderate X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8} X-UserAgeClass: Unknown X-BM-Market: US X-BM-DateFormat: M/d/yyyy X-CortanaAccessAboveLock: false X-Device-OSSKU: 48 X-BM-DTZ: 60 X-BM-FirstEnabledTime: 132061327679472806 X-DeviceID: 0100748C0900D485 X-BM-DeviceScale: 100 X-Search-TimeZone: Bias=-60; StandardBias=0; TimeZoneKeyName=W. Europe Standard Time X-BM-Theme: 000000;0078d7 X-BM-DeviceDimensionsLogical: 1232x1024 X-BM-DeviceDimensions: 1232x1024 X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJPQDsAAcrCUQHVmc1QWYMPz0DXFqeRx8wamoowmwbwUSyNYpjtyJpJRDfEtLg1rKS4/zxABCoKsuMFRUBIP7PFid4xD2qKyl0URDzKuBMFjFkKzlG3Ps9MGF%2BBZXTdKnpAzZrlgOtRPCtamchXz28q0CRmPxXD6ZHI2rcMOvnUBLbt1zkoTBTKYibaVaGygpAEYQDTKkpAamKV8eOep8EnHN50LiR92MCKiQtLylSx/qTDVfvmE81bne2UzPZEbqlm/DPuKdzajAWp%2BXa91MUXk%2BgPu95uggy8QPGrNOWbn7lkTjFjqBdAhJ5m/BiU45rQu3ck%2B6RC%2BU%2BEalYU42PwbfQmsDwDZgAACHBtXI8rJNLaqAG5bveMLq14sdqoo9yPGDTdHxA7OjsAOmIxUTUXgi%2B44zK9rStYOMPMq4e6et15tJFBbG2jKGVdJMY3ZkTFu%2BHWNopmckOWLVgFNq79y3hmsdxc1wOedU50wO01k4tR95v4Imjx%2BJujGLa9TWHvuxeDQi9Y4ybY/y9vY1LteXSo0kKHbGazTsLNxyFfmSDOcn8ClbW9bmk0c4jHKD1yRpmMUoJ6GMEDPMqNOCkwrk63Ab7wPb/Ik//Xt/R1gr%2Bom7Tc2OeYYcdyru5UC/xxsJOAvl6NlTvqnrrwv3tNwIcpsdUqBF6TuxWSlAQvZrc4R0FfqAmC1gmCnHgcn6LOJmRb0NP4X2cysqVe7yMirSTCCMByWMIyPaVuut%2BME7E/g1i7%2BF6GOmOb4jaw5esWXZItZITutJph%2B%2BiB5Jhj5m5K8KwagRMAS5gWCtioSFd8CezxoiPqJxEvqdn2z7PYPJa2IEPLnuo8hgVRtHuU8/aTQiACqk%2BA7ilNPbpjD1XsiVE35rwQalWYecZgjOX1bVhMm1bTSpRC5s14qea2UC8ENIkJSR9nRsud1AE%3D%26p%3D X-Agent-DeviceId: 0100748C0900D485 X-BM-CBT: 1646732532 X-Device-isOptin: true X-Device-Touch: false X-Device-ClientSession: B3FD0EB2977A44E390C07B484049F516 X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI X-BM-ClientFeatures: pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: www.bing.com Content-Length: 87238 Connection: Keep-Alive Cache-Control: no-cache Cookie: MUID=BEEBF15262804E24A8DF6781500AB975; _SS=CPID=1653677609279&AC=1&CPH=4ef661f2
2022-05-27 18:54:02 UTC	179	OUT	Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 31 66 61 37 30 66 62 64 31 62 66 63 34 39 66 61 38 64 65 65 61 62 63 31 34 36 35 65 65 61 64 62 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.ClientInst</T><IG>1fa70fbd1bfc49fa8deeabc1465eeadb</IG><D><![CDATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,Ambie
2022-05-27 18:54:02 UTC	195	OUT	Data Raw: 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 54 22 3a 22 43 49 2e 51 46 50 65 72 66 50 69 6e 67 22 2c 22 53 54 22 3a 22 41 70 70 43 61 63 68 65 22 2c 22 43 56 49 44 22 3a 22 66 37 62 31 38 31 62 34 62 39 38 31 34 33 32 36 38 63 34 66 62 35 66 63 33 61 61 39 63 30 30 39 22 2c 22 4f 46 46 53 45 54 53 22 3a 5b 7b 22 49 22 3a 35 2c 22 45 22 3a 7b 22 30 Data Ascii: CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader","T":"CI.QFPerfPing","ST":"AppCache","CVID":"f7b181b4b98143268c4fb5fc3aa9c009","OFFSETS":[{"I":5,"E":{"0
2022-05-27 18:54:02 UTC	211	OUT	Data Raw: 31 33 2c 22 32 39 36 22 3a 31 7d 2c 22 66 62 63 53 63 6f 72 65 22 3a 30 2e 38 32 34 39 31 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 32 2c 22 51 22 3a 22 43 68 6f 6f 73 65 20 61 20 64 65 66 61 75 6c 74 20 77 65 62 20 62 72 6f 77 73 65 72 22 2c 22 4d 51 22 3a 22 64 65 66 61 75 6c 74 20 62 72 6f 77 73 65 72 22 2c 22 56 61 6c 22 3a 22 53 54 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 38 31 32 36 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 41 41 41 5f 53 79 73 74 65 6d 53 65 74 74 69 6e 67 73 5f 44 65 66 61 75 6c 74 41 70 70 73 5f 42 72 6f 77 73 65 72 22 2c 22 44 4e 61 6d 65 22 3a 22 43 68 6f 6f Data Ascii: 13,"296":1},"fbcScore":0.82491}},{"T":"D.Url","K":1002,"Q":"Choose a default web browser","MQ":"default browser","Val":"ST","Ho":2,"Gr":1,"DeviceSignals":{"Rank":8126,"PHits":"System.ParsingName","Id":"AAA_SystemSettings_DefaultApps_Browser","DName":"Choo

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:54:02 UTC	227	OUT	Data Raw: 51 75 65 72 79 22 20 76 61 6c 75 65 3d 22 66 61 6c 73 65 22 2f 3e 3c 72 65 71 75 65 73 74 49 6e 66 6f 20 6b 65 79 3d 22 46 6f 72 6d 22 20 76 61 6c 75 65 3d 22 22 2f 3e 3c 75 73 65 72 49 6e 66 6f 20 6b 65 79 3d 22 41 70 70 4e 61 6d 65 22 20 76 61 6c 75 65 3d 22 53 6d 61 72 74 53 65 61 72 63 68 22 2f 3e 3c 2f 4f 76 72 3e 3c 2f 4d 3e 3c 2f 47 72 6f 75 70 3e 3c 47 72 6f 75 70 3e 3c 4d 3e 3c 49 47 3e 66 61 66 39 62 35 31 32 61 35 38 61 34 61 30 61 38 33 66 33 36 64 62 30 30 34 36 63 61 32 33 34 3c 2f 49 47 3e 3c 44 53 3e 3c 21 5b 43 44 41 54 41 5b 5b 7b 22 54 22 3a 22 44 2e 41 67 67 72 65 67 61 74 6f 72 22 2c 22 53 65 72 76 69 63 65 22 3a 22 41 75 74 6f 53 75 67 67 65 73 74 22 2c 22 53 63 65 6e 61 72 69 6f 22 3a 22 41 67 67 72 65 67 61 74 6f 72 22 2c 22 41 70 Data Ascii: Query" value="false"/><requestInfo key="Form" value=""/><userInfo key="AppName" value="SmartSearch"/></Ovr></M></Group><Group><M><IG>faf9b512a58a4a0a83f36db0046ca234</IG><DS><![CDATA[[{"T":"D.Aggregator","Service":"AutoSuggest","Scenario":"Aggregator","Ap
2022-05-27 18:54:02 UTC	243	OUT	Data Raw: 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 41 41 41 5f 53 65 74 74 69 6e 67 73 50 61 67 65 4e 65 74 77 6f 72 6b 53 74 61 74 75 73 22 2c 22 44 4e 61 6d 65 22 3a 22 4e 65 74 77 6f 72 6b 20 73 74 61 74 75 73 22 2c 22 4d 44 4e 22 3a 31 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 33 2c 22 51 22 3a 22 43 68 65 63 6b 20 6e 65 74 77 6f 72 6b 20 73 74 61 74 75 73 22 2c 22 56 61 6c 22 3a 22 53 54 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 31 32 38 30 30 31 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 41 41 41 5f 53 65 74 74 69 6e 67 73 5f 47 72 6f 75 70 Data Ascii: ts":"System.ParsingName","Id":"AAA_SettingsPageNetworkStatus","DName":"Network status","MDN":1}},{"T":"D.Url","K":1003,"Q":"Check network status","Val":"ST","Ho":2,"Gr":1,"DeviceSignals":{"Rank":128001,"PHits":"System.ParsingName","Id":"AAA_Settings_Group
2022-05-27 18:54:02 UTC	259	OUT	Data Raw: 2e 35 2c 22 31 33 36 22 3a 31 2c 22 31 33 37 22 3a 31 36 2c 22 31 35 37 22 3a 31 2c 22 31 35 39 22 3a 36 39 34 36 2c 22 31 36 39 22 3a 31 2c 22 32 36 34 22 3a 31 2c 22 32 36 39 22 3a 36 39 34 36 2c 22 32 36 39 22 3a 31 2c 22 32 32 36 34 22 3a 31 2c 22 32 36 39 22 3a 36 39 34 36 2c 22 32 38 34 22 3a 38 2c 22 32 39 36 22 3a 31 7d 2c 22 6d 72 75 53 75 70 70 72 65 73 73 69 6f 6e 53 63 6f 72 65 22 3a 30 2e 31 34 37 34 38 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 35 2c 22 51 22 3a 22 42 6c 6f 63 6b 20 6f 72 20 61 6c 6c 6f 77 20 70 6f 70 2d 75 70 73 22 2c 22 56 61 6c 22 3a 22 53 54 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 38 36 38 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 Data Ascii: .5,"136":1,"137":16,"157":1,"159":6946,"169":1,"264":1,"269":6946,"270":6946,"284":8,"296":1},"mruSuppressionScore":0.14748}},{"T":"D.Url","K":1005,"Q":"Block or allow pop-ups","Val":"ST","Ho":2,"Gr":1,"DeviceSignals":{"Rank":868,"PHits":"System.ParsingNa
2022-05-27 18:54:02 UTC	265	IN	HTTP/1.1 204 No Content Access-Control-Allow-Origin: * X-Cache: CONFIG_NOCACHE Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: C21A1E4AC24540C487651A4AB63B939E Ref B: FRA31EDGE0214 Ref C: 2022-05-27T18:54:02Z Date: Fri, 27 May 2022 18:54:01 GMT Connection: close

Statistics

Behavior



chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **2344**, Parent PID: **1496**

General	
Target ID:	0
Start time:	20:53:45
Start date:	27/05/2022
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://triarail-mx.w3spaces.com/
Imagebase:	0x7ff7964c0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7964FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **2740**, Parent PID: **2344**

General	
Target ID:	1
Start time:	20:53:47
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,4377966088719049101,2550601486194537045,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1964 /prefetch:8
Imagebase:	0x7ff7964c0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly