ID: 800717
Cookbook: browseurl.jbs
Time: 18:40:17
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

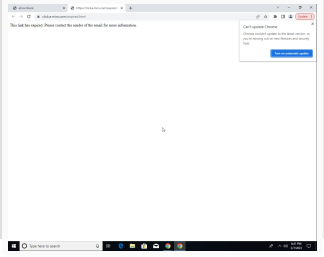
Windows Analysis Report

https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b...

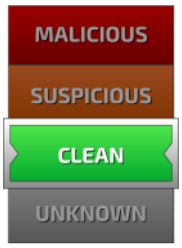
Overview

General Information

Sample URL:	https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac...64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e
Analysis ID:	800717
Infos:	



Detection

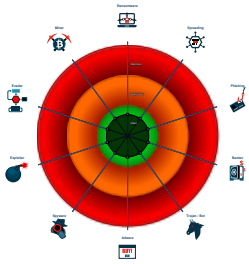


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 3312 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2640 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=1696 --field-trial-handle=1700,i,6389677442699171845,17054306635293568143,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6180 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e 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

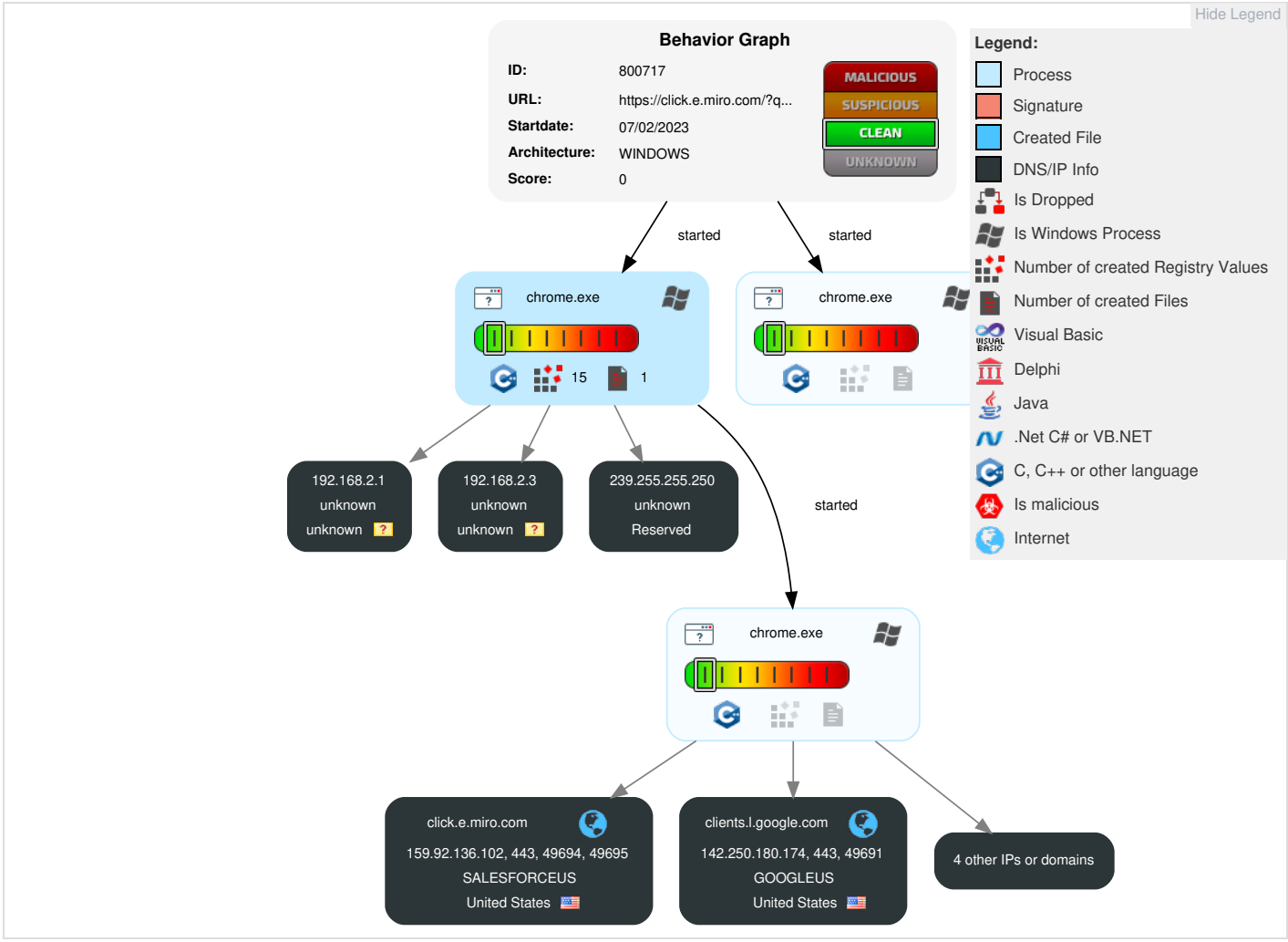
Joe Sandbox Signatures

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	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

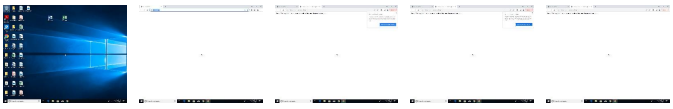
Behavior Graph

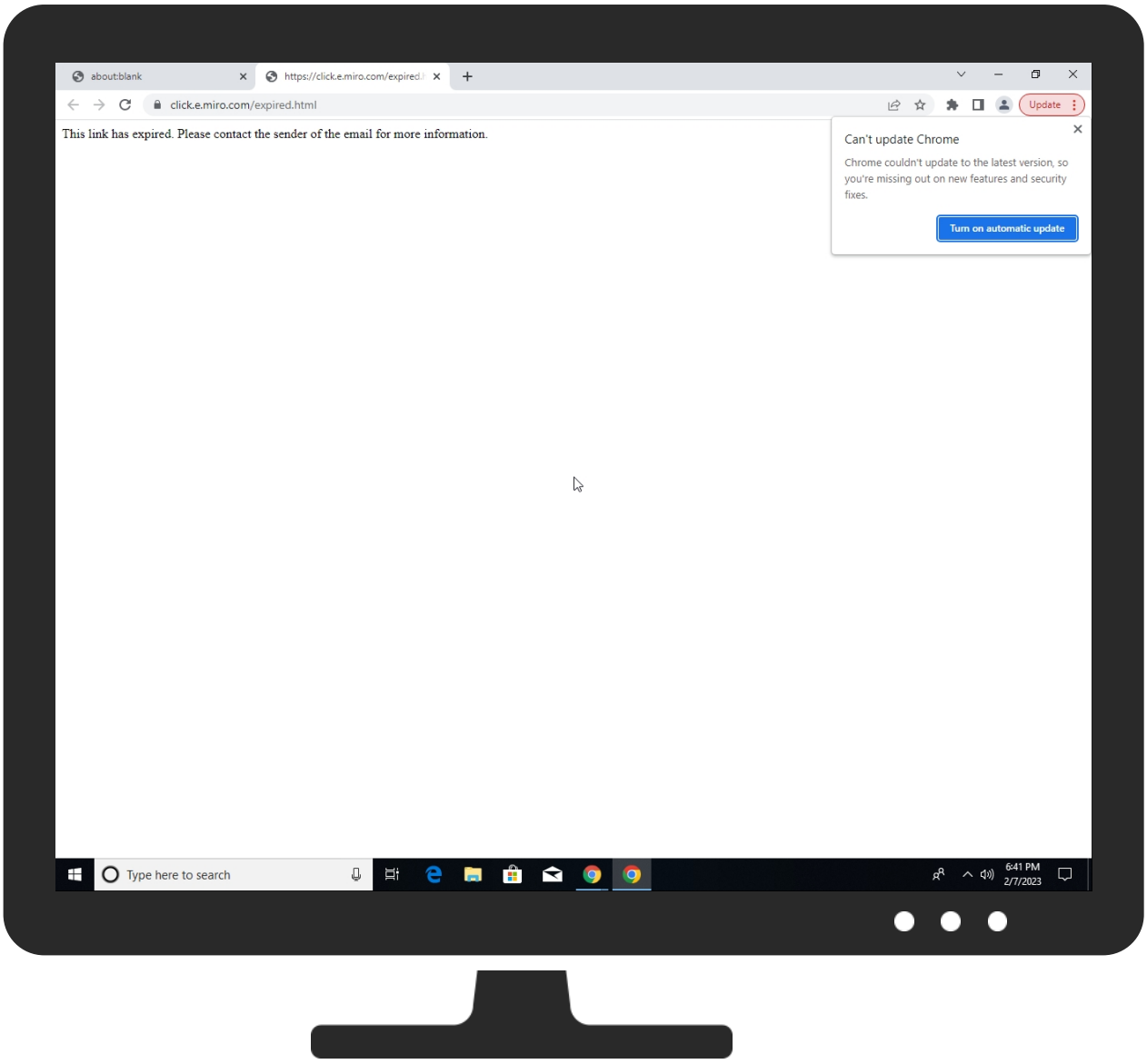


Screenshots

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://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e	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://https://click.e.miro.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

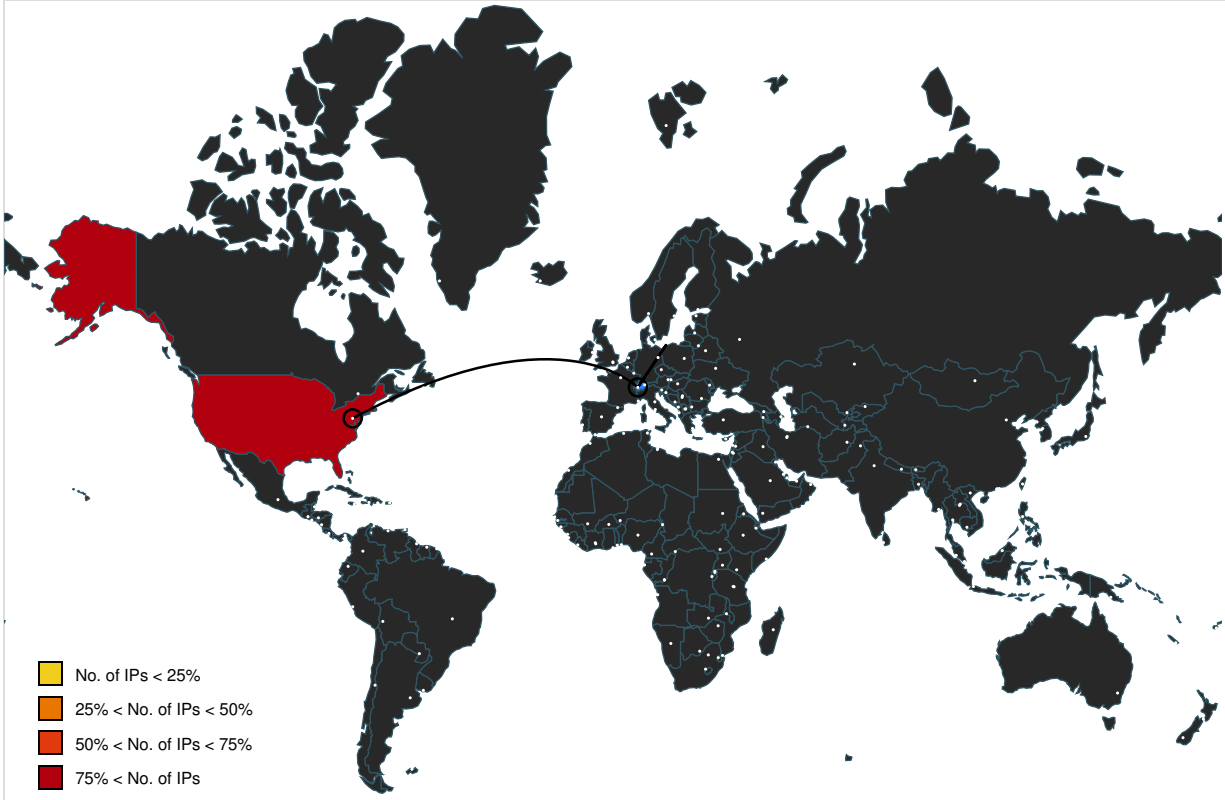
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
click.e.miro.com	159.92.136.102	true	false		unknown
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-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://click.e.miro.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.92.136.102	click.e.miro.com	United States		14340	SALESFORCEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800717
Start date and time:	2023-02-07 18:40:17 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e
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:	CLEAN
Classification:	clean0.win@26/0@8/8
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): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.250.180.163
- 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
- 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

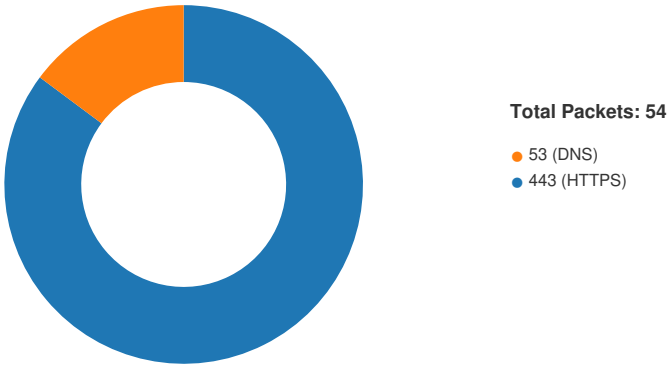
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:21.323513985 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:21.323571920 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.323673010 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:21.323971033 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:21.324002028 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:21.324071884 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:21.324769020 CET	49691	443	192.168.2.4	142.250.180.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:21.324795008 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.325571060 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:21.325584888 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:21.417732000 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:21.418148994 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:21.418191910 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:21.420877934 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:21.420980930 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:21.439961910 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.449426889 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:21.449446917 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.450499058 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.450603962 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:21.452377081 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:21.452466965 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:21.563389063 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:21.563432932 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:21.563515902 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:21.563900948 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:21.563930035 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:21.660068035 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:21.707281113 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.473896027 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.473968029 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.477674961 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.477840900 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.883197069 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:22.883256912 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.883589029 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.883620977 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:22.883639097 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.883847952 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:22.883900881 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.884226084 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.890285969 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:22.890331984 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.890584946 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.890614033 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.891107082 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.891150951 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.891184092 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.925384998 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:22.925578117 CET	49694	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:22.927272081 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.927412987 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:22.927470922 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.927584887 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:22.927676916 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:22.935434103 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:22.956634045 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.956748009 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:22.956808090 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.956990957 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:22.957072973 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:23.214082003 CET	49692	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:41:23.214121103 CET	443	49692	216.58.209.45	192.168.2.4
Feb 7, 2023 18:41:23.215550900 CET	49691	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:41:23.215579033 CET	443	49691	142.250.180.174	192.168.2.4
Feb 7, 2023 18:41:23.508069992 CET	49694	443	192.168.2.4	159.92.136.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:23.508112907 CET	443	49694	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.518492937 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.518601894 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.518764973 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.519186020 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.519229889 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.578073978 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.578545094 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.578598022 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.579303026 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.580159903 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.580205917 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.580319881 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.580435038 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.580455065 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.630546093 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.630666018 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.630736113 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.662408113 CET	49695	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.662436962 CET	443	49695	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.779560089 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.779612064 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.779781103 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.780145884 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.780181885 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.842941046 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.843678951 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.843720913 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.844499111 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.845912933 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.845942020 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.846084118 CET	49697	443	192.168.2.4	159.92.136.102
Feb 7, 2023 18:41:23.846097946 CET	443	49697	159.92.136.102	192.168.2.4
Feb 7, 2023 18:41:23.846142054 CET	443	49697	159.92.136.102	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:21.212063074 CET	61105	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:21.212933064 CET	56572	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:21.240099907 CET	53	61105	8.8.8.8	192.168.2.4
Feb 7, 2023 18:41:21.241527081 CET	53	56572	8.8.8.8	192.168.2.4
Feb 7, 2023 18:41:21.341901064 CET	50911	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:21.362142086 CET	53	50911	8.8.8.8	192.168.2.4
Feb 7, 2023 18:41:23.198276043 CET	58565	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:23.218149900 CET	53	58565	8.8.8.8	192.168.2.4
Feb 7, 2023 18:41:24.656378984 CET	61007	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:24.674410105 CET	53	61007	8.8.8.8	192.168.2.4
Feb 7, 2023 18:41:24.680270910 CET	60686	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:41:24.698158979 CET	53	60686	8.8.8.8	192.168.2.4
Feb 7, 2023 18:42:24.716645956 CET	63746	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:42:24.755263090 CET	53	63746	8.8.8.8	192.168.2.4
Feb 7, 2023 18:42:24.759188890 CET	50622	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:42:24.779109001 CET	53	50622	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
Feb 7, 2023 18:41:21.212063074 CET	192.168.2.4	8.8.8.8	0xa30d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:21.212933064 CET	192.168.2.4	8.8.8.8	0xcd00	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:21.341901064 CET	192.168.2.4	8.8.8.8	0x94ce	Standard query (0)	click.e.miro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:23.198276043 CET	192.168.2.4	8.8.8.8	0xe97	Standard query (0)	click.e.miro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:24.656378984 CET	192.168.2.4	8.8.8.8	0x8ae3	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:24.680270910 CET	192.168.2.4	8.8.8.8	0x38ac	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:42:24.716645956 CET	192.168.2.4	8.8.8.8	0x9b05	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:42:24.759188890 CET	192.168.2.4	8.8.8.8	0x72aa	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

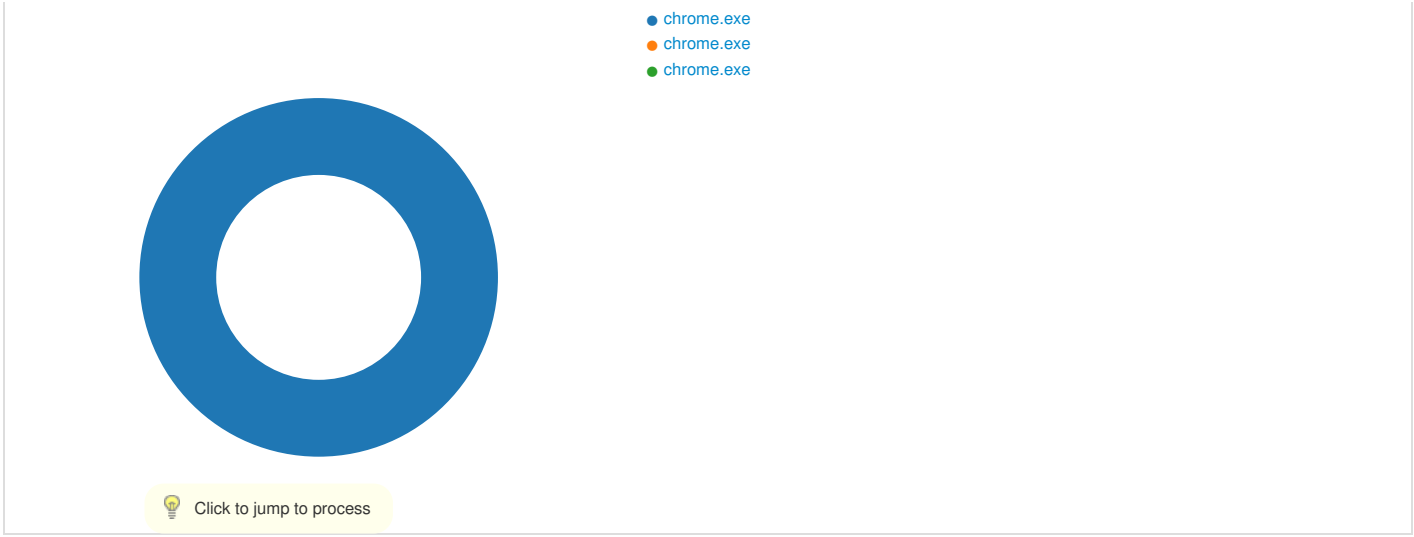
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:41:21.240099907 CET	8.8.8.8	192.168.2.4	0xa30d	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:21.241527081 CET	8.8.8.8	192.168.2.4	0xcd00	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:41:21.241527081 CET	8.8.8.8	192.168.2.4	0xcd00	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:21.362142086 CET	8.8.8.8	192.168.2.4	0x94ce	No error (0)	click.e.miro.com		159.92.136.102	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:23.218149900 CET	8.8.8.8	192.168.2.4	0xe97	No error (0)	click.e.miro.com		159.92.136.102	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:24.674410105 CET	8.8.8.8	192.168.2.4	0x8ae3	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:24.698158979 CET	8.8.8.8	192.168.2.4	0x38ac	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:42:24.755263090 CET	8.8.8.8	192.168.2.4	0x9b05	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:42:24.779109001 CET	8.8.8.8	192.168.2.4	0x72aa	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- click.e.miro.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3312, Parent PID: 2348

General

Target ID:	0
Start time:	18:41:18
Start date:	07/02/2023
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

Registry Activities

Analysis Process: chrome.exe PID: 2640, Parent PID: 3312

General

Target ID:	1
Start time:	18:41:19
Start date:	07/02/2023
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=1696 --field-trial-handle=1700,i,6389677442699171845,17054306635293568143,131072 --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: **6180**, Parent PID: **2348**

General

Target ID:	2
Start time:	18:41:20
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://click.e.miro.com/?qs=8297420c8082a45c5c65a9162d67fce2f624d64ce9c4ac4f6be3f5a7f522b1ae66bb8478daf59e934b6193f0bca9bd6e93f4cd8fc202659e
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

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