ID: 715050
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 15:28:56
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

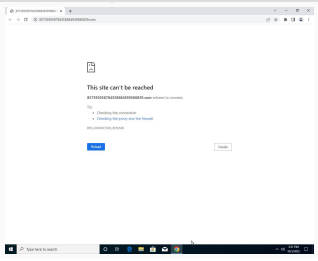
Windows Analysis Report

http://857393058784358684939586839.com

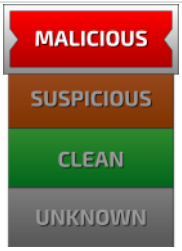
Overview

General Information

Sample URL:	http://857393058784358684939586839.com
Analysis ID:	715050
Infos:	



Detection

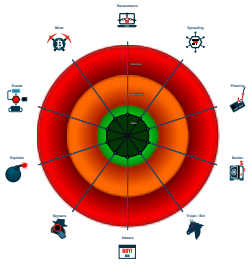


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6128 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://857393058784358684939586839.com/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 3680 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=2040 --field-trial-handle=1792,i,17993609517420769768,3007672708723663153,131072 --disable-features =OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **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

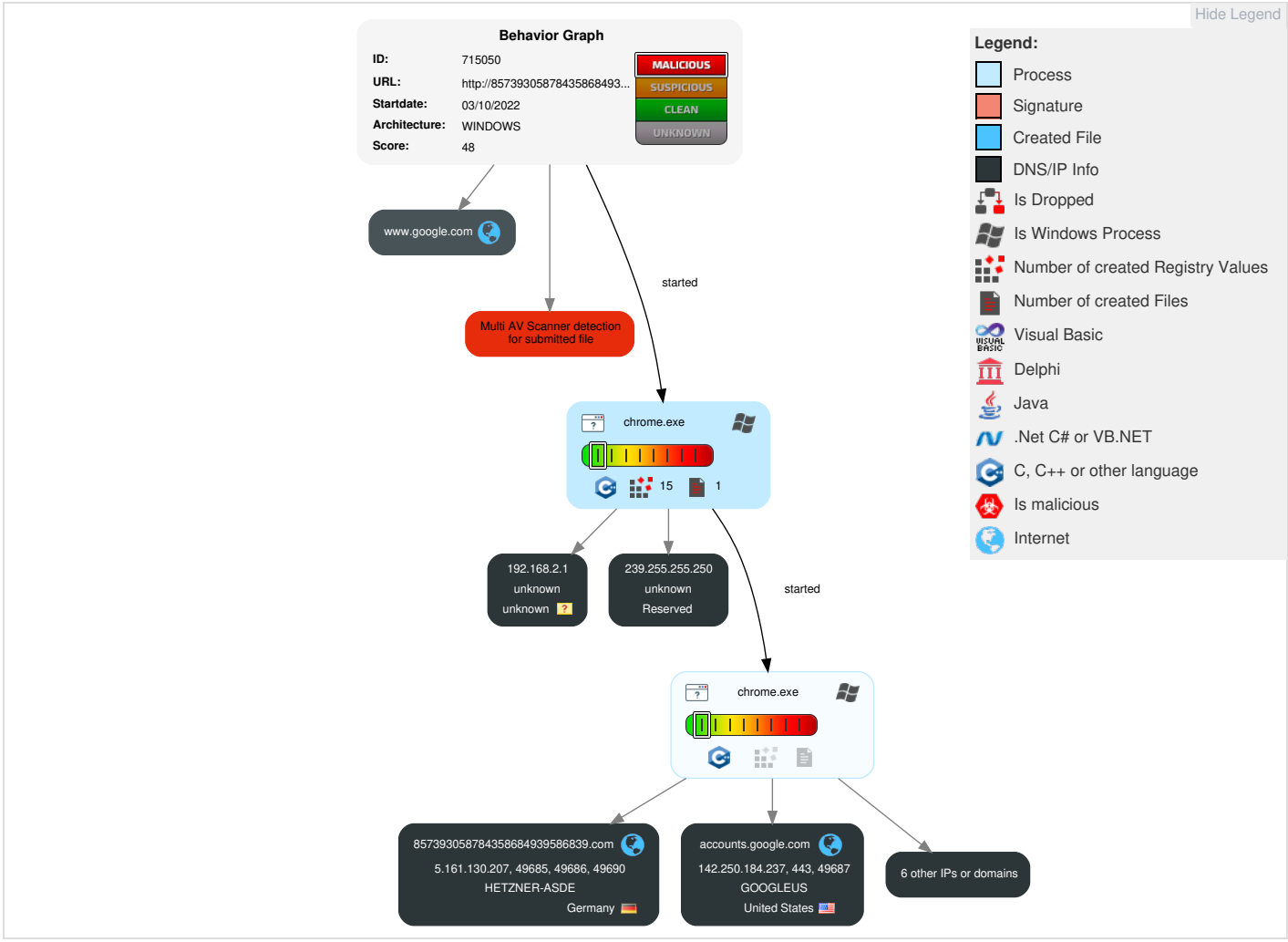
AV Detection

Multi AV Scanner detection for submitted file

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

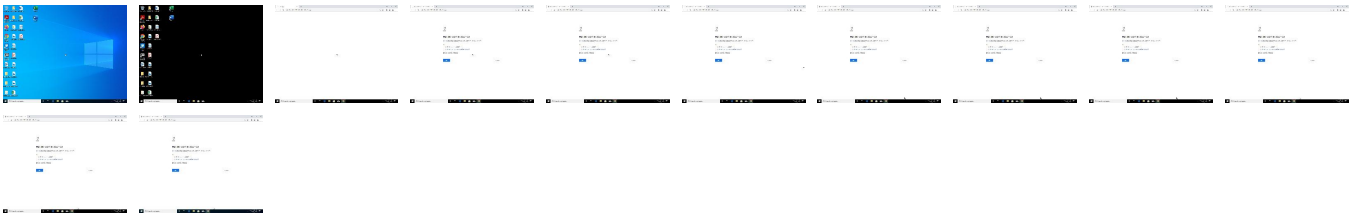
Behavior Graph

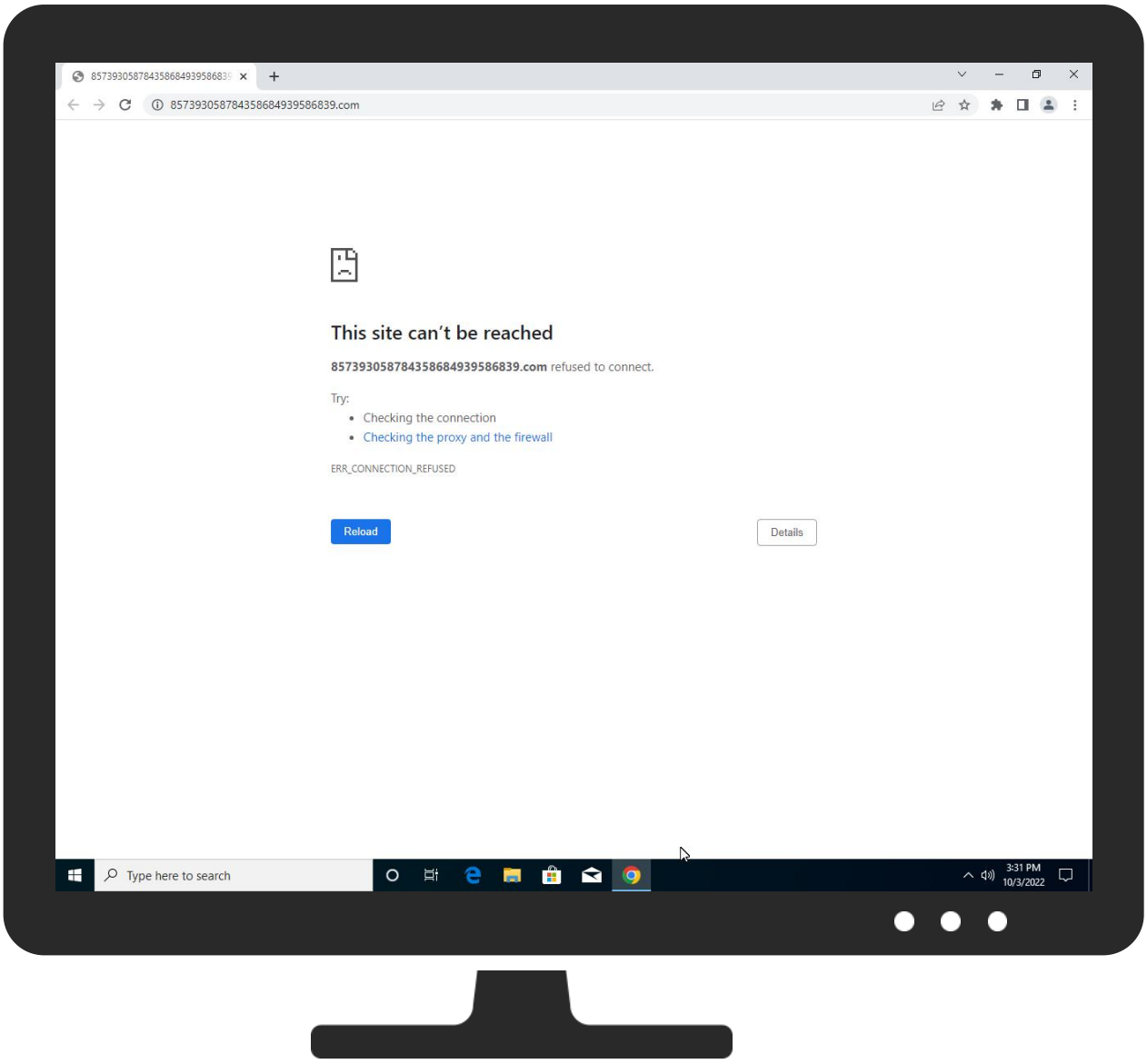


Screenshots

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://857393058784358684939586839.com	11%	Virustotal		Browse
http://857393058784358684939586839.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

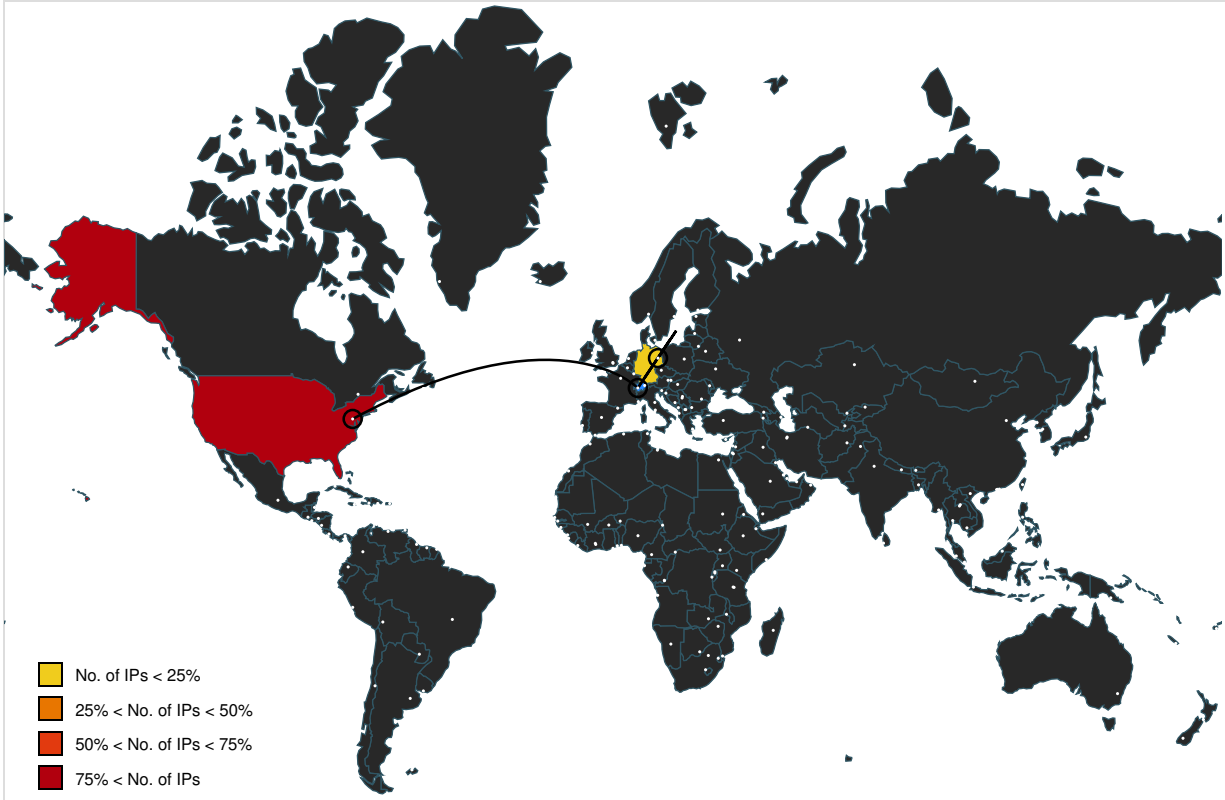
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.237	true	false		high
www.google.com	172.217.16.132	true	false		high
clients.l.google.com	172.217.18.14	true	false		high
85739305878435868493958683 9.com	5.161.130.207	true	false		unknown
clients2.google.com	unknown	unknown	false		high

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=104.0.5112.102&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
142.250.186.68	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.18.14	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.186.132	unknown	United States		15169	GOOGLEUS	false
5.161.130.207	85739305878435868493958683 9.com	Germany		24940	HETZNER-ASDE	false

Private

IP
192.168.2.1
127.0.0.1

IP

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715050
Start date and time:	2022-10-03 15:28:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://857393058784358684939586839.com
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	12
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:	mal48.win@32/0@10/8
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): SgrmBroker.exe, usocoreworker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.159.0, 20.190.159.64, 20.190.159.2, 20.190.159.4, 20.190.159.23, 40.126.31.73, 40.126.31.69, 20.190.159.73, 142.250.186.163, 34.104.35.123, 142.250.185.99
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prda.aadg.msidentity.com, edgedl.me.gvt1.com, login.live.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- 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

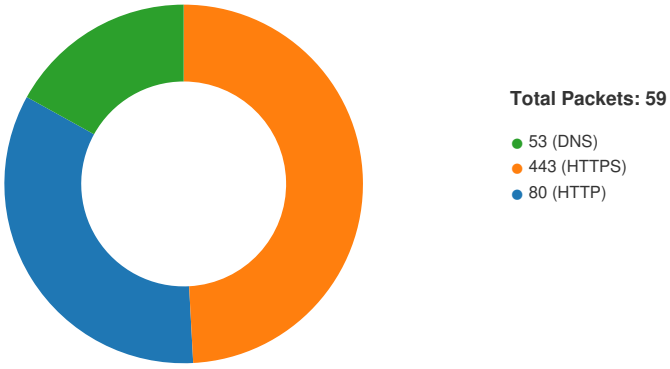
No created / dropped files found

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 15:29:25.373655081 CEST	49685	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:25.374178886 CEST	49686	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:25.382494926 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.382560968 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.382714033 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.383152962 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.383179903 CEST	443	49689	172.217.18.14	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:29:25.383243084 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.401318073 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.401344061 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.401915073 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.401964903 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.481059074 CEST	80	49685	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:25.484199047 CEST	80	49686	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:25.518209934 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.521816969 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.533040047 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.533061981 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.533257961 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.533299923 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.533682108 CEST	49690	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:25.533832073 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.533932924 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.535542011 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.535639048 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.535665035 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.535783052 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.640825033 CEST	80	49690	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:25.867151022 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.867171049 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.867475033 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.868129015 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.868185043 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.868314981 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.868330956 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.868431091 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.868834972 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.868869066 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.902055979 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.902230024 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.902250051 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.902328014 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.902431011 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.909449100 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.915810108 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.916182995 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.916277885 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.944514036 CEST	49687	443	192.168.2.3	142.250.184.237
Oct 3, 2022 15:29:25.944562912 CEST	443	49687	142.250.184.237	192.168.2.3
Oct 3, 2022 15:29:25.959943056 CEST	49689	443	192.168.2.3	172.217.18.14
Oct 3, 2022 15:29:25.959964991 CEST	443	49689	172.217.18.14	192.168.2.3
Oct 3, 2022 15:29:25.981476068 CEST	49685	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:25.984447002 CEST	49686	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:26.088609934 CEST	80	49685	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:26.094590902 CEST	80	49686	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:26.142478943 CEST	49690	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:26.249495983 CEST	80	49690	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:26.588666916 CEST	49685	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:26.595529079 CEST	49686	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:26.696041107 CEST	80	49685	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:26.706114054 CEST	80	49686	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:26.750720024 CEST	49690	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:26.857935905 CEST	80	49690	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:27.196732998 CEST	49685	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:27.207585096 CEST	49686	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:27.304114103 CEST	80	49685	5.161.130.207	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:29:27.318110943 CEST	80	49686	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:27.358669996 CEST	49690	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:27.465890884 CEST	80	49690	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:27.805737972 CEST	49685	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:27.819713116 CEST	49686	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:27.913227081 CEST	80	49685	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:27.930357933 CEST	80	49686	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:27.966646910 CEST	49690	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:28.074064016 CEST	80	49690	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:28.936947107 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:28.937026024 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:28.937140942 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:28.937428951 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:28.937458038 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:28.963128090 CEST	49699	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:28.967551947 CEST	49700	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:29.004170895 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.005069971 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:29.005137920 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.006331921 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.006457090 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:29.008521080 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:29.008547068 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.008672953 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.049766064 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:29.049818039 CEST	443	49698	142.250.186.68	192.168.2.3
Oct 3, 2022 15:29:29.070013046 CEST	80	49699	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:29.077758074 CEST	80	49700	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:29.091809988 CEST	49698	443	192.168.2.3	142.250.186.68
Oct 3, 2022 15:29:29.216371059 CEST	49702	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:29.323290110 CEST	80	49702	5.161.130.207	192.168.2.3
Oct 3, 2022 15:29:29.570760965 CEST	49699	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:29.578829050 CEST	49700	80	192.168.2.3	5.161.130.207
Oct 3, 2022 15:29:29.677803040 CEST	80	49699	5.161.130.207	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:29:25.279970884 CEST	58725	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:29:25.281572104 CEST	60153	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:29:25.283171892 CEST	56653	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:29:25.298841000 CEST	53	60153	1.1.1.1	192.168.2.3
Oct 3, 2022 15:29:25.301059961 CEST	53	56653	1.1.1.1	192.168.2.3
Oct 3, 2022 15:29:25.310689926 CEST	53	58725	1.1.1.1	192.168.2.3
Oct 3, 2022 15:29:28.881680012 CEST	52116	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:29:28.899502039 CEST	53	52116	1.1.1.1	192.168.2.3
Oct 3, 2022 15:29:28.916841984 CEST	52642	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:29:28.935511112 CEST	53	52642	1.1.1.1	192.168.2.3
Oct 3, 2022 15:30:28.942328930 CEST	60975	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:30:28.962332010 CEST	53	60975	1.1.1.1	192.168.2.3
Oct 3, 2022 15:30:28.966101885 CEST	50566	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:30:28.983422041 CEST	53	50566	1.1.1.1	192.168.2.3
Oct 3, 2022 15:31:12.110995054 CEST	62540	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:31:12.281361103 CEST	53	62540	1.1.1.1	192.168.2.3
Oct 3, 2022 15:31:28.994138002 CEST	65113	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:31:29.012002945 CEST	53	65113	1.1.1.1	192.168.2.3
Oct 3, 2022 15:31:29.017400980 CEST	63929	53	192.168.2.3	1.1.1.1
Oct 3, 2022 15:31:29.035084009 CEST	53	63929	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:29:25.279970884 CEST	192.168.2.3	1.1.1.1	0x2fb3	Standard query (0)	8573930587 8435868493 9586839.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:25.281572104 CEST	192.168.2.3	1.1.1.1	0x8cf6	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:25.283171892 CEST	192.168.2.3	1.1.1.1	0xc998	Standard query (0)	accounts.g oogle.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:28.881680012 CEST	192.168.2.3	1.1.1.1	0x9c0d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:28.916841984 CEST	192.168.2.3	1.1.1.1	0x5a85	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:30:28.942328930 CEST	192.168.2.3	1.1.1.1	0xa9a8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:30:28.966101885 CEST	192.168.2.3	1.1.1.1	0xc721	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:12.110995054 CEST	192.168.2.3	1.1.1.1	0xca15	Standard query (0)	8573930587 8435868493 9586839.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:28.994138002 CEST	192.168.2.3	1.1.1.1	0x6ad8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:29.017400980 CEST	192.168.2.3	1.1.1.1	0xc29a	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 15:29:25.298841000 CEST	1.1.1.1	192.168.2.3	0x8cf6	No error (0)	clients2.g oogle.com	clients.l.google .com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 15:29:25.298841000 CEST	1.1.1.1	192.168.2.3	0x8cf6	No error (0)	clients.l. google.com		172.217.18.14	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:25.301059961 CEST	1.1.1.1	192.168.2.3	0xc998	No error (0)	accounts.g oogle.com		142.250.184.2 37	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:25.310689926 CEST	1.1.1.1	192.168.2.3	0x2fb3	No error (0)	8573930587 8435868493 9586839.com		5.161.130.207	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:28.899502039 CEST	1.1.1.1	192.168.2.3	0x9c0d	No error (0)	www.google .com		172.217.16.13 2	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:29:28.935511112 CEST	1.1.1.1	192.168.2.3	0x5a85	No error (0)	www.google .com		142.250.186.6 8	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:30:28.962332010 CEST	1.1.1.1	192.168.2.3	0xa9a8	No error (0)	www.google .com		142.250.186.1 32	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:30:28.983422041 CEST	1.1.1.1	192.168.2.3	0xc721	No error (0)	www.google .com		142.250.186.1 32	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:12.281361103 CEST	1.1.1.1	192.168.2.3	0xca15	No error (0)	8573930587 8435868493 9586839.com		5.161.130.207	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:29.012002945 CEST	1.1.1.1	192.168.2.3	0x6ad8	No error (0)	www.google .com		142.250.186.1 32	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:31:29.035084009 CEST	1.1.1.1	192.168.2.3	0xc29a	No error (0)	www.google .com		172.217.16.13 2	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49689	172.217.18.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:29:25 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=104.0.5112.102&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-104.0.5112.102 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 13:29:25 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-LhCw9XC2ia1vYPZpakrH4A' '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 13:29:25 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 23365 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 13:29:25 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 33 33 36 35 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="23365"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 13:29:25 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 13:29:25 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

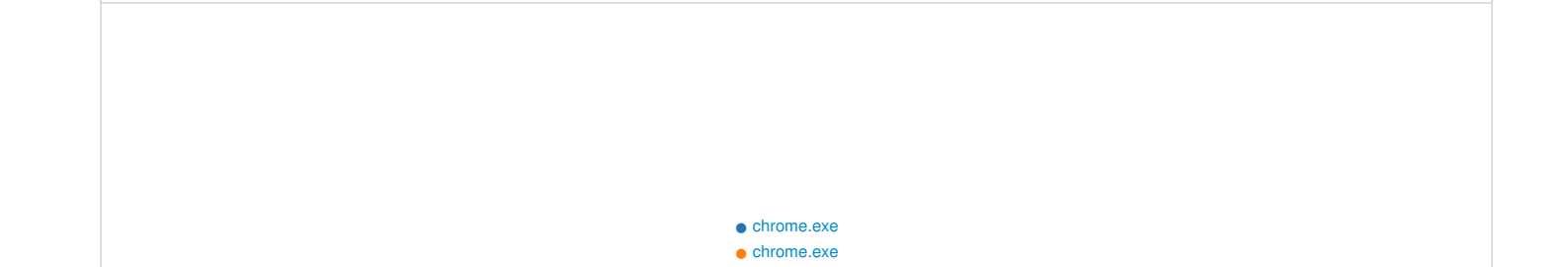
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49687	142.250.184.237	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:29:25 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 Cookie: CONSENT=PENDING+620; __Secure-ENID=6.SE=cJKCBuSaL1dV3R8z2Y2aI7-m2m5bGA74lqbYYkqC3uy-NtZ1f6n_bCBr25tlnnjvdmLpGQ81ZKzP3Te5vVjpSQjYWCwvlOMApK7tmZNWcORu0p4wniPJGQfTslQNnpQWhG9q kwkEgy49-6UG3UQ1eiUyFolJZWLeUM1p4KvjM9E
2022-10-03 13:29:25 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-10-03 13:29:25 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 13:29:25 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-Ghoy5wDAVxteVz3jYeftsw' '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 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" 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"; 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 13:29:25 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 13:29:25 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: **6128**, Parent PID: **2516**

General

Target ID:	0
Start time:	15:29:22
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 --single-argument http://857393058784358684939586839.com/
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: **3680**, Parent PID: **6128**

General	
Target ID:	1
Start time:	15:29:23
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=2040 --field-trial-handle=1792,i,17993609517420769768,3007672708723663153,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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.

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