ID: 715052
Cookbook: browseurl.jbs
Time: 15:32:34
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://va.mite.gov.it 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 7
General Information 8
Errors 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
Network Behavior 9
Network Port Distribution 9
TCP Packets 9
UDP Packets 11
DNS Queries 11
DNS Answers 11
HTTP Request Dependency Graph 12
HTTPS Proxied Packets 12
Statistics 13
Behavior 13
System Behavior 14
Analysis Process: chrome.exePID: 6000, Parent PID: 2296 14
General 14
File Activities 14
Registry Activities 14
Analysis Process: chrome.exePID: 5596, Parent PID: 6000 14
General 14
File Activities 15
Analysis Process: chrome.exePID: 5260, Parent PID: 2296 15
General 15
Registry Activities 15
Disassembly 15

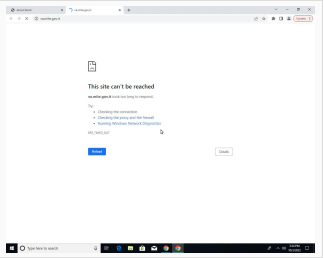
Windows Analysis Report

https://va.mite.gov.it

Overview

General Information

Sample URL:	http://https://va.mite.gov.it
Analysis ID:	715052
Infos:	



Errors

URL not reachable

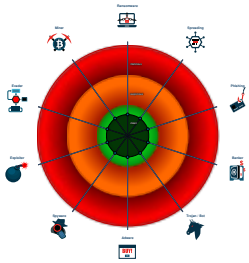
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6000 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5596 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=1952 --field-trial-handle=1632,i,15863442640589831431,16015343658342383034,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5260 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://va.mite.gov.it 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

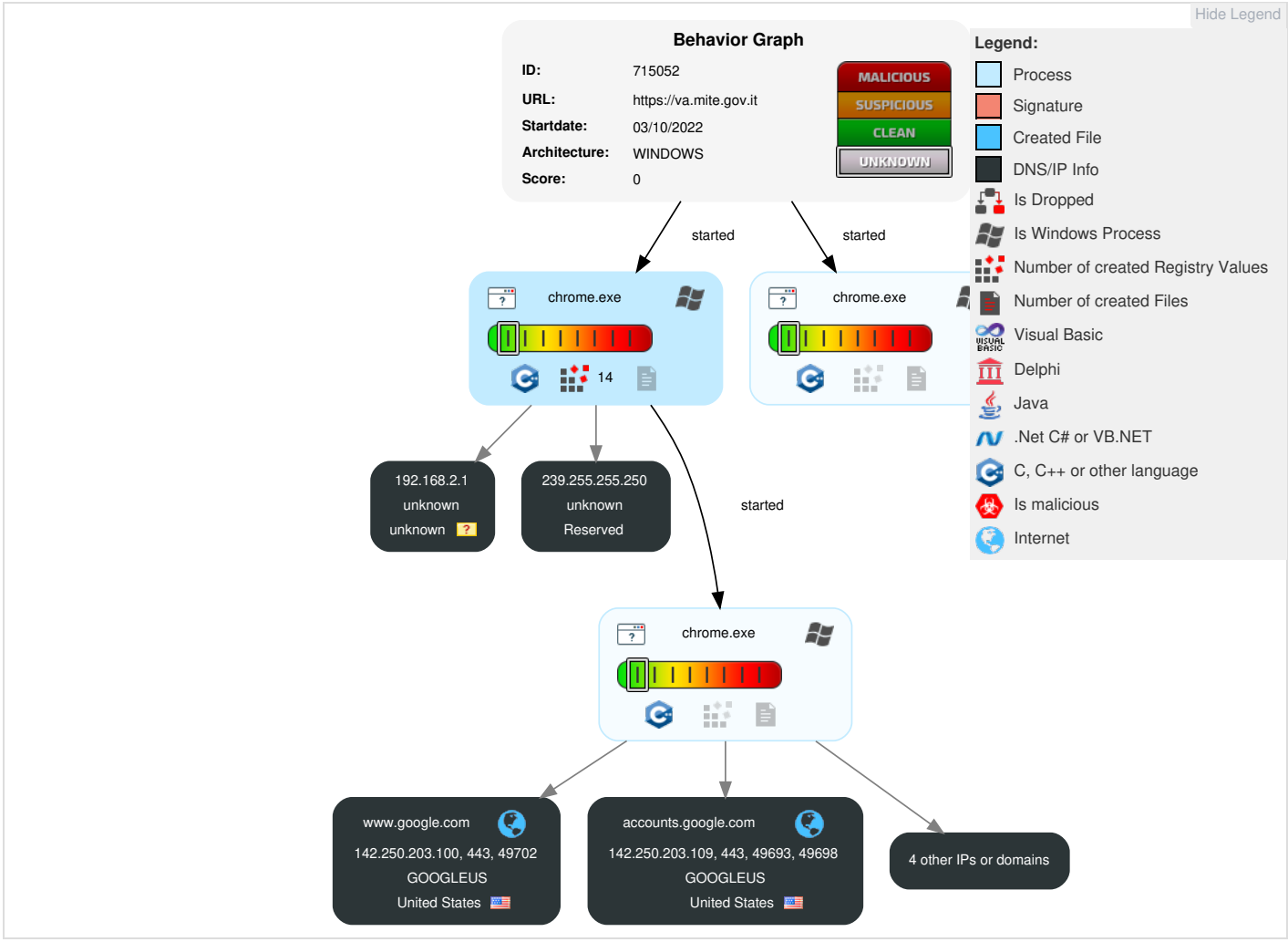
Joe Sandbox Signatures

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	1 Process Injection	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	Rootkit	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

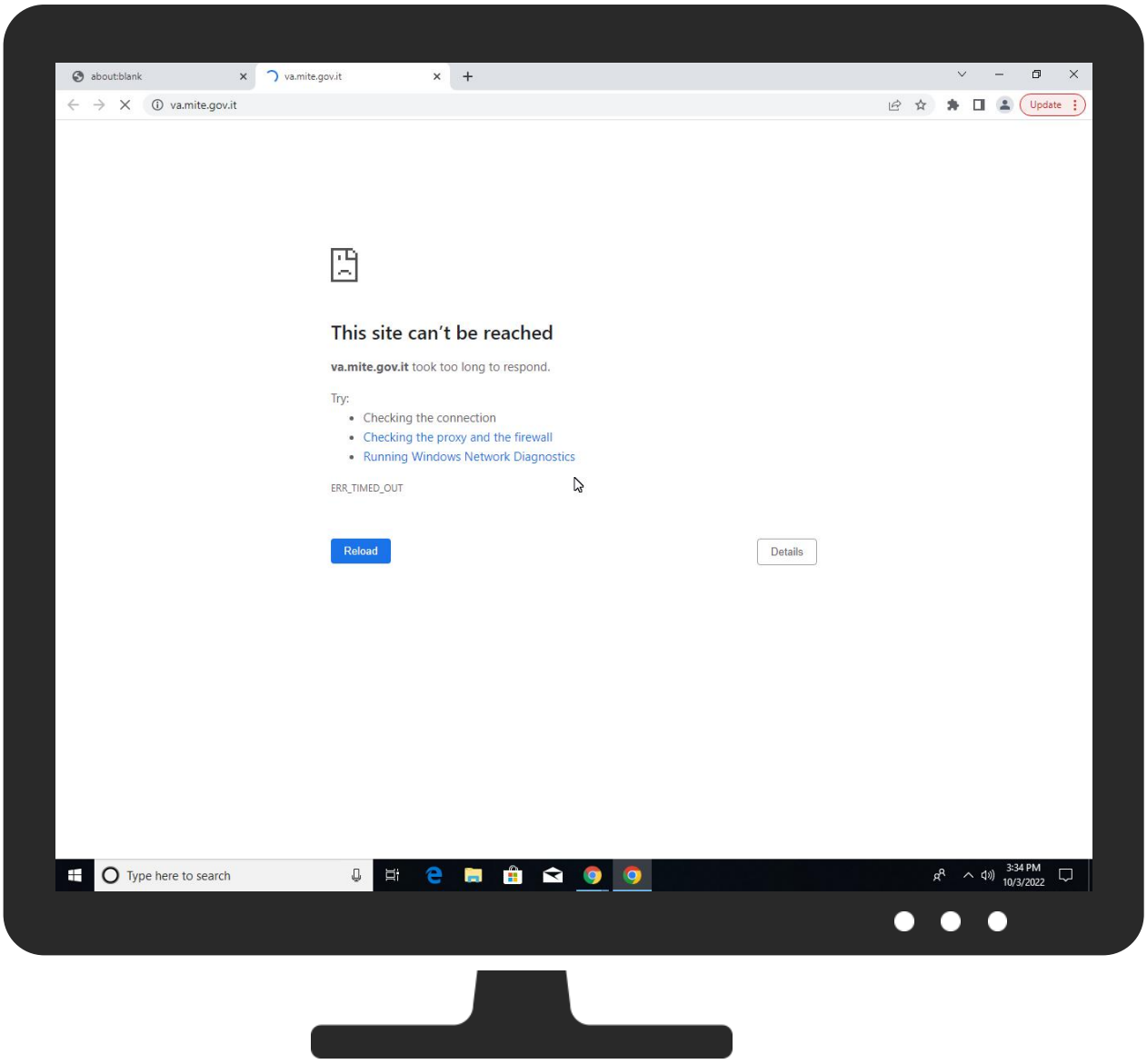
Behavior Graph



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://va.mite.gov.it	0%	Virustotal		Browse
http://https://va.mite.gov.it	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

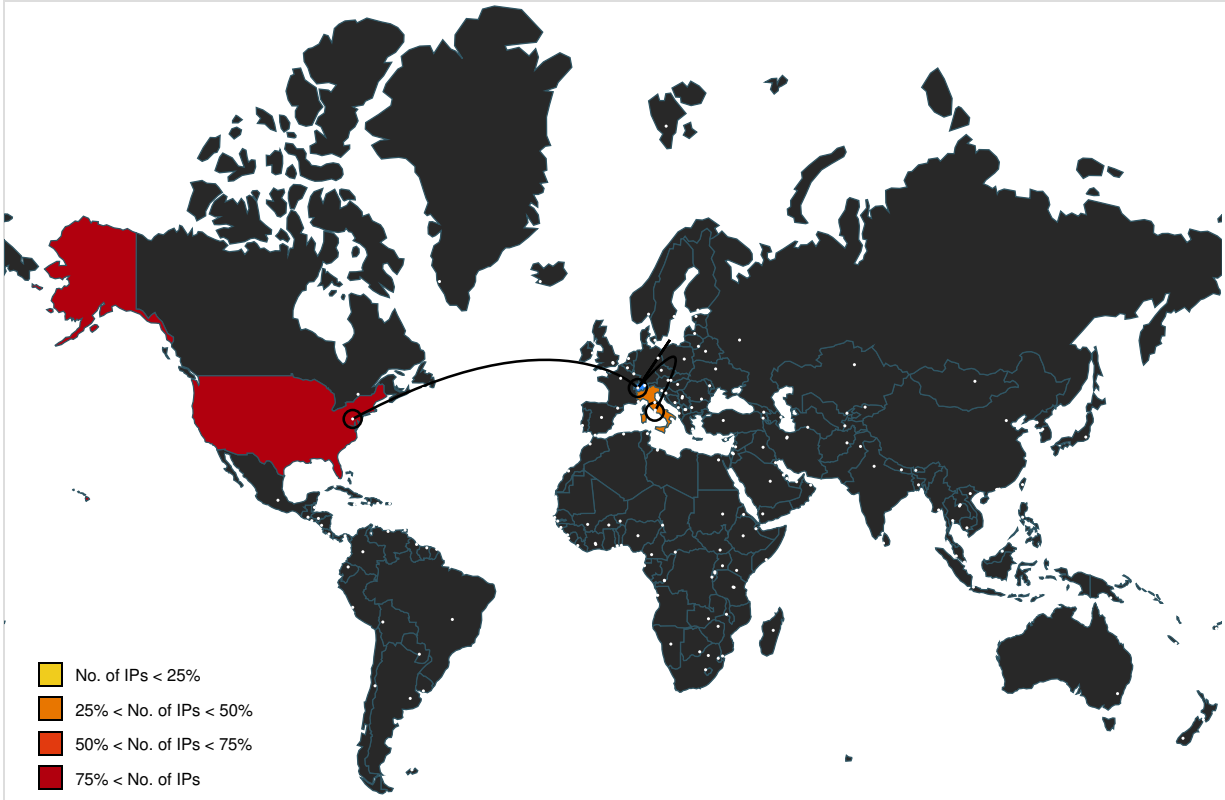
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
va.mite.gov.it	89.119.252.152	true	false		unknown
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://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
89.119.252.152	va.mite.gov.it	Italy		8968	BT-ITALIAIT	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715052
Start date and time:	2022-10-03 15:32:34 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://va.mite.gov.it
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:	3
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:	UNKNOWN
Classification:	unknown0.win@26/0@4/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• **URL browsing timeout or error**

Errors

- URL not reachable

Warnings

- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 93.184.221.240
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, clientservices.googleapis.com, ctldl.windowsupdate.com, www.gstatic.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

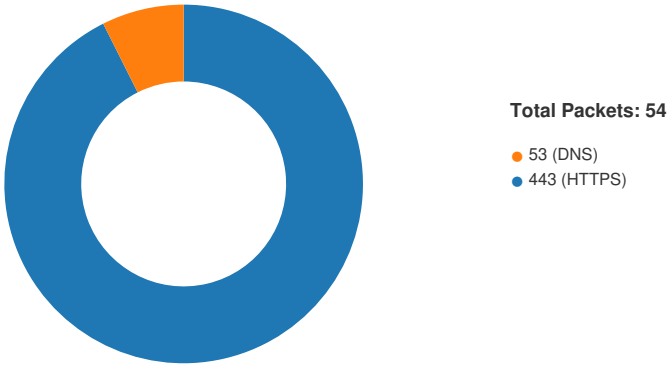
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:33:38.170361996 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.170423031 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.170502901 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.170752048 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.170836926 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.170927048 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.171117067 CEST	49695	443	192.168.2.5	89.119.252.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:33:38.171183109 CEST	443	49695	89.119.252.152	192.168.2.5
Oct 3, 2022 15:33:38.171283007 CEST	49695	443	192.168.2.5	89.119.252.152
Oct 3, 2022 15:33:38.173464060 CEST	49697	443	192.168.2.5	89.119.252.152
Oct 3, 2022 15:33:38.173511028 CEST	443	49697	89.119.252.152	192.168.2.5
Oct 3, 2022 15:33:38.173584938 CEST	49697	443	192.168.2.5	89.119.252.152
Oct 3, 2022 15:33:38.174043894 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.174093962 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.174165964 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.174700022 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.174745083 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.174845934 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.175292969 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.175317049 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.175935984 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.176040888 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.176103115 CEST	49695	443	192.168.2.5	89.119.252.152
Oct 3, 2022 15:33:38.176137924 CEST	443	49695	89.119.252.152	192.168.2.5
Oct 3, 2022 15:33:38.176629066 CEST	49697	443	192.168.2.5	89.119.252.152
Oct 3, 2022 15:33:38.176661968 CEST	443	49697	89.119.252.152	192.168.2.5
Oct 3, 2022 15:33:38.176843882 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.176866055 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.177113056 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.177144051 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.316009998 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.330148935 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.344223022 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.361542940 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.410968065 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.411029100 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.411590099 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.411621094 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.411742926 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.411777973 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.411947012 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.411961079 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.412566900 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.412669897 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.413219929 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.413260937 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.413320065 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.413814068 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.413883924 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.413961887 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.415132046 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.415245056 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.415724039 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.415822983 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:38.415838003 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.415844917 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:38.415904999 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:38.415920973 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.497859001 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.497864008 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:38.516016006 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.033945084 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.033965111 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.034050941 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.034101009 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.034187078 CEST	443	49693	142.250.203.109	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:33:39.034477949 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.034516096 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.034574032 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.034605980 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.034645081 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.034704924 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.034754992 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.034774065 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.034821987 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.034848928 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.034872055 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.070630074 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.070811033 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.070852041 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.071041107 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.072526932 CEST	49699	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.072566986 CEST	443	49699	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.087490082 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.087562084 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.087585926 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.087676048 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.087738991 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.103184938 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.103214025 CEST	443	49698	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.105658054 CEST	49693	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:39.105695009 CEST	443	49693	142.250.203.109	192.168.2.5
Oct 3, 2022 15:33:39.114898920 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.114934921 CEST	443	49694	142.250.203.110	192.168.2.5
Oct 3, 2022 15:33:39.214932919 CEST	49694	443	192.168.2.5	142.250.203.110
Oct 3, 2022 15:33:39.297899961 CEST	49698	443	192.168.2.5	142.250.203.109
Oct 3, 2022 15:33:40.147397995 CEST	49702	443	192.168.2.5	142.250.203.100
Oct 3, 2022 15:33:40.147452116 CEST	443	49702	142.250.203.100	192.168.2.5
Oct 3, 2022 15:33:40.147548914 CEST	49702	443	192.168.2.5	142.250.203.100
Oct 3, 2022 15:33:40.148031950 CEST	49702	443	192.168.2.5	142.250.203.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:33:38.079639912 CEST	58648	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:33:38.082092047 CEST	56894	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:33:38.083623886 CEST	50295	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:33:38.100917101 CEST	53	50295	8.8.8.8	192.168.2.5
Oct 3, 2022 15:33:38.107141972 CEST	53	58648	8.8.8.8	192.168.2.5
Oct 3, 2022 15:33:38.113842964 CEST	53	56894	8.8.8.8	192.168.2.5
Oct 3, 2022 15:33:40.111716986 CEST	51441	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:33:40.131578922 CEST	53	51441	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:33:38.079639912 CEST	192.168.2.5	8.8.8.8	0x234f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:38.082092047 CEST	192.168.2.5	8.8.8.8	0xa2	Standard query (0)	va.mite.gov.it	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:38.083623886 CEST	192.168.2.5	8.8.8.8	0xd61f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:40.111716986 CEST	192.168.2.5	8.8.8.8	0x6b6f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 15:33:38.100917101 CEST	8.8.8.8	192.168.2.5	0xd61f	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:38.107141972 CEST	8.8.8.8	192.168.2.5	0x234f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 15:33:38.107141972 CEST	8.8.8.8	192.168.2.5	0x234f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:38.113842964 CEST	8.8.8.8	192.168.2.5	0xa2	No error (0)	va.mite.gov.it		89.119.252.152	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:33:40.131578922 CEST	8.8.8.8	192.168.2.5	0x6b6f	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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49693	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:33:39 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 13:33:39 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-10-03 13:33:39 UTC	2	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 13:33:39 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: script-src 'report-sample' 'nonce-hboXmqypvi0YxOaLgU1ctg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

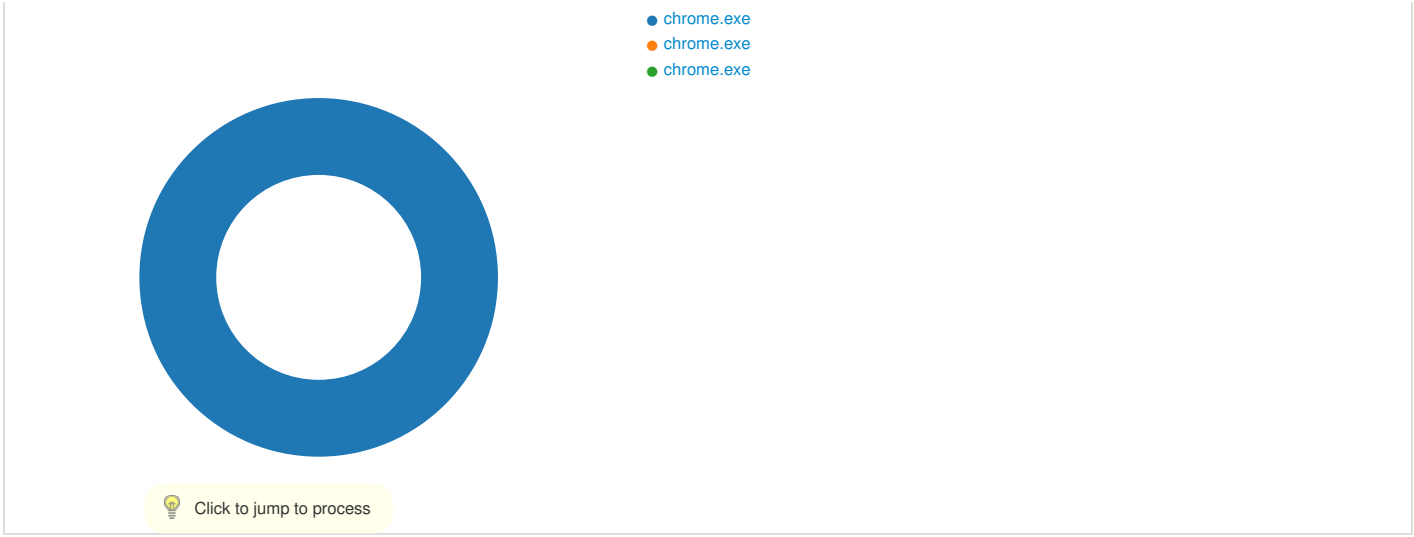
Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:33:39 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-10-03 13:33:39 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49699	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:33:39 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 13:33:39 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-1jlefdrTK1cUAI-EsBVePw' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 13:33:39 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 23619 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 13:33:39 UTC	2	IN	Data Raw: 32 63 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 33 36 31 39 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="23619"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 13:33:39 UTC	2	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgm ieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a 4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 13:33:39 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6000, Parent PID: 2296

General

Target ID:	0
Start time:	15:33:33
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7d31b0000
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

Registry Activities

Analysis Process: chrome.exe PID: 5596, Parent PID: 6000

General

Target ID:	1
Start time:	15:33:34
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1952 --field-trial-handle=1632,i,15863442640589831431,16015343658342383034,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8

Imagebase:	0x7ff7d31b0000
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: **5260**, Parent PID: **2296**

General

Target ID:	2
Start time:	15:33:35
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://va.mite.gov.it
Imagebase:	0x7ff7d31b0000
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