ID: 800694
Cookbook: browseurl.jbs
Time: 18:18:58
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

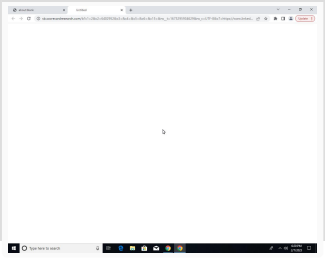
Windows Analysis Report

http://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934...

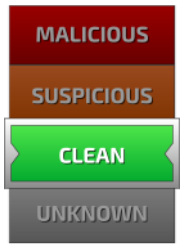
Overview

General Information

Sample URL:	sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=16752...934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=
Analysis ID:	800694
Infos:	



Detection

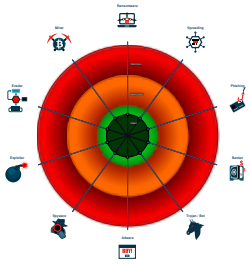


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 4964 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1648 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=1944 --field-trial-handle=1748,i,13924636935230247093,10287414604649073630,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2944 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9= 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

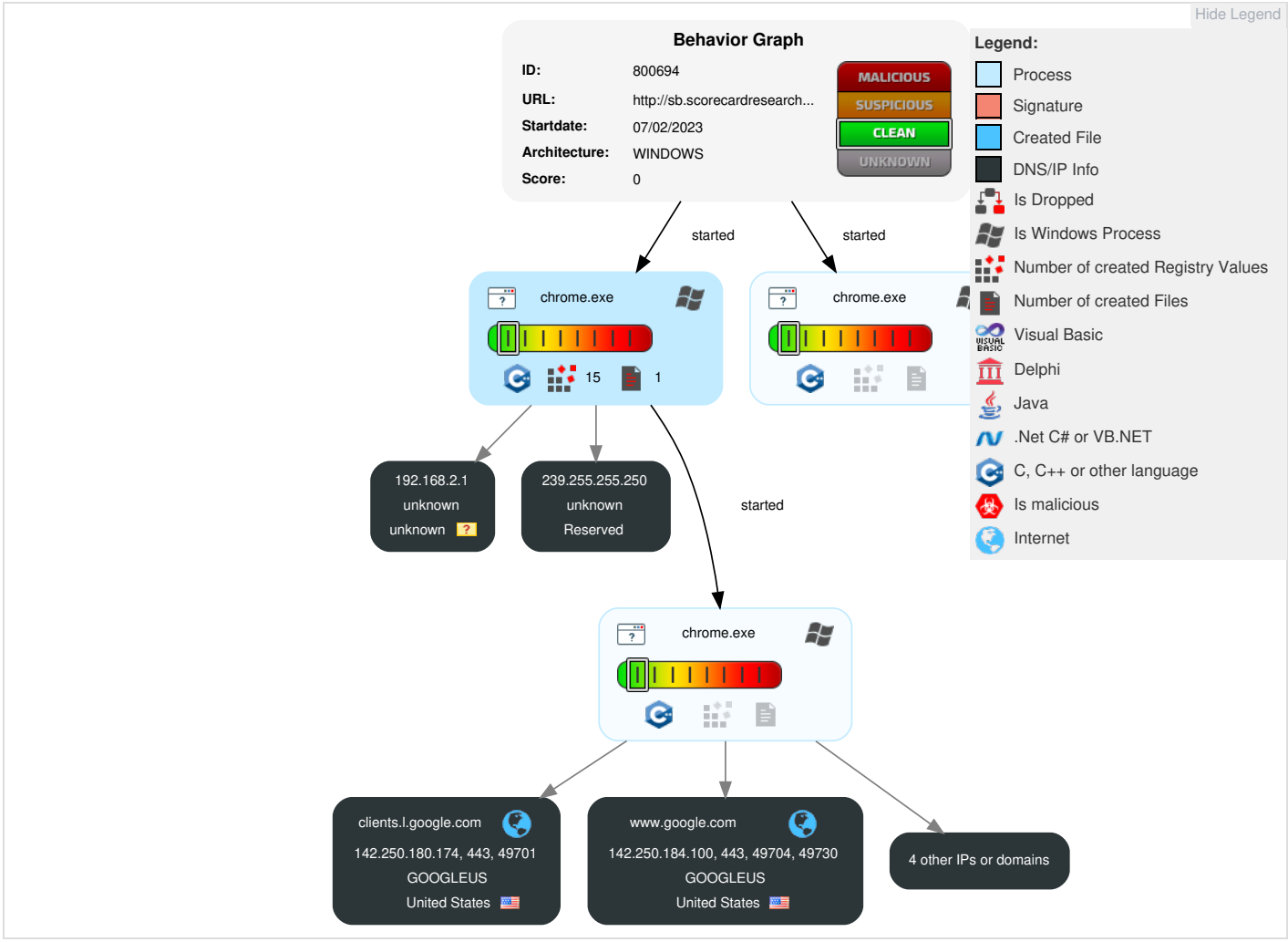
Joe Sandbox Signatures

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

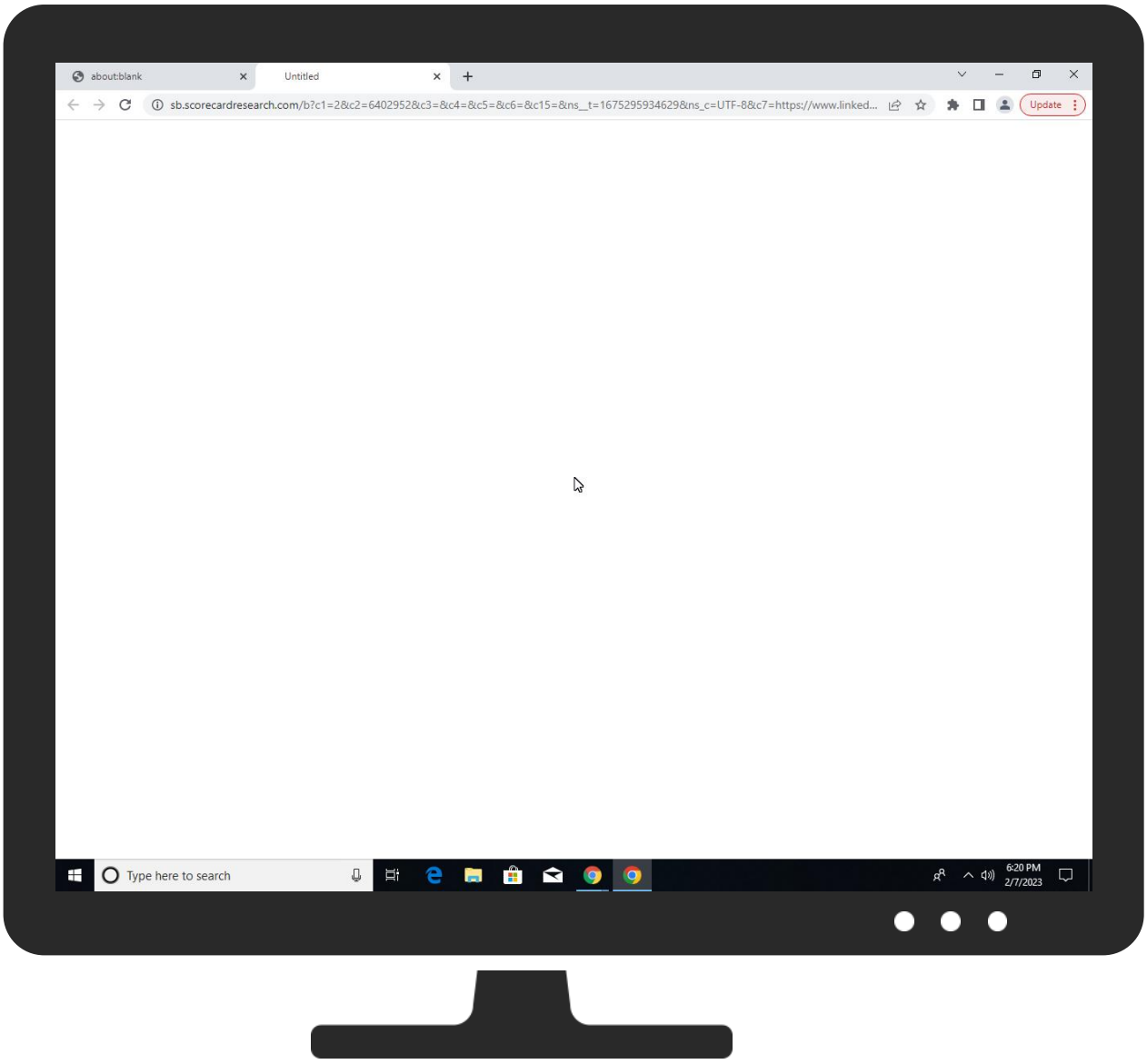
Behavior Graph



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://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=	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://sb.scorecardresearch.com/b2?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=	0%	Avira URL Cloud	safe	

Domains and IPs

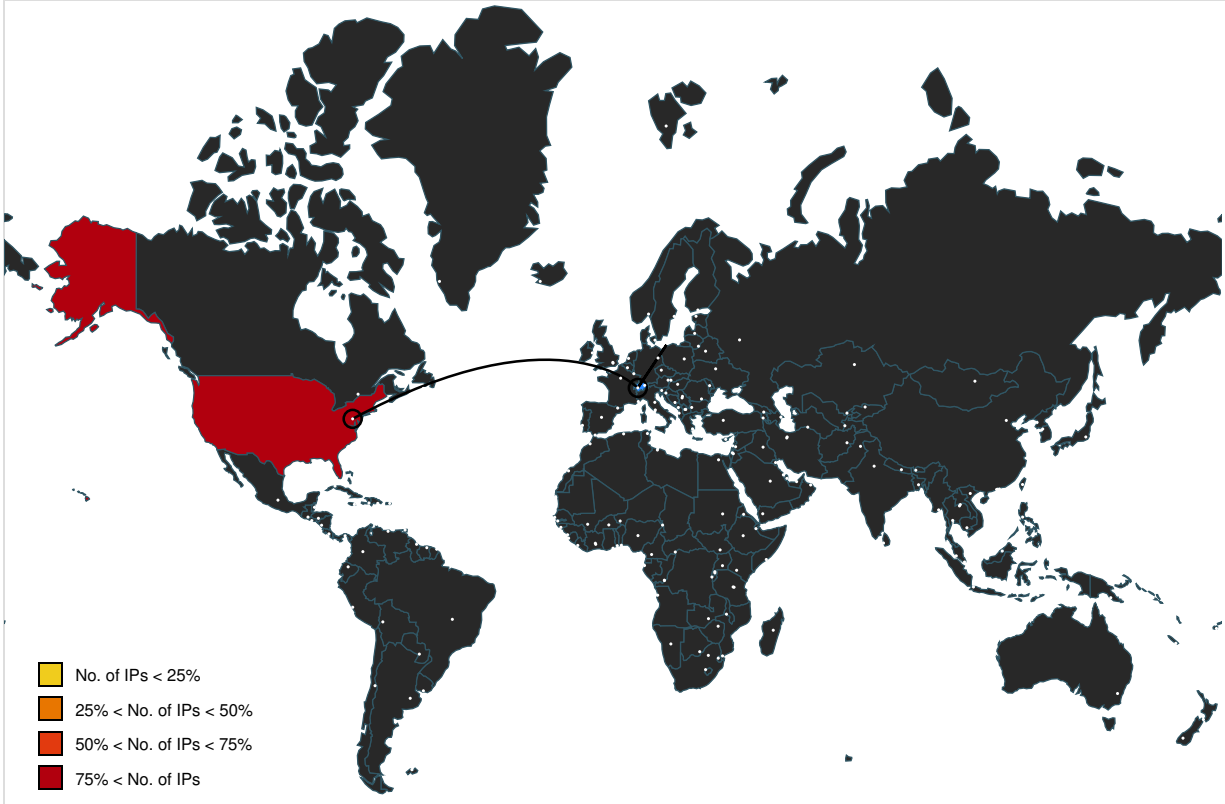
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
sb.scorecardresearch.com	13.224.103.60	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://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=	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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://sb.scorecardresearch.com/b2?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.103.60	sb.scorecardresearch.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800694
Start date and time:	2023-02-07 18:18:58 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=
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:	8
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@24/0@5/7
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, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, conhost.exe
- 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, edgedl.me.gvt1.com, login.live.com, tile-service.weather.microsoft.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

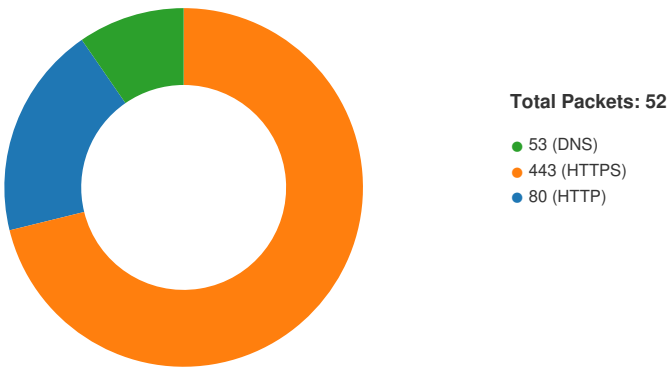
No created / dropped files found

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 18:20:05.732501030 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.734225988 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:05.734299898 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:05.734414101 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:05.735934019 CET	49700	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.737338066 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:05.737374067 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:05.744061947 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.744252920 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.747445107 CET	80	49700	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.747759104 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.747831106 CET	49700	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.747842073 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.747931957 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.748390913 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.748415947 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.749773979 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.761475086 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.769701004 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.811115026 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:05.822870016 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.838092089 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:05.886651039 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:05.888503075 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.898973942 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.899017096 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.899305105 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:05.899331093 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:05.899679899 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.899791002 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.901518106 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:05.901526928 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:05.901694059 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:05.901941061 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.041098118 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:06.366352081 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.366447926 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:06.366611958 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.366626978 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:06.366667986 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:06.366842031 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:06.366869926 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.367115021 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.367336988 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:06.367369890 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.411986113 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.412146091 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:06.412159920 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.412237883 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:06.413670063 CET	49701	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:20:06.413722038 CET	443	49701	142.250.180.174	192.168.2.5
Feb 7, 2023 18:20:06.432389021 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:06.432605028 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:06.432625055 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.432683945 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.434312105 CET	49698	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:20:06.434350967 CET	443	49698	216.58.209.45	192.168.2.5
Feb 7, 2023 18:20:08.280395031 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.280494928 CET	443	49704	142.250.184.100	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:08.280596972 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.281091928 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.281132936 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.369160891 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.380392075 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.380417109 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.381795883 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.381872892 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.392890930 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:08.392921925 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.393063068 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.598723888 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:08.599612951 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:18.338906050 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:18.339034081 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:18.339157104 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:22.061120987 CET	49704	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:20:22.061166048 CET	443	49704	142.250.184.100	192.168.2.5
Feb 7, 2023 18:20:35.758924961 CET	80	49700	13.224.103.60	192.168.2.5
Feb 7, 2023 18:20:35.759124994 CET	49700	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:50.989067078 CET	49697	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:20:51.000827074 CET	80	49697	13.224.103.60	192.168.2.5
Feb 7, 2023 18:21:08.334916115 CET	49700	80	192.168.2.5	13.224.103.60
Feb 7, 2023 18:21:08.335474968 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:08.335525036 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.335633039 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:08.336812019 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:08.336834908 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.346503973 CET	80	49700	13.224.103.60	192.168.2.5
Feb 7, 2023 18:21:08.401797056 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.402482986 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:08.402517080 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.403059959 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.403882027 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:08.403912067 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.404023886 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:08.466547966 CET	49730	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:21:18.399393082 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:18.399486065 CET	443	49730	142.250.184.100	192.168.2.5
Feb 7, 2023 18:21:18.399636030 CET	49730	443	192.168.2.5	142.250.184.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:20:05.459229946 CET	60841	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:20:05.459430933 CET	61893	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:20:05.479124069 CET	53	60841	8.8.8.8	192.168.2.5
Feb 7, 2023 18:20:05.485682011 CET	53	61893	8.8.8.8	192.168.2.5
Feb 7, 2023 18:20:05.637465954 CET	51441	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:20:05.673083067 CET	53	51441	8.8.8.8	192.168.2.5
Feb 7, 2023 18:20:08.250581026 CET	65323	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:20:08.278068066 CET	53	65323	8.8.8.8	192.168.2.5
Feb 7, 2023 18:21:08.312211037 CET	60284	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:21:08.332212925 CET	53	60284	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:20:05.459229946 CET	192.168.2.5	8.8.8.8	0x2fa0	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.459430933 CET	192.168.2.5	8.8.8.8	0x64d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.637465954 CET	192.168.2.5	8.8.8.8	0x4222	Standard query (0)	sb.scorecardresearch.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:08.250581026 CET	192.168.2.5	8.8.8.8	0x1741	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:21:08.312211037 CET	192.168.2.5	8.8.8.8	0x715e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

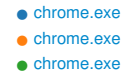
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:20:05.479124069 CET	8.8.8.8	192.168.2.5	0x2fa0	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.485682011 CET	8.8.8.8	192.168.2.5	0x64d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:20:05.485682011 CET	8.8.8.8	192.168.2.5	0x64d	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.673083067 CET	8.8.8.8	192.168.2.5	0x4222	No error (0)	sb.scorecardresearch.com		13.224.103.60	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.673083067 CET	8.8.8.8	192.168.2.5	0x4222	No error (0)	sb.scorecardresearch.com		13.224.103.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.673083067 CET	8.8.8.8	192.168.2.5	0x4222	No error (0)	sb.scorecardresearch.com		13.224.103.91	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:05.673083067 CET	8.8.8.8	192.168.2.5	0x4222	No error (0)	sb.scorecardresearch.com		13.224.103.48	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:20:08.278068066 CET	8.8.8.8	192.168.2.5	0x1741	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:21:08.332212925 CET	8.8.8.8	192.168.2.5	0x715e	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

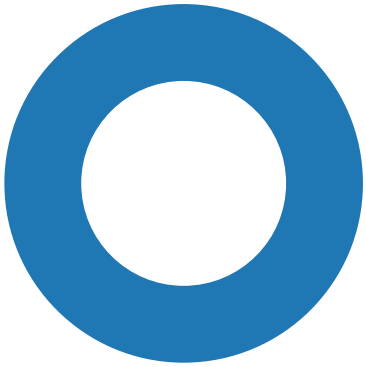
HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- sb.scorecardresearch.com

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **4964**, Parent PID: **2296**

General

Target ID:	0
Start time:	18:20:00
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:	0x7ff7d31b0000
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: **1648**, Parent PID: **4964**

General

Target ID:	1
Start time:	18:20:02
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=1944 --field-trial-handle=1748,i,13924636935230247093,10287414604649073630,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
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: **2944**, Parent PID: **2296**

General

Target ID:	2
Start time:	18:20:03
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" "http://sb.scorecardresearch.com/b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=1675295934629&ns_c=UTF-8&c7=https://www.linkedin.com/in/ritu-sharma-9318a61b1/&c9=
Imagebase:	0x7ff7d31b0000
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