ID: 800712
Cookbook: browseurl.jbs
Time: 18:33:34
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

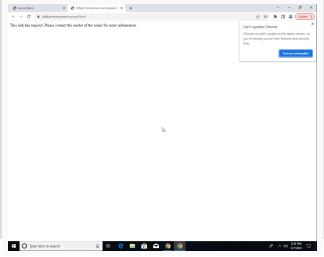
Windows Analysis Report

https://click.e.miro.com/?qs=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629e..

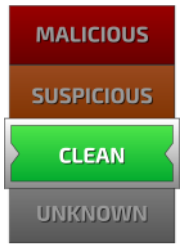
Overview

General Information

Sample URL:	https://click.e.miro.com/?qs=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f...d8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863
Analysis ID:	800712
Infos:	



Detection

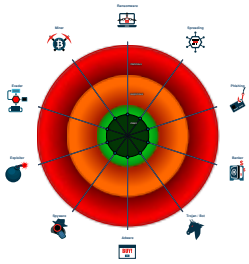


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5812 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6004 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=1932 --field-trial-handle=1724,i,2876507980441582479,18001650036527390366,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4520 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://click.e.miro.com/?qs=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863 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

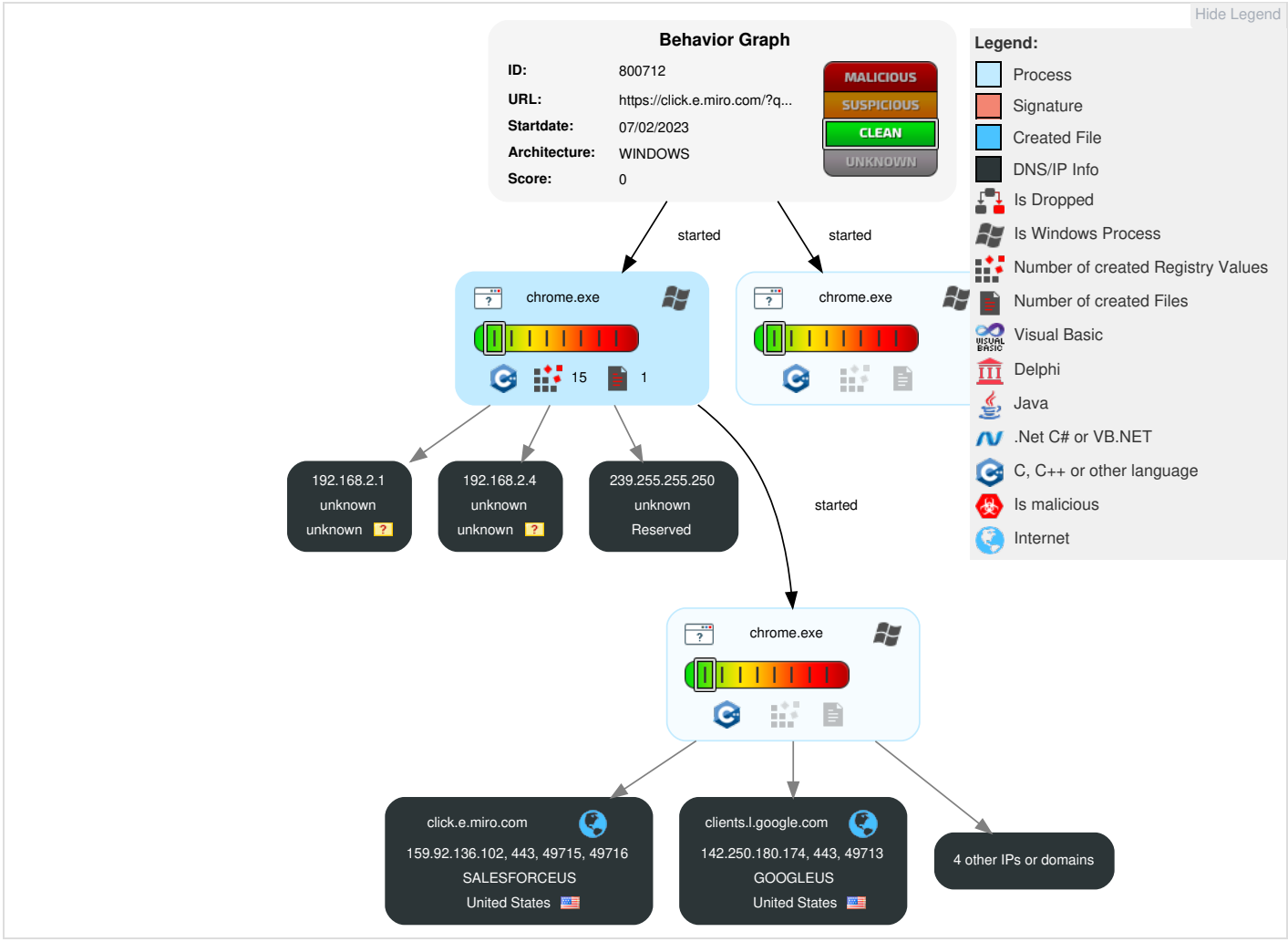
Joe Sandbox Signatures

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

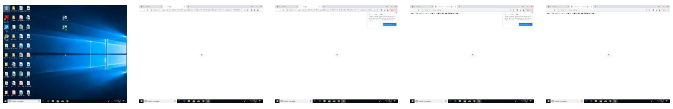
Behavior Graph

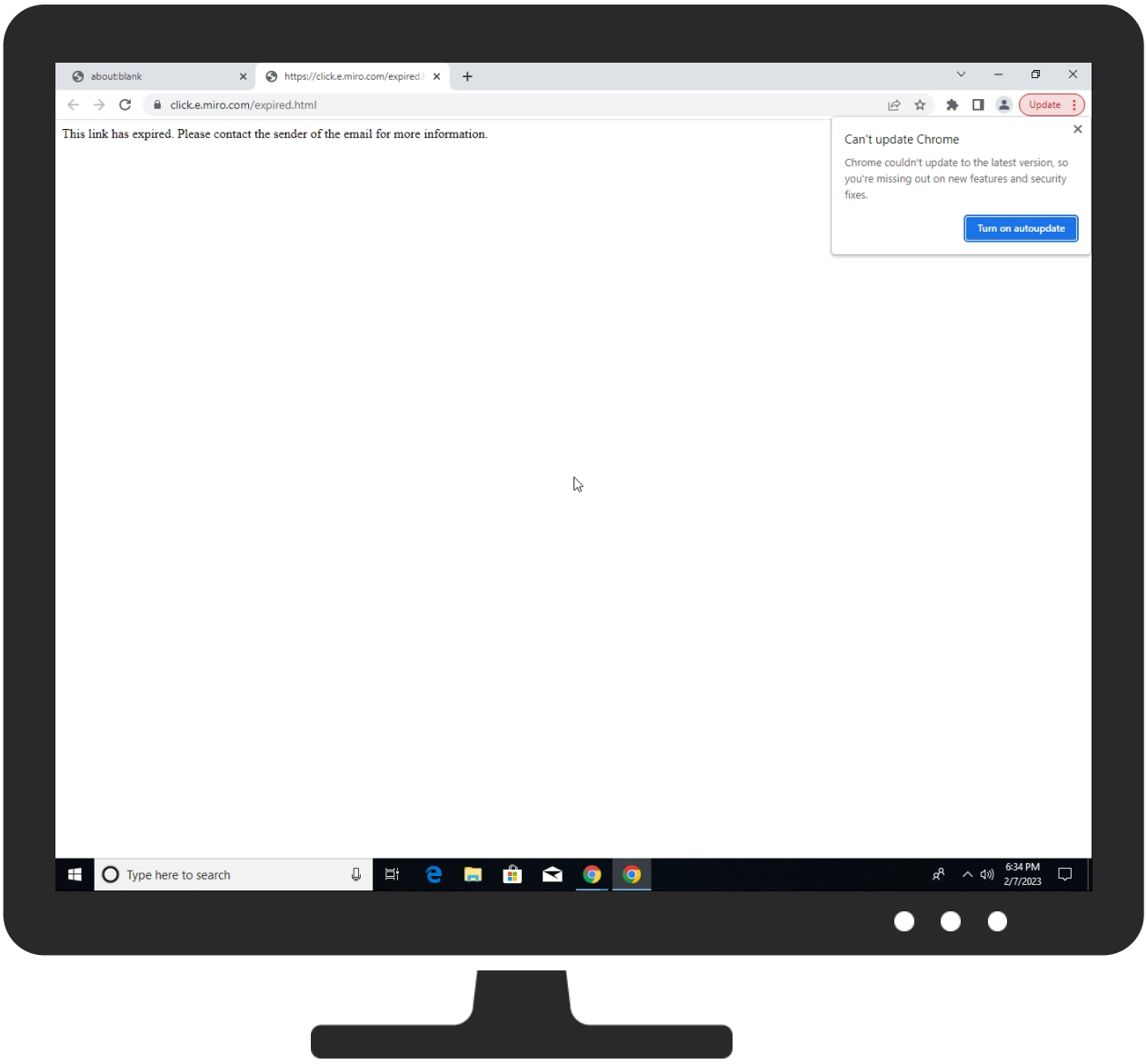


Screenshots

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=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863	0%	Virustotal		Browse
http://https://click.e.miro.com/?qs=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863	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

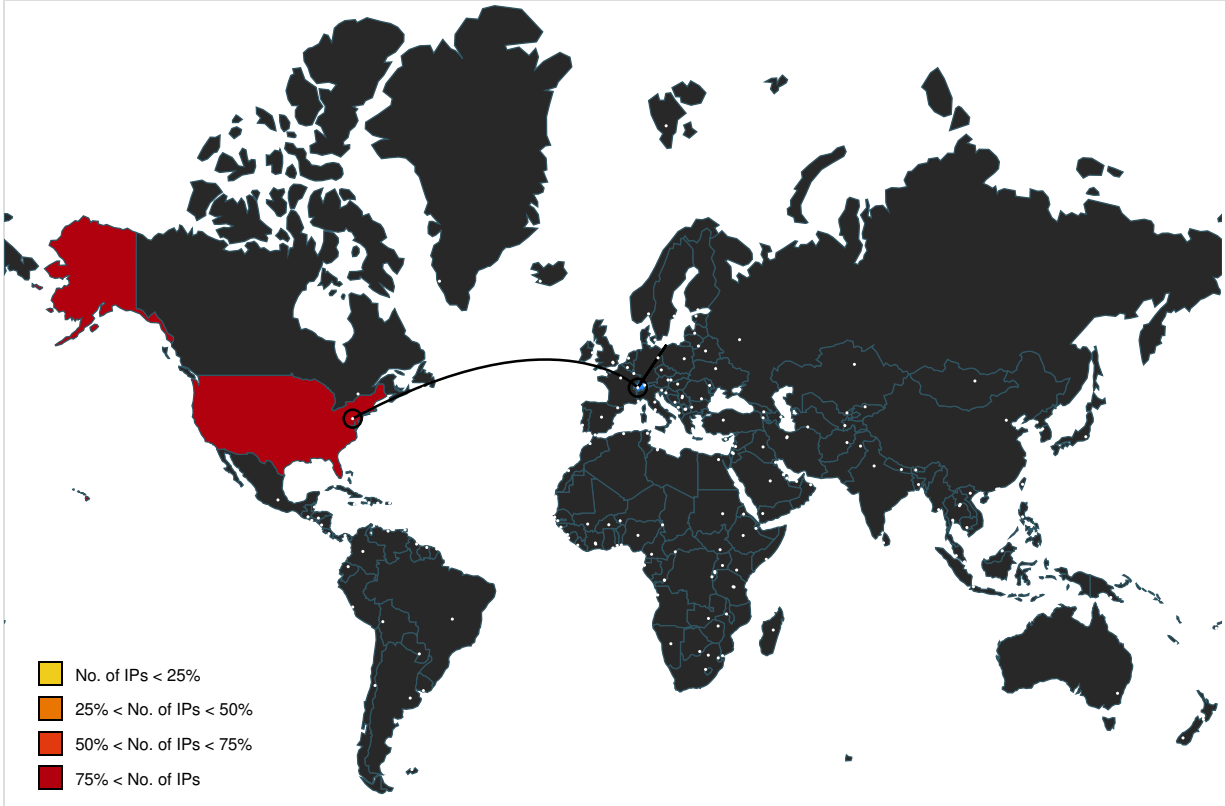
Contacted Domains

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-US&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=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800712
Start date and time:	2023-02-07 18:33:34 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://click.e.miro.com/?qs=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863
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:	11
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, backgroundTaskHost.exe, svchost.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): www.bing.com, client.wns.windows.com, fs.microsoft.com, edgedl.me.gvt1.com, login.live.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

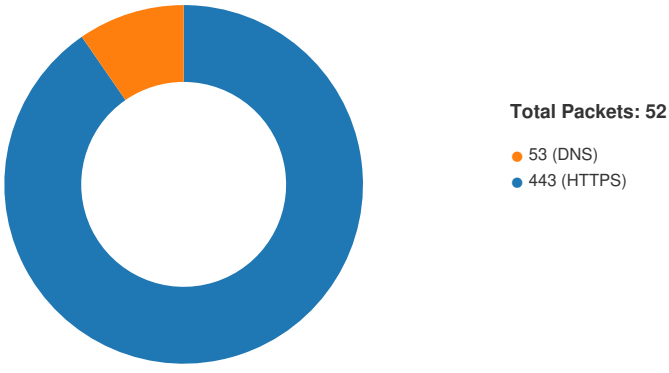
No created / dropped files found

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 18:34:41.689753056 CET	49713	443	192.168.2.7	142.250.180.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:41.689815998 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:41.689889908 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:41.690248966 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:41.690291882 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:41.690361977 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:41.690685987 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:41.690726042 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:41.690797091 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:41.692467928 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:41.692497969 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:41.692990065 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:41.693020105 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:41.693567038 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:41.693584919 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:41.810769081 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:41.826823950 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:41.845438957 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:41.866954088 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:41.874937057 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:41.974988937 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:42.221183062 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:42.221223116 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:42.227319956 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:42.227427959 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:42.227504015 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:42.230400085 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:42.230443954 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:42.230746031 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:42.230783939 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:42.231617928 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:42.231637955 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:42.231801987 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:42.232466936 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:42.232661009 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:42.233311892 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:42.233424902 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:42.274995089 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.005573988 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:43.005652905 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.005899906 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.005959988 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:43.005974054 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.006944895 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:43.006987095 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.007134914 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:43.007148027 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.007369995 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.007394075 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.007441998 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.007606983 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.007654905 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.007678986 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.048363924 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.048465014 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.048505068 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.048578024 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:43.048607111 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.048738956 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.048821926 CET	49713	443	192.168.2.7	142.250.180.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:43.071314096 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.071453094 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:43.071484089 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.071695089 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.071768999 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:43.179939985 CET	49714	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:34:43.180010080 CET	443	49714	216.58.209.45	192.168.2.7
Feb 7, 2023 18:34:43.187951088 CET	49713	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:34:43.187999964 CET	443	49713	142.250.180.174	192.168.2.7
Feb 7, 2023 18:34:43.365984917 CET	49715	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.366015911 CET	443	49715	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.370598078 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.370650053 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.370764017 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.371145010 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.371162891 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.432178020 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.443118095 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.443161964 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.444225073 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.445157051 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.445188046 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.445318937 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.445494890 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.445506096 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.490669012 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.491390944 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.491453886 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.492955923 CET	49716	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.492986917 CET	443	49716	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.752362013 CET	49719	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.752413034 CET	443	49719	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.752506018 CET	49719	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.752805948 CET	49719	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.752825022 CET	443	49719	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.813182116 CET	443	49719	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.813718081 CET	49719	443	192.168.2.7	159.92.136.102
Feb 7, 2023 18:34:43.813756943 CET	443	49719	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.814476967 CET	443	49719	159.92.136.102	192.168.2.7
Feb 7, 2023 18:34:43.815272093 CET	49719	443	192.168.2.7	159.92.136.102

