ID: 715094
Cookbook: browseurl.jbs
Time: 16:14:17
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

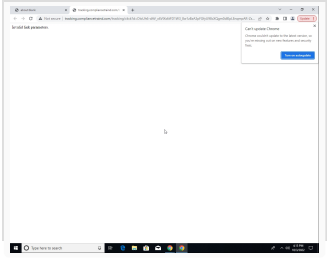
Windows Analysis Report

http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1zBzA3pFGf...

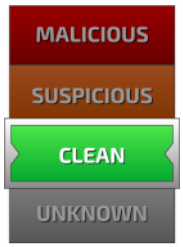
Overview

General Information

Sample URL:	tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1...-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLr
Analysis ID:	715094
Infos:	



Detection

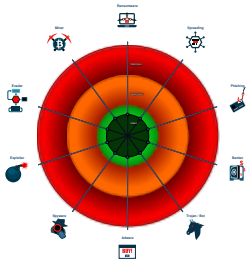


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1948 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2224 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1944 --field-trial-handle=1712,i,7630922266140671930,1016259520647040626,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4852 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wIEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQlwZtQY_eA1&d=DwMGaQ MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

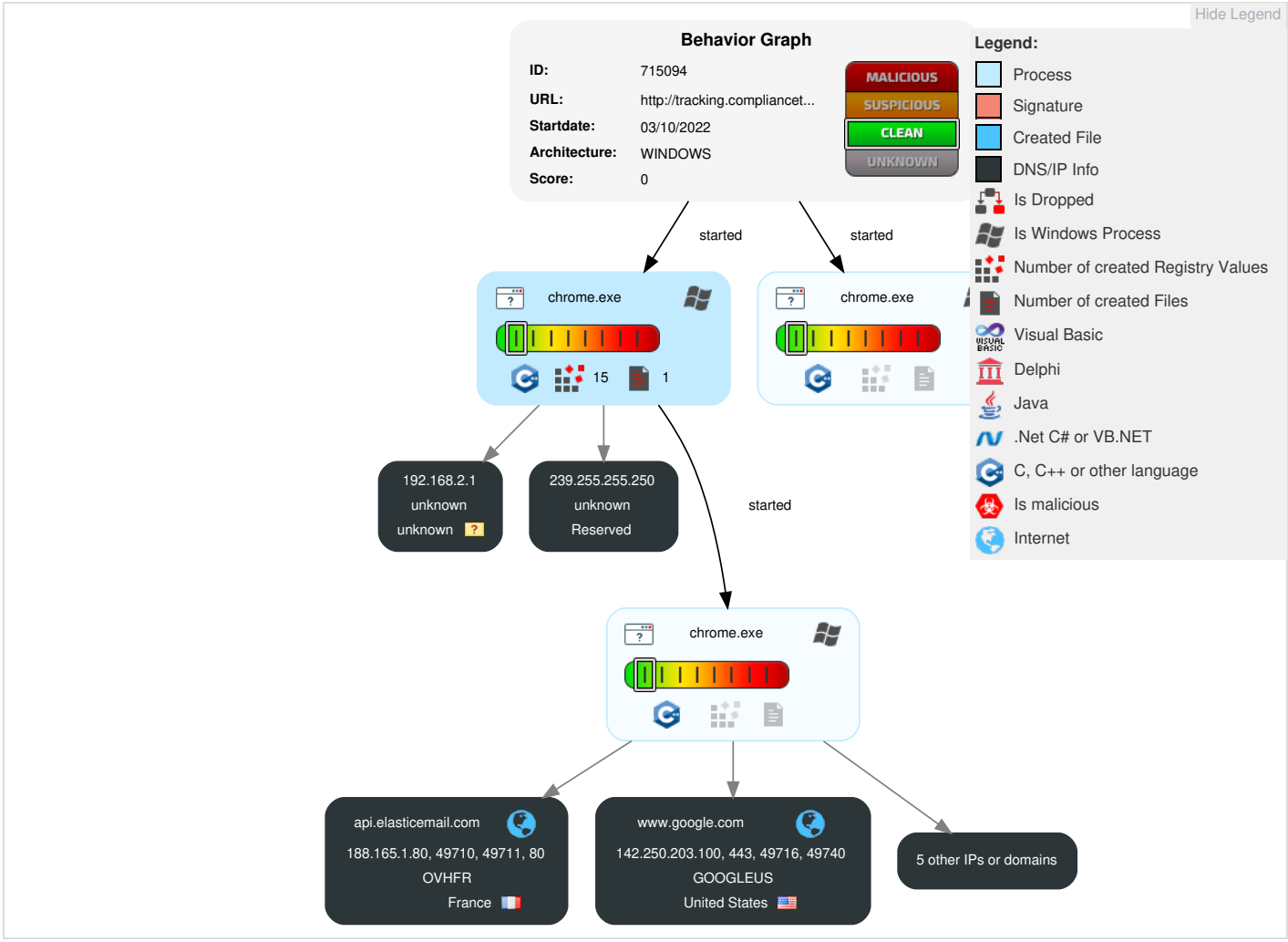
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	2 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	3 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	4 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	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

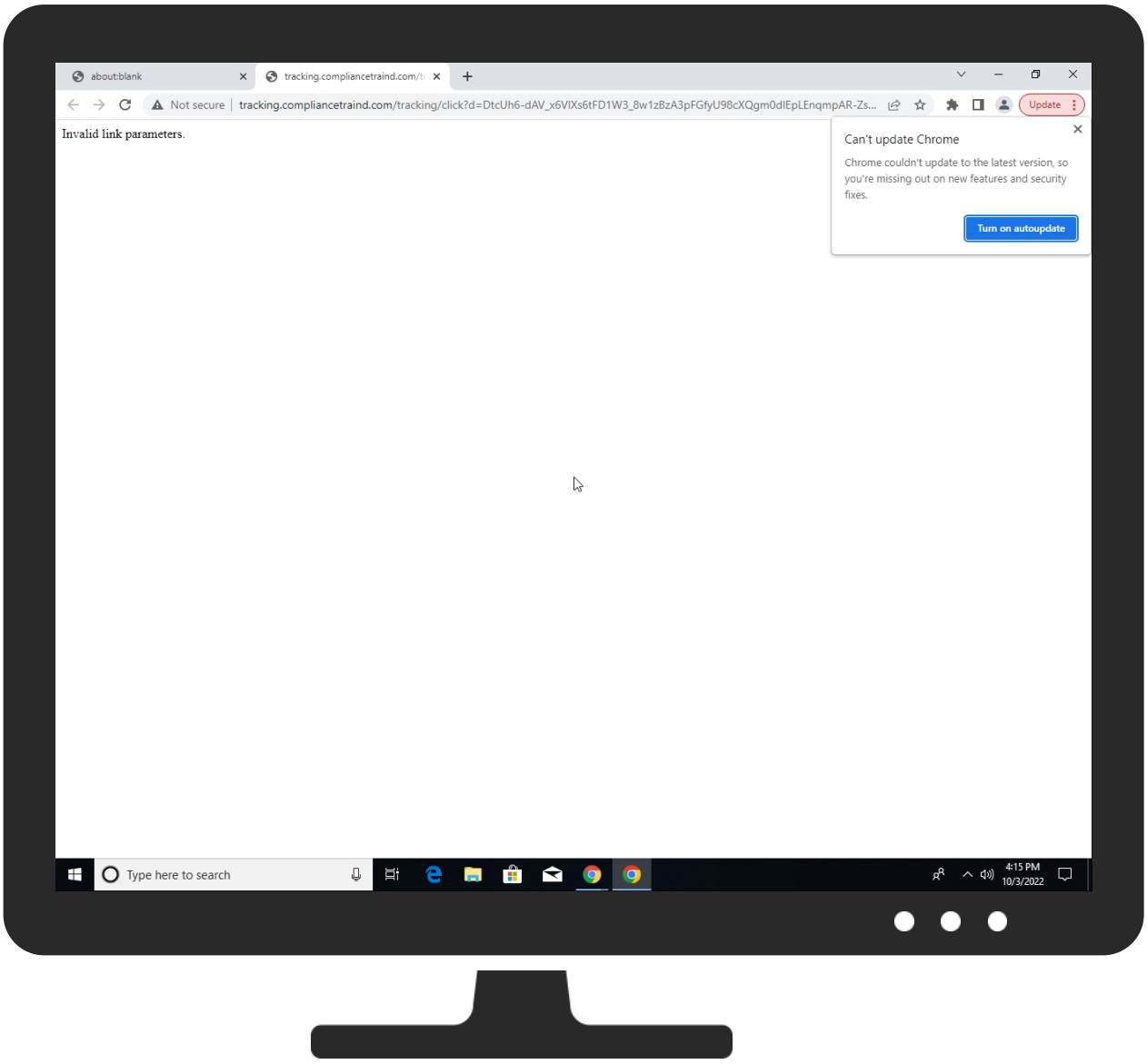
Behavior Graph



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://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VIXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQIwZtQY_eA1&d=DwMGaQ	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tracking.compliancetraind.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

