ID: 800691
Cookbook: browseurl.jbs
Time: 18:13:45
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

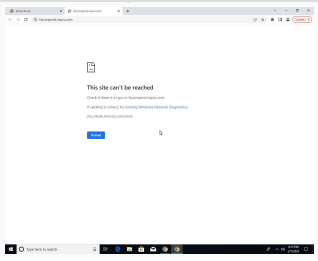
Windows Analysis Report

https://fsscmsprod.wipro.com/

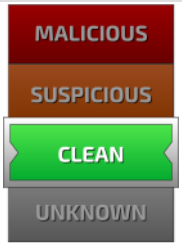
Overview

General Information

Sample URL:	http://https://fsscmsprod.wipro.com/
Analysis ID:	800691
Infos:	



Detection

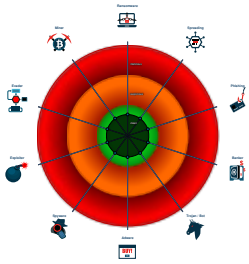


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 3124 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1876 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=1660 --field-trial-handle=1732,i,3982568901732112948,1407788595426497895,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6152 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://fsscmsprod.wipro.com/ 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

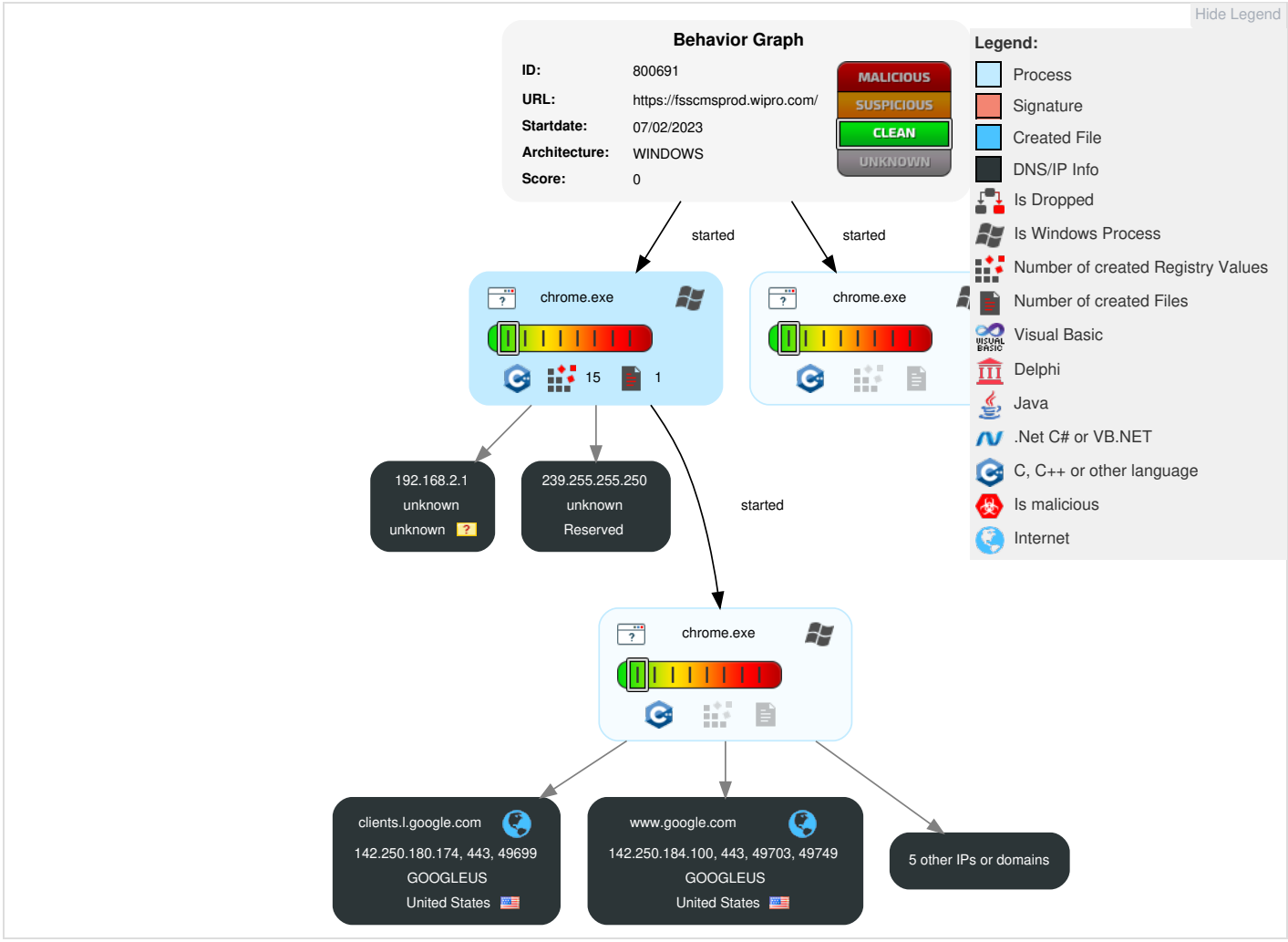
Joe Sandbox Signatures

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

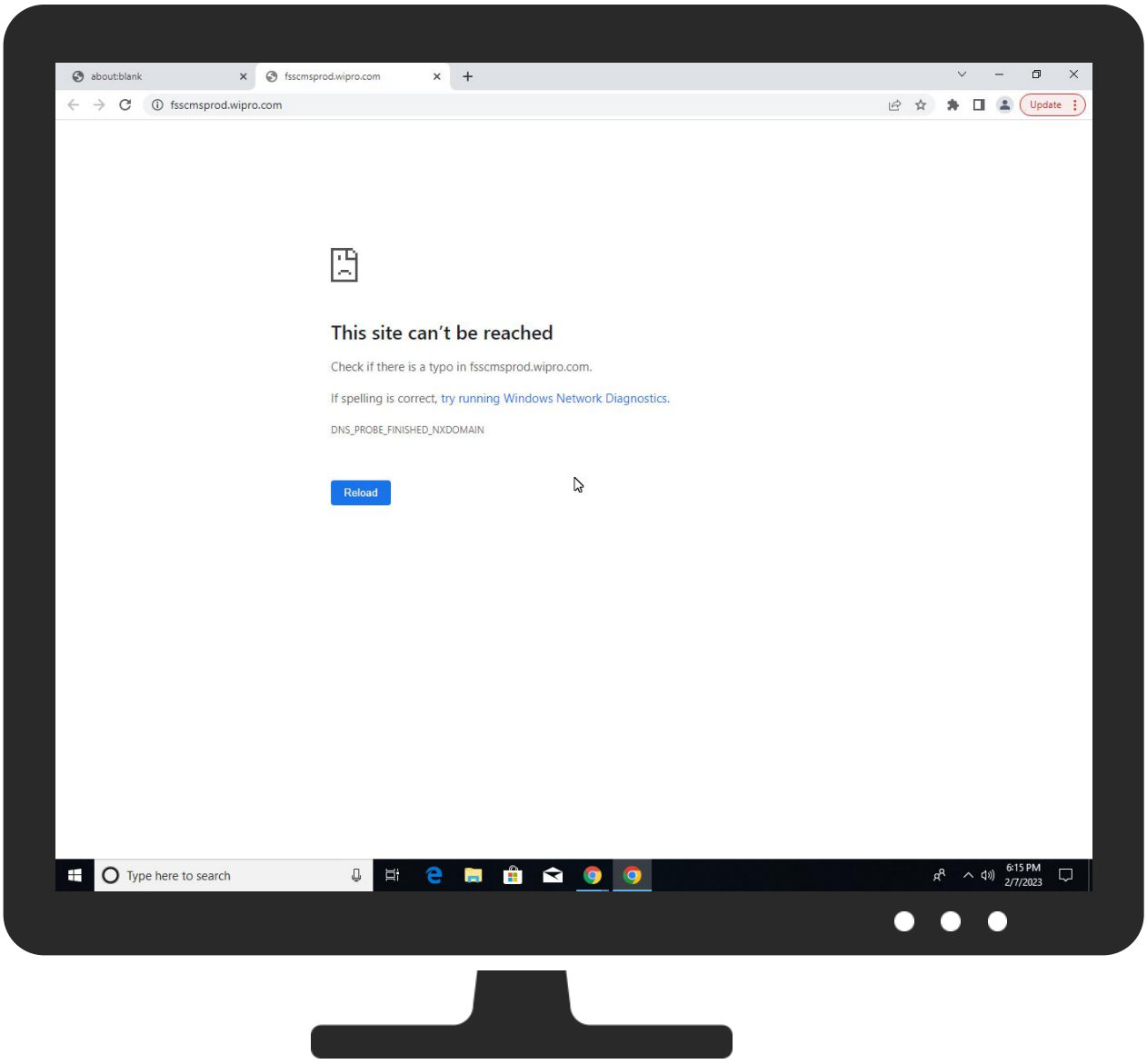
Behavior Graph



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://fsscmsprod.wipro.com/	0%	Virustotal		Browse
http://https://fsscmsprod.wipro.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

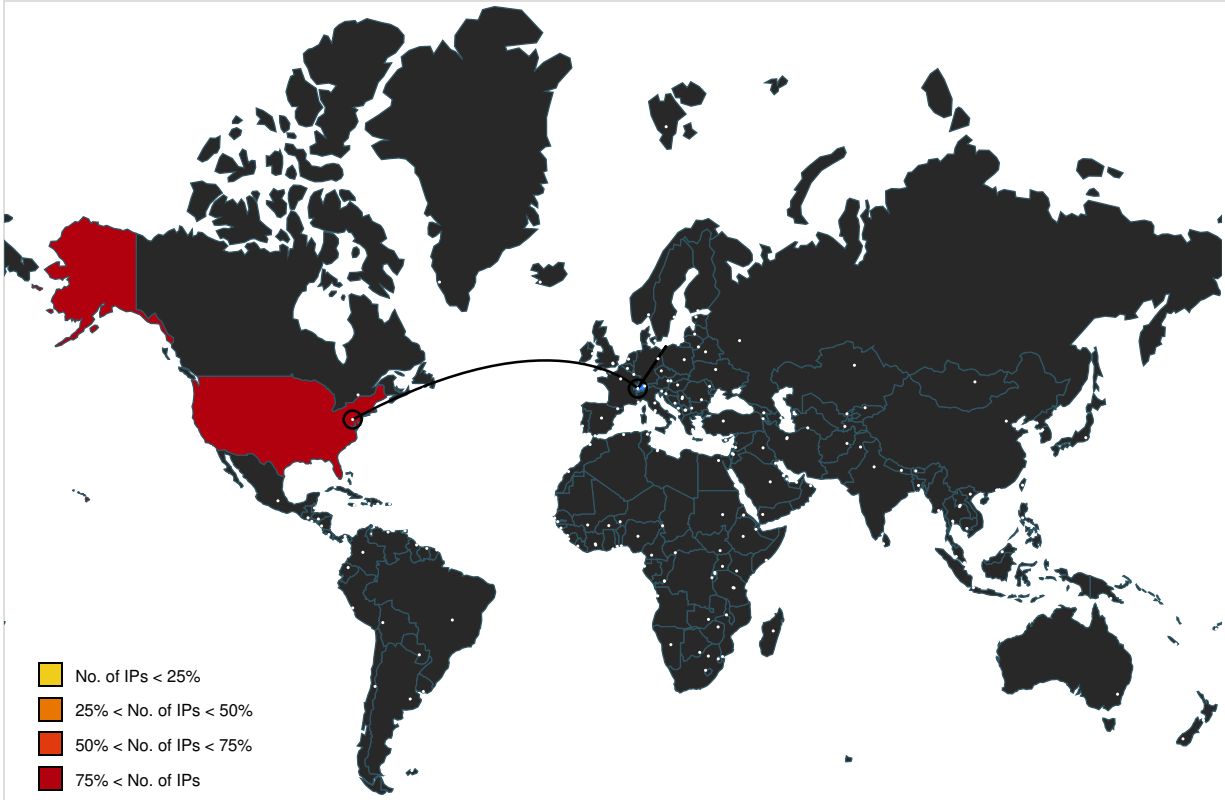
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	142.251.209.14	true	false		high
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
fsscmsprod.wipro.com	unknown	unknown	false		high
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://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
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:	800691
Start date and time:	2023-02-07 18:13:45 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://fsscmsprod.wipro.com/
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@30/0@9/6
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
- 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, 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

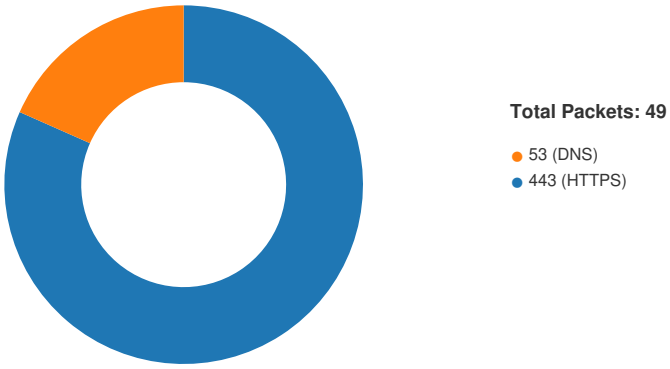
No created / dropped files found

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 18:14:57.288343906 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.288394928 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.288670063 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.289661884 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.289724112 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.289840937 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.292113066 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.292140007 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.293378115 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.293402910 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.483403921 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.484039068 CET	443	49699	142.250.180.174	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:14:57.552762985 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.596004009 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.596062899 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.596491098 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.596524954 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.597012997 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.597042084 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.597146988 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.599802971 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:57.599973917 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:57.600169897 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.600229979 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:57.600286961 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:57.652796030 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.117115974 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.117175102 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.117331028 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.117455959 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.117491961 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.117719889 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:58.117769003 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.117876053 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:58.117889881 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.118025064 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.162638903 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.162784100 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:58.162816048 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.162913084 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.162967920 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:58.166218042 CET	49699	443	192.168.2.5	142.250.180.174
Feb 7, 2023 18:14:58.166253090 CET	443	49699	142.250.180.174	192.168.2.5
Feb 7, 2023 18:14:58.183661938 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.183808088 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.183830976 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.185111046 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.185201883 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.186825991 CET	49701	443	192.168.2.5	216.58.209.45
Feb 7, 2023 18:14:58.186855078 CET	443	49701	216.58.209.45	192.168.2.5
Feb 7, 2023 18:14:58.915904045 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:58.915951014 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:58.916050911 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:58.920074940 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:58.920099020 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:58.998572111 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.001359940 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:59.001408100 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.003814936 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.003993034 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:59.006789923 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:59.006819963 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.007064104 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.052901030 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:14:59.052920103 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:14:59.152889013 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:08.969372988 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:08.969458103 CET	443	49703	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:08.969584942 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:14.296684980 CET	49703	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:14.296722889 CET	443	49703	142.250.184.100	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:15:58.776391983 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:58.776454926 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.776557922 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:58.777013063 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:58.777026892 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.842084885 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.850186110 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:58.850228071 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.850797892 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.851706982 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:15:58.851722002 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.851814985 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:15:58.897332907 CET	49749	443	192.168.2.5	142.250.184.100
Feb 7, 2023 18:16:08.824709892 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:16:08.824803114 CET	443	49749	142.250.184.100	192.168.2.5
Feb 7, 2023 18:16:08.824922085 CET	49749	443	192.168.2.5	142.250.184.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:14:57.099898100 CET	60649	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:57.103879929 CET	51441	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:57.118413925 CET	53	60649	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:57.126085997 CET	53	51441	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:57.127448082 CET	49724	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:57.154201031 CET	53	49724	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:58.324964046 CET	65323	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:58.326065063 CET	51484	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:58.344638109 CET	53	65323	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:58.346194983 CET	53	51484	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:58.738246918 CET	56751	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:58.756057978 CET	53	56751	8.8.8.8	192.168.2.5
Feb 7, 2023 18:14:59.511797905 CET	60975	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:14:59.535020113 CET	53	60975	8.8.8.8	192.168.2.5
Feb 7, 2023 18:15:05.027570009 CET	56682	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:15:05.045797110 CET	53	56682	8.8.8.8	192.168.2.5
Feb 7, 2023 18:15:35.354403019 CET	56687	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:15:35.374531984 CET	53	56687	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 18:14:57.099898100 CET	192.168.2.5	8.8.8.8	0x5e88	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:57.103879929 CET	192.168.2.5	8.8.8.8	0xfa2b	Standard query (0)	fsscmsprod.wipro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:57.127448082 CET	192.168.2.5	8.8.8.8	0x646a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.324964046 CET	192.168.2.5	8.8.8.8	0x8a83	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.326065063 CET	192.168.2.5	8.8.8.8	0x4f63	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.738246918 CET	192.168.2.5	8.8.8.8	0xbac1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:59.511797905 CET	192.168.2.5	8.8.8.8	0xc715	Standard query (0)	fsscmsprod.wipro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:15:05.027570009 CET	192.168.2.5	8.8.8.8	0xf597	Standard query (0)	fsscmsprod.wipro.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:15:35.354403019 CET	192.168.2.5	8.8.8.8	0xff52	Standard query (0)	fsscmsprod.wipro.com	A (IP address)	IN (0x0001)	false

DNS Answers

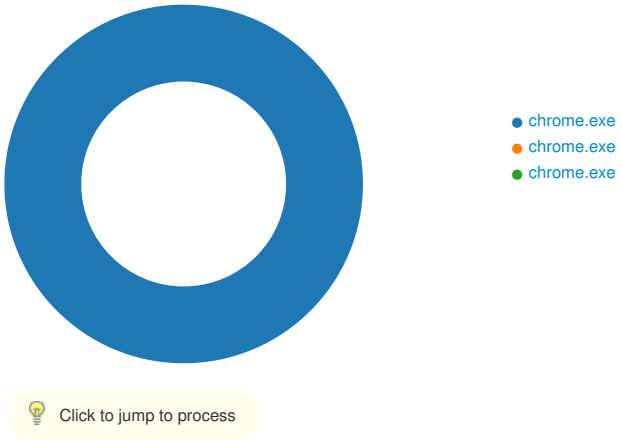
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:14:57.118413925 CET	8.8.8.8	192.168.2.5	0x5e88	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:57.154201031 CET	8.8.8.8	192.168.2.5	0x646a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:14:57.154201031 CET	8.8.8.8	192.168.2.5	0x646a	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.344638109 CET	8.8.8.8	192.168.2.5	0x8a83	No error (0)	google.com		142.251.209.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.346194983 CET	8.8.8.8	192.168.2.5	0x4f63	No error (0)	google.com		142.251.209.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:58.756057978 CET	8.8.8.8	192.168.2.5	0xbac1	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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **3124**, Parent PID: **2984**

General

Target ID:	0
Start time:	18:14:51
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: **1876**, Parent PID: **3124**

General

Target ID:	1
Start time:	18:14:53
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=1660 --field-trial-handle=1732,i,3982568901732112948,1407788595426497895,131072 --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: **6152**, Parent PID: **2984**

General

Target ID:	2
Start time:	18:14:54
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" "https://fsscmsprod.wipro.com/
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