ID: 715101
Cookbook: browseurl.jbs
Time: 16:19:21
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

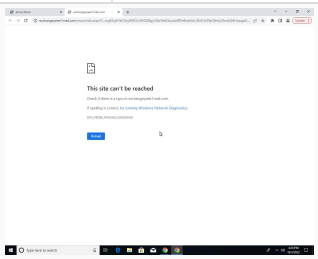
Windows Analysis Report

https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3QbVddQIcydo0B...

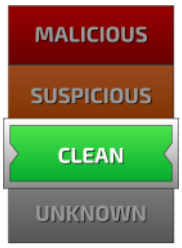
Overview

General Information

Sample URL:	https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3Qb...BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com
Analysis ID:	715101
Infos:	



Detection

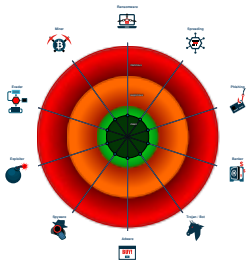


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 2864 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2884 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=1968 --field-trial-handle=1684,i,2147605262261161 70,2327631706366296599,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 748 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3QbVddQIcydo0BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

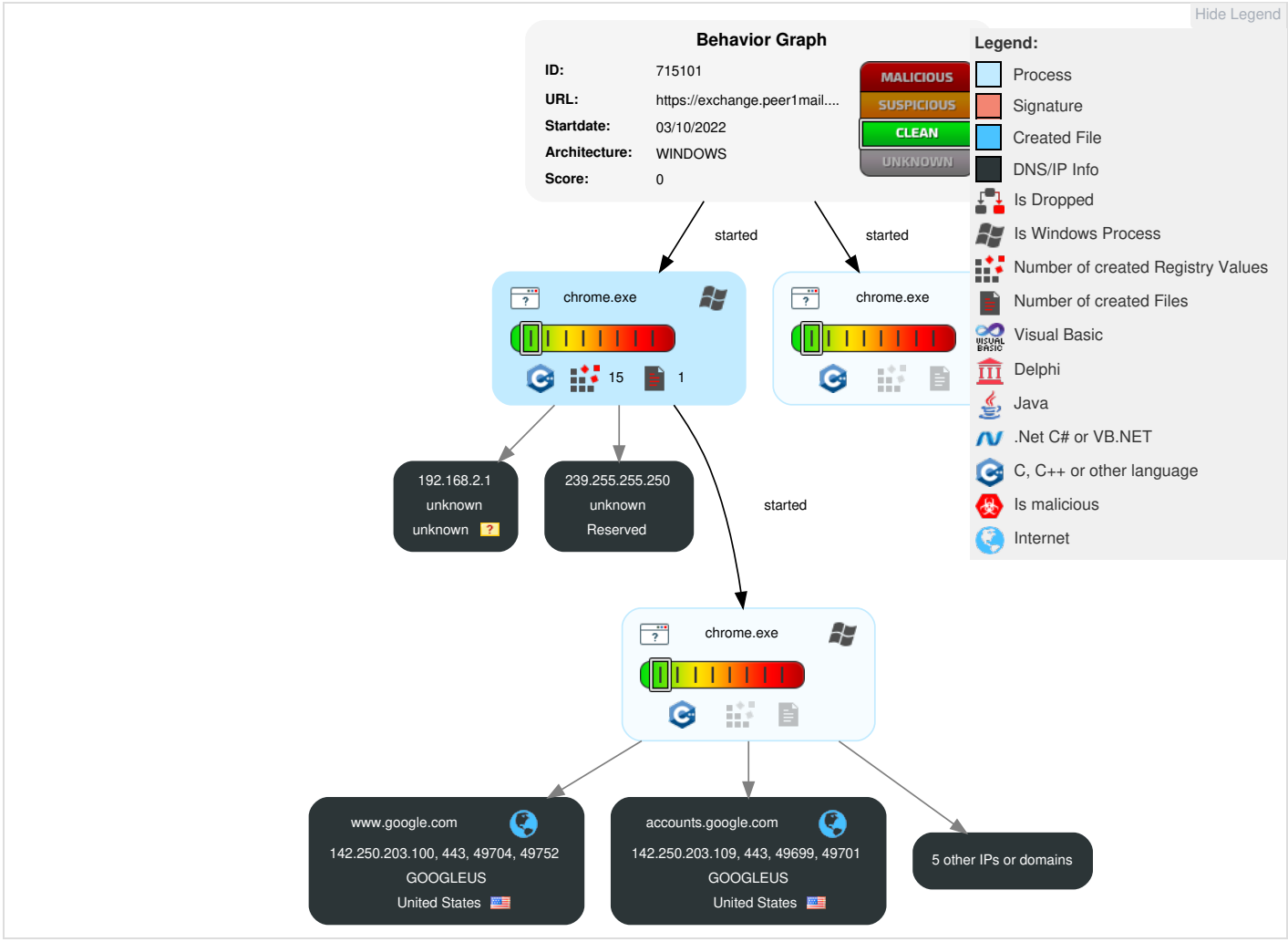
There are no malicious signatures, click here to show all signatures.

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

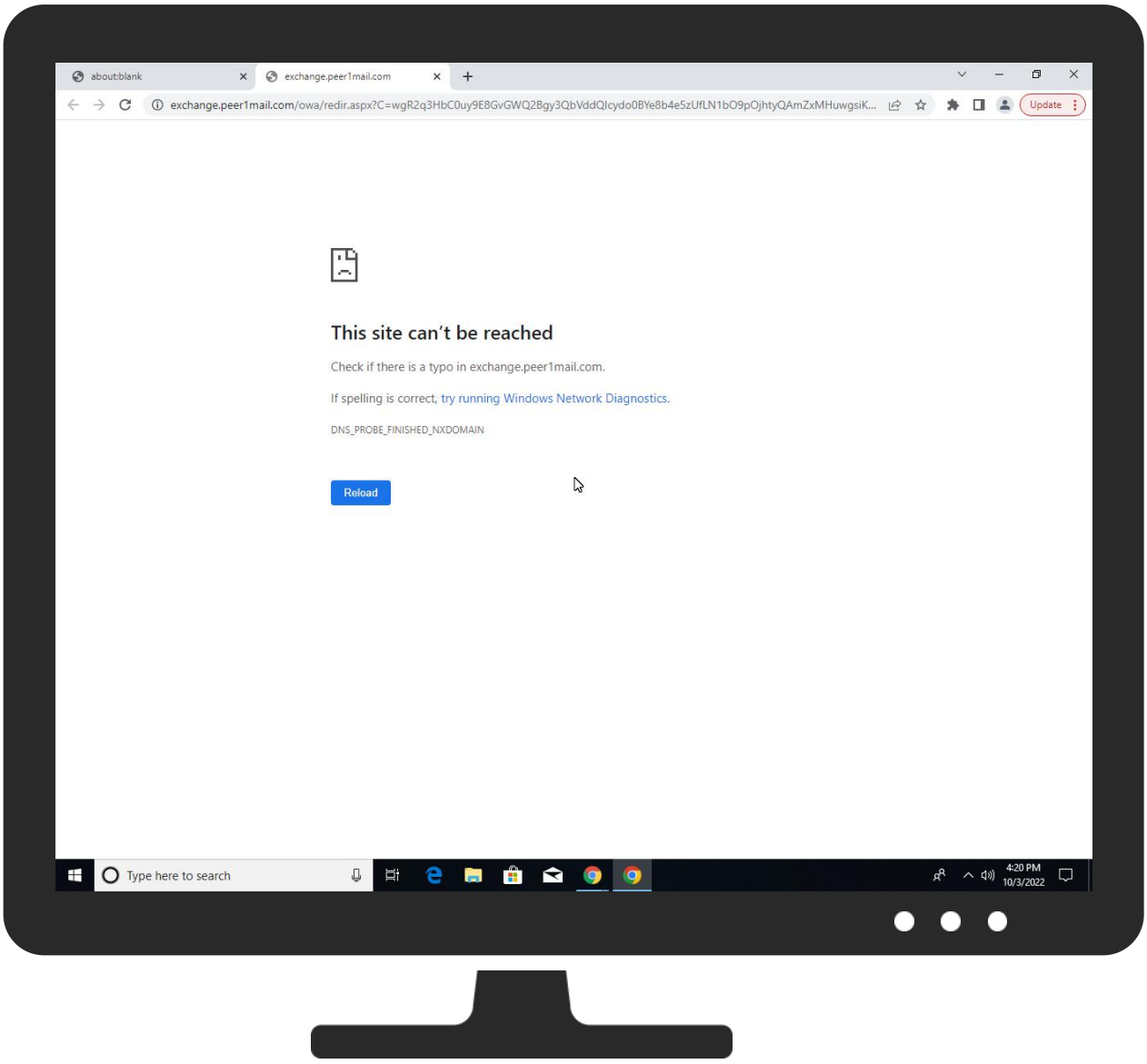
Copyright Joe Security LLC 2022



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://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3QbVddQlcydo0BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com	0%	Virustotal		Browse
http://https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3QbVddQlcydo0BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

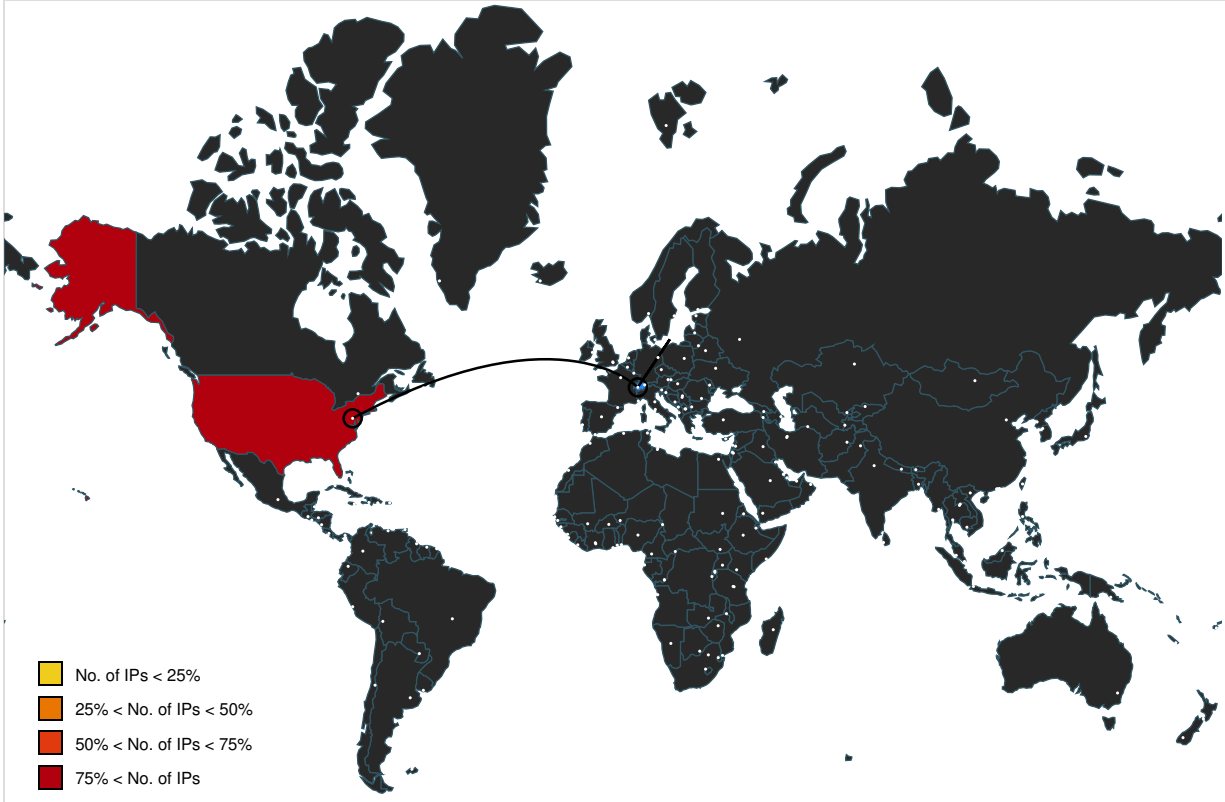
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	172.217.168.14	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
exchange.peer1mail.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://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

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
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

Copyright Joe Security LLC 2022

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715101
Start date and time:	2022-10-03 16:19:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3QbVddQIcydo0BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com
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:	5
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@30/0@9/6
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): MpCmdRun.exe, conhost.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): edgedl.me.gvt1.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.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

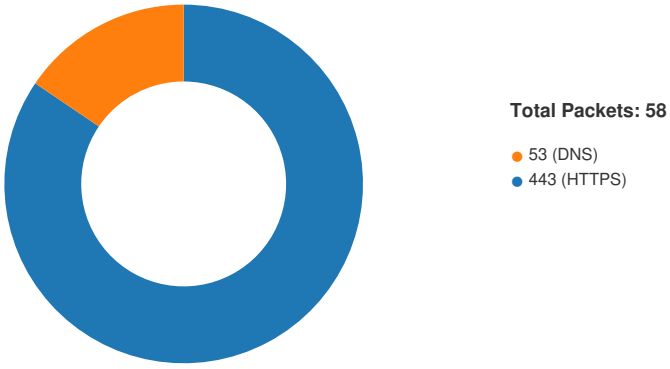
No created / dropped files found

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 16:20:24.051779032 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.051829100 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.051951885 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.053767920 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.053848028 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.053989887 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.060194016 CEST	49701	443	192.168.2.5	142.250.203.109

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:20:24.060250998 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.060343981 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.061919928 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.061943054 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.063038111 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.063128948 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.064266920 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.064296007 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.133338928 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.165659904 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.191157103 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.232955933 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.232968092 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.233134985 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.256387949 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.256407976 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.258845091 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.258898973 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.258961916 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.259130001 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.259161949 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.259751081 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.259778023 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.259900093 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.259924889 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.260004997 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.260826111 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.260929108 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.260962009 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.261513948 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.261615992 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.335514069 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.335521936 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.658035040 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.658066988 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.658158064 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.658191919 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.658246994 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.658354998 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.658482075 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.658505917 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.658624887 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.658659935 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.658668995 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.658955097 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.658970118 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.691628933 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.691787004 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.691813946 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.691879988 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.691936016 CEST	49698	443	192.168.2.5	142.250.203.110
Oct 3, 2022 16:20:24.713380098 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.713491917 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.713524103 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.713629007 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.713707924 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.733463049 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.733503103 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.840573072 CEST	49698	443	192.168.2.5	142.250.203.110

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:20:24.840615988 CEST	443	49698	142.250.203.110	192.168.2.5
Oct 3, 2022 16:20:24.842269897 CEST	49699	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:24.842303991 CEST	443	49699	142.250.203.109	192.168.2.5
Oct 3, 2022 16:20:24.933002949 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:20:25.543442965 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.543503046 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.543601990 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.543943882 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.543970108 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.608477116 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.609059095 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.609102964 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.611253977 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.611355066 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.613387108 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.613409996 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.613637924 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.658992052 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:25.659014940 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:25.758991003 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:35.583921909 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:35.584045887 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:20:35.584132910 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:37.342545986 CEST	49704	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:20:37.342590094 CEST	443	49704	142.250.203.100	192.168.2.5
Oct 3, 2022 16:21:09.748512030 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:21:09.748539925 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:21:25.175247908 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:21:25.175491095 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:21:25.175936937 CEST	443	49701	142.250.203.109	192.168.2.5
Oct 3, 2022 16:21:25.176187992 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:21:25.176187992 CEST	49701	443	192.168.2.5	142.250.203.109
Oct 3, 2022 16:21:25.545409918 CEST	49752	443	192.168.2.5	142.250.203.100
Oct 3, 2022 16:21:25.545455933 CEST	443	49752	142.250.203.100	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:20:23.419025898 CEST	61893	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:23.421101093 CEST	60649	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:23.438765049 CEST	49177	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:23.441421032 CEST	53	61893	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:23.449239016 CEST	53	60649	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:23.456290960 CEST	53	49177	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:24.841840029 CEST	61452	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:24.843733072 CEST	65323	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:24.859486103 CEST	53	61452	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:24.883538961 CEST	53	65323	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:25.484333992 CEST	56751	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:25.503818035 CEST	53	56751	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:25.737596989 CEST	55039	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:25.759984016 CEST	53	55039	8.8.8.8	192.168.2.5
Oct 3, 2022 16:20:30.830960989 CEST	55068	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:20:30.853333950 CEST	53	55068	8.8.8.8	192.168.2.5
Oct 3, 2022 16:21:00.953989983 CEST	61344	53	192.168.2.5	8.8.8.8
Oct 3, 2022 16:21:00.974195957 CEST	53	61344	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:20:23.419025898 CEST	192.168.2.5	8.8.8.8	0x97ec	Standard query (0)	exchange.peer1mail.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:23.421101093 CEST	192.168.2.5	8.8.8.8	0x8c3a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:23.438765049 CEST	192.168.2.5	8.8.8.8	0xc44e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:24.841840029 CEST	192.168.2.5	8.8.8.8	0x9acf	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:24.843733072 CEST	192.168.2.5	8.8.8.8	0x6d32	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:25.484333992 CEST	192.168.2.5	8.8.8.8	0x998b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:25.737596989 CEST	192.168.2.5	8.8.8.8	0x43aa	Standard query (0)	exchange.peer1mail.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:30.830960989 CEST	192.168.2.5	8.8.8.8	0xa1fe	Standard query (0)	exchange.peer1mail.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:21:00.953989983 CEST	192.168.2.5	8.8.8.8	0x4ff5	Standard query (0)	exchange.peer1mail.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 16:20:23.441421032 CEST	8.8.8.8	192.168.2.5	0x97ec	Name error (3)	exchange.peer1mail.com	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:23.449239016 CEST	8.8.8.8	192.168.2.5	0x8c3a	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:23.456290960 CEST	8.8.8.8	192.168.2.5	0xc44e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:20:23.456290960 CEST	8.8.8.8	192.168.2.5	0xc44e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:24.859486103 CEST	8.8.8.8	192.168.2.5	0x9acf	No error (0)	google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:24.883538961 CEST	8.8.8.8	192.168.2.5	0x6d32	No error (0)	google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:25.503818035 CEST	8.8.8.8	192.168.2.5	0x998b	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:25.759984016 CEST	8.8.8.8	192.168.2.5	0x43aa	Name error (3)	exchange.peer1mail.com	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:20:30.853333950 CEST	8.8.8.8	192.168.2.5	0xa1fe	Name error (3)	exchange.peer1mail.com	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:21:00.974195957 CEST	8.8.8.8	192.168.2.5	0x4ff5	Name error (3)	exchange.peer1mail.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49699	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:20:24 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/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:20:24 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-10-03 14:20:24 UTC	2	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 14:20:24 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-slJLjbT4dUTD-cSvEIqnUw' '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.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist 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-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* 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-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} 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
2022-10-03 14:20:24 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 14:20:24 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

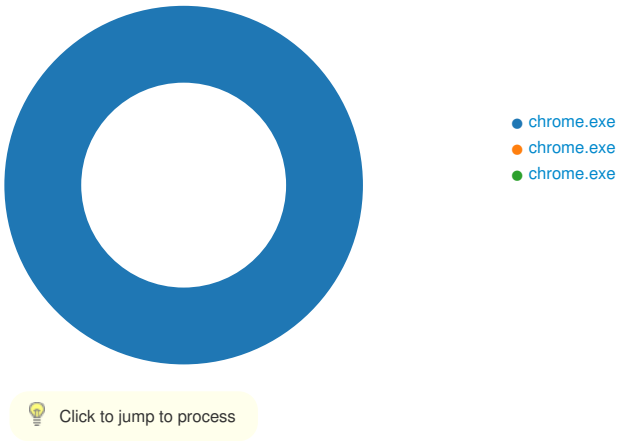
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49698	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:20:24 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

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:20:24 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-qAeFj--oiOXtK19BNsBCVQ' '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 14:20:24 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 26424 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 14:20:24 UTC	2	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 34 32 34 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="26424"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 14:20:24 UTC	2	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 14:20:24 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2864**, Parent PID: **3924**

General

Target ID:	0
Start time:	16:20:18
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:	0x7ff7d31b0000
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: **2884**, Parent PID: **2864**

General

Target ID:	1
Start time:	16:20:19
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=1968 --field-trial-handle=1684,i,2147605262261161 70,2327631706366296599,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
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: **748**, Parent PID: **3924**

General	
Target ID:	2
Start time:	16:20:20
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" "https://exchange.peer1mail.com/owa/redir.aspx?C=wgR2q3HbC0uy9E8GvGWQ2Bgy3Q bVddQIcydo0BYe8b4e5zUfLN1bO9pOjhtyQAmZxMHuwgsiKX8.&URL=http%3a%2f%2fwww.pay2global.com
Imagebase:	0x7ff7d31b0000
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