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:34:41.567933083 CET	63926	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:34:41.573301077 CET	51007	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:34:41.575326920 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:34:41.586741924 CET	53	63926	8.8.8.8	192.168.2.7
Feb 7, 2023 18:34:41.594961882 CET	53	51007	8.8.8.8	192.168.2.7
Feb 7, 2023 18:34:41.596585035 CET	53	50513	8.8.8.8	192.168.2.7
Feb 7, 2023 18:34:43.804826021 CET	50024	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:34:43.822906017 CET	53	50024	8.8.8.8	192.168.2.7
Feb 7, 2023 18:35:43.869703054 CET	63187	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:35:43.889578104 CET	53	63187	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
Feb 7, 2023 18:34:41.567933083 CET	192.168.2.7	8.8.8.8	0x24da	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:41.573301077 CET	192.168.2.7	8.8.8.8	0x7271	Standard query (0)	click.e.miro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:41.575326920 CET	192.168.2.7	8.8.8.8	0x4480	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:43.804826021 CET	192.168.2.7	8.8.8.8	0x26a7	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.869703054 CET	192.168.2.7	8.8.8.8	0x57e1	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 18:34:41.586741924 CET	8.8.8.8	192.168.2.7	0x24da	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:41.594961882 CET	8.8.8.8	192.168.2.7	0x7271	No error (0)	click.e.miro.com		159.92.136.102	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:41.596585035 CET	8.8.8.8	192.168.2.7	0x4480	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:41.596585035 CET	8.8.8.8	192.168.2.7	0x4480	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:43.822906017 CET	8.8.8.8	192.168.2.7	0x26a7	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.889578104 CET	8.8.8.8	192.168.2.7	0x57e1	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

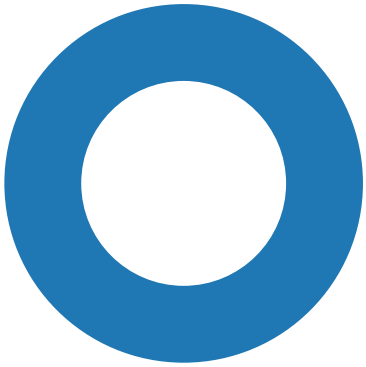
HTTP Request Dependency Graph

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

Statistics

Behavior

chrome.exe
chrome.exe
chrome.exe



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **5812**, Parent PID: **64**

General

Target ID:	0
Start time:	18:34:37
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:	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **6004**, Parent PID: **5812**

General

Target ID:	1
Start time:	18:34:39
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-US --service-sandbox-type=none --mojo-platform-channel-handle=1932 --field-trial-handle=1724,i,2876507980441582479,18001650036527390366,131072 --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: **4520**, Parent PID: **64**

General

Target ID:	2
Start time:	18:34:39
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=c3e69aad2d9381bc648c78299feae71fdb22ac757a070f4e5905cd8c7629ef7e370f37ef935070c1c307b7ee869054f949dffacb0988454aa20b89404a806863
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

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