ID: 800695
Cookbook: browseurl.jbs
Time: 18:19:31
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

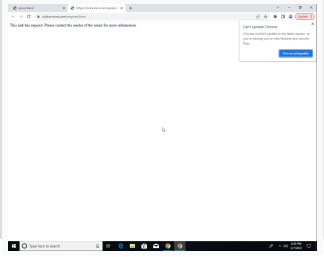
Windows Analysis Report

https://click.e.miro.com/?qs=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e77...

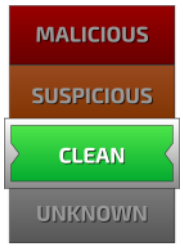
Overview

General Information

Sample URL:	https://click.e.miro.com/?qs=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe3...7e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096
Analysis ID:	800695
Infos:	



Detection

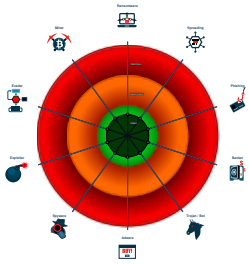


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 6140 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4512 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=1976 --field-trial-handle=1764,i,13624171276759586457,679474072376911802,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2288 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://click.e.miro.com/?qs=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096 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

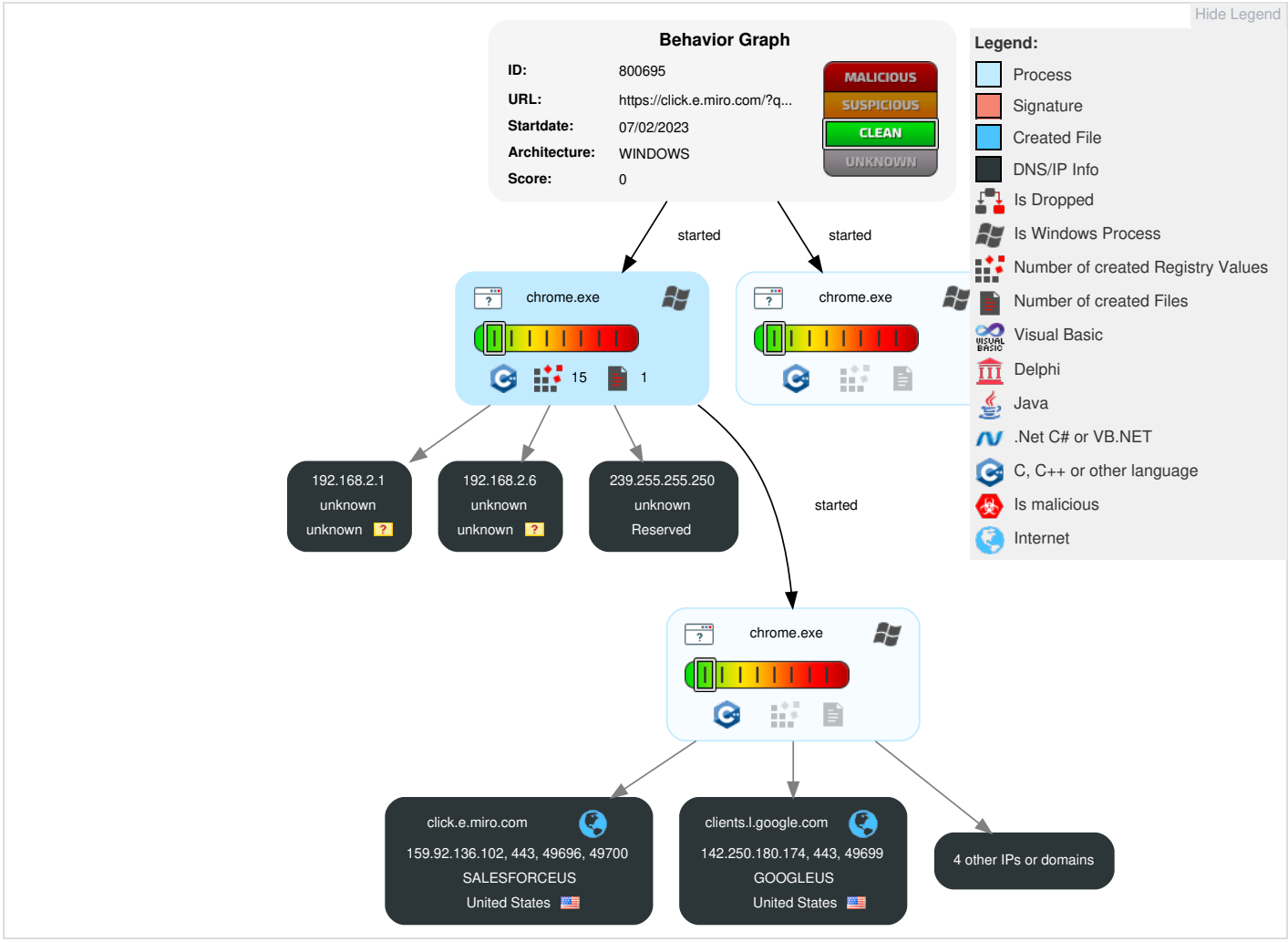
Joe Sandbox Signatures

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

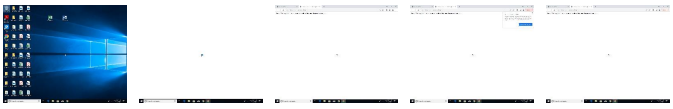
Behavior Graph

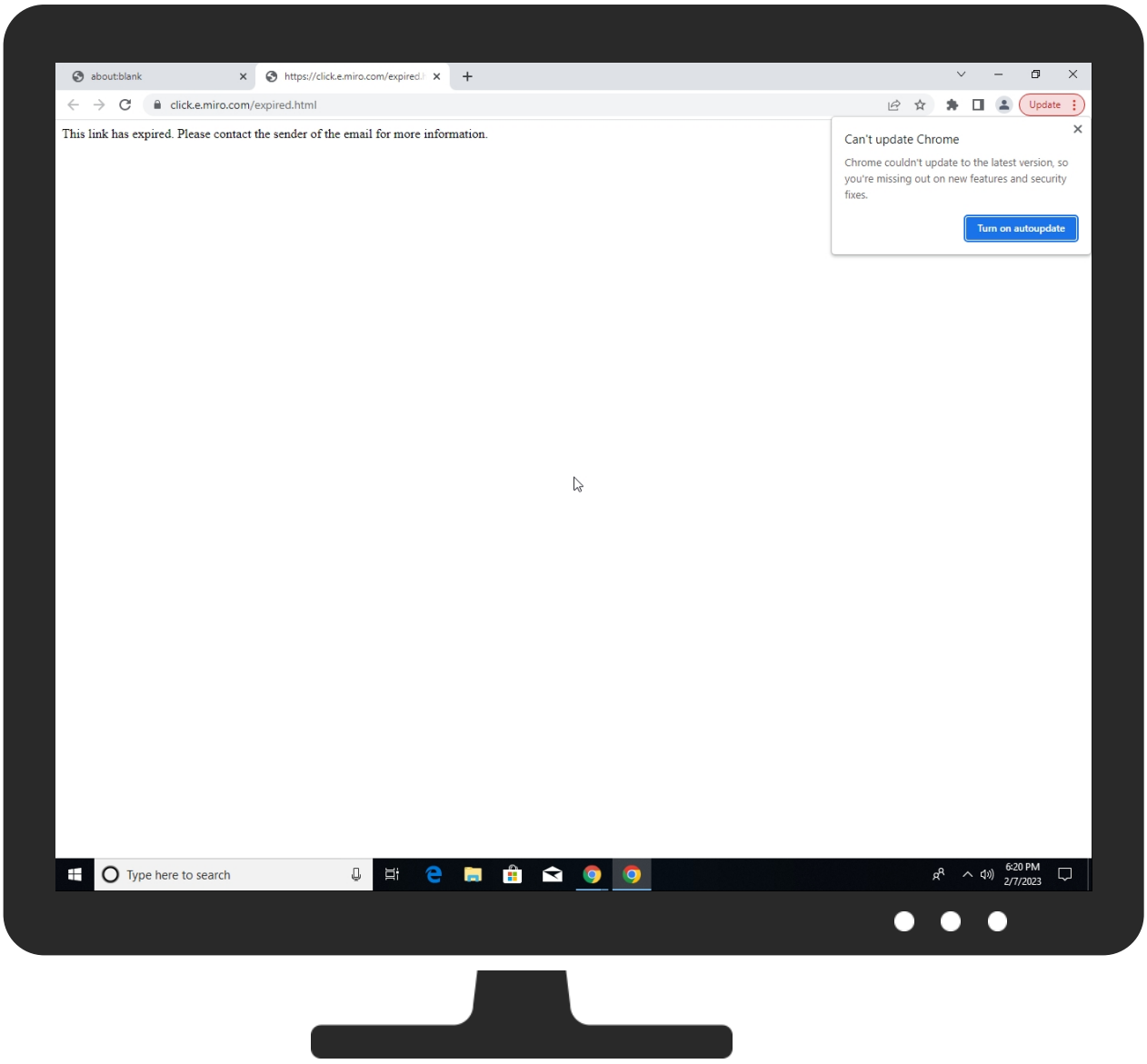


Screenshots

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=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096	0%	Virustotal		Browse
http://https://click.e.miro.com/?qs=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096	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

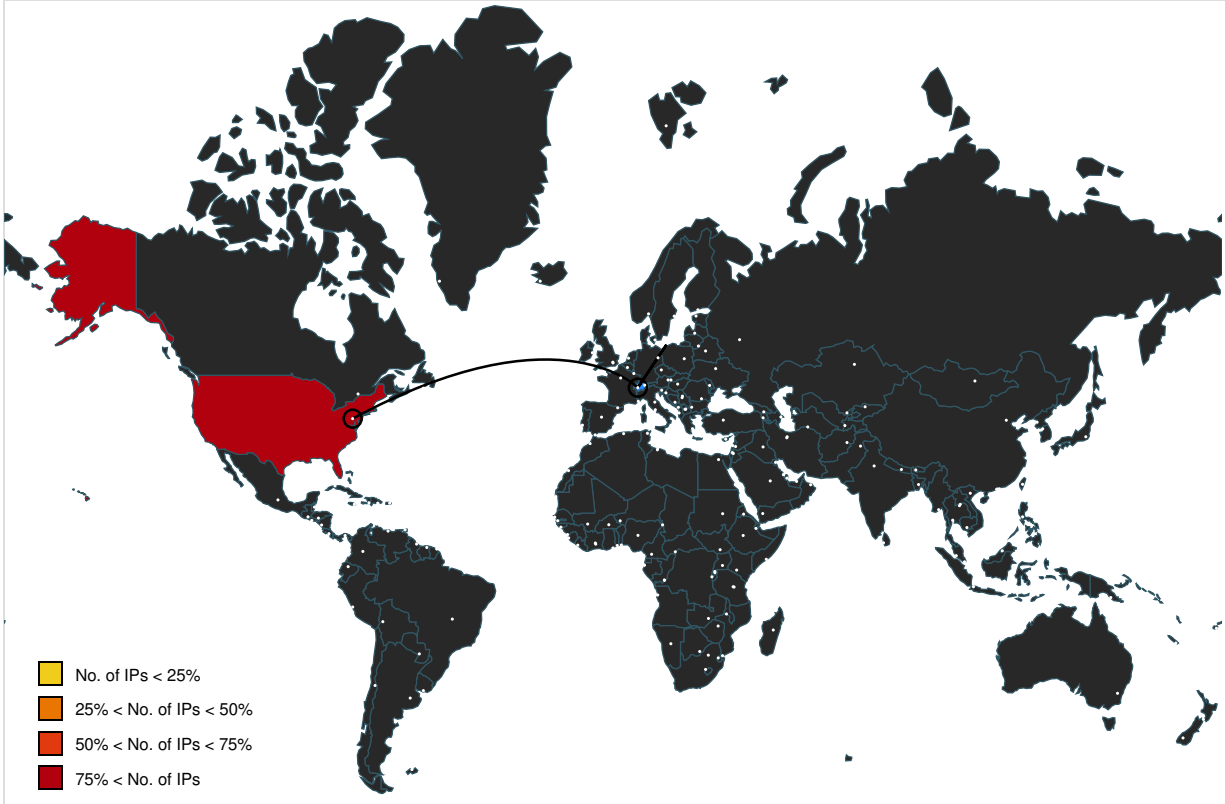
Contacted Domains

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=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096	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
127.0.0.1
192.168.2.6

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800695
Start date and time:	2023-02-07 18:19:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://click.e.miro.com/?qs=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096
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@4/8
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): 142.250.184.99, 34.104.35.123, 142.250.180.163
- 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

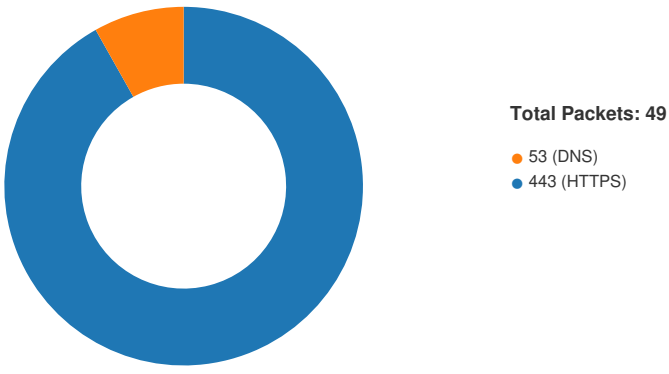
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:37.174387932 CET	49696	443	192.168.2.3	159.92.136.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:37.174448013 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.174554110 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.175224066 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.175272942 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.175355911 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.176482916 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.176502943 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.178776979 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.178816080 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.186110020 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.186148882 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.186227083 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.187226057 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.187249899 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.272943974 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.273571014 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.273612022 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.274475098 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.274559021 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.277061939 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.277154922 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.300688982 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.305073977 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.352119923 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.352157116 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.352411985 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.352471113 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.354342937 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.354419947 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.354521990 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.354541063 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.354598999 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.477201939 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.614636898 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.614676952 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.614967108 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.615147114 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.615173101 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.615483999 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.615521908 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.615746021 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.615868092 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.615890026 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.616018057 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.616039991 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.616085052 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.616682053 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.616700888 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.655364037 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.655448914 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.658533096 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.658623934 CET	49696	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.658637047 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.658657074 CET	443	49696	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.658672094 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.658756971 CET	443	49699	142.250.180.174	192.168.2.3
Feb 7, 2023 18:20:37.658838034 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.661602020 CET	49699	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:20:37.661639929 CET	443	49699	142.250.180.174	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:37.664212942 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.664294958 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.664432049 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.665018082 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.665054083 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.686500072 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.686599970 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.686628103 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.686774015 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.686839104 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.694909096 CET	49697	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:20:37.694938898 CET	443	49697	216.58.209.45	192.168.2.3
Feb 7, 2023 18:20:37.725220919 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.726789951 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.726821899 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.727358103 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.727845907 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.727875948 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.727982998 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.728153944 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.728168011 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.778300047 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.778449059 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.778536081 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.844383955 CET	49700	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.844429016 CET	443	49700	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.989955902 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.990010977 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:37.990106106 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.990734100 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:37.990750074 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.052170992 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.056896925 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:38.056929111 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.057497978 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.058131933 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:38.058155060 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.058235884 CET	443	49702	159.92.136.102	192.168.2.3
Feb 7, 2023 18:20:38.058362007 CET	49702	443	192.168.2.3	159.92.136.102
Feb 7, 2023 18:20:38.058372021 CET	443	49702	159.92.136.102	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:37.143177986 CET	49977	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:20:37.144668102 CET	57840	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:20:37.147380114 CET	57990	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:20:37.163120031 CET	53	49977	8.8.8.8	192.168.2.3
Feb 7, 2023 18:20:37.167141914 CET	53	57990	8.8.8.8	192.168.2.3
Feb 7, 2023 18:20:37.184602022 CET	53	57840	8.8.8.8	192.168.2.3
Feb 7, 2023 18:20:39.441003084 CET	49302	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:20:39.468055010 CET	53	49302	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
Feb 7, 2023 18:20:37.143177986 CET	192.168.2.3	8.8.8.8	0xa80d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:37.144668102 CET	192.168.2.3	8.8.8.8	0xc59c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:20:37.147380114 CET	192.168.2.3	8.8.8.8	0x4bd0	Standard query (0)	click.e.miro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:39.441003084 CET	192.168.2.3	8.8.8.8	0x194e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

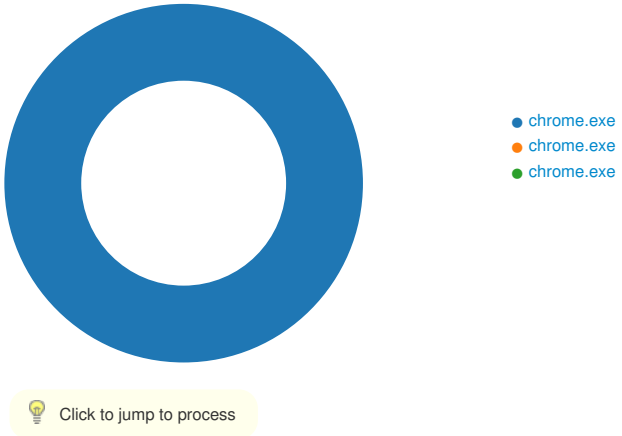
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:20:37.163120031 CET	8.8.8.8	192.168.2.3	0xa80d	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:37.167141914 CET	8.8.8.8	192.168.2.3	0x4bd0	No error (0)	click.e.miro.com		159.92.136.102	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:37.184602022 CET	8.8.8.8	192.168.2.3	0xc59c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:37.184602022 CET	8.8.8.8	192.168.2.3	0xc59c	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:39.468055010 CET	8.8.8.8	192.168.2.3	0x194e	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6140**, Parent PID: **2400**

General

Target ID:	0
Start time:	18:20:31
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:	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: **4512**, Parent PID: **6140**

General

Target ID:	1
Start time:	18:20:33
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=1976 --field-trial-handle=1764,i,13624171276759586457,67947407237691180 2,131072 --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

Analysis Process: chrome.exe PID: **2288**, Parent PID: **2400**

General	
Target ID:	2
Start time:	18:20:34
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=71ec040b00af2a7e15c4a00e338d6ed0afd5e86f0dffe31bba3547e216e7734b1d06c2ac32f20d2f03a7c89cefc8ab9152d116ce107afbcb055fd22492a6e096
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