ID: 764032
Cookbook: browseurl.jbs
Time: 10:33:25
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

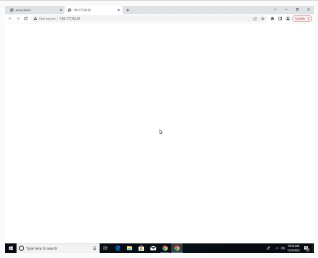
Windows Analysis Report

http://185.177.92.29

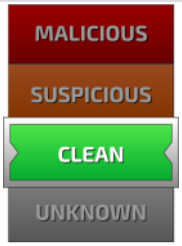
Overview

General Information

Sample URL:	http://185.177.92.29
Analysis ID:	764032
Infos:	



Detection

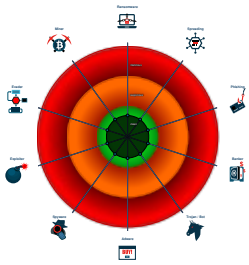


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5488 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5200 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=1808,i,17095270601027462 92,9450787675187643490,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2224 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://185.177.92.29 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

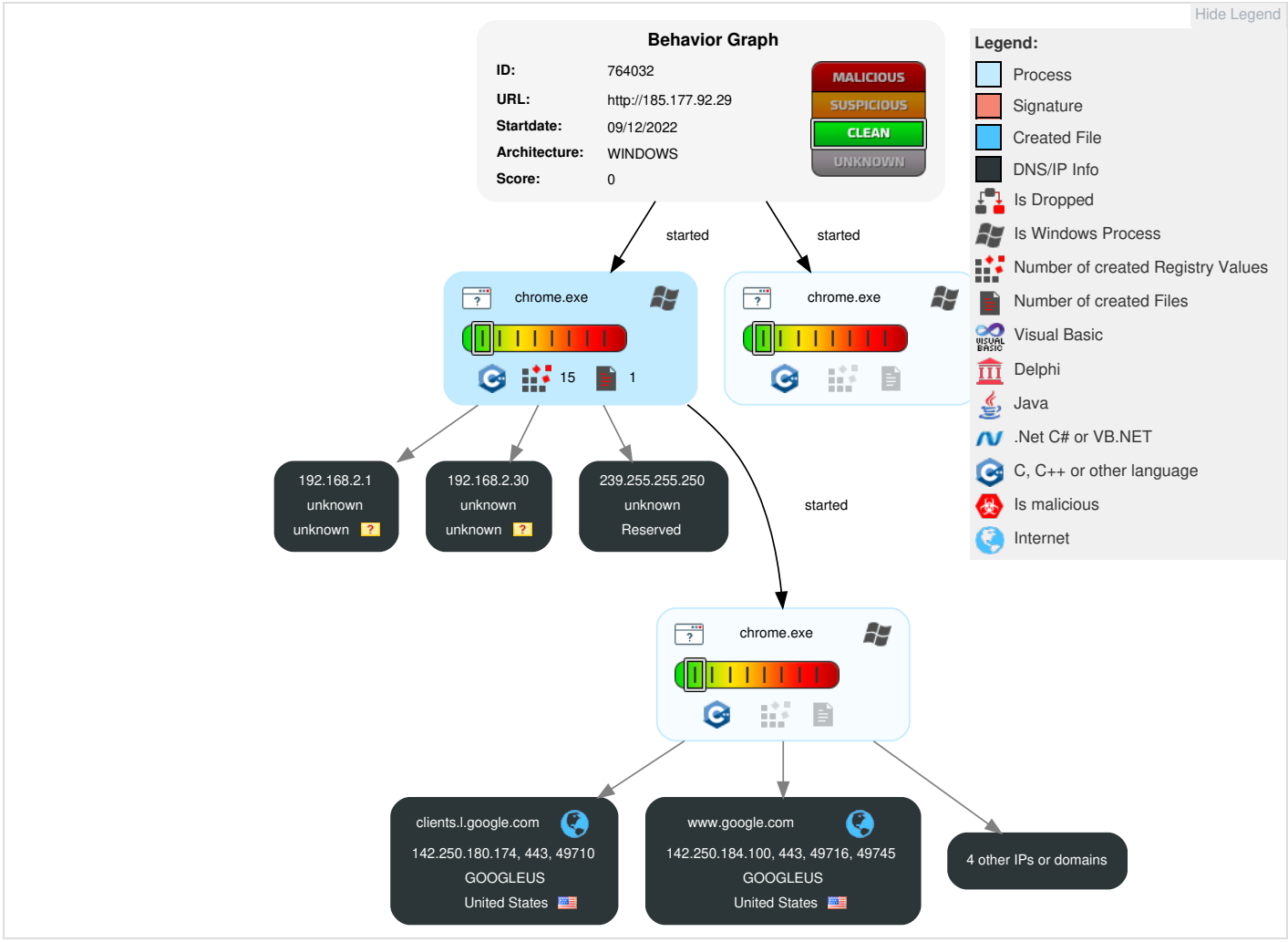
Joe Sandbox Signatures

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

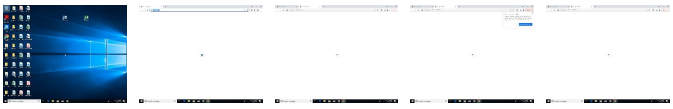
Behavior Graph

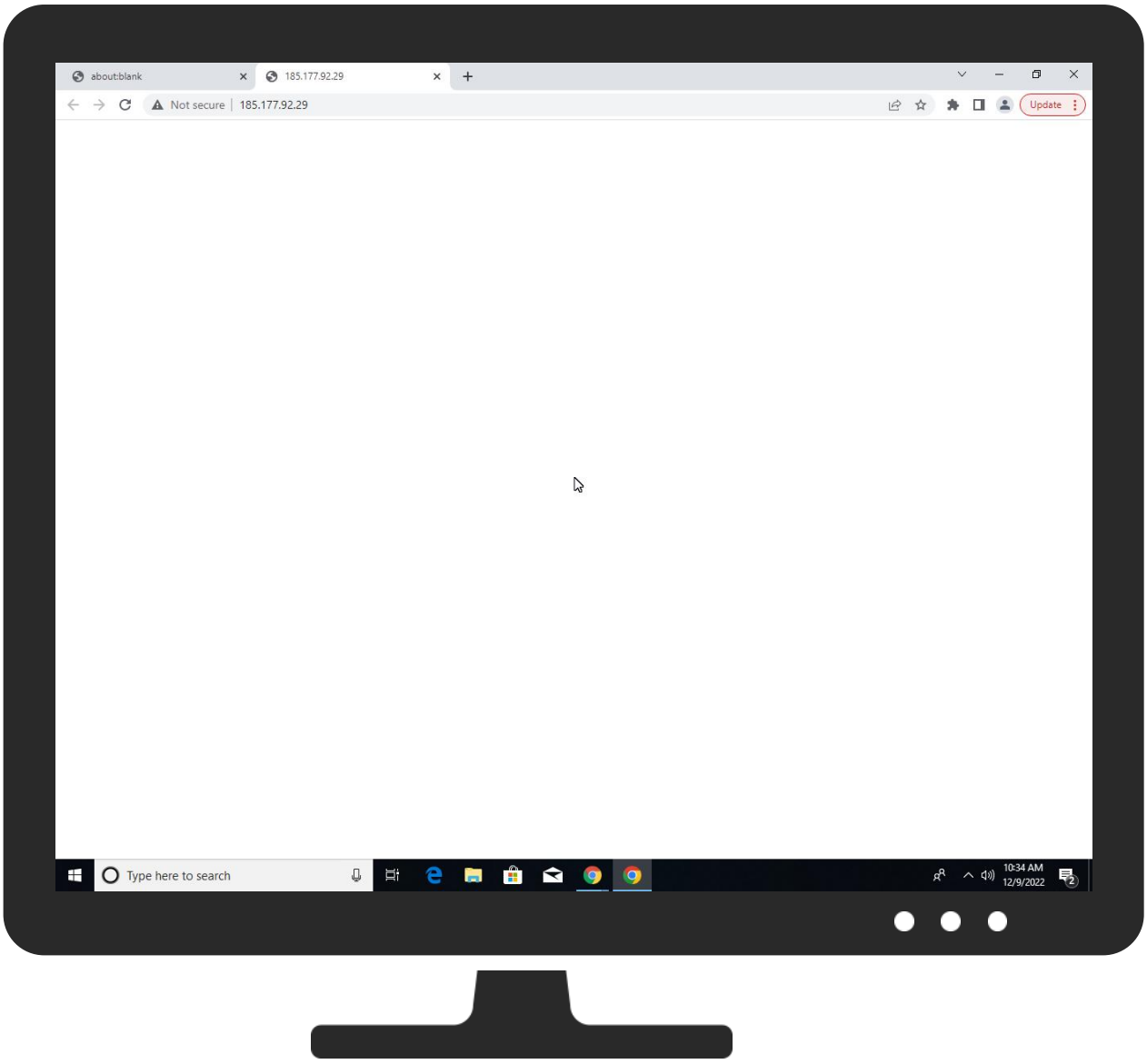


Screenshots

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://185.177.92.29	1%	Virustotal		Browse
http://185.177.92.29	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://185.177.92.29/	0%	Avira URL Cloud	safe	
http://185.177.92.29/favicon.ico	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://185.177.92.29/	1%	Virustotal		Browse

Domains and IPs

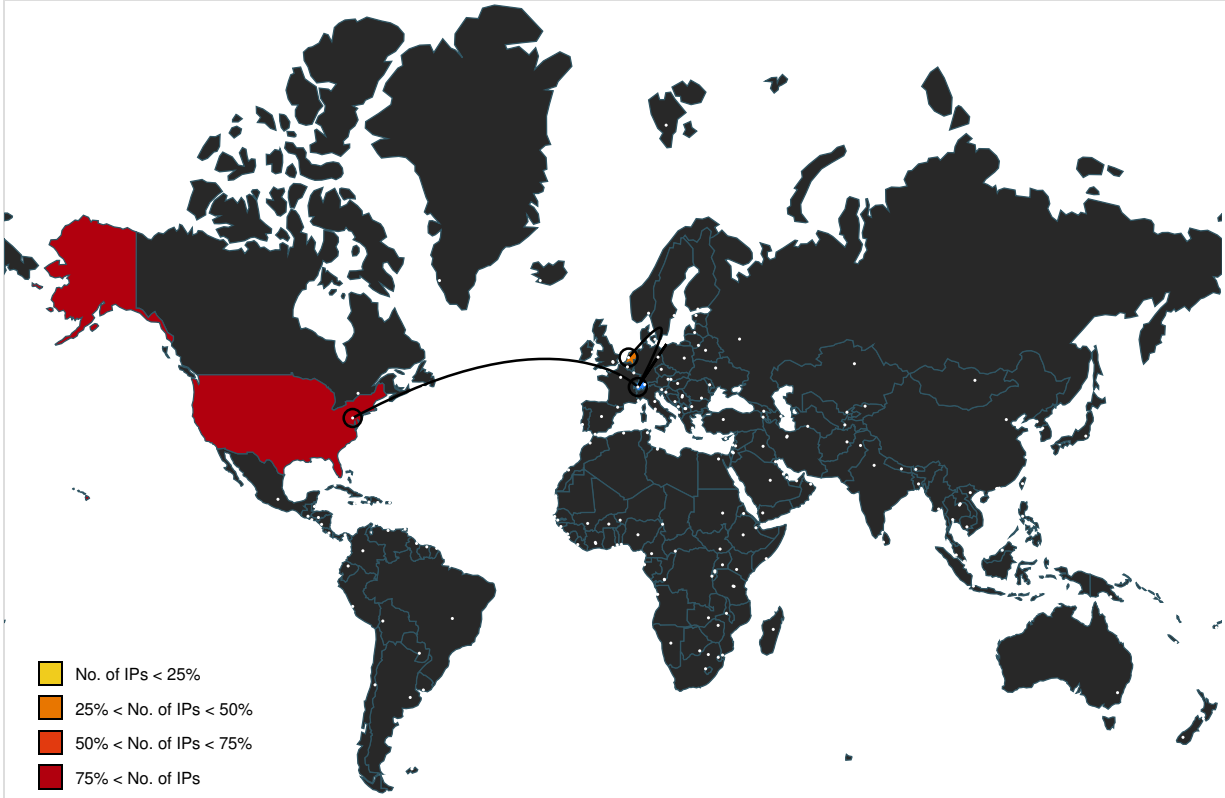
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.45	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	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://185.177.92.29/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.177.92.29/favicon.ico	false	• Avira URL Cloud: safe	unknown
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
142.250.184.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
185.177.92.29	unknown	Netherlands		39572	ADVANCEDHOSTERS-ASNL	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.30
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764032
Start date and time:	2022-12-09 10:33:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://185.177.92.29
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:	10
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@6/8
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, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.131
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, 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

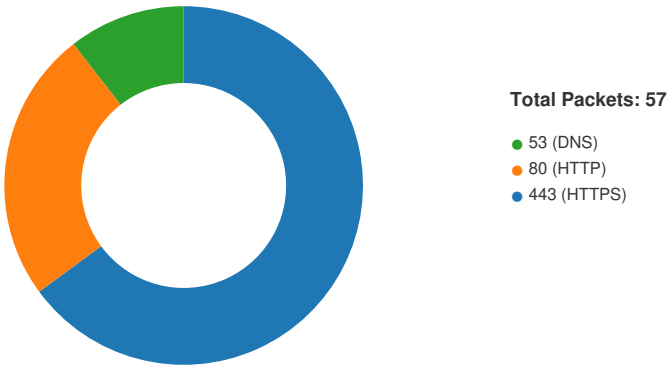
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:34:22.735033989 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.735081911 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:22.735143900 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.735780954 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.735807896 CET	443	49710	142.250.180.174	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:34:22.754671097 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:22.754729986 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:22.754796028 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:22.755620956 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:22.755667925 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:22.863084078 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:22.866375923 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:22.866501093 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:22.869489908 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.869518042 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:22.869862080 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:22.869924068 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:22.870202065 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:22.870269060 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.872394085 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:22.872399092 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:22.872478962 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:22.872961044 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:22.891906023 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:22.892153978 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:22.912318945 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.200963974 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:24.201046944 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.201324940 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.201419115 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.201471090 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.201757908 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.201817989 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.201828957 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.202291012 CET	49713	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:24.202711105 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:24.202781916 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.234795094 CET	80	49713	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:24.234926939 CET	49713	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:24.249095917 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.249267101 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:24.249281883 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.249387980 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:24.272407055 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.272469044 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.275439978 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.275511980 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.275543928 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.276645899 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.276937008 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.305089951 CET	49711	443	192.168.2.6	142.250.184.45
Dec 9, 2022 10:34:24.305161953 CET	443	49711	142.250.184.45	192.168.2.6
Dec 9, 2022 10:34:24.305927038 CET	49710	443	192.168.2.6	142.250.180.174
Dec 9, 2022 10:34:24.305963993 CET	443	49710	142.250.180.174	192.168.2.6
Dec 9, 2022 10:34:24.637243032 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:24.972381115 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:25.002809048 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:25.003992081 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:25.072685957 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:25.540122986 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:25.570705891 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:25.672586918 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:26.015187979 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.015254021 CET	443	49716	142.250.184.100	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:34:26.015337944 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.015674114 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.015711069 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.098593950 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.102895975 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.102962017 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.104382038 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.104476929 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.122087955 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.122143030 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.122371912 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.284734011 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:26.284784079 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:26.471683979 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:35.571254015 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:34:35.571433067 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:36.075532913 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:36.075679064 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:36.076024055 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:39.502851009 CET	49712	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:34:39.502976894 CET	49716	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:34:39.503002882 CET	443	49716	142.250.184.100	192.168.2.6
Dec 9, 2022 10:34:39.531876087 CET	80	49712	185.177.92.29	192.168.2.6
Dec 9, 2022 10:35:09.247124910 CET	49713	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:35:09.275846958 CET	80	49713	185.177.92.29	192.168.2.6
Dec 9, 2022 10:35:24.265500069 CET	80	49713	185.177.92.29	192.168.2.6
Dec 9, 2022 10:35:24.265609026 CET	49713	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:35:26.065893888 CET	49713	80	192.168.2.6	185.177.92.29
Dec 9, 2022 10:35:26.094943047 CET	80	49713	185.177.92.29	192.168.2.6
Dec 9, 2022 10:35:26.160391092 CET	49745	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:35:26.160454988 CET	443	49745	142.250.184.100	192.168.2.6
Dec 9, 2022 10:35:26.160525084 CET	49745	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:35:26.160809040 CET	49745	443	192.168.2.6	142.250.184.100
Dec 9, 2022 10:35:26.160835028 CET	443	49745	142.250.184.100	192.168.2.6
Dec 9, 2022 10:35:26.245858908 CET	443	49745	142.250.184.100	192.168.2.6
Dec 9, 2022 10:35:26.247443914 CET	49745	443	192.168.2.6	142.250.184.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:34:22.673918009 CET	50506	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:34:22.699500084 CET	53	50506	8.8.8.8	192.168.2.6
Dec 9, 2022 10:34:22.721760988 CET	59082	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:34:22.739170074 CET	53	59082	8.8.8.8	192.168.2.6
Dec 9, 2022 10:34:25.973275900 CET	63229	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:34:25.992341995 CET	53	63229	8.8.8.8	192.168.2.6
Dec 9, 2022 10:34:25.996773005 CET	62538	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:34:26.013273001 CET	53	62538	8.8.8.8	192.168.2.6
Dec 9, 2022 10:35:26.042067051 CET	60032	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:35:26.064016104 CET	53	60032	8.8.8.8	192.168.2.6
Dec 9, 2022 10:35:26.068048000 CET	49232	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:35:26.094676018 CET	53	49232	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:34:22.673918009 CET	192.168.2.6	8.8.8.8	0xe616	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:34:22.721760988 CET	192.168.2.6	8.8.8.8	0x1f0f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:34:25.973275900 CET	192.168.2.6	8.8.8.8	0x3204	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:34:25.996773005 CET	192.168.2.6	8.8.8.8	0x4318	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:26.042067051 CET	192.168.2.6	8.8.8.8	0x751a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:26.068048000 CET	192.168.2.6	8.8.8.8	0x5959	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

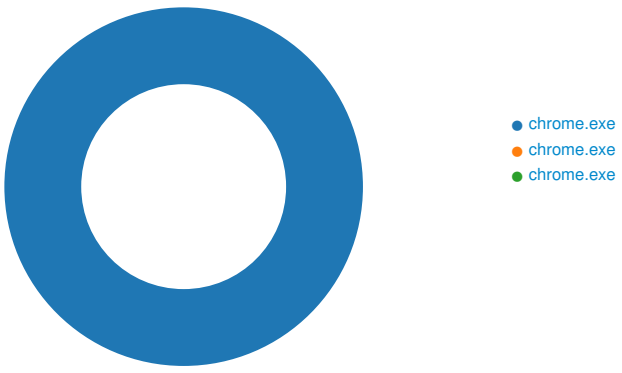
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:34:22.699500084 CET	8.8.8.8	192.168.2.6	0xe616	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:34:22.699500084 CET	8.8.8.8	192.168.2.6	0xe616	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:34:22.739170074 CET	8.8.8.8	192.168.2.6	0x1f0f	No error (0)	accounts.google.com		142.250.184.45	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:34:25.992341995 CET	8.8.8.8	192.168.2.6	0x3204	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:34:26.013273001 CET	8.8.8.8	192.168.2.6	0x4318	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:26.064016104 CET	8.8.8.8	192.168.2.6	0x751a	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:26.094676018 CET	8.8.8.8	192.168.2.6	0x5959	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- 185.177.92.29

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5488, Parent PID: 3016

General

Target ID:	0
Start time:	10:34:19
Start date:	09/12/2022
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:	0x7ff6f9750000
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: 5200, Parent PID: 5488

General

Target ID:	1
Start time:	10:34:21
Start date:	09/12/2022
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=1808,i,17095270601027462 92,9450787675187643490,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
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: **2224**, Parent PID: **3016**

General

Target ID:	2
Start time:	10:34:22
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://185.177.92.29
Imagebase:	0x7ff6f9750000
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