ID: 800693
Cookbook: browseurl.jbs
Time: 18:18:53
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

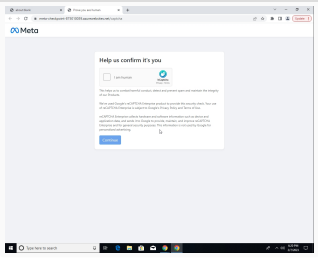
Windows Analysis Report

https://meta-checkpoint-875010059.azurewebsites.net/captcha

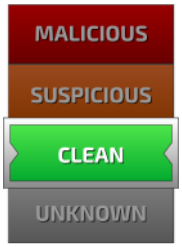
Overview

General Information

Sample URL:	http://https://meta-checkpoint-875010059.azurewebsites.net/captcha
Analysis ID:	800693
Infos:	



Detection

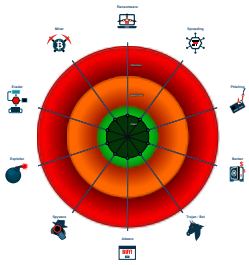


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5576 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4904 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=1908 --field-trial-handle=1704,i,16132118233755685620,6475161574412490261,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5656 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://meta-checkpoint-875010059.azurewebsites.net/captcha 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

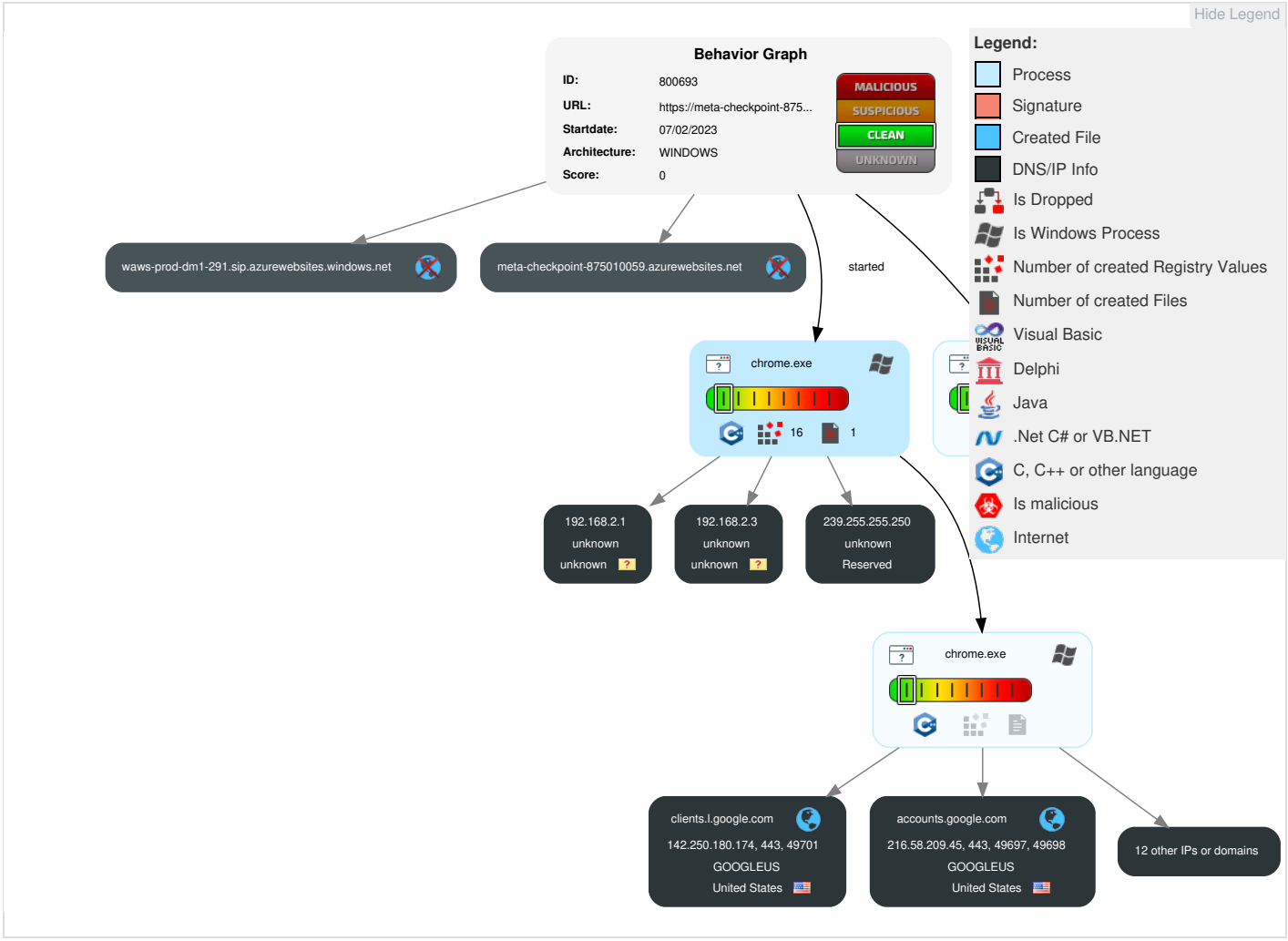
Joe Sandbox Signatures

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

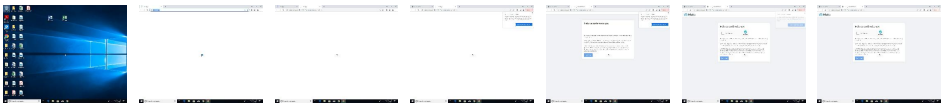
Behavior Graph

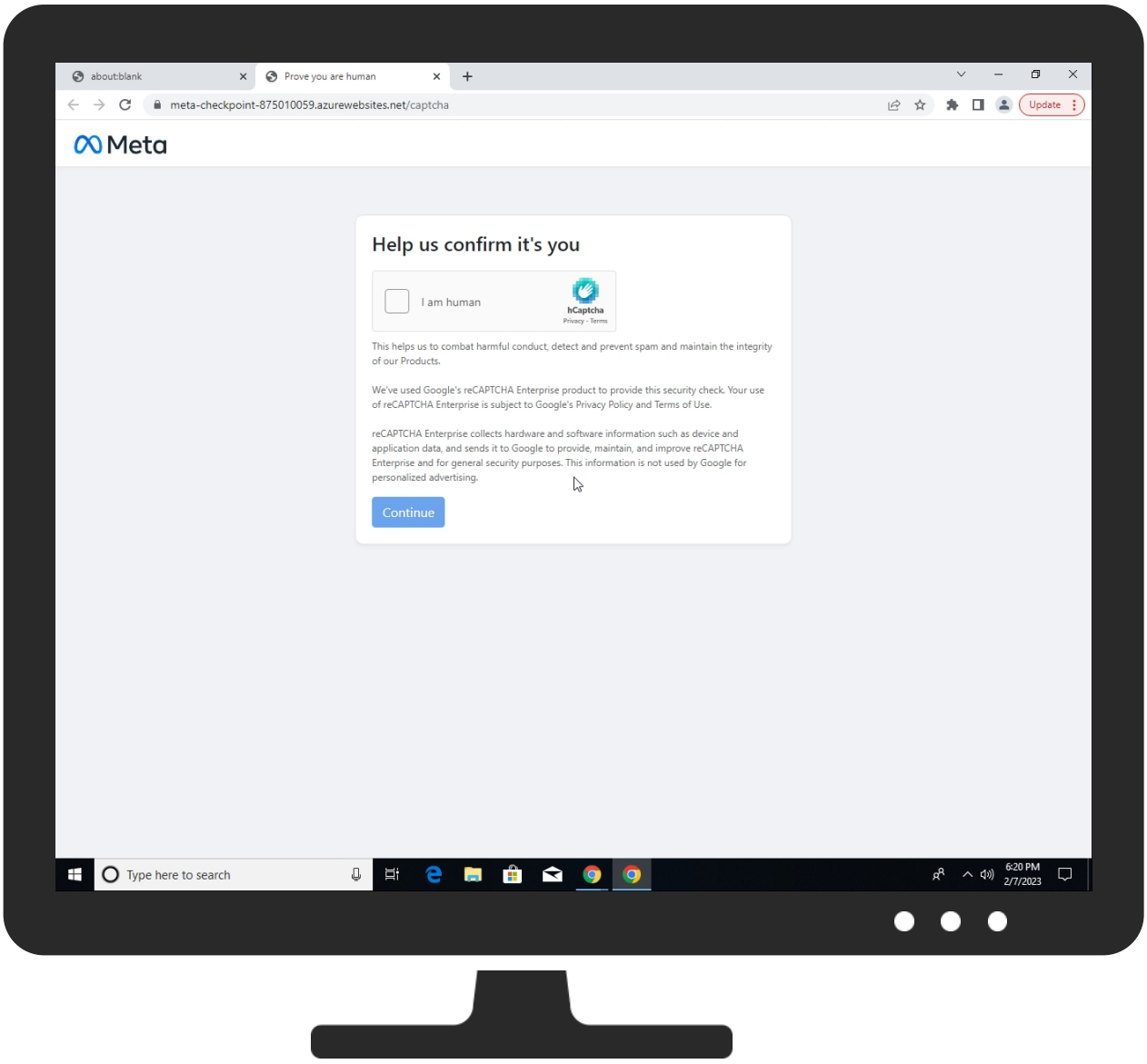


Screenshots

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://https://meta-checkpoint-875010059.azurewebsites.net/captcha	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://newassets.hcaptcha.com/captcha/v1/5a6011a/hcaptcha.js	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/i/b2a3a9e/e	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/captcha/v1/5a6011a/static/hcaptcha.html	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://hcaptcha.com/checksiteconfig?v=5a6011a&host=meta-checkpoint-875010059.azurewebsites.net&sitekey=2090dde0-1a4a-4119-ac94-68dbc4180559&sc=1&swa=1	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/c/b2a3a9e/hsw.js	0%	Avira URL Cloud	safe	
http://https://js.hcaptcha.com/1/api.js	0%	Avira URL Cloud	safe	

Domains and IPs

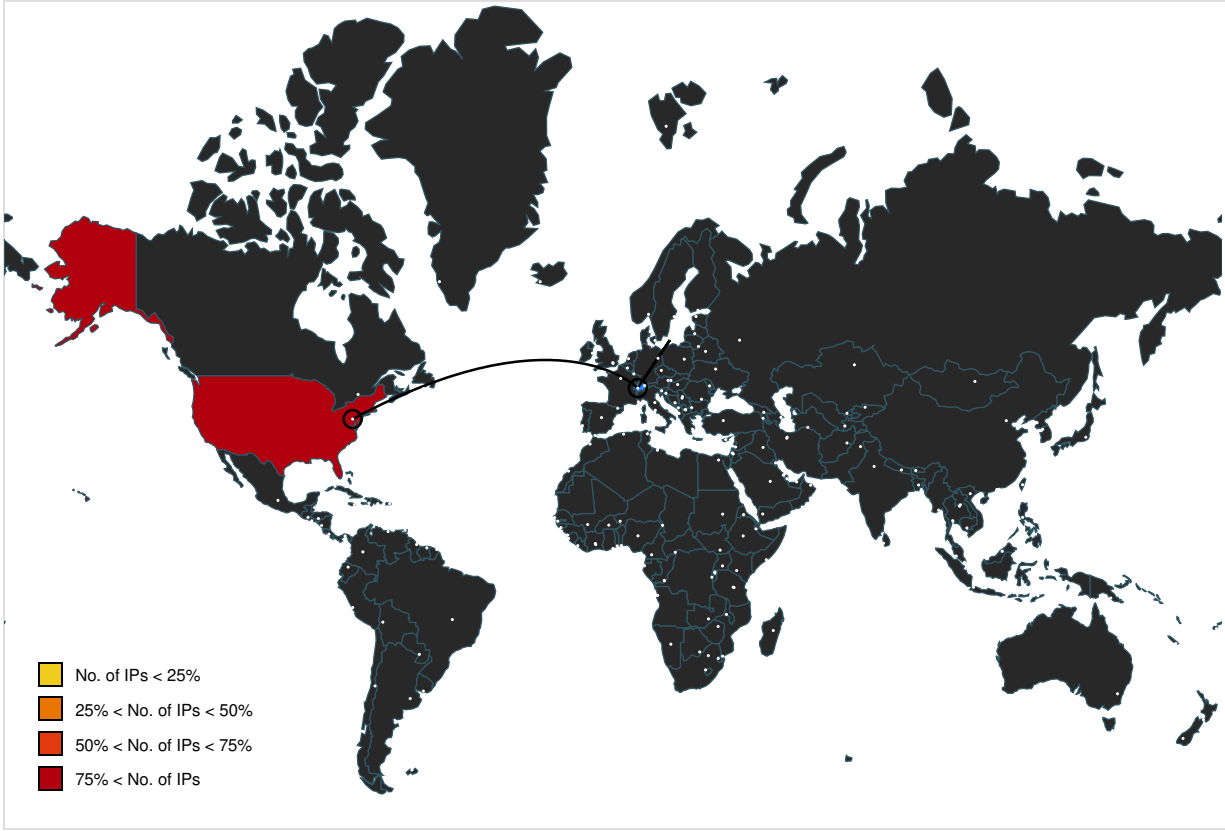
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jsdelivr.map.fastly.net	151.101.1.229	true	false		unknown
hcaptcha.com	104.16.168.131	true	false		unknown
accounts.google.com	216.58.209.45	true	false		high
js.hcaptcha.com	104.16.169.131	true	false		unknown
clients.l.google.com	142.250.180.174	true	false		high
newassets.hcaptcha.com	104.16.168.131	true	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
meta-checkpoint-875010059.azurewebsites.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://newassets.hcaptcha.com/captcha/v1/5a6011a/hcaptcha.js	false	• Avira URL Cloud: safe	unknown
http://https://cdn.jsdelivr.net/npm/bootstrap@4.6.2/dist/js/bootstrap.bundle.min.js	false		high
http://https://cdn.jsdelivr.net/npm/bootstrap@4.6.2/dist/css/bootstrap.min.css	false		high
http://https://meta-checkpoint-875010059.azurewebsites.net/captcha	false		unknown
http://https://js.hcaptcha.com/1/api.js	false	• Avira URL Cloud: safe	unknown
http://https://hcaptcha.com/checksiteconfig?v=5a6011a&host=meta-checkpoint-875010059.azurewebsites.net&sitekey=2090dde0-1a4a-4119-ac94-68dbc4180559&sc=1&swa=1	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/captcha/v1/5a6011a/static/hcaptcha.html	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/i/b2a3a9e/e	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://newassets.hcaptcha.com/captcha/v1/5a6011a/static/hcaptcha.html#frame=checkbox&id=0x37lmbbefh&host=meta-checkpoint-875010059.azurewebsites.net&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=true&custom=false&hl=en&tplinks=on&sitekey=2090dde0-1a4a-4119-ac94-68dbc4180559&theme=light&origin=https%3A%2F%2Fmeta-checkpoint-875010059.azurewebsites.net	false		unknown
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://newassets.hcaptcha.com/c/b2a3a9e/hsw.js	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/captcha/v1/5a6011a/static/hcaptcha.html#frame=challenge&id=0x37lmbbefh&host=meta-checkpoint-875010059.azurewebsites.net&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=true&custom=false&hl=en&tplinks=on&sitekey=2090dde0-1a4a-4119-ac94-68dbc4180559&theme=light&origin=https%3A%2F%2Fmeta-checkpoint-875010059.azurewebsites.net	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.229	jsdelivr.map.fastly.net	United States		54113	FASTLYUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
104.16.168.131	hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
104.16.169.131	js.hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.3
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800693
Start date and time:	2023-02-07 18:18:53 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://meta-checkpoint-875010059.azurewebsites.net/captcha
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:	6
Number of new started drivers analysed:	1
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@10/11
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.hcaptcha.com/what-is-hcaptcha-about?ref=meta-checkpoint-875010059.azurewebsites.net&utm_campaign=2090dde0-1a4a-4119-ac94-68dbc4180559&utm_medium=checkbox

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, qwavedrv.sys, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 20.118.40.5, 34.104.35.123, 69.16.175.42, 69.16.175.10, 216.58.209.42, 142.250.184.74, 142.250.184.106, 142.250.180.138, 142.250.180.170, 142.251.209.10, 142.251.209.42, 142.250.180.163
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, edgedl.me.gvt1.com, content-autofill.googleapis.com, update.googleapis.com, clientservices.googleapis.com, waws-prod-dm1-291-10e4.centralus.cloudapp.azure.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

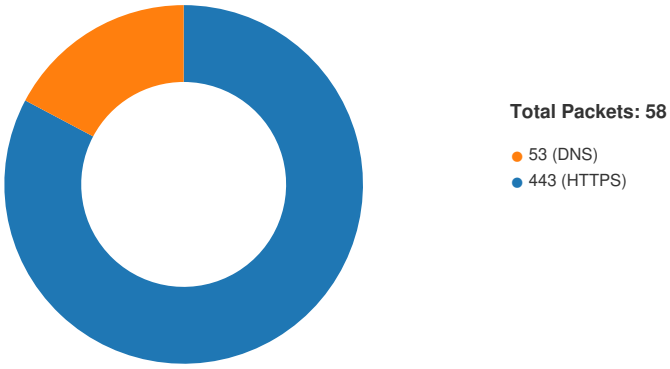
No created / dropped files found

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 18:20:00.933419943 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.933479071 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:00.933562040 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.934957027 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.935015917 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:00.935157061 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.936250925 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.936275005 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:00.936831951 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:00.936865091 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.030666113 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.038204908 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.163450956 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.163454056 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.192429066 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.192441940 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.192922115 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.192950964 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.194277048 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:01.194304943 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.194370031 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:01.194828033 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:01.194847107 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.195781946 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.195816040 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.195863008 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.196065903 CET	443	49698	216.58.209.45	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:01.196110010 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:01.196199894 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.271945000 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.367671967 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.367681026 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:01.383192062 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:01.383233070 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.384099007 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.384128094 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.384236097 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:01.385417938 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:01.385509014 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.332178116 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.332211971 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.332418919 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.333858967 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.333892107 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.334076881 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.334305048 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.334333897 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.334449053 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.334481001 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.334508896 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.334821939 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.334851027 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.380517006 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.380598068 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.380630016 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.380728006 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.380778074 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.399115086 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.399204016 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.399229050 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.399280071 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.399336100 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.431128979 CET	49698	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.431184053 CET	443	49698	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.432689905 CET	49701	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:20:02.432732105 CET	443	49701	142.250.180.174	192.168.2.4
Feb 7, 2023 18:20:02.462120056 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:02.462203979 CET	443	49697	216.58.209.45	192.168.2.4
Feb 7, 2023 18:20:02.572112083 CET	49697	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:20:04.626022100 CET	49705	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.626080036 CET	443	49705	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.626153946 CET	49705	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.626555920 CET	49706	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.626636982 CET	443	49706	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.626780987 CET	49706	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.626936913 CET	49705	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.626980066 CET	443	49705	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.627397060 CET	49706	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.627456903 CET	443	49706	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.633565903 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.633622885 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.633691072 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.634074926 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.634100914 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.694519997 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.695061922 CET	49708	443	192.168.2.4	104.16.169.131

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:04.695151091 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.696408033 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.696640015 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.698877096 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.698900938 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.699137926 CET	49708	443	192.168.2.4	104.16.169.131
Feb 7, 2023 18:20:04.699155092 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.699383020 CET	443	49708	104.16.169.131	192.168.2.4
Feb 7, 2023 18:20:04.705585003 CET	443	49706	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.710768938 CET	443	49705	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.712101936 CET	49705	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.712142944 CET	443	49705	151.101.1.229	192.168.2.4
Feb 7, 2023 18:20:04.712306023 CET	49706	443	192.168.2.4	151.101.1.229
Feb 7, 2023 18:20:04.712372065 CET	443	49706	151.101.1.229	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:19:59.198380947 CET	58565	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:19:59.200052023 CET	52239	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:19:59.218504906 CET	53	58565	8.8.8.8	192.168.2.4
Feb 7, 2023 18:19:59.228020906 CET	53	52239	8.8.8.8	192.168.2.4
Feb 7, 2023 18:19:59.746064901 CET	56807	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:01.534621954 CET	56807	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:04.606581926 CET	55570	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:04.608758926 CET	64906	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:04.609189987 CET	59446	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:04.624273062 CET	53	55570	8.8.8.8	192.168.2.4
Feb 7, 2023 18:20:04.631174088 CET	53	64906	8.8.8.8	192.168.2.4
Feb 7, 2023 18:20:05.173593998 CET	50861	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:05.196141005 CET	53	50861	8.8.8.8	192.168.2.4
Feb 7, 2023 18:20:06.399524927 CET	64700	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:06.419892073 CET	53	64700	8.8.8.8	192.168.2.4
Feb 7, 2023 18:20:15.766108990 CET	54521	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:20:40.730106115 CET	138	138	192.168.2.4	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:19:59.198380947 CET	192.168.2.4	8.8.8.8	0x4668	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:19:59.200052023 CET	192.168.2.4	8.8.8.8	0x6533	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:19:59.746064901 CET	192.168.2.4	8.8.8.8	0xe524	Standard query (0)	meta-checkpoint-875010059.azurewebsites.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:01.534621954 CET	192.168.2.4	8.8.8.8	0xe524	Standard query (0)	meta-checkpoint-875010059.azurewebsites.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.606581926 CET	192.168.2.4	8.8.8.8	0xc5c8	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.608758926 CET	192.168.2.4	8.8.8.8	0x80e0	Standard query (0)	js.hcaptcha.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.609189987 CET	192.168.2.4	8.8.8.8	0xc15e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.173593998 CET	192.168.2.4	8.8.8.8	0x89	Standard query (0)	newassets.hcaptcha.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:06.399524927 CET	192.168.2.4	8.8.8.8	0x5e8b	Standard query (0)	hcaptcha.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:15.766108990 CET	192.168.2.4	8.8.8.8	0x783b	Standard query (0)	meta-checkpoint-875010059.azurewebsites.net	A (IP address)	IN (0x0001)	false

DNS Answers

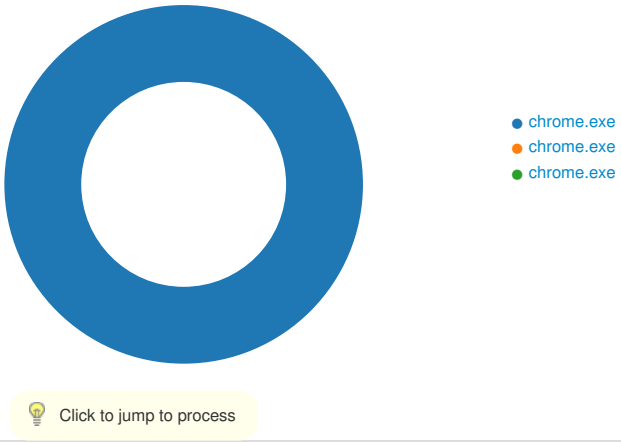
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:19:59.218504906 CET	8.8.8.8	192.168.2.4	0x4668	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:19:59.218504906 CET	8.8.8.8	192.168.2.4	0x4668	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:19:59.228020906 CET	8.8.8.8	192.168.2.4	0x6533	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:19:59.807743073 CET	8.8.8.8	192.168.2.4	0xe524	No error (0)	meta-checkpoint-875010059.azurewebsites.net	waws-prod-dm1-291.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:19:59.807743073 CET	8.8.8.8	192.168.2.4	0xe524	No error (0)	waws-prod-dm1-291.sip.azurewebsites.windows.net	waws-prod-dm1-291-10e4.centralus.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:01.553240061 CET	8.8.8.8	192.168.2.4	0xe524	No error (0)	meta-checkpoint-875010059.azurewebsites.net	waws-prod-dm1-291.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:01.553240061 CET	8.8.8.8	192.168.2.4	0xe524	No error (0)	waws-prod-dm1-291.sip.azurewebsites.windows.net	waws-prod-dm1-291-10e4.centralus.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:04.624273062 CET	8.8.8.8	192.168.2.4	0xc5c8	No error (0)	cdn.jsdelivr.net	jsdelivr.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:04.624273062 CET	8.8.8.8	192.168.2.4	0xc5c8	No error (0)	jsdelivr.map.fastly.net		151.101.1.229	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.624273062 CET	8.8.8.8	192.168.2.4	0xc5c8	No error (0)	jsdelivr.map.fastly.net		151.101.65.229	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.624273062 CET	8.8.8.8	192.168.2.4	0xc5c8	No error (0)	jsdelivr.map.fastly.net		151.101.129.229	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.624273062 CET	8.8.8.8	192.168.2.4	0xc5c8	No error (0)	jsdelivr.map.fastly.net		151.101.193.229	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.631139040 CET	8.8.8.8	192.168.2.4	0xc15e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:04.631174088 CET	8.8.8.8	192.168.2.4	0x80e0	No error (0)	js.hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:04.631174088 CET	8.8.8.8	192.168.2.4	0x80e0	No error (0)	js.hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.196141005 CET	8.8.8.8	192.168.2.4	0x89	No error (0)	newassets.hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.196141005 CET	8.8.8.8	192.168.2.4	0x89	No error (0)	newassets.hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:06.419892073 CET	8.8.8.8	192.168.2.4	0x5e8b	No error (0)	hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:06.419892073 CET	8.8.8.8	192.168.2.4	0x5e8b	No error (0)	hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:15.808466911 CET	8.8.8.8	192.168.2.4	0x783b	No error (0)	meta-checkpoint-875010059.azurewebsites.net	waws-prod-dm1-291.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:15.808466911 CET	8.8.8.8	192.168.2.4	0x783b	No error (0)	waws-prod-dm1-291.sip.azurewebsites.windows.net	waws-prod-dm1-291-10e4.centralus.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- https:
  - js.hcaptcha.com
  - cdn.jsdelivr.net
  - newassets.hcaptcha.com
  - hcaptcha.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5576**, Parent PID: **4040**

General

Target ID:	0
Start time:	18:19:54
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: **4904**, Parent PID: **5576**

General

Target ID:	1
Start time:	18:19:55
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=1908 --field-trial-handle=1704,i,16132118233755685620,6475161574412490261,131072 --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: **5656**, Parent PID: **4040**

General

Target ID:	2
Start time:	18:19:56
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://meta-checkpoint-875010059.azurewebsites.net/captcha
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