ID: 882694
Cookbook: browseurl.jbs
Time: 17:07:50
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

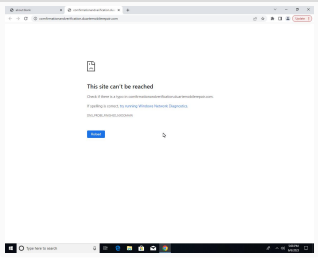
Windows Analysis Report

https://comfirmationandverification.duartemobilerepair.com/

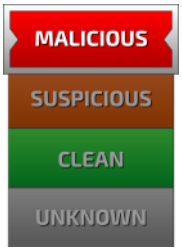
Overview

General Information

Sample URL:	http://https://comfirmationandverification.duartemobilerepair.com/
Analysis ID:	882694
Infos:	



Detection

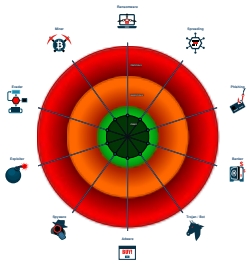


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4196 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2720 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=1868 --field-trial-handle=1672,i,17582304814663474974,3067264136992902369,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6256 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://comfirmationandverification.duartemobilerepair.com/ 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

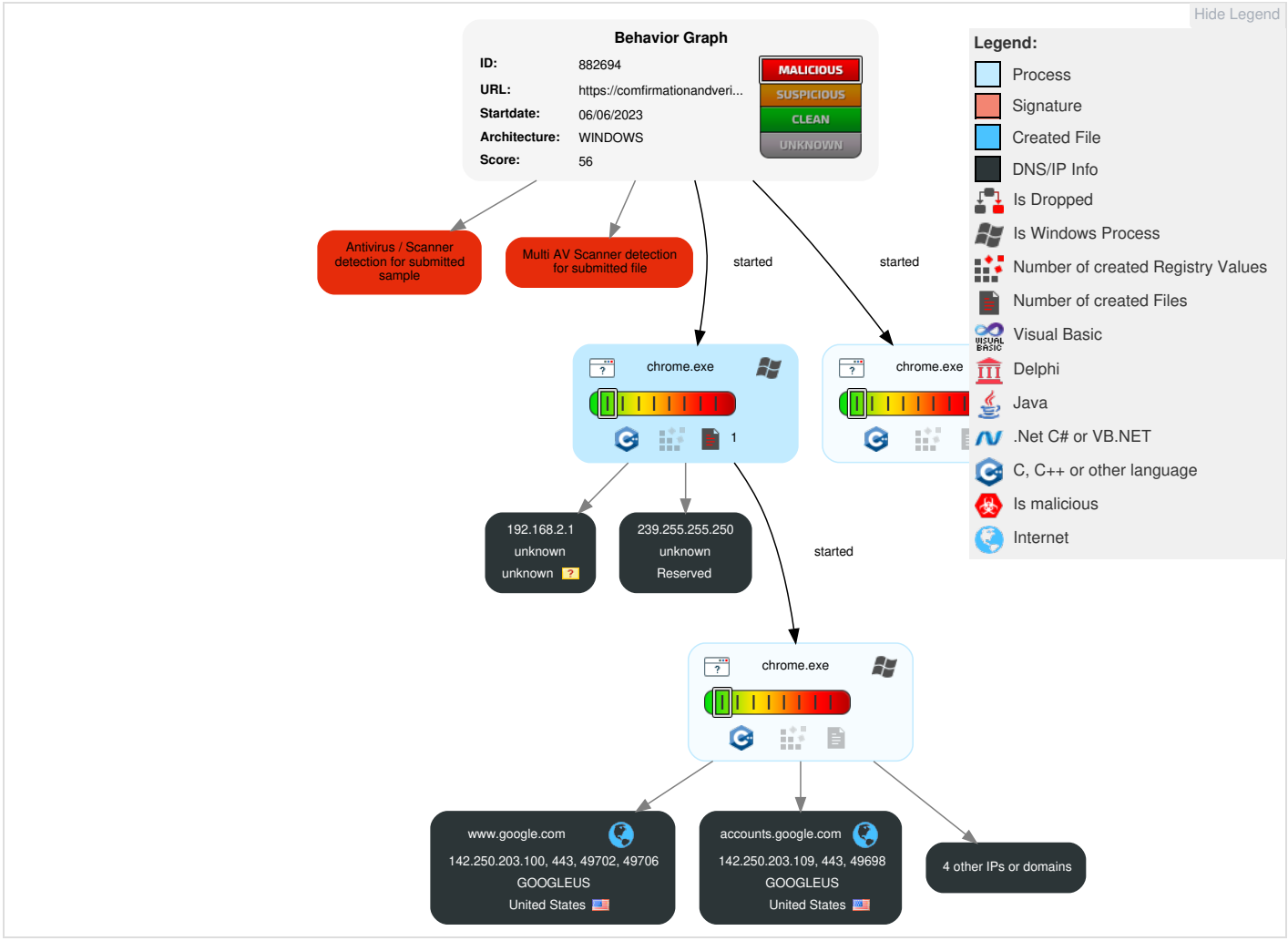
Antivirus / Scanner detection for submitted sample

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

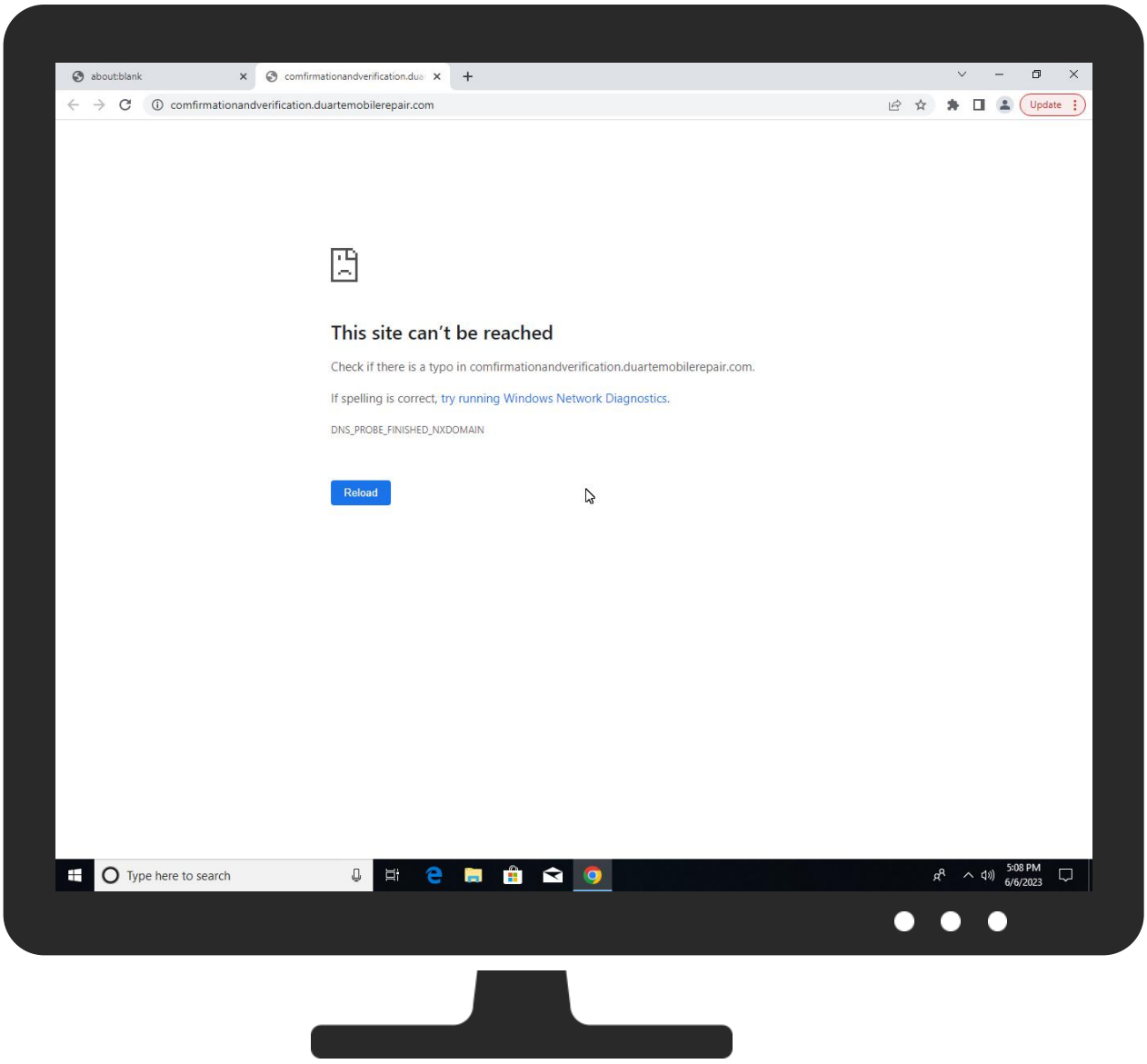
Behavior Graph



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://https://comfirmationandverification.duartemobilerepair.com/	16%	Virustotal		Browse
http://https://comfirmationandverification.duartemobilerepair.com/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://comfirmationandverification.duartemobilerepair.com/	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

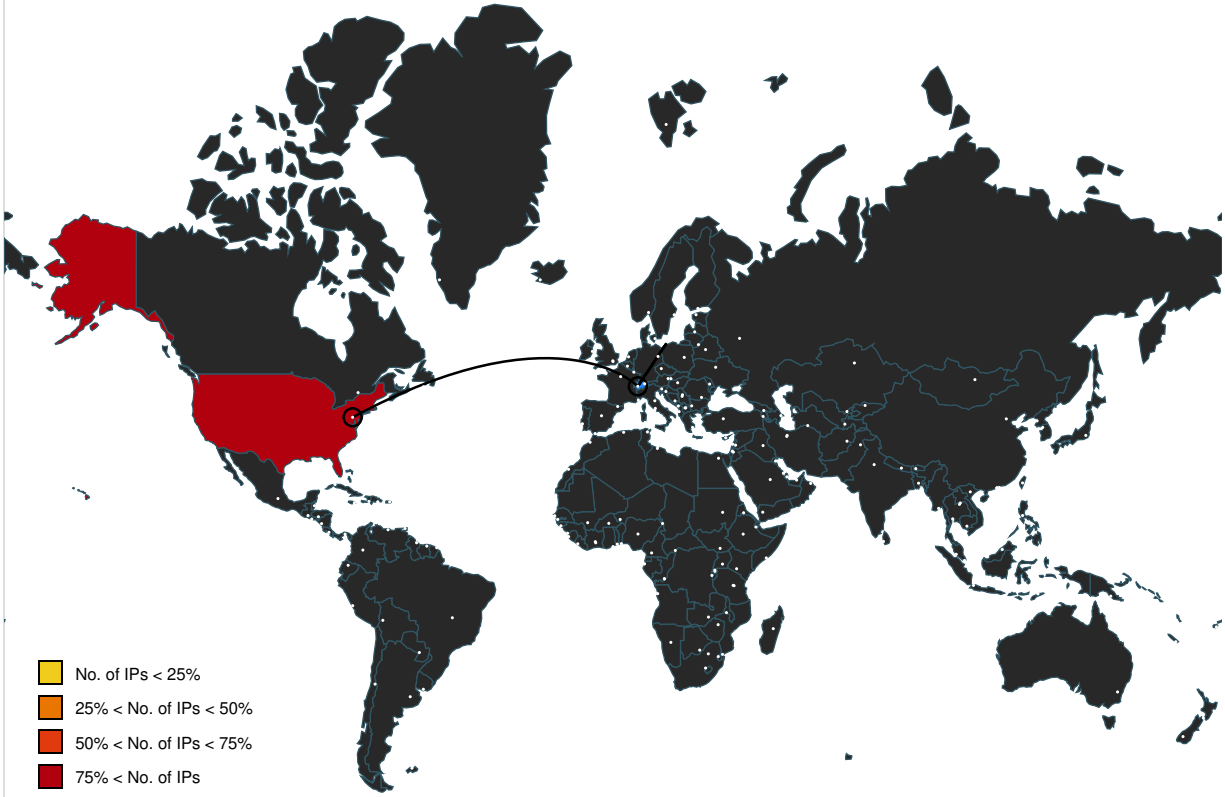
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	172.217.168.14	true	false		high
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
comfirmationandverification.duartemobilerepair.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882694
Start date and time:	2023-06-06 17:07:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://comfirmationandverification.duartemobilerepair.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@29/0@10/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, update.googleapis.com, 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

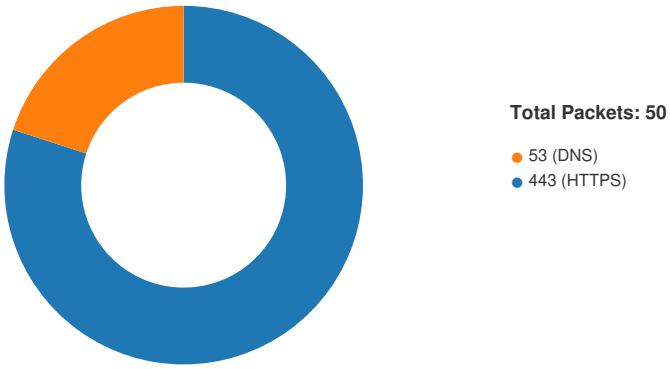
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:08:45.380315065 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.380371094 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.380469084 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.381230116 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.381253004 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.386117935 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.386159897 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.386264086 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.386945963 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.386961937 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.443064928 CEST	443	49699	142.250.203.110	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:08:45.443576097 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.443619967 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.444308996 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.444410086 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.445719004 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.445816994 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.455070019 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.486571074 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.486612082 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.490339041 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.490467072 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.703689098 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.703819990 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.703831911 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.703852892 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.704000950 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.704159975 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.704178095 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.704219103 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.738687992 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.738831043 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.738842964 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.738912106 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.740395069 CEST	49699	443	192.168.2.7	142.250.203.110
Jun 6, 2023 17:08:45.740430117 CEST	443	49699	142.250.203.110	192.168.2.7
Jun 6, 2023 17:08:45.753892899 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.753920078 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.755528927 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.755673885 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.755693913 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.755712032 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:45.755779028 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.761751890 CEST	49698	443	192.168.2.7	142.250.203.109
Jun 6, 2023 17:08:45.761786938 CEST	443	49698	142.250.203.109	192.168.2.7
Jun 6, 2023 17:08:49.237433910 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.237504959 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.237623930 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.238171101 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.238207102 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.294507027 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.295001030 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.295028925 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.297172070 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.297331095 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.299526930 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.299784899 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.346774101 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:49.346802950 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:49.393657923 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:08:59.284885883 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:59.285042048 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:08:59.285156965 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:01.926543951 CEST	49702	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:01.926601887 CEST	443	49702	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.293812037 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:49.293894053 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.293986082 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:49.294378042 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:49.294425011 CEST	443	49706	142.250.203.100	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:09:49.348510981 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.348855019 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:49.348891020 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.349498987 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.350012064 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:49.350145102 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:49.402086020 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:09:59.339152098 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:59.339287043 CEST	443	49706	142.250.203.100	192.168.2.7
Jun 6, 2023 17:09:59.339364052 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:10:00.651706934 CEST	49706	443	192.168.2.7	142.250.203.100
Jun 6, 2023 17:10:00.651768923 CEST	443	49706	142.250.203.100	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:08:45.344707012 CEST	50835	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:45.345045090 CEST	50505	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:45.364765882 CEST	53	50835	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:45.377528906 CEST	53	50505	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:47.386004925 CEST	50513	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:47.413769960 CEST	53	50513	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:47.825562954 CEST	60765	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:47.826566935 CEST	58283	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:47.859121084 CEST	53	58283	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:47.870527029 CEST	53	60765	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:48.843966007 CEST	49516	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:48.877031088 CEST	53	49516	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:49.201595068 CEST	62679	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:49.229950905 CEST	53	62679	8.8.8.8	192.168.2.7
Jun 6, 2023 17:08:53.914726019 CEST	59006	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:08:53.936469078 CEST	53	59006	8.8.8.8	192.168.2.7
Jun 6, 2023 17:09:23.996646881 CEST	58514	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:09:24.030297995 CEST	53	58514	8.8.8.8	192.168.2.7
Jun 6, 2023 17:09:49.271342039 CEST	60837	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:09:49.291591883 CEST	53	60837	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:08:45.344707012 CEST	192.168.2.7	8.8.8.8	0xf442	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:45.345045090 CEST	192.168.2.7	8.8.8.8	0x922e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.386004925 CEST	192.168.2.7	8.8.8.8	0xa2b	Standard query (0)	comfirmationandverification.duartemobilerepair.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.825562954 CEST	192.168.2.7	8.8.8.8	0x8fe0	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.826566935 CEST	192.168.2.7	8.8.8.8	0xc0b3	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:48.843966007 CEST	192.168.2.7	8.8.8.8	0x2b9e	Standard query (0)	comfirmationandverification.duartemobilerepair.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:49.201595068 CEST	192.168.2.7	8.8.8.8	0x4cd6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:53.914726019 CEST	192.168.2.7	8.8.8.8	0xd3a0	Standard query (0)	comfirmationandverification.duartemobilerepair.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:09:23.996646881 CEST	192.168.2.7	8.8.8.8	0x268f	Standard query (0)	comfirmationandverification.duartemobilerepair.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:09:49.271342039 CEST	192.168.2.7	8.8.8.8	0xacc4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

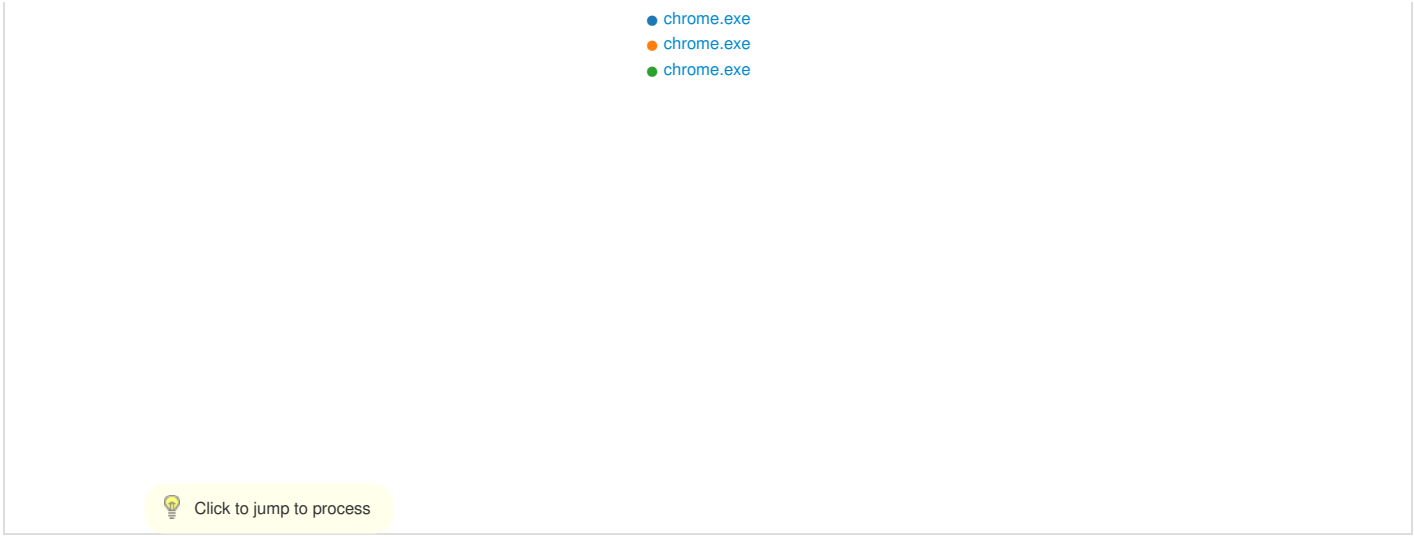
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:08:45.364765882 CEST	8.8.8.8	192.168.2.7	0xf442	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:45.377528906 CEST	8.8.8.8	192.168.2.7	0x922e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jun 6, 2023 17:08:45.377528906 CEST	8.8.8.8	192.168.2.7	0x922e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.413769960 CEST	8.8.8.8	192.168.2.7	0xa2b	Name error (3)	comfirmationandverification.duartemobilerepair.com	none	none	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.859121084 CEST	8.8.8.8	192.168.2.7	0xc0b3	No error (0)	google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:47.870527029 CEST	8.8.8.8	192.168.2.7	0x8fe0	No error (0)	google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:48.877031088 CEST	8.8.8.8	192.168.2.7	0x2b9e	Name error (3)	comfirmationandverification.duartemobilerepair.com	none	none	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:49.229950905 CEST	8.8.8.8	192.168.2.7	0x4cd6	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:08:53.936469078 CEST	8.8.8.8	192.168.2.7	0xd3a0	Name error (3)	comfirmationandverification.duartemobilerepair.com	none	none	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:09:24.030297995 CEST	8.8.8.8	192.168.2.7	0x268f	Name error (3)	comfirmationandverification.duartemobilerepair.com	none	none	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:09:49.291591883 CEST	8.8.8.8	192.168.2.7	0xacc4	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4196, Parent PID: 5264

General

Target ID:	0
Start time:	17:08:43
Start date:	06/06/2023
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:	0x7ff7c2920000
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

Analysis Process: chrome.exe PID: 2720, Parent PID: 4196

General

Target ID:	1
Start time:	17:08:44
Start date:	06/06/2023
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=1868 --field-trial-handle=1672,i,17582304814663474974,3067264136992902369,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c2920000

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: **6256**, Parent PID: **5264**

General

Target ID:	2
Start time:	17:08:47
Start date:	06/06/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://comfirmationandverification.duartemobilerepair.com/
Imagebase:	0x7ff7c2920000
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