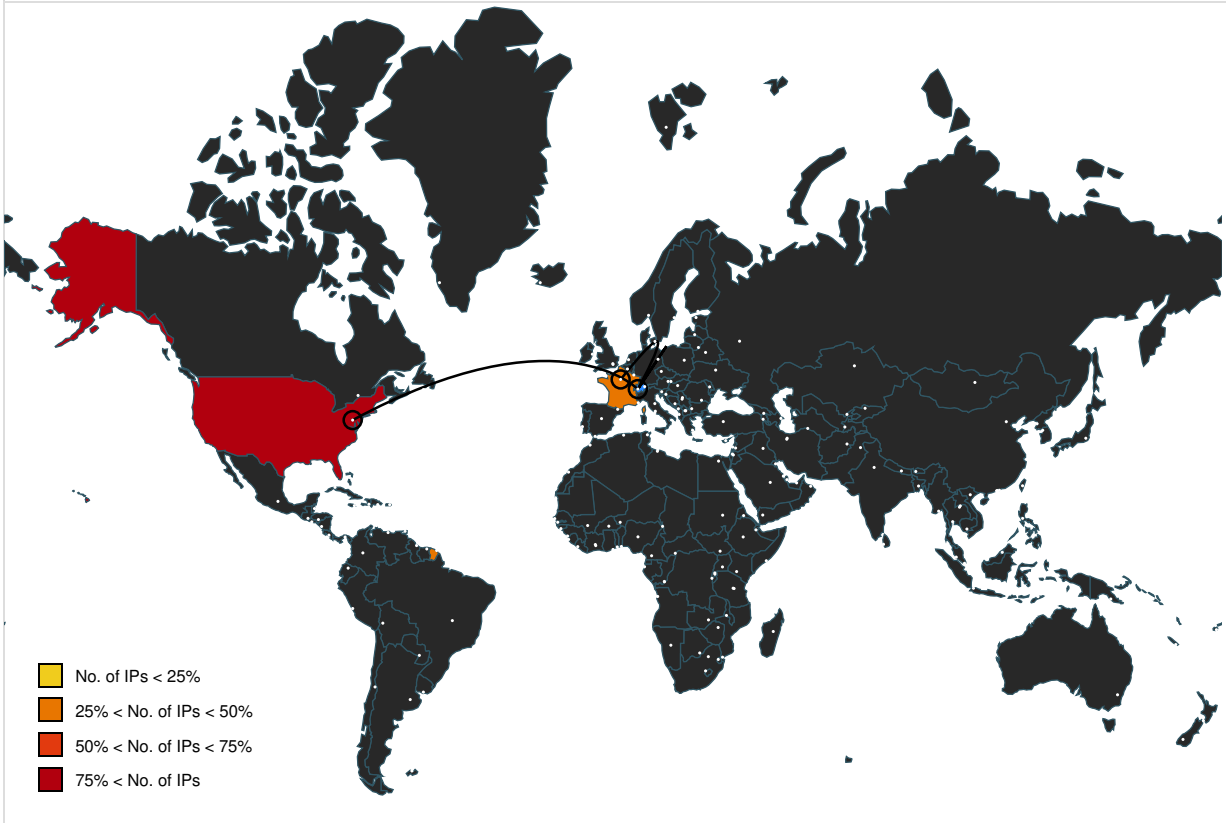
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.elasticemail.com	188.165.1.80	true	false		high
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
tracking.compliancetraind.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://tracking.compliancetraind.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VIXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdlmQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQlwZtQY_eA1&d=DwMGaQ	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VIXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdlmQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQlwZtQY_eA1&d=DwMGaQ	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
188.165.1.80	api.elasticemail.com	France		16276	OVHFR	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:	36.0.0 Rainbow Opal
Analysis ID:	715094
Start date and time:	2022-10-03 16:14:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VIXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wIEuP-Y4_gdcVIPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4PIj78AGkWhLAOfT_LrBL6FoPVQIwZtQY_eA1&d=DwMGaQ
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@24/0@5/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, edgedl.me.gvt1.com, login.live.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, arc.msn.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

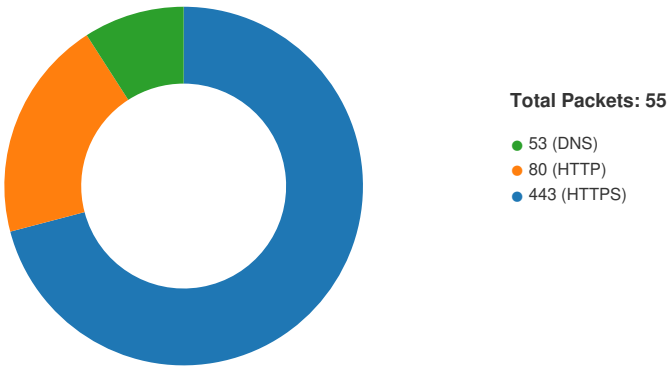
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:15.778753042 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:15.778825045 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:15.778923035 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:15.779259920 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:15.779311895 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:15.779400110 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:15.780126095 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:15.780159950 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:15.780471087 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:15.780519009 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:15.927896976 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:15.928271055 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:15.969216108 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:15.970370054 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:16.555800915 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:16.555871010 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:16.556157112 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:16.556225061 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:16.557851076 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:16.557933092 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:16.558275938 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:16.558353901 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:16.560075045 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:16.560148001 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.405853033 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.405904055 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.406337976 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.406393051 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.406411886 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.442564964 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.442706108 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.442732096 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.442755938 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.442811012 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.525677919 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:17.525762081 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.525949955 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.529723883 CEST	49708	443	192.168.2.3	142.250.203.110
Oct 3, 2022 16:15:17.529764891 CEST	443	49708	142.250.203.110	192.168.2.3
Oct 3, 2022 16:15:17.533277988 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:17.533333063 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.591794014 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.591897011 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:17.591952085 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.592197895 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.592278004 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:17.683842897 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:17.696861982 CEST	49711	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:17.697370052 CEST	49709	443	192.168.2.3	142.250.203.109
Oct 3, 2022 16:15:17.697432041 CEST	443	49709	142.250.203.109	192.168.2.3
Oct 3, 2022 16:15:17.711128950 CEST	80	49710	188.165.1.80	192.168.2.3
Oct 3, 2022 16:15:17.711297989 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:17.724101067 CEST	80	49711	188.165.1.80	192.168.2.3
Oct 3, 2022 16:15:17.724179029 CEST	49711	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:17.724962950 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:17.752522945 CEST	80	49710	188.165.1.80	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:17.955717087 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:18.042577028 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:18.072113991 CEST	80	49710	188.165.1.80	192.168.2.3
Oct 3, 2022 16:15:18.155487061 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:15:18.983203888 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:18.983247995 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:18.983326912 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:18.983697891 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:18.983722925 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.051814079 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.058005095 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:19.058054924 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.059438944 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.059611082 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:19.061773062 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:19.061808109 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.061935902 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.172872066 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:19.172902107 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:19.361439943 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:29.055571079 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:29.055701017 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:15:29.055784941 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:33.167306900 CEST	49716	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:15:33.167370081 CEST	443	49716	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:02.730037928 CEST	49711	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:16:02.757400990 CEST	80	49711	188.165.1.80	192.168.2.3
Oct 3, 2022 16:16:03.089471102 CEST	49710	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:16:03.116869926 CEST	80	49710	188.165.1.80	192.168.2.3
Oct 3, 2022 16:16:19.057466030 CEST	49711	80	192.168.2.3	188.165.1.80
Oct 3, 2022 16:16:19.058293104 CEST	49740	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:16:19.058341980 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.058410883 CEST	49740	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:16:19.060005903 CEST	49740	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:16:19.060033083 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.084745884 CEST	80	49711	188.165.1.80	192.168.2.3
Oct 3, 2022 16:16:19.113675117 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.114222050 CEST	49740	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:16:19.114270926 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.114713907 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.115300894 CEST	49740	443	192.168.2.3	142.250.203.100
Oct 3, 2022 16:16:19.115334034 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.115421057 CEST	443	49740	142.250.203.100	192.168.2.3
Oct 3, 2022 16:16:19.169048071 CEST	49740	443	192.168.2.3	142.250.203.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:15.642076015 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:15:15.644387960 CEST	56924	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:15:15.670049906 CEST	53	56924	8.8.8.8	192.168.2.3
Oct 3, 2022 16:15:15.680258036 CEST	53	52387	8.8.8.8	192.168.2.3
Oct 3, 2022 16:15:16.168637991 CEST	49302	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:15:16.212208986 CEST	53	49302	8.8.8.8	192.168.2.3
Oct 3, 2022 16:15:18.962086916 CEST	57134	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:15:18.981436014 CEST	53	57134	8.8.8.8	192.168.2.3
Oct 3, 2022 16:16:19.037903070 CEST	52547	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:16:19.055330992 CEST	53	52547	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:15.642076015 CEST	192.168.2.3	8.8.8.8	0xfb7f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:15.644387960 CEST	192.168.2.3	8.8.8.8	0xd4bc	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.168637991 CEST	192.168.2.3	8.8.8.8	0x5f9b	Standard query (0)	tracking.compliancetraind.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:18.962086916 CEST	192.168.2.3	8.8.8.8	0x6fd2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:19.037903070 CEST	192.168.2.3	8.8.8.8	0xae48	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:15.670049906 CEST	8.8.8.8	192.168.2.3	0xd4bc	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:15:15.670049906 CEST	8.8.8.8	192.168.2.3	0xd4bc	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:15.680258036 CEST	8.8.8.8	192.168.2.3	0xfb7f	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	tracking.compliancetraind.com	api.elasticemail.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	api.elasticemail.com		188.165.1.80	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	api.elasticemail.com		94.23.161.19	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	api.elasticemail.com		164.132.95.123	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	api.elasticemail.com		46.105.88.234	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:16.212208986 CEST	8.8.8.8	192.168.2.3	0x5f9b	No error (0)	api.elasticemail.com		54.38.226.140	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:18.981436014 CEST	8.8.8.8	192.168.2.3	0x6fd2	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:19.055330992 CEST	8.8.8.8	192.168.2.3	0xae48	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- tracking.compliancetraind.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49708	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49709	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49710	188.165.1.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:15:17.724962950 CEST	88	OUT	GET /tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQIwZtQY_eA1&d=DwMGaQ HTTP/1.1 Host: tracking.compliancetraind.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/104.0.0.0 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 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Oct 3, 2022 16:15:17.752522945 CEST	89	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/10.0 Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, X-ElasticEmail-ApiKey, X-ElasticEmail-BrowserToken, X-ElasticEmail-ImpersonateAs Access-Control-Expose-Headers: X-ElasticEmail-BrowserToken, X-Total-Count, X-ElasticEmail-AccessToken X-Robots-Tag: noindex, nofollow X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Mon, 03 Oct 2022 14:15:16 GMT Content-Length: 24 Data Raw: 49 6e 76 61 6c 69 64 20 6c 69 6e 6b 20 70 61 72 61 6d 65 74 65 72 73 2e Data Ascii: Invalid link parameters.
Oct 3, 2022 16:15:18.042577028 CEST	89	OUT	GET /favicon.ico HTTP/1.1 Host: tracking.compliancetraind.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Referer: http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQIwZtQY_eA1&d=DwMGaQ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Oct 3, 2022 16:15:18.072113991 CEST	90	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/10.0 Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, X-ElasticEmail-ApiKey, X-ElasticEmail-BrowserToken, X-ElasticEmail-ImpersonateAs Access-Control-Expose-Headers: X-ElasticEmail-BrowserToken, X-Total-Count, X-ElasticEmail-AccessToken X-Robots-Tag: noindex, nofollow X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Mon, 03 Oct 2022 14:15:17 GMT Content-Length: 23 Data Raw: 55 6e 61 75 74 68 6f 72 69 7a 65 64 3a 20 44 61 73 68 62 6f 61 72 64 Data Ascii: Unauthorized: Dashboard

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49711	188.165.1.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49708	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:17 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%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 X-Goog-Update-Updater: chromecrx-104.0.5112.81 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/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:17 UTC	0	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-NW5Pysy00YWGyquD5qSB9w' '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: Mon, 03 Oct 2022 14:15:17 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 26117 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"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 14:15:17 UTC	1	IN	Data Raw: 32 63 39 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 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 36 31 31 37 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: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="26117"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 14:15:17 UTC	1	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 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 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 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgm ieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a 4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 14:15:17 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

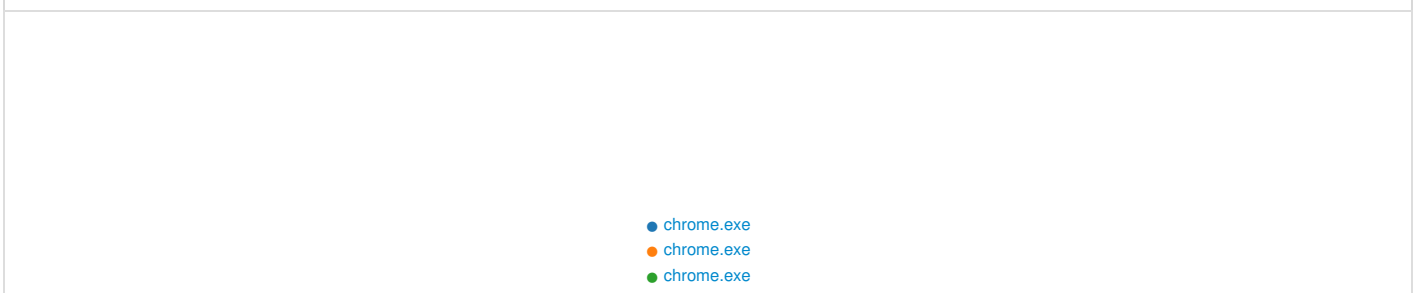
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49709	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

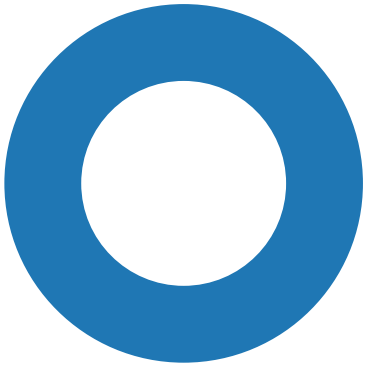
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:17 UTC	2	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/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+904; AEC=AakniGO7HqlHWlnoY-P22_SwwnNSfVGxlF1NgK5nuj5WLe313NyJi16g7z4; SOCS=CAISHAgCEhJnd3NfMjAyMjA4MDgtMF9SQzEaAmVuIAEaBgiAvOuXBg; NID=511=nUT82hOv6CVwMNqDg-sTtCMJJ6SQ1v_cCpfCpf5nt8EolEbal01GWFyjG01tqWQgh9ciRU880J6nLd2gdbhAJs44PsHAZaVQAFIbrqe2FmF gjrAAK7W9Z8u5LDvwsuZRng98jP6E23SJ4fsPIs326YmnuCwa92dRRCcB6MNeI_o
2022-10-03 14:15:17 UTC	3	OUT	Data Raw: 20 Data Ascii:
2022-10-03 14:15:17 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: Mon, 03 Oct 2022 14:15:17 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-8e6zJlSAd91Iw_9ih7De2w' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.g oogle.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allo wlist Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/rep ort-to/IdentityListAccountsHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-M odel, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" 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"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 14:15:17 UTC	4	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",[]]
2022-10-03 14:15:17 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **1948**, Parent PID: **3104**

General

Target ID:	0
Start time:	16:15:11
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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

Analysis Process: chrome.exe PID: **2224**, Parent PID: **1948**

General

Target ID:	1
Start time:	16:15:13
Start date:	03/10/2022
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 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1944 --field-trial-handle=1712,i,7630922266140671930,1016259520647040626,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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	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

Analysis Process: chrome.exe PID: **4852**, Parent PID: **3104**

General

Target ID:	2
Start time:	16:15:14
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://tracking.compliancetraind.com/tracking/click?d=DtcUh6-dAV_x6VlXs6tFD1W3_8w1zBzA3pFGfyU98cXQgm0dIEpLEnqmpAR-ZssGv0wlEuP-Y4_gdcVlPNAbZRvbiHEQTEPFT7vz8nCKVhBGhk7Dj8xCk7UFhyosgV3DnAdJKE1q1SHgLgylLrfILK4UWNFmQfjLC8x4cSpTq093Kom3AQvWS9jyD19nnWmMGAihEuA8ZmRmWrtCRUdImQ4fBj6kKXnLcS3n54fMHUSv595DV6b4Plj78AGkWhLAOfT_LrBL6FoPVQlwZtQY_eA1&d=DwMGaQ
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly