ID: 791888
Cookbook: browseurl.jbs
Time: 23:35:21
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

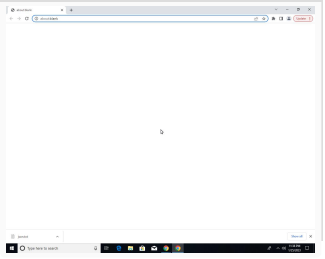
Windows Analysis Report

http://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwC...

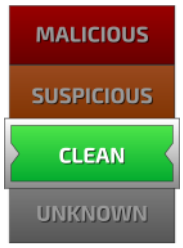
Overview

General Information

Sample URL:	clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvR...g&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Analysis ID:	791888
Infos:	



Detection

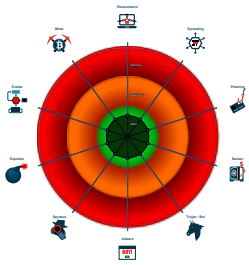


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5272 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5444 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=1740 --field-trial-handle=1860,i,9632146488442511452,3354182686509041322,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5692 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 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

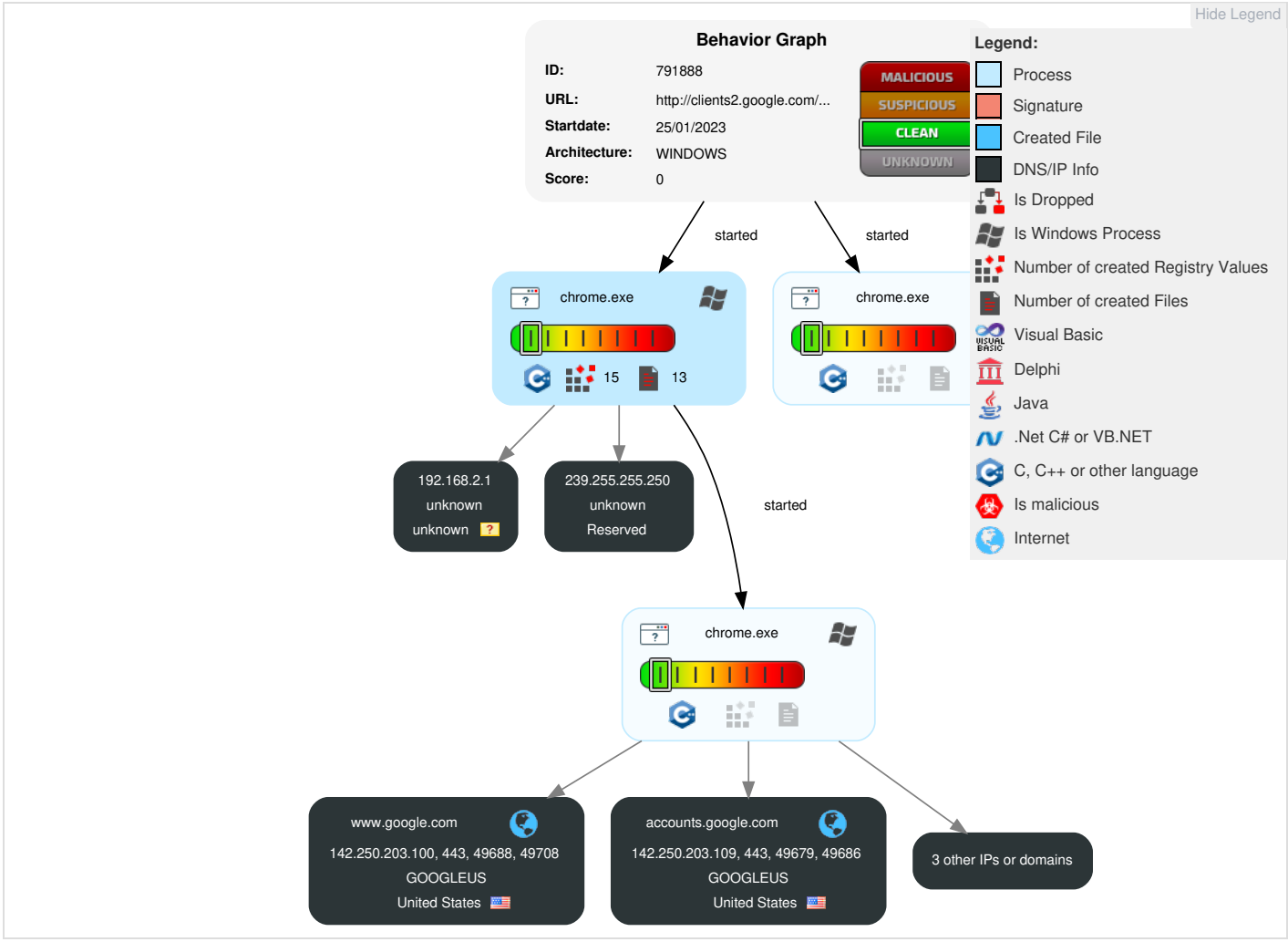
Joe Sandbox Signatures

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	3 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

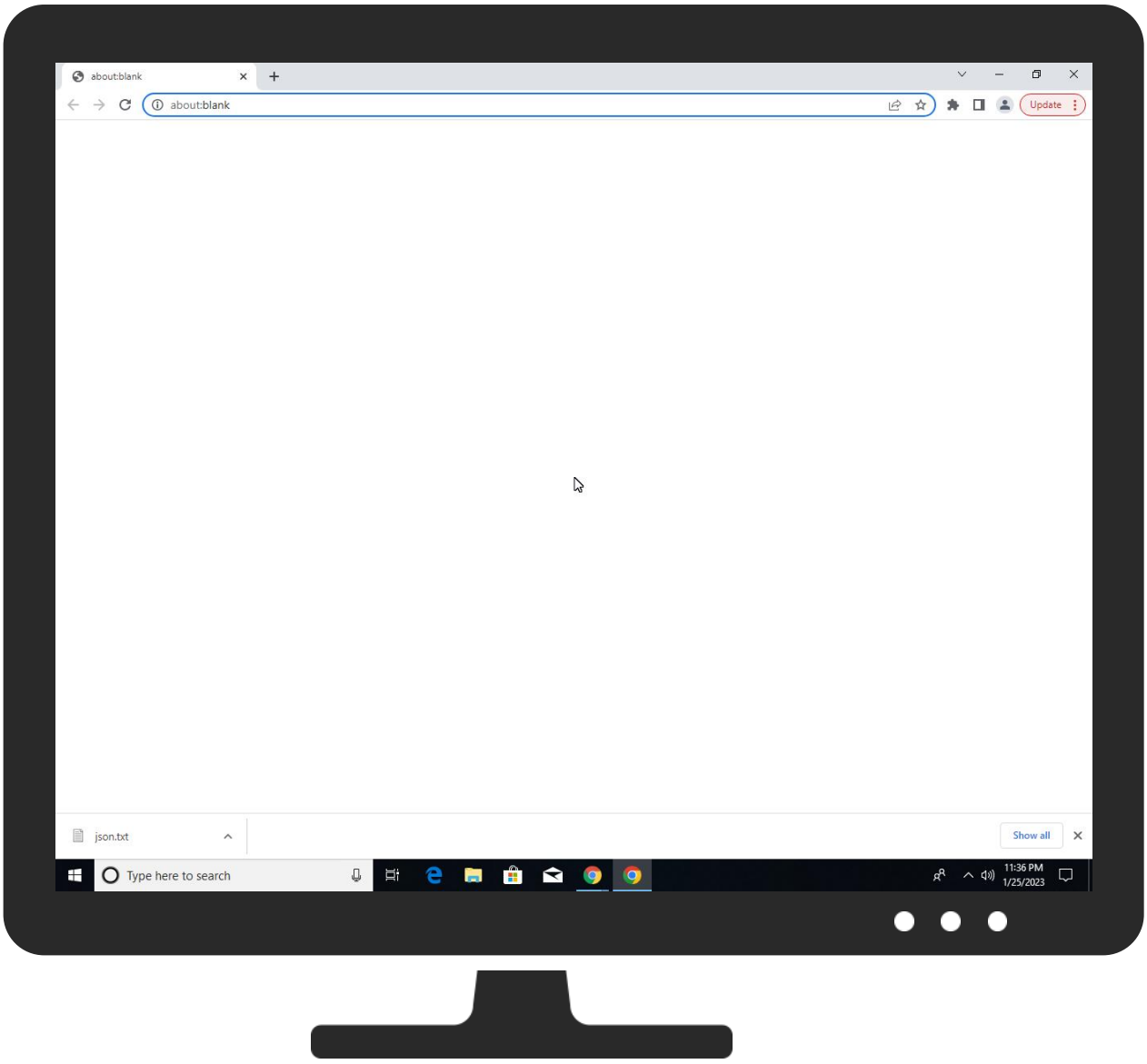
Behavior Graph



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://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	0%	Virustotal		Browse
http://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	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

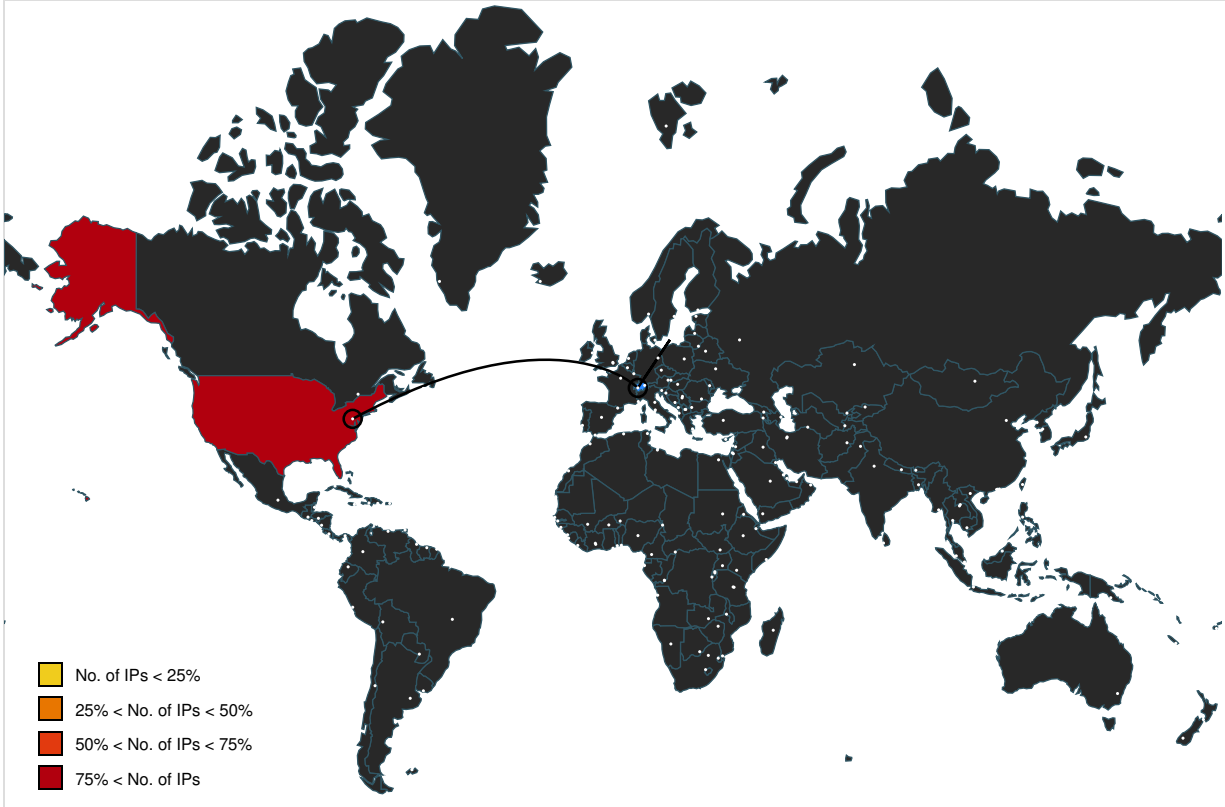
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	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

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://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	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

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791888
Start date and time:	2023-01-25 23:35:21 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@26/3@4/6
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): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.35.236.109, 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, edgedl.me.gvt1.com, e16604.g.akamaiedge.net, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.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

C:\Users\user\Downloads\6d9bc226-77cc-44fa-85f1-07543759e5b4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	79
Entropy (8bit):	4.928727704087349
Encrypted:	false
SSDEEP:	3:VQ3X4l1Wce1R6JHDlQXfMhWRXJo/XAn:VQ3e1WujeXEWxC4n
MD5:	56415F32FE2800C44E70C685DDF51273
SHA1:	08231AB77735BBFAA25BB43016000A04A69D7EC8
SHA-256:	F8B979F3CC1930EA1BC0759EDF600B4346ED5E3604B30738986603B3179C6349
SHA-512:	AF39B478A5A9D62F57B4D3C9EF77A54B88B2A09DADF381C077AF20FCB18E022BDEF79AFC33CBD9CDE86EF71E541A1A6DD8D7D017F5E7730C794E00CC7FE7 3B6
Malicious:	false
Reputation:	low
Preview:	)]}'.{"current_time_millis":1674686193248,"server_nonce":3.9963421519700253E-4}

C:\Users\user\Downloads\json.txt (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	79
Entropy (8bit):	4.928727704087349
Encrypted:	false
SSDEEP:	3:VQ3X4l1Wce1R6JHDlQXfMhWRXJo/XAn:VQ3e1WujeXEWxC4n
MD5:	56415F32FE2800C44E70C685DDF51273
SHA1:	08231AB77735BBFAA25BB43016000A04A69D7EC8
SHA-256:	F8B979F3CC1930EA1BC0759EDF600B4346ED5E3604B30738986603B3179C6349
SHA-512:	AF39B478A5A9D62F57B4D3C9EF77A54B88B2A09DADF381C077AF20FCB18E022BDEF79AFC33CBD9CDE86EF71E541A1A6DD8D7D017F5E7730C794E00CC7FE7 3B6
Malicious:	false
Reputation:	low
Preview:	)]}'.{"current_time_millis":1674686193248,"server_nonce":3.9963421519700253E-4}

C:\Users\user\Downloads\json.txt.crdownload (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	79

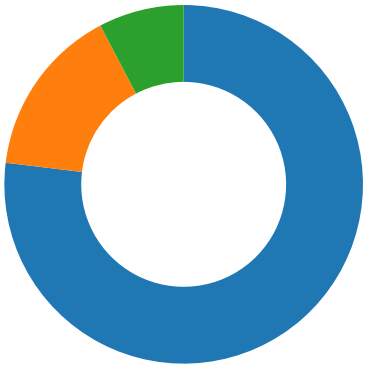
Entropy (8bit):	4.928727704087349
Encrypted:	false
SSDEEP:	3:VQ3X4l1Wce1R6JHDlQXfMhWRXJo/XAn:VQ3e1WujeXEWxC4n
MD5:	56415F32FE2800C44E70C685DDF51273
SHA1:	08231AB77735BBFAA25BB43016000A04A69D7EC8
SHA-256:	F8B979F3CC1930EA1BC0759EDF600B4346ED5E3604B30738986603B3179C6349
SHA-512:	AF39B478A5A9D62F57B4D3C9EF77A54B88B2A09DADF381C077AF20FCB18E022BDEF79AFC33CBD9CDE86EF71E541A1A6DD8D7D017F5E7730C794E00CC7FE7 3B6
Malicious:	false
Reputation:	low
Preview:	)]}'.{"current_time_millis":1674686193248,"server_nonce":3.9963421519700253E-4}

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 52

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 23:36:33.146045923 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.146096945 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.146177053 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.147042990 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.147078037 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.147146940 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.147371054 CET	49682	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.149326086 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.149342060 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.149415016 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.154017925 CET	49685	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.154638052 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.154670000 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.154768944 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.155205011 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.155225039 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.155700922 CET	49687	80	192.168.2.3	142.250.203.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 23:36:33.156909943 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.156934023 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.158010006 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.158029079 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.158376932 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.158401012 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.165597916 CET	80	49682	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.165692091 CET	49682	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.167963028 CET	49682	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.171526909 CET	80	49685	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.171652079 CET	49685	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.173753023 CET	80	49687	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.173842907 CET	49687	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.186000109 CET	80	49682	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.231266975 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.234055996 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.234107018 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.235488892 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.235590935 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.247256994 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.249763012 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.249819994 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.251130104 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.251246929 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.262196064 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.266411066 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.266453981 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.267122030 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.267250061 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.268085957 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.268174887 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.268235922 CET	80	49682	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.268265009 CET	80	49682	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.268348932 CET	49682	80	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.273974895 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.275046110 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.275079012 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.275779963 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.275959015 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.276803017 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.277165890 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.666359901 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.666438103 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.666564941 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.667057991 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.667081118 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.730966091 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.753254890 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.753304005 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.756953955 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.757143021 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.852842093 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.852874994 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.852931976 CET	49686	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.852943897 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.853079081 CET	443	49686	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.853142977 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.853267908 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.853295088 CET	443	49681	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 23:36:33.853368044 CET	49684	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.853388071 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.853517056 CET	443	49684	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.853565931 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.860328913 CET	49688	443	192.168.2.3	142.250.203.100
Jan 25, 2023 23:36:33.860383034 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.860574007 CET	443	49688	142.250.203.100	192.168.2.3
Jan 25, 2023 23:36:33.860716105 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.860744953 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.861134052 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.861161947 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.896981001 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.897133112 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.897154093 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.897172928 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.897264004 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.898474932 CET	49681	443	192.168.2.3	142.250.203.110
Jan 25, 2023 23:36:33.898492098 CET	443	49681	142.250.203.110	192.168.2.3
Jan 25, 2023 23:36:33.935215950 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.935384035 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.935419083 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.935622931 CET	443	49679	142.250.203.109	192.168.2.3
Jan 25, 2023 23:36:33.935703993 CET	49679	443	192.168.2.3	142.250.203.109
Jan 25, 2023 23:36:33.938369989 CET	49679	443	192.168.2.3	142.250.203.109

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 23:36:31.042781115 CET	64953	53	192.168.2.3	8.8.8.8
Jan 25, 2023 23:36:31.043081999 CET	54264	53	192.168.2.3	8.8.8.8
Jan 25, 2023 23:36:31.062387943 CET	53	64953	8.8.8.8	192.168.2.3
Jan 25, 2023 23:36:31.081307888 CET	53	54264	8.8.8.8	192.168.2.3
Jan 25, 2023 23:36:33.645991087 CET	65522	53	192.168.2.3	8.8.8.8
Jan 25, 2023 23:36:33.663678885 CET	53	65522	8.8.8.8	192.168.2.3
Jan 25, 2023 23:37:33.716484070 CET	51139	53	192.168.2.3	8.8.8.8
Jan 25, 2023 23:37:33.734278917 CET	53	51139	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 25, 2023 23:36:32.707323074 CET	192.168.2.3	8.8.8.8	d010	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 23:36:31.042781115 CET	192.168.2.3	8.8.8.8	0xb4e7	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:36:31.043081999 CET	192.168.2.3	8.8.8.8	0xbf44	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:36:33.645991087 CET	192.168.2.3	8.8.8.8	0x8a6f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:37:33.716484070 CET	192.168.2.3	8.8.8.8	0xa623	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
Jan 25, 2023 23:36:31.062387943 CET	8.8.8.8	192.168.2.3	0xb4e7	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

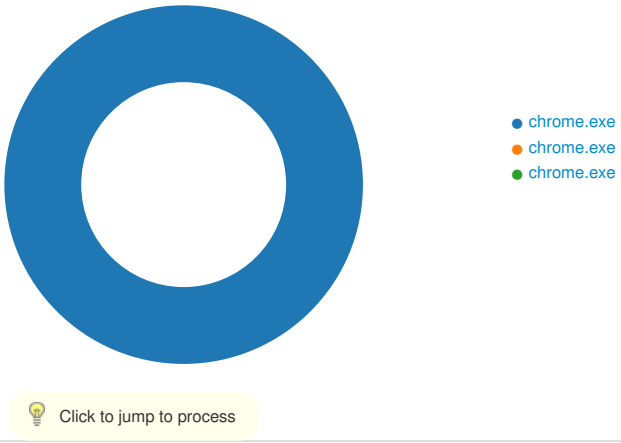
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 23:36:31.062387943 CET	8.8.8.8	192.168.2.3	0xb4e7	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:36:31.081307888 CET	8.8.8.8	192.168.2.3	0xbf44	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:36:33.663678885 CET	8.8.8.8	192.168.2.3	0x8a6f	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 23:37:33.734278917 CET	8.8.8.8	192.168.2.3	0xa623	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5272**, Parent PID: **2680**

General	
Target ID:	0
Start time:	23:36:27
Start date:	25/01/2023
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: **5444**, Parent PID: **5272**

General

Target ID:	1
Start time:	23:36:28
Start date:	25/01/2023
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=1740 --field-trial-handle=1860,i,9632146488442511452,3354182686509041322,131072 --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

Analysis Process: chrome.exe PID: **5692**, Parent PID: **2680**

General

Target ID:	2
Start time:	23:36:29
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://clients2.google.com/time/1/current?cup2key=6:ja9_47WTwmkUfr4-NZaxb631Hv9CvRDs5qiwCNTf1Ag&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
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