ID: 800714
Cookbook: browseurl.jbs
Time: 18:34:39
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2023

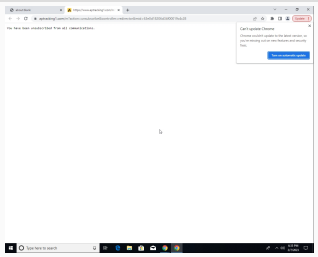
Windows Analysis Report

https://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28

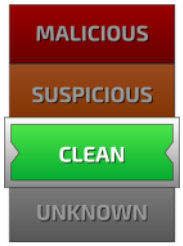
Overview

General Information

Sample URL:	http://https://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28
Analysis ID:	800714
Infos:	



Detection

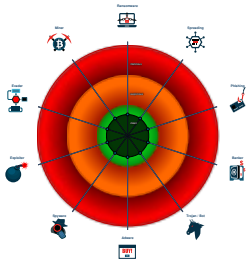


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5872 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6040 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=1792 --field-trial-handle=1624,i,16112150467919112305,13076742474032387525,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5464 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

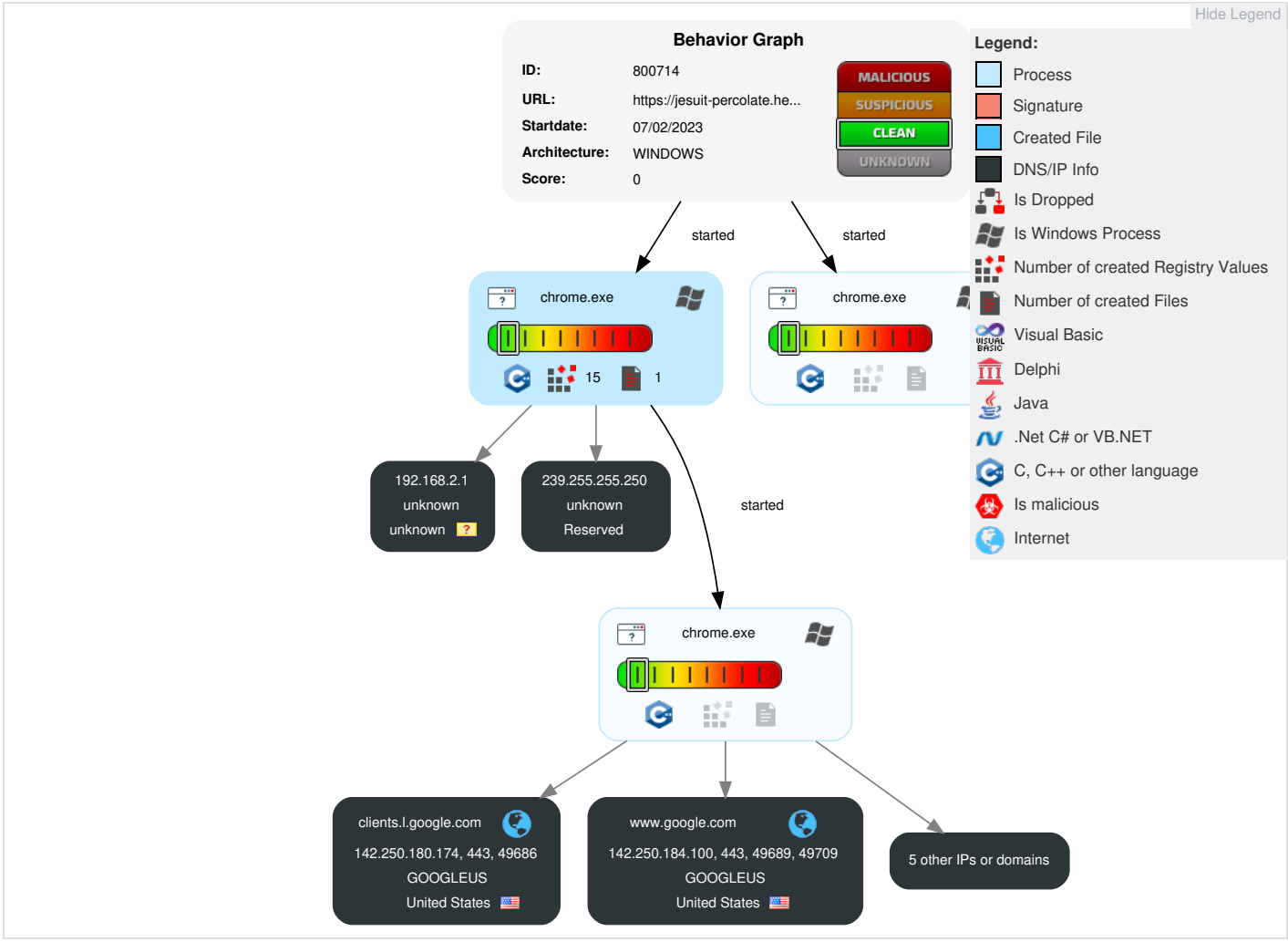
There are no malicious signatures, click here to show all signatures.

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

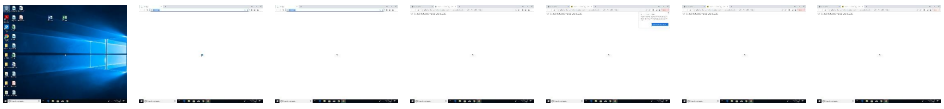
Copyright Joe Security LLC 2023

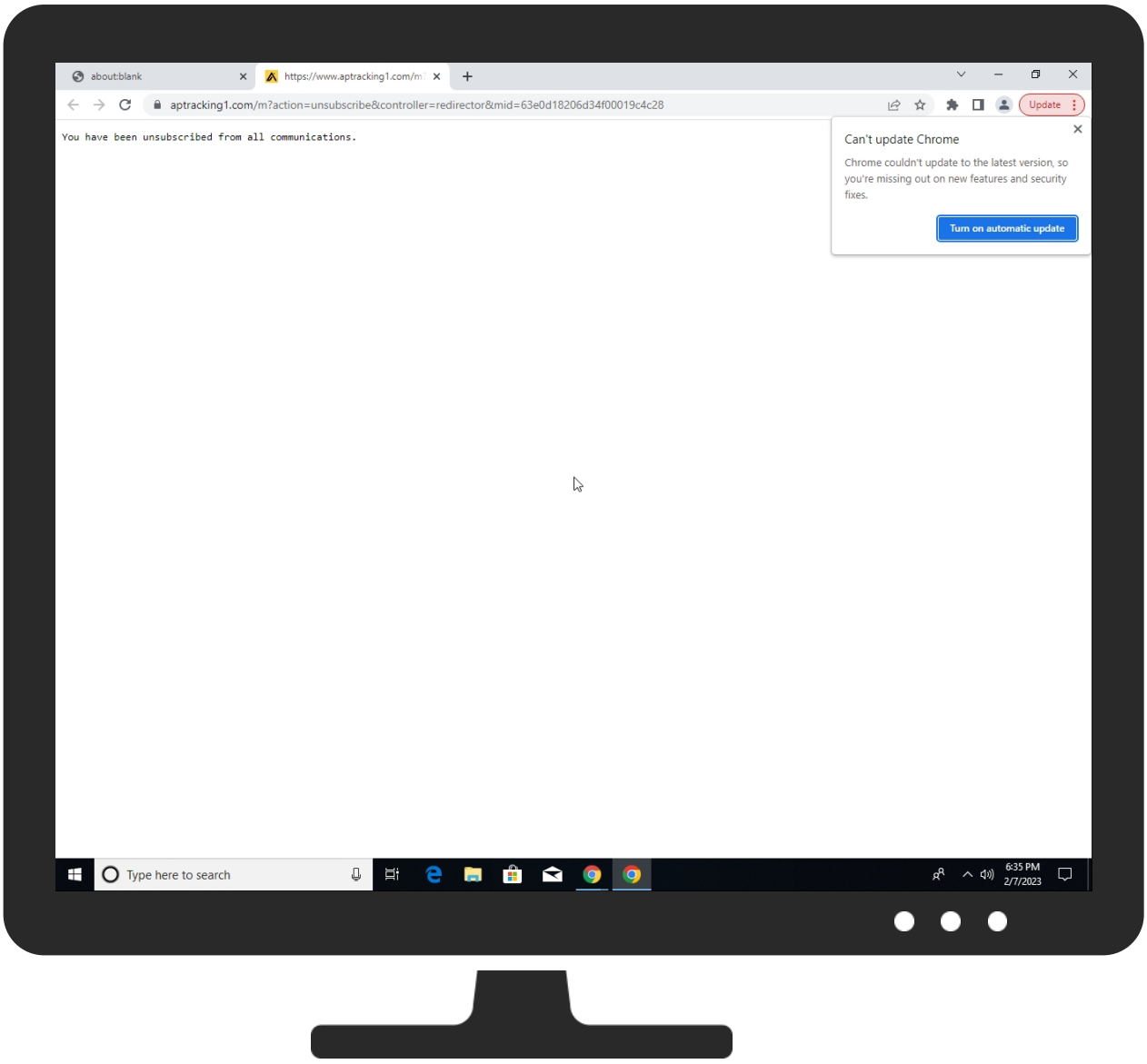


Screenshots

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://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28	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://www.aptracking1.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.aptracking1.com/favicon.ico	0%	Virustotal		Browse

Copyright Joe Security LLC 2023

Domains and IPs

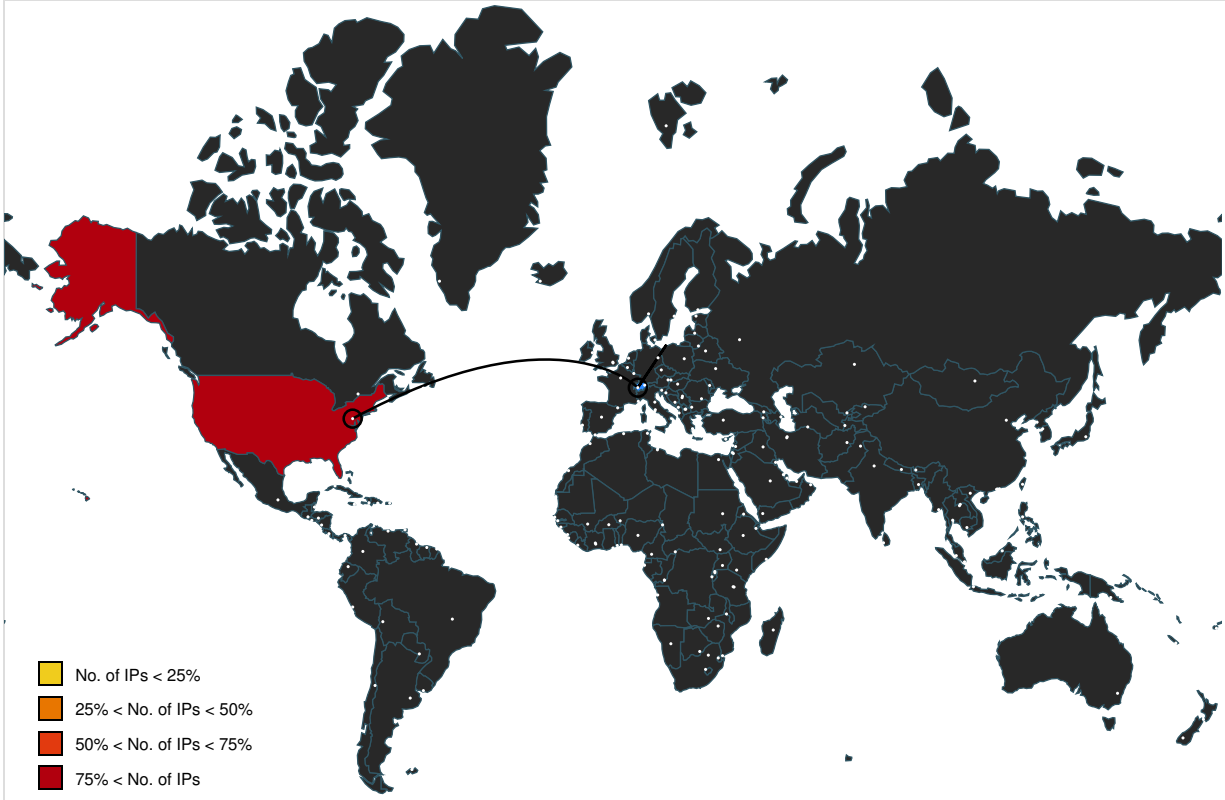
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
www.aptracking1.com	34.102.184.244	true	false		unknown
jesuit-percolate.herokuapp.com	54.235.77.118	true	false		unknown
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.aptracking1.com/m?action=unsubscribe&controller=redirector&mid=63e0d18206d34f00019c4c28	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://www.aptracking1.com/m?action=unsubscribe&controller=redirector&mid=63e0d18206d34f00019c4c28	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28	false		unknown
http://https://www.aptracking1.com/favicon.ico	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.184.244	www.aptracking1.com	United States		15169	GOOGLEUS	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

Copyright Joe Security LLC 2023

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false
54.235.77.118	jesuit-percolate.herokuapp.com	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800714
Start date and time:	2023-02-07 18:34:39 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28
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@25/0@6/8
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, 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

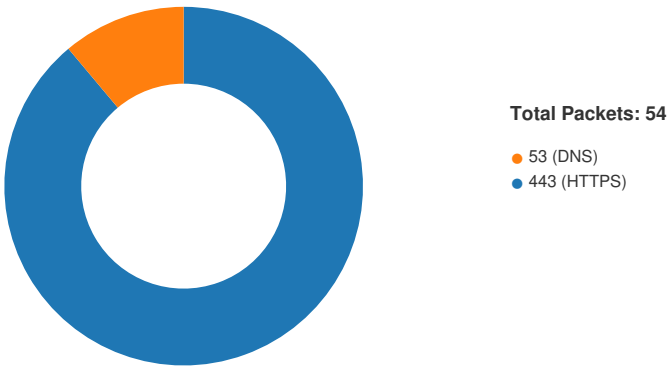
No created / dropped files found

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 18:35:41.488641024 CET	49685	443	192.168.2.4	216.58.209.45

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:35:41.488703012 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:41.488816977 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:41.489483118 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.489526033 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.489679098 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.490318060 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:41.490353107 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:41.490782022 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.490808964 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.609663010 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.611794949 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:41.652956963 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:41.656397104 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:41.656428099 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:41.656641960 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.656676054 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.657493114 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.657643080 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.660139084 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:41.660219908 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:41.660765886 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:41.660872936 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.485111952 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.485155106 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.485395908 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.485642910 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.485666037 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.486402035 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:44.486439943 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.486640930 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.487185955 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:44.487221956 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.527091026 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.527184010 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.527308941 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.527770996 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.527802944 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.530352116 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.530421972 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:44.530446053 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.530518055 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.530589104 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:44.532202959 CET	49686	443	192.168.2.4	142.250.180.174
Feb 7, 2023 18:35:44.532227993 CET	443	49686	142.250.180.174	192.168.2.4
Feb 7, 2023 18:35:44.551974058 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.552090883 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.552123070 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.553200960 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.553330898 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.553978920 CET	49685	443	192.168.2.4	216.58.209.45
Feb 7, 2023 18:35:44.553998947 CET	443	49685	216.58.209.45	192.168.2.4
Feb 7, 2023 18:35:44.826946974 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.827012062 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.827124119 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.827805042 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.827821016 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.910646915 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.911201954 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.911235094 CET	443	49689	142.250.184.100	192.168.2.4

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:35:44.917021036 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.917179108 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.939685106 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:44.939726114 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.939965963 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:44.977454901 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.977968931 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.978008986 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.979363918 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.979476929 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.983998060 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.984033108 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.984249115 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:44.984328032 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:44.984337091 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:45.002137899 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:45.002159119 CET	443	49689	142.250.184.100	192.168.2.4
Feb 7, 2023 18:35:45.058182001 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:45.058217049 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:45.102200031 CET	49689	443	192.168.2.4	142.250.184.100
Feb 7, 2023 18:35:45.131697893 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:45.131776094 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:45.132574081 CET	49688	443	192.168.2.4	54.235.77.118
Feb 7, 2023 18:35:45.132599115 CET	443	49688	54.235.77.118	192.168.2.4
Feb 7, 2023 18:35:45.169049978 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.169128895 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.169240952 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.169729948 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.169765949 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.231842995 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.232264996 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.232290030 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.234971046 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.235126972 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.238512039 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.238534927 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.238823891 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.238960981 CET	49691	443	192.168.2.4	34.102.184.244
Feb 7, 2023 18:35:45.238977909 CET	443	49691	34.102.184.244	192.168.2.4
Feb 7, 2023 18:35:45.302166939 CET	49691	443	192.168.2.4	34.102.184.244

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:35:41.172270060 CET	57417	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:41.175772905 CET	50982	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:41.192024946 CET	53	57417	8.8.8.8	192.168.2.4
Feb 7, 2023 18:35:41.195833921 CET	53	50982	8.8.8.8	192.168.2.4
Feb 7, 2023 18:35:43.278944016 CET	61105	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:43.311228991 CET	53	61105	8.8.8.8	192.168.2.4
Feb 7, 2023 18:35:44.492228985 CET	50911	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:44.522151947 CET	53	50911	8.8.8.8	192.168.2.4
Feb 7, 2023 18:35:44.682373047 CET	59683	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:44.702332973 CET	53	59683	8.8.8.8	192.168.2.4
Feb 7, 2023 18:35:45.137000084 CET	58565	53	192.168.2.4	8.8.8.8
Feb 7, 2023 18:35:45.165163994 CET	53	58565	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 18:35:41.172270060 CET	192.168.2.4	8.8.8.8	0x2a3d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:41.175772905 CET	192.168.2.4	8.8.8.8	0x654f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.278944016 CET	192.168.2.4	8.8.8.8	0xd069	Standard query (0)	jesuit-percolate.herokuapp.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:44.492228985 CET	192.168.2.4	8.8.8.8	0xd038	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:44.682373047 CET	192.168.2.4	8.8.8.8	0x9603	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:45.137000084 CET	192.168.2.4	8.8.8.8	0xd19d	Standard query (0)	www.aptracking1.com	A (IP address)	IN (0x0001)	false

DNS Answers

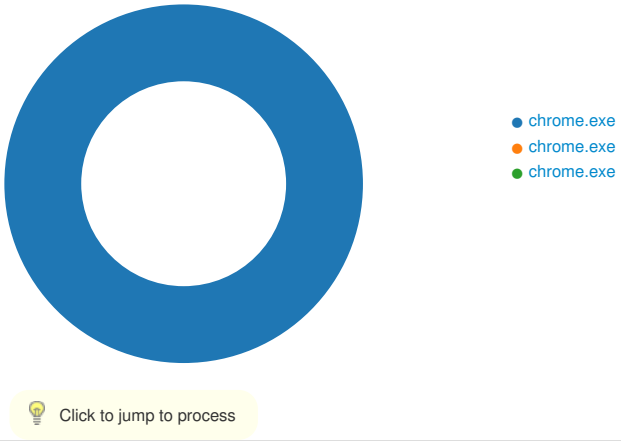
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:35:41.192024946 CET	8.8.8.8	192.168.2.4	0x2a3d	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:41.195833921 CET	8.8.8.8	192.168.2.4	0x654f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:35:41.195833921 CET	8.8.8.8	192.168.2.4	0x654f	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.311228991 CET	8.8.8.8	192.168.2.4	0xd069	No error (0)	jesuit-percolate.herokuapp.com		54.235.77.118	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.311228991 CET	8.8.8.8	192.168.2.4	0xd069	No error (0)	jesuit-percolate.herokuapp.com		174.129.128.48	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.311228991 CET	8.8.8.8	192.168.2.4	0xd069	No error (0)	jesuit-percolate.herokuapp.com		54.205.8.205	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:43.311228991 CET	8.8.8.8	192.168.2.4	0xd069	No error (0)	jesuit-percolate.herokuapp.com		18.211.231.38	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:44.522151947 CET	8.8.8.8	192.168.2.4	0xd038	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:44.702332973 CET	8.8.8.8	192.168.2.4	0x9603	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:35:45.165163994 CET	8.8.8.8	192.168.2.4	0xd19d	No error (0)	www.aptracking1.com		34.102.184.244	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- jesuit-percolate.herokuapp.com
- www.aptracking1.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5872**, Parent PID: **2532**

General

Target ID:	0
Start time:	18:35:38
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: **6040**, Parent PID: **5872**

General

Target ID:	1
Start time:	18:35:39
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe

Copyright Joe Security LLC 2023

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=1792 --field-trial-handle=1624,i,16112150467919112305,13076742474032387525,131072 --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: **5464**, Parent PID: **2532**

General

Target ID:	2
Start time:	18:35:40
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://jesuit-percolate.herokuapp.com/m?mid=63e0d18206d34f00019c4c28
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