ID: 1581151
Cookbook: browseurl.jbs
Time: 06:29:20
Date: 27/12/2024
Version: 41.0.0 Charoite

Table of Contents

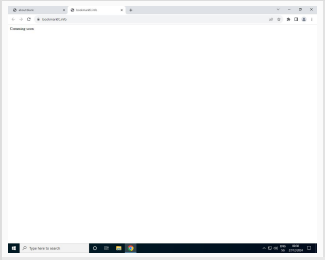
Windows Analysis Report

http://bookmarkfc.info

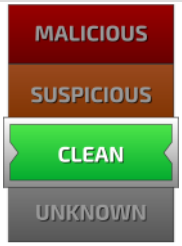
Overview

General Information

Sample URL:	http://bookmarkfc.info
Analysis ID:	1581151
Infos:	



Detection

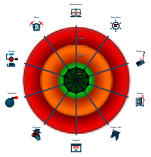


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2148 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 4428 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=2320 --field-trial-handle=2228,i,11652739893889807078,4869841092454622456,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6560 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "http://bookmarkfc.info" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

No Suricata rule has matched

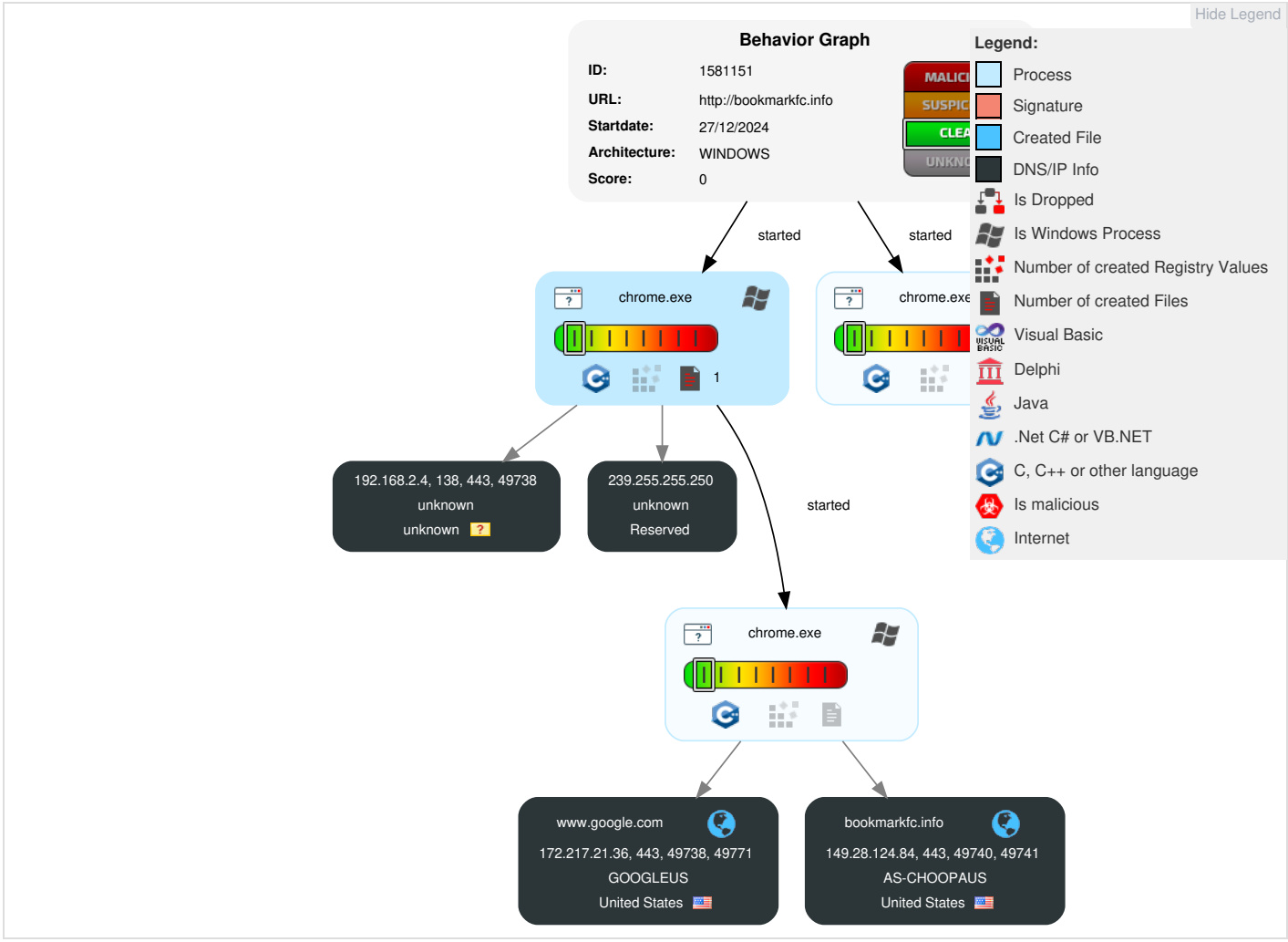
Joe Sandbox Signatures

There are no malicious signatures

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	2 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	3 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

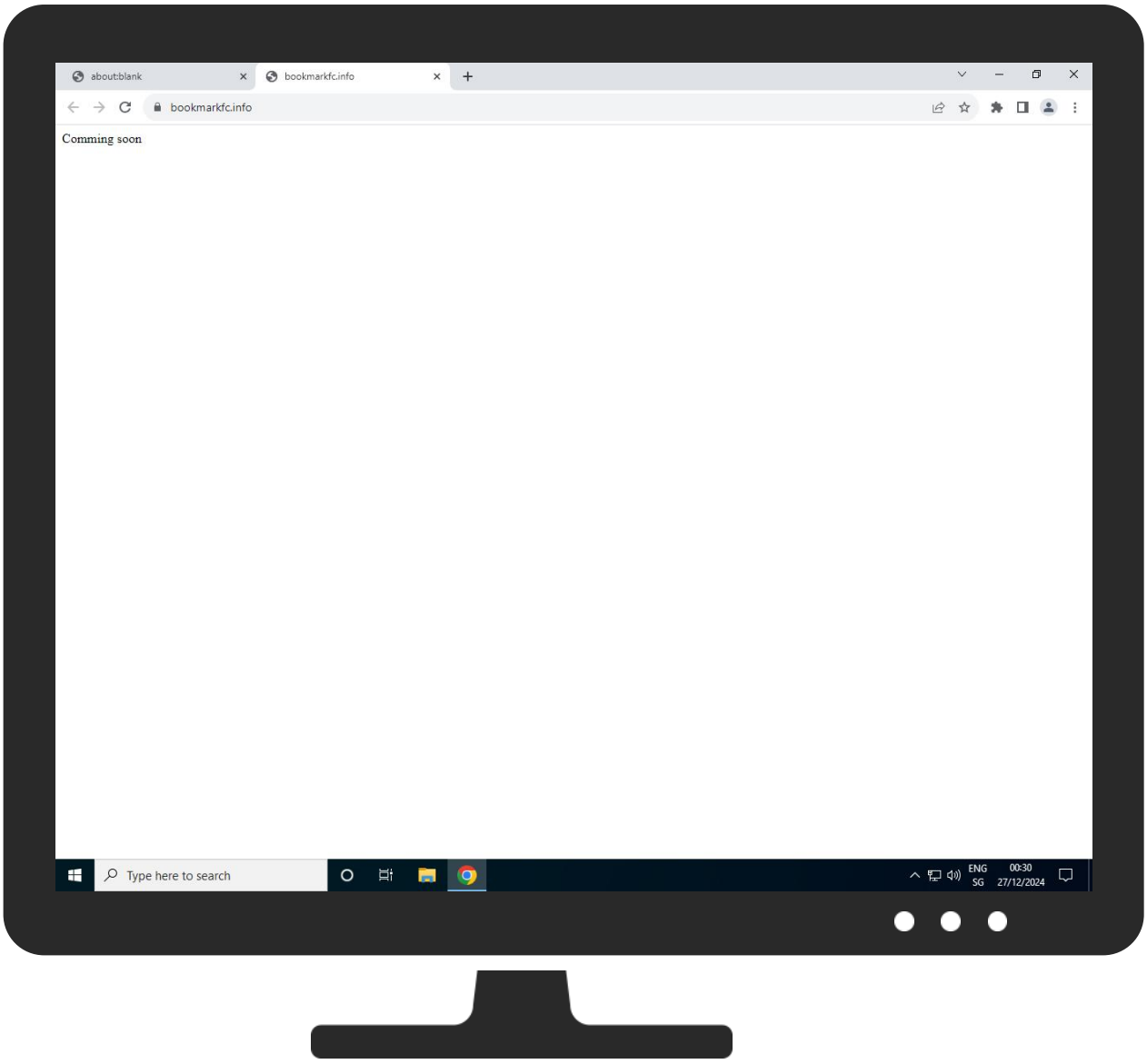
Behavior Graph



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://bookmarkfc.info	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://bookmarkfc.info/	0%	Avira URL Cloud	safe	
http://https://bookmarkfc.info/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

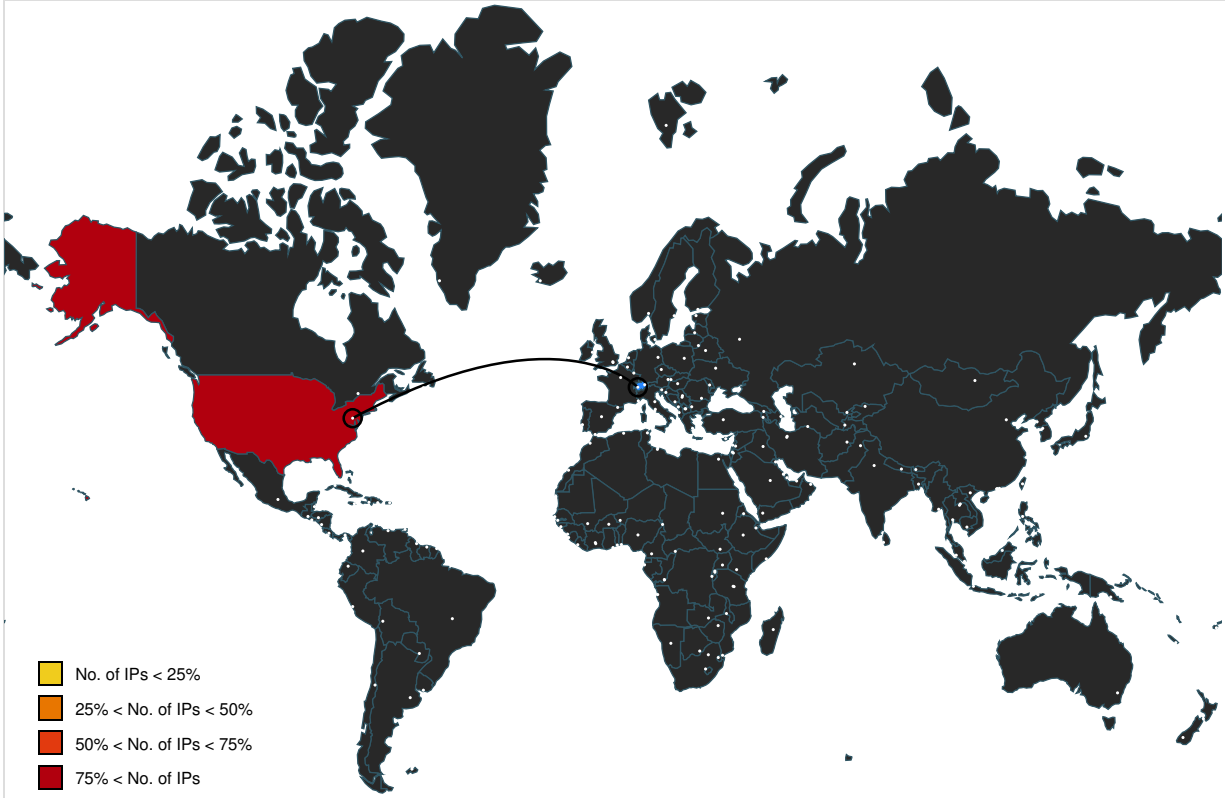
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bookmarkfc.info	149.28.124.84	true	false		unknown
www.google.com	172.217.21.36	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bookmarkfc.info/	false	• Avira URL Cloud: safe	unknown
http://https://bookmarkfc.info/	false		unknown
http://https://bookmarkfc.info/favicon.ico	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.21.36	www.google.com	United States		15169	GOOGLEUS	false
149.28.124.84	bookmarkfc.info	United States		20473	AS-CHOOPAUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1581151
Start date and time:	2024-12-27 06:29:20 +01:00

Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 2m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://bookmarkfc.info
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@17/2@8/4
EGA 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, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.21.35, 172.217.19.238, 173.194.220.84, 172.217.17.46, 199.232.210.172, 192.229.221.95, 172.217.17.35, 184.30.17.174, 4.245.163.56, 13.107.246.63
- Excluded domains from analysis (whitelisted): fs.microsoft.com, accounts.google.com, slscr.update.microsoft.com, otelrules.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, fe3cr.delivery.mp.microsoft.com, clients2.google.com, ocsp.digicert.com, edgedl.me.gvt1.com, redirector.gvt1.com, update.googleapis.com, clients.l.google.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: http://bookmarkfc.info

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

Chrome Cache Entry: 43

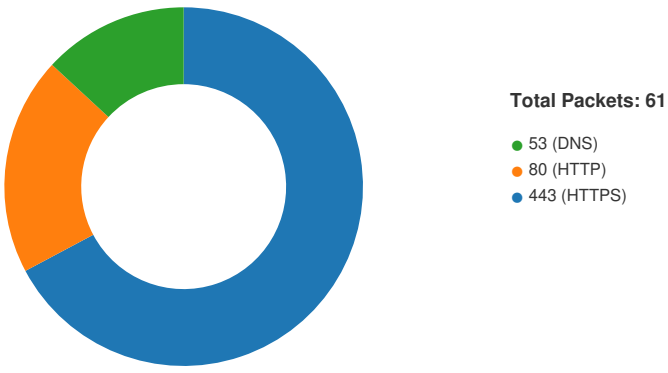
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	12
Entropy (8bit):	2.8553885422075336
Encrypted:	false
SSDEEP:	3:mKQn:Wn
MD5:	5F41670A7460D03DCA5911FF21C912DE
SHA1:	094008AA1820979932EBA729E834E0217C424101
SHA-256:	E705DE99EEFC7F4D4E68CBF4A8F8BF05F0DA9190091D2E5EB7EAEE5532A97F9A
SHA-512:	B55D0E6784BF470766AC1F5D351FB7BB879D60C73D6DC6649BEE68D7EE344E3ECF5FFE5333A01F8F4F96C4EC3BFA3710833F399DDE77CCD7388C31F2A254FE8F
Malicious:	false
Reputation:	low
URL:	http://https://bookmarkfc.info/
Preview:	Comming soon

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2024 06:30:07.339488983 CET	49675	443	192.168.2.4	173.222.162.32
Dec 27, 2024 06:30:16.946455956 CET	49675	443	192.168.2.4	173.222.162.32
Dec 27, 2024 06:30:20.938450098 CET	49738	443	192.168.2.4	172.217.21.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2024 06:30:20.938486099 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:20.941268921 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:20.941268921 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:20.941301107 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.545937061 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.546713114 CET	49741	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.636313915 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.637094975 CET	49742	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.637346983 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:22.637362003 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.638346910 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.638453960 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:22.639448881 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:22.639512062 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.665425062 CET	80	49740	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:22.665514946 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.665704966 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.666112900 CET	80	49741	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:22.666382074 CET	49741	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.684709072 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:22.684721947 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:22.732243061 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:22.756524086 CET	80	49742	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:22.756686926 CET	49742	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:22.785284996 CET	80	49740	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:23.937585115 CET	80	49740	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:23.986216068 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:24.132823944 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:24.132858992 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:24.132944107 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:24.133368969 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:24.133383989 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.431133032 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.431448936 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.431489944 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.432493925 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.432564974 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.436960936 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.437026978 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.437263012 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.437273026 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.478465080 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.907059908 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.907130957 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.907291889 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.908193111 CET	49744	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.908214092 CET	443	49744	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.972774982 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.972842932 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:25.972956896 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.973211050 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:25.973227978 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.266623020 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.267028093 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.267061949 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.267395973 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.267716885 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.267776966 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.267878056 CET	49745	443	192.168.2.4	149.28.124.84

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2024 06:30:27.315332890 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.729033947 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.729111910 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.729176044 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.729779005 CET	49745	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.729800940 CET	443	49745	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.872440100 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.872479916 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:27.872551918 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.872766972 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:27.872781992 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.165411949 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.165657043 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.165685892 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.166661024 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.166719913 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.167057991 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.167125940 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.167202950 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.167215109 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.213146925 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.631623983 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.631697893 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.632843018 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.632874966 CET	443	49746	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:29.632916927 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:29.633186102 CET	49746	443	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:32.343842030 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:32.343911886 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:32.344002962 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:33.105480909 CET	49738	443	192.168.2.4	172.217.21.36
Dec 27, 2024 06:30:33.105509043 CET	443	49738	172.217.21.36	192.168.2.4
Dec 27, 2024 06:30:38.937289953 CET	80	49740	149.28.124.84	192.168.2.4
Dec 27, 2024 06:30:38.937361956 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:39.105993032 CET	49740	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:30:39.225533962 CET	80	49740	149.28.124.84	192.168.2.4
Dec 27, 2024 06:31:07.682229996 CET	49741	80	192.168.2.4	149.28.124.84
Dec 27, 2024 06:31:07.760374069 CET	49742	80	192.168.2.4	149.28.124.84

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2024 06:30:16.380825996 CET	53	52377	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:16.390126944 CET	53	51971	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:19.222909927 CET	53	58288	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:20.792557001 CET	52603	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:20.792557001 CET	61411	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:20.929800034 CET	53	61411	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:20.935349941 CET	53	52603	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:22.369261026 CET	56400	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:22.370054960 CET	58337	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:22.506906033 CET	53	56400	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:22.907480955 CET	53	58337	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:23.970129967 CET	59592	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:23.970279932 CET	62757	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:24.109648943 CET	53	62757	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:24.114483118 CET	53	59592	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:27.733831882 CET	65387	53	192.168.2.4	1.1.1.1
Dec 27, 2024 06:30:27.733983040 CET	55026	53	192.168.2.4	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 27, 2024 06:30:27.871795893 CET	53	55026	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:27.872010946 CET	53	65387	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:34.064795017 CET	138	138	192.168.2.4	192.168.2.255
Dec 27, 2024 06:30:36.181329012 CET	53	50715	1.1.1.1	192.168.2.4
Dec 27, 2024 06:30:55.149323940 CET	53	57775	1.1.1.1	192.168.2.4
Dec 27, 2024 06:31:16.293432951 CET	53	51196	1.1.1.1	192.168.2.4
Dec 27, 2024 06:31:17.835587978 CET	53	53068	1.1.1.1	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 27, 2024 06:30:22.907641888 CET	192.168.2.4	1.1.1.1	c22e	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 27, 2024 06:30:20.792557001 CET	192.168.2.4	1.1.1.1	0xeeef	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:20.792557001 CET	192.168.2.4	1.1.1.1	0xfa6f	Standard query (0)	www.google.com	65	IN (0x0001)	false
Dec 27, 2024 06:30:22.369261026 CET	192.168.2.4	1.1.1.1	0x38a	Standard query (0)	bookmarkfc.info	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:22.370054960 CET	192.168.2.4	1.1.1.1	0xe095	Standard query (0)	bookmarkfc.info	65	IN (0x0001)	false
Dec 27, 2024 06:30:23.970129967 CET	192.168.2.4	1.1.1.1	0x5cae	Standard query (0)	bookmarkfc.info	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:23.970279932 CET	192.168.2.4	1.1.1.1	0xdeca	Standard query (0)	bookmarkfc.info	65	IN (0x0001)	false
Dec 27, 2024 06:30:27.733831882 CET	192.168.2.4	1.1.1.1	0xe0c9	Standard query (0)	bookmarkfc.info	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:27.733983040 CET	192.168.2.4	1.1.1.1	0x3058	Standard query (0)	bookmarkfc.info	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 27, 2024 06:30:20.929800034 CET	1.1.1.1	192.168.2.4	0xfa6f	No error (0)	www.google.com			65	IN (0x0001)	false
Dec 27, 2024 06:30:20.935349941 CET	1.1.1.1	192.168.2.4	0xeeef	No error (0)	www.google.com		172.217.21.36	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:22.506906033 CET	1.1.1.1	192.168.2.4	0x38a	No error (0)	bookmarkfc.info		149.28.124.84	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:24.114483118 CET	1.1.1.1	192.168.2.4	0x5cae	No error (0)	bookmarkfc.info		149.28.124.84	A (IP address)	IN (0x0001)	false
Dec 27, 2024 06:30:27.872010946 CET	1.1.1.1	192.168.2.4	0xe0c9	No error (0)	bookmarkfc.info		149.28.124.84	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- bookmarkfc.info
- https:

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: 2148, Parent PID: 5768

General

Target ID:	0
Start time:	00:30:11
Start date:	27/12/2024
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:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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

Analysis Process: chrome.exe PID: 4428, Parent PID: 2148

General

Target ID:	2
Start time:	00:30:14
Start date:	27/12/2024
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=2320 --field-trial-handle=2228,i,11652739893889807078,4869841092454622456,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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: **6560**, Parent PID: **5768**

General

Target ID:	3
Start time:	00:30:20
Start date:	27/12/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" "http://bookmarkfc.info"
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly