ID: 753422
Cookbook: browseurl.jbs
Time: 19:52:32
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

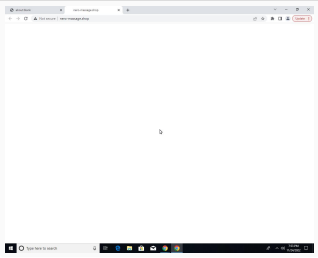
Windows Analysis Report

http://nero-massage.shop

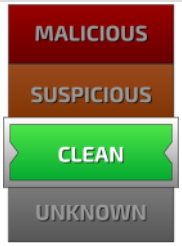
Overview

General Information

Sample URL:	http://nero-massage.shop
Analysis ID:	753422
Infos:	



Detection

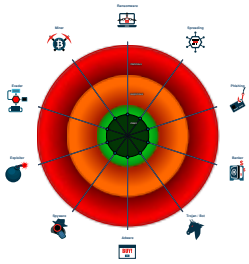


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 2328 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5152 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=1956 --field-trial-handle=1812,i,3518441739163221011,6637184233728530685,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5352 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://nero-massage.shop 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

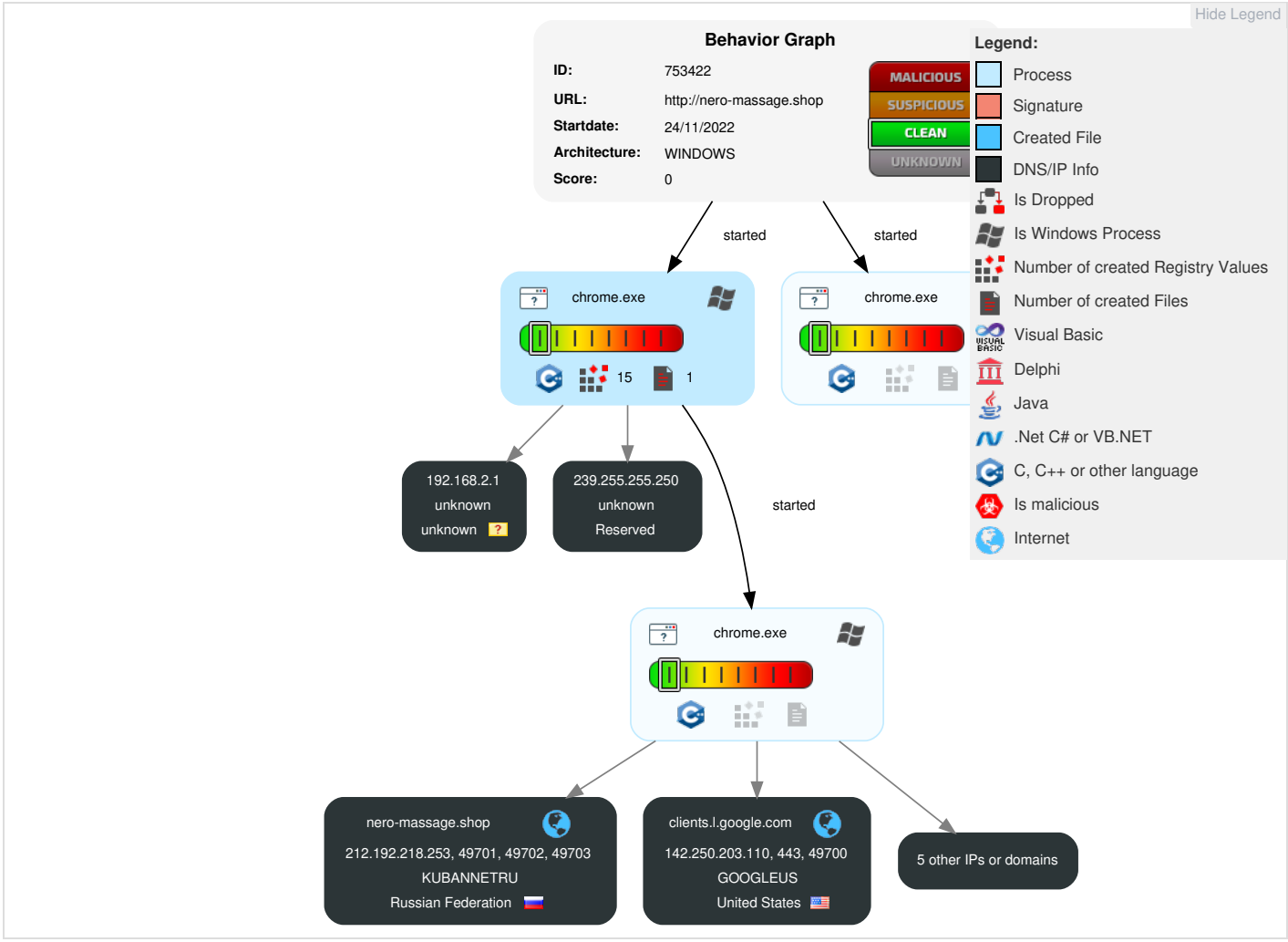
Joe Sandbox Signatures

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

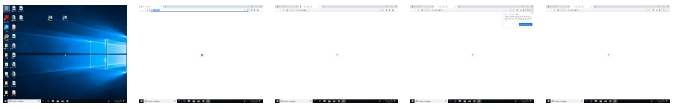
Behavior Graph

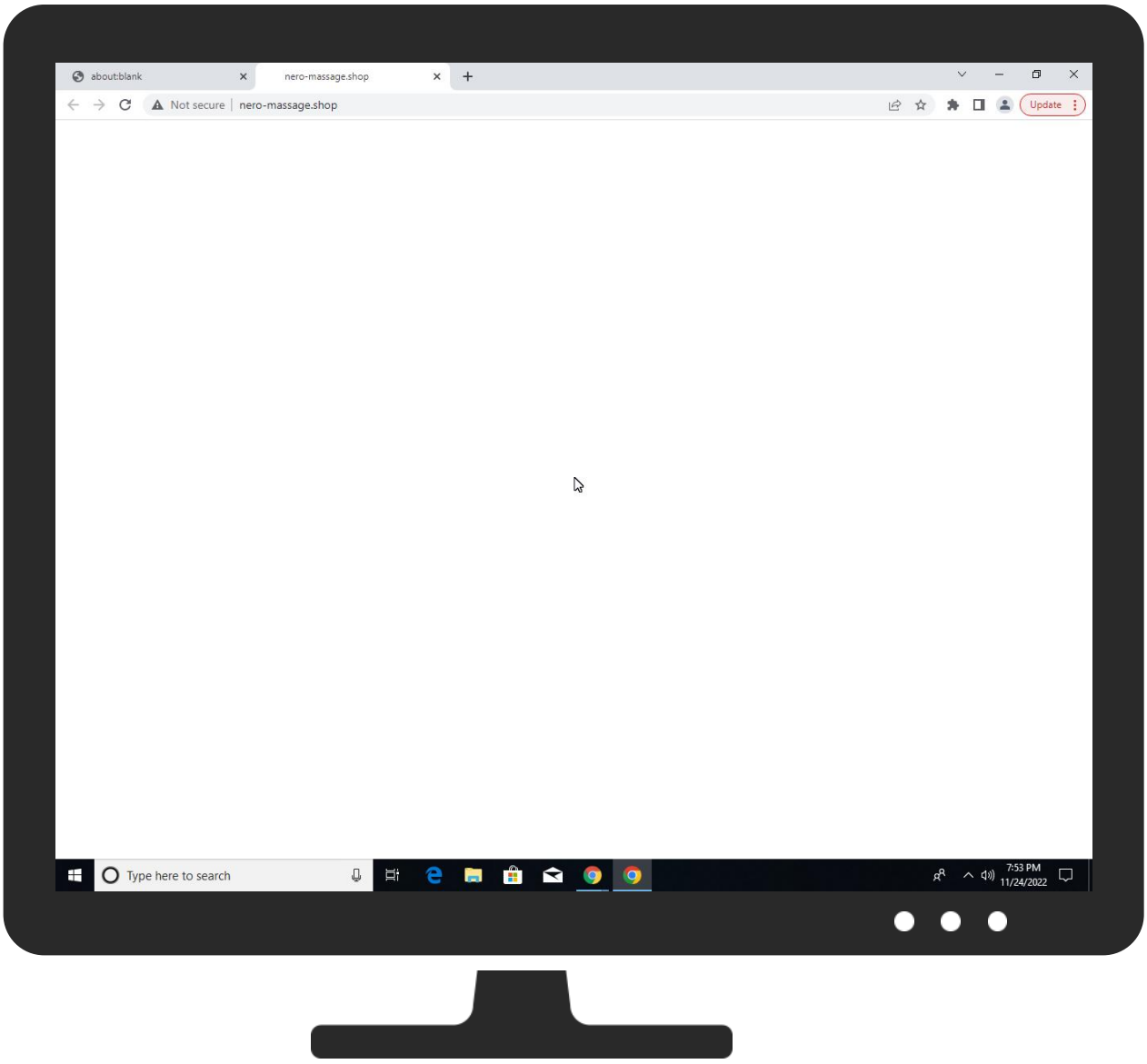


Screenshots

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://nero-massage.shop	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://nero-massage.shop/favicon.ico	0%	Avira URL Cloud	safe	
http://nero-massage.shop/	0%	Avira URL Cloud	safe	

Domains and IPs

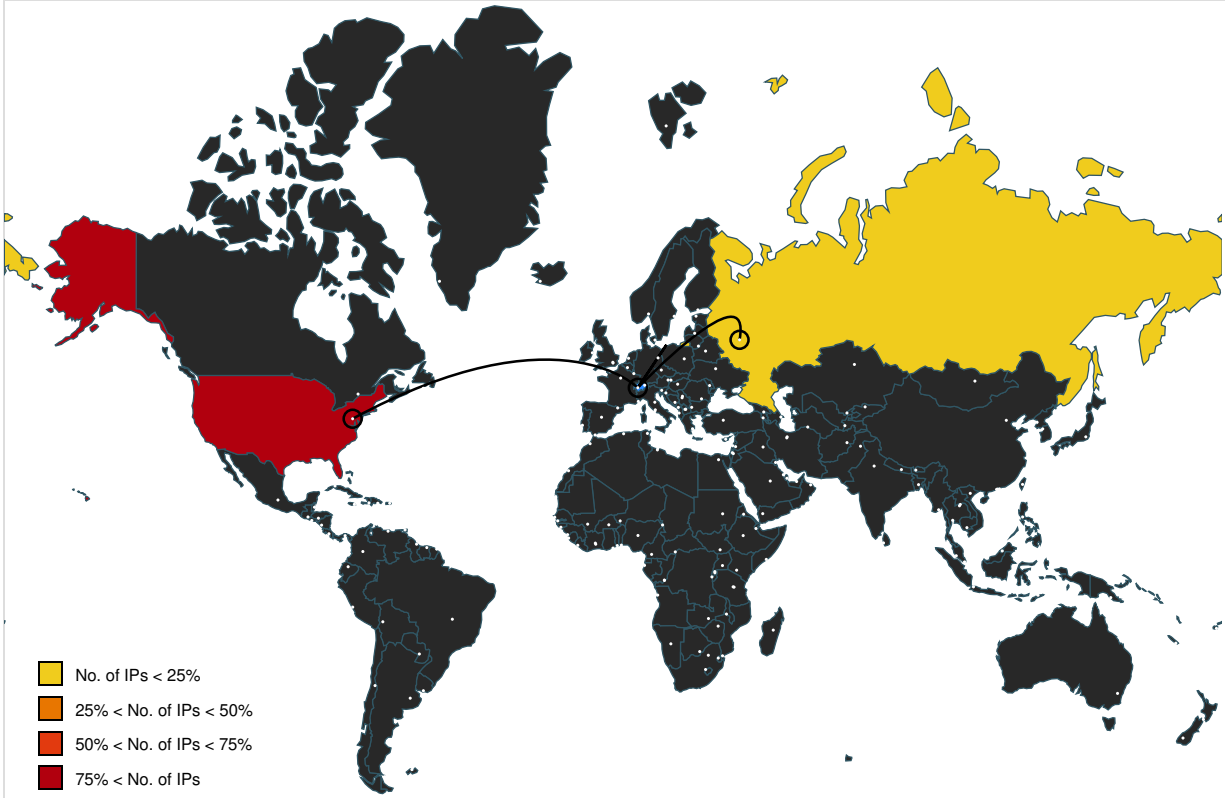
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
nero-massage.shop	212.192.218.253	true	false		unknown
www.google.com	172.217.168.36	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
http://nero-massage.shop/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://nero-massage.shop/	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.68	unknown	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
212.192.218.253	nero-massage.shop	Russian Federation		8663	KUBANNETRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753422
Start date and time:	2022-11-24 19:52:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://nero-massage.shop
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:	12
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@25/0@5/8
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): 172.217.168.67, 34.104.35.123
- Excluded domains from analysis (whitelisted): 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

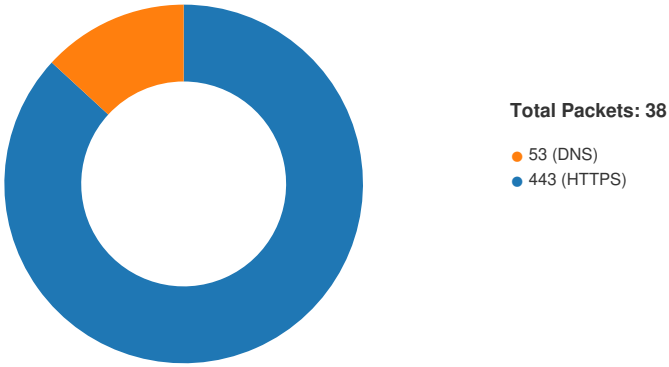
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:53:31.423285007 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:31.423355103 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:31.423434973 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:31.424011946 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:31.424046993 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:31.493980885 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:31.499541044 CET	49698	443	192.168.2.3	172.217.168.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:53:31.499573946 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:31.501488924 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:31.501599073 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:31.539515972 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.539561987 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.539634943 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.539920092 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.539932013 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.610112906 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.746639013 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.968321085 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.968385935 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.970623970 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.970649958 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.970714092 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.972928047 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:31.973007917 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:31.973042011 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.046624899 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:32.914686918 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:32.914762020 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.914999962 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:32.915014029 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.915146112 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.915210962 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:32.915245056 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.915534019 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.915927887 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:32.915965080 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.949918985 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.950086117 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:32.950143099 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.950196028 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:32.950251102 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:32.993544102 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.993673086 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:32.993729115 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.994059086 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:32.994124889 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:33.118357897 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.118360043 CET	49700	443	192.168.2.3	142.250.203.110
Nov 24, 2022 19:53:33.118438959 CET	443	49700	142.250.203.110	192.168.2.3
Nov 24, 2022 19:53:33.120249987 CET	49698	443	192.168.2.3	172.217.168.45
Nov 24, 2022 19:53:33.120311022 CET	443	49698	172.217.168.45	192.168.2.3
Nov 24, 2022 19:53:33.124341965 CET	49702	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.170217991 CET	49703	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.220031977 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.220130920 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.227030039 CET	80	49702	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.227173090 CET	49702	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.273191929 CET	80	49703	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.273358107 CET	49703	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.322195053 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.424112082 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.426261902 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.514729977 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.674765110 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:33.777182102 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.777218103 CET	80	49701	212.192.218.253	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:53:33.777236938 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:53:33.777350903 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:53:34.531985044 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.532059908 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.532160044 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.532707930 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.532824993 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.594708920 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.595299959 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.595340967 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.597248077 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.597320080 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.614911079 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.614952087 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.615217924 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.761991024 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:34.762031078 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:34.961536884 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:44.584458113 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:44.584551096 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:53:44.584625959 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:46.052603006 CET	49707	443	192.168.2.3	172.217.168.36
Nov 24, 2022 19:53:46.052645922 CET	443	49707	172.217.168.36	192.168.2.3
Nov 24, 2022 19:54:18.240581036 CET	49702	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:54:18.287508965 CET	49703	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:54:18.342931986 CET	80	49702	212.192.218.253	192.168.2.3
Nov 24, 2022 19:54:18.390132904 CET	80	49703	212.192.218.253	192.168.2.3
Nov 24, 2022 19:54:18.787626028 CET	49701	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:54:18.889396906 CET	80	49701	212.192.218.253	192.168.2.3
Nov 24, 2022 19:54:33.334175110 CET	80	49702	212.192.218.253	192.168.2.3
Nov 24, 2022 19:54:33.334989071 CET	49702	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:54:33.376420021 CET	80	49703	212.192.218.253	192.168.2.3
Nov 24, 2022 19:54:33.376907110 CET	49703	80	192.168.2.3	212.192.218.253
Nov 24, 2022 19:54:34.607464075 CET	49703	80	192.168.2.3	212.192.218.253

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:53:31.290333033 CET	52387	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:53:31.293097973 CET	56924	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:53:31.318754911 CET	53	56924	8.8.8.8	192.168.2.3
Nov 24, 2022 19:53:31.332197905 CET	53	52387	8.8.8.8	192.168.2.3
Nov 24, 2022 19:53:32.778382063 CET	60625	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:53:32.800947905 CET	53	60625	8.8.8.8	192.168.2.3
Nov 24, 2022 19:53:34.503326893 CET	60582	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:53:34.522851944 CET	53	60582	8.8.8.8	192.168.2.3
Nov 24, 2022 19:54:34.580152988 CET	60749	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:54:34.599622011 CET	53	60749	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:53:31.290333033 CET	192.168.2.3	8.8.8.8	0xe865	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:31.293097973 CET	192.168.2.3	8.8.8.8	0x1a75	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:32.778382063 CET	192.168.2.3	8.8.8.8	0xe00f	Standard query (0)	nero-massage.shop	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:34.503326893 CET	192.168.2.3	8.8.8.8	0x8233	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:54:34.580152988 CET	192.168.2.3	8.8.8.8	0x9fe9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

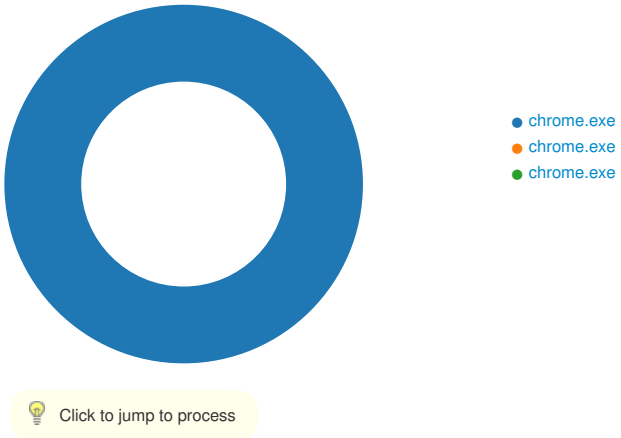
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:53:31.318754911 CET	8.8.8.8	192.168.2.3	0x1a75	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:31.332197905 CET	8.8.8.8	192.168.2.3	0xe865	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:53:31.332197905 CET	8.8.8.8	192.168.2.3	0xe865	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:32.800947905 CET	8.8.8.8	192.168.2.3	0xe00f	No error (0)	nero-massage.shop		212.192.218.253	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:53:34.522851944 CET	8.8.8.8	192.168.2.3	0x8233	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:34.599622011 CET	8.8.8.8	192.168.2.3	0x9fe9	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- nero-massage.shop

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2328**, Parent PID: **2464**

General

Target ID:	0
Start time:	19:53:28
Start date:	24/11/2022
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:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5152**, Parent PID: **2328**

General

Target ID:	1
Start time:	19:53:29
Start date:	24/11/2022
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=1956 --field-trial-handle=1812,i,3518441739163221011,6637184233728530685,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5352**, Parent PID: **2464**

General	
Target ID:	2
Start time:	19:53:30
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://nero-massage.shop
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly