ID: 876159
Cookbook: browseurl.jbs
Time: 11:34:22
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

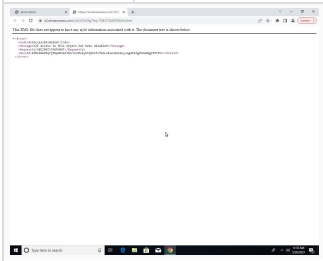
Windows Analysis Report

https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html

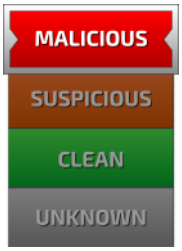
Overview

General Information

Sample URL:	http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html
Analysis ID:	876159
Infos:	



Detection

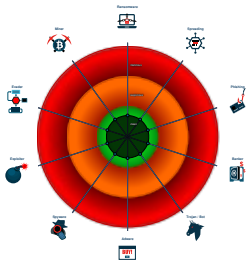


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5508 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2968 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1768,i,3249229338383296899,15023654663304245028,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6384 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html 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

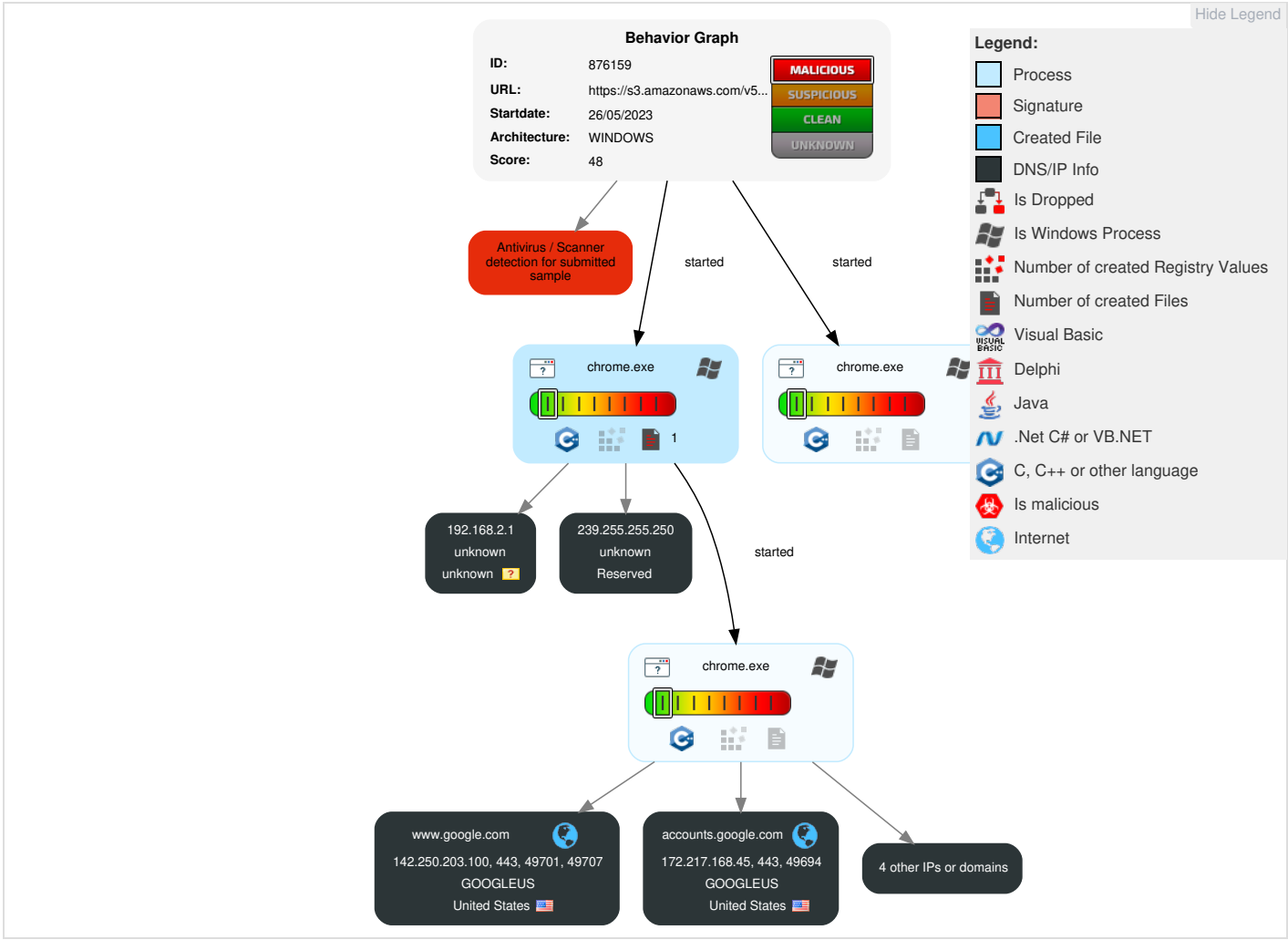
AV Detection

Antivirus / Scanner detection for submitted sample

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

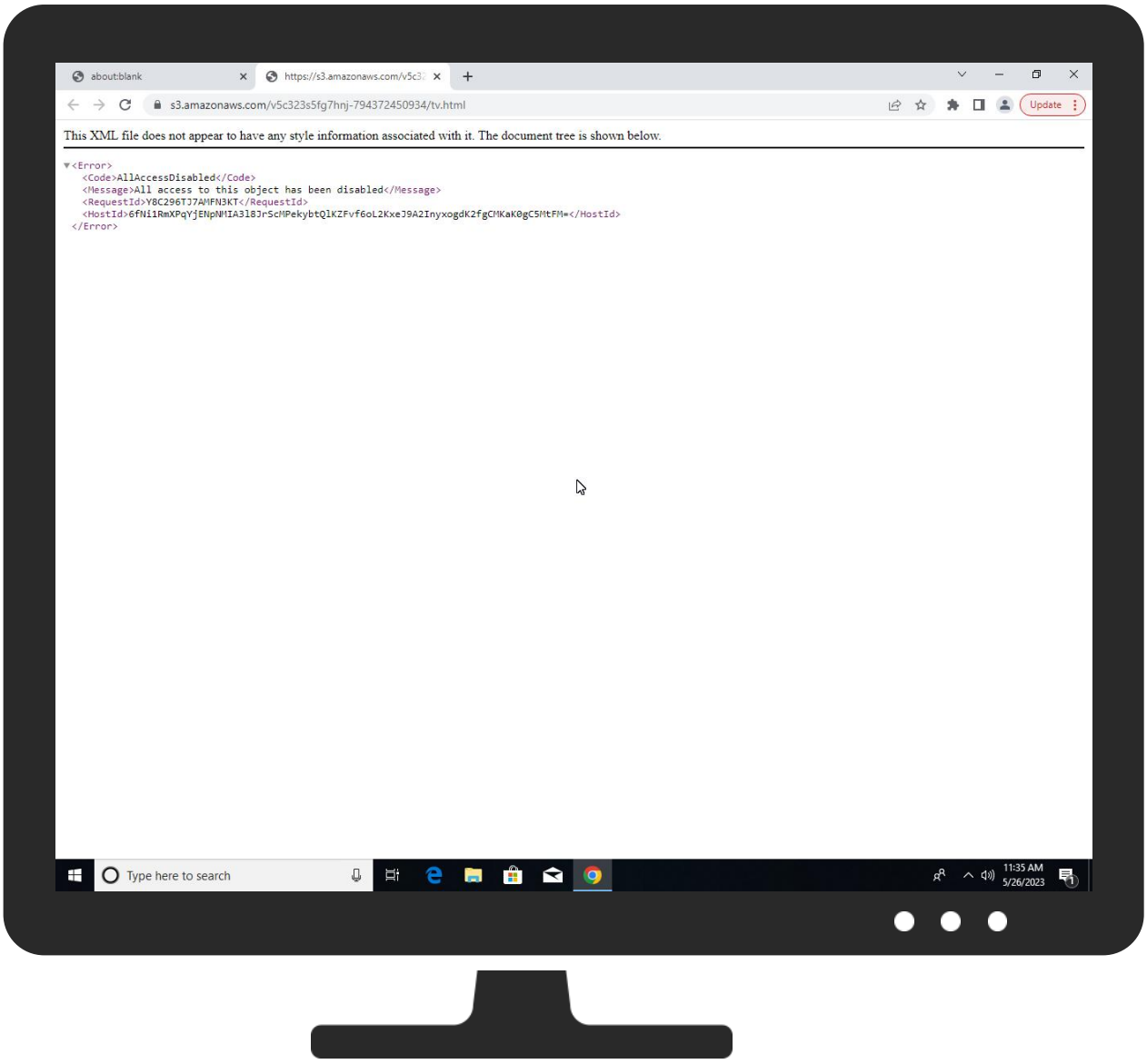
Behavior Graph



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://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html	1%	Virustotal		Browse
http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html	0%	Avira URL Cloud	safe	
http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

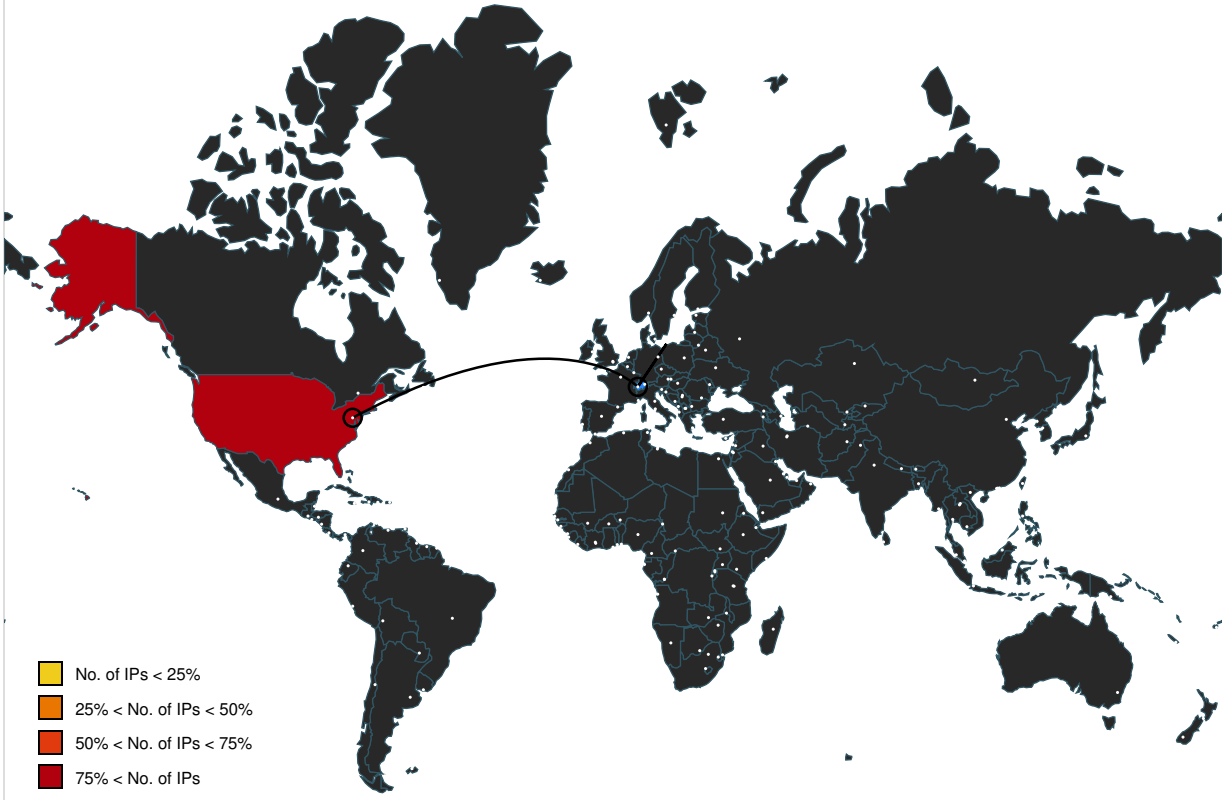
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3.amazonaws.com	52.217.122.24	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://s3.amazonaws.com/favicon.ico	false		high
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-GB&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
http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
52.217.87.206	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876159
Start date and time:	2023-05-26 11:34:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html
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:	4
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@25/2@8/6
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): audiodg.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.3, 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

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

Chrome Cache Entry: 108

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, ASCII text
Category:	downloaded
Size (bytes):	243
Entropy (8bit):	5.586091561179429
Encrypted:	false
SSDEEP:	6:TMVBd/ZbZjZvKtWRVzj8w6ZHA789oKQfjan:TMHd9BZKtWRiPZ9oKEja
MD5:	27974EB90ABB7EA2DC21DEC3164E1574
SHA1:	42A3B6EA1BF10FB516708A5CC8879CE4AE65EE7E
SHA-256:	F2625034C23539AEE0E6D98CD8CA485E5904B3A4ECFD3AE50F0AAA58F4EFC390
SHA-512:	DD334C5109E0B9C750C9C2C8B7E14BE33BF3898CE6F22A8C09ECE864CA491919AF72B452FB1E98368028F49EE1816F9626EC15D8B452BDCFF224A226305647D5
Malicious:	false
Reputation:	low
URL:	http://https://s3.amazonaws.com/favicon.ico
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>Y8CCG2DGN0BEJGMA</RequestId><HostId>BzPI/Sv9BOIUGL69gAZjEbasHPDcxQuOjRZfTJo0/K/4L6na+qMBO1MJlPK+/+pTT1p/zrQwfg8=</HostId></Error>

Chrome Cache Entry: 109

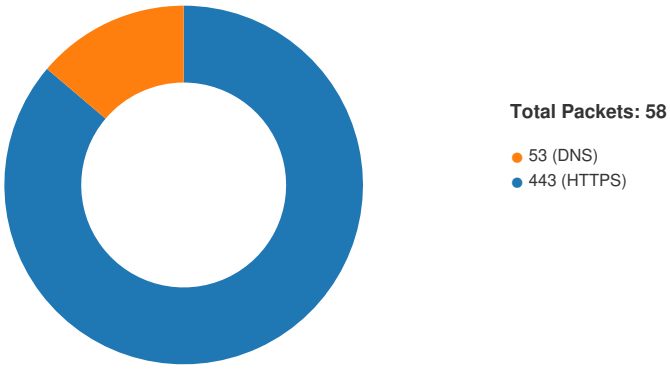
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, ASCII text
Category:	downloaded
Size (bytes):	278
Entropy (8bit):	5.517021707644157
Encrypted:	false
SSDEEP:	6:TMVBd/ZbZjtkLRWHtouHjBWlQj8YARuQsr1yRwCTaK0an:TMHd9BtkRWHt3BW57uQsr1gwCia
MD5:	D06C0007FD1727FE8E31A03109F23FBF
SHA1:	8C8DCB4833A1035290ACB999B16E74E582CC16DE
SHA-256:	2757D4B59099600F5D7EA43253A1F3C7106735597A06BDB0C8983DD874374066
SHA-512:	15C2EAE9AA58A0D697B8B358F6E86E7D6B234C23A403C65CBE7BA9F409B5739D7F3AC03F1FE77D100282E026A36F8281113F35B26AD0924A38ED1C3E0AA764E6
Malicious:	false
Reputation:	low
URL:	http://https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<Error><Code>AllAccessDisabled</Code><Message>All access to this object has been disabled</Message><RequestId>Y8C296TJ7AMFN3KT</RequestId><HostId>6fNi1RmXPqYjENpNMIA3l8JrScMPekybtQlKZFvf6oL2KxeJ9A2InyxogdK2fgCMKaK0gC5MtFM=</HostId></Error>

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:35:21.357336998 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.357378960 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.357716084 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.361365080 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.361428022 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.361779928 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.361804962 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.365412951 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.365664959 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.365689993 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.457201004 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.458122015 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.458158970 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.460268974 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.460680962 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.467622995 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.469197989 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.469227076 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.470082045 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.470705032 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.471538067 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.471682072 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.914797068 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.914963961 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.914978981 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.915069103 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.915169001 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.915272951 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.915299892 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.915605068 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.949713945 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.950046062 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.958477974 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.958477974 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.958523035 CEST	49694	443	192.168.2.4	172.217.168.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:35:21.958545923 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.963731050 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.964092970 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:21.971482038 CEST	49696	443	192.168.2.4	216.58.215.238
May 26, 2023 11:35:21.971517086 CEST	443	49696	216.58.215.238	192.168.2.4
May 26, 2023 11:35:21.976207972 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.977390051 CEST	49694	443	192.168.2.4	172.217.168.45
May 26, 2023 11:35:21.977411985 CEST	443	49694	172.217.168.45	192.168.2.4
May 26, 2023 11:35:23.700810909 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.700886965 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:23.700999022 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.701056004 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:23.701491117 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.701584101 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.701827049 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.701843023 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:23.702042103 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:23.702111006 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.174681902 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.175060034 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.175117016 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.177350044 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.177469015 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.180619001 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.185590982 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.185641050 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.187103987 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.187192917 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.193033934 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.193300009 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.193329096 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.193393946 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.193480968 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.193641901 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.234900951 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.234951973 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.256455898 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.256491899 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.277427912 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.338887930 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.339318991 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.339490891 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.341901064 CEST	49698	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.341944933 CEST	443	49698	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.356478930 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.450030088 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.492290974 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.590883970 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.591017962 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:24.593758106 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.599240065 CEST	49699	443	192.168.2.4	52.217.87.206
May 26, 2023 11:35:24.599275112 CEST	443	49699	52.217.87.206	192.168.2.4
May 26, 2023 11:35:25.061476946 CEST	49701	443	192.168.2.4	142.250.203.100
May 26, 2023 11:35:25.061554909 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.061670065 CEST	49701	443	192.168.2.4	142.250.203.100
May 26, 2023 11:35:25.061944008 CEST	49701	443	192.168.2.4	142.250.203.100
May 26, 2023 11:35:25.061975002 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.126295090 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.127171040 CEST	49701	443	192.168.2.4	142.250.203.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:35:25.127222061 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.128665924 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.128772974 CEST	49701	443	192.168.2.4	142.250.203.100
May 26, 2023 11:35:25.130856037 CEST	49701	443	192.168.2.4	142.250.203.100
May 26, 2023 11:35:25.130992889 CEST	443	49701	142.250.203.100	192.168.2.4
May 26, 2023 11:35:25.186908007 CEST	49701	443	192.168.2.4	142.250.203.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:35:21.320544004 CEST	58565	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:21.320785999 CEST	52239	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:21.344490051 CEST	53	58565	8.8.8.8	192.168.2.4
May 26, 2023 11:35:21.353564024 CEST	53	52239	8.8.8.8	192.168.2.4
May 26, 2023 11:35:23.267402887 CEST	61124	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:23.290643930 CEST	53	61124	8.8.8.8	192.168.2.4
May 26, 2023 11:35:23.571897984 CEST	59444	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:23.586622000 CEST	53	59444	8.8.8.8	192.168.2.4
May 26, 2023 11:35:25.011336088 CEST	64906	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:25.034842968 CEST	53	64906	8.8.8.8	192.168.2.4
May 26, 2023 11:35:25.037049055 CEST	59446	53	192.168.2.4	8.8.8.8
May 26, 2023 11:35:25.060481071 CEST	53	59446	8.8.8.8	192.168.2.4
May 26, 2023 11:36:25.071326971 CEST	50433	53	192.168.2.4	8.8.8.8
May 26, 2023 11:36:25.100013971 CEST	53	50433	8.8.8.8	192.168.2.4
May 26, 2023 11:36:25.104962111 CEST	53498	53	192.168.2.4	8.8.8.8
May 26, 2023 11:36:25.119862080 CEST	53	53498	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 11:35:21.320544004 CEST	192.168.2.4	8.8.8.8	0xbcea	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:21.320785999 CEST	192.168.2.4	8.8.8.8	0x98c9	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.267402887 CEST	192.168.2.4	8.8.8.8	0x50a1	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.571897984 CEST	192.168.2.4	8.8.8.8	0x5f3d	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:25.011336088 CEST	192.168.2.4	8.8.8.8	0xbb10	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:25.037049055 CEST	192.168.2.4	8.8.8.8	0xb6ff	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:36:25.071326971 CEST	192.168.2.4	8.8.8.8	0x32e0	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:36:25.104962111 CEST	192.168.2.4	8.8.8.8	0x100f	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
May 26, 2023 11:35:21.344490051 CEST	8.8.8.8	192.168.2.4	0xbcea	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:21.353564024 CEST	8.8.8.8	192.168.2.4	0x98c9	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:35:21.353564024 CEST	8.8.8.8	192.168.2.4	0x98c9	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		52.217.122.24	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		54.231.163.16	A (IP address)	IN (0x0001)	false

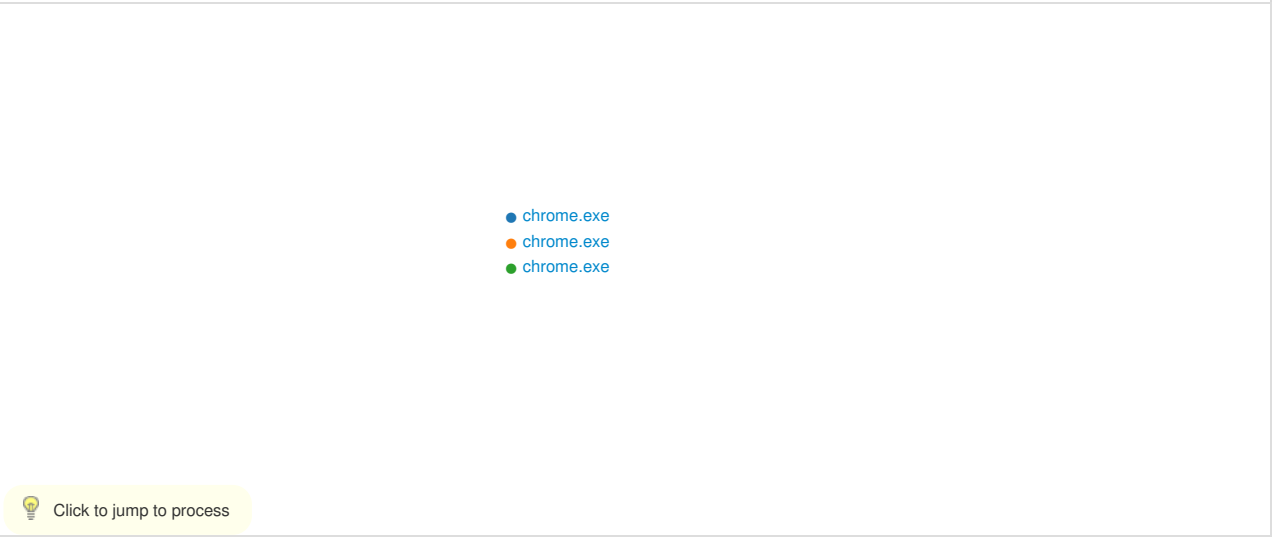
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		52.217.227.232	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		52.216.92.133	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		54.231.232.80	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		52.217.229.224	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		54.231.170.216	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.290643930 CEST	8.8.8.8	192.168.2.4	0x50a1	No error (0)	s3.amazonaws.com		3.5.19.157	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.217.87.206	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.216.176.37	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.216.33.88	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.217.41.206	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		54.231.199.88	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.217.196.200	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		54.231.195.176	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:23.586622000 CEST	8.8.8.8	192.168.2.4	0x5f3d	No error (0)	s3.amazonaws.com		52.217.121.96	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:25.034842968 CEST	8.8.8.8	192.168.2.4	0xbb10	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:35:25.060481071 CEST	8.8.8.8	192.168.2.4	0xb6ff	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:36:25.100013971 CEST	8.8.8.8	192.168.2.4	0x32e0	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:36:25.119862080 CEST	8.8.8.8	192.168.2.4	0x100f	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
- s3.amazonaws.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5508**, Parent PID: **3176**

General

Target ID:	0
Start time:	11:35:19
Start date:	26/05/2023
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:	0x7ff683680000
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

Analysis Process: chrome.exe PID: **2968**, Parent PID: **5508**

General

Target ID:	2
Start time:	11:35:20
Start date:	26/05/2023

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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1768,i,3249229338383296899,15023654663304245028,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
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: **6384**, Parent PID: **3176**

General

Target ID:	3
Start time:	11:35:23
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://s3.amazonaws.com/v5c323s5fg7hnj-794372450934/tv.html
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly