ID: 1416195
Cookbook: browseurl.jbs
Time: 04:36:24
Date: 27/03/2024
Version: 40.0.0 Tourmaline

Table of Contents

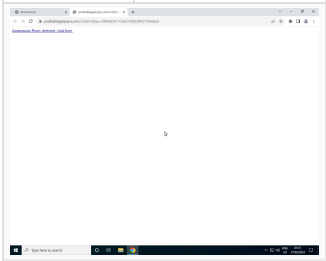
Windows Analysis Report

https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9

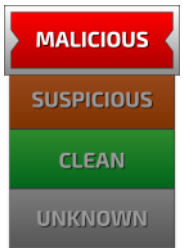
Overview

General Information

Sample URL:	http://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9
Analysis ID:	1416195
Infos:	



Detection

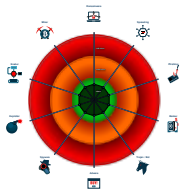


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for dom...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3496 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 6008 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=2428 --field-trial-handle=2376,i,12535326634719702236,3848146617297136620,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6544 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **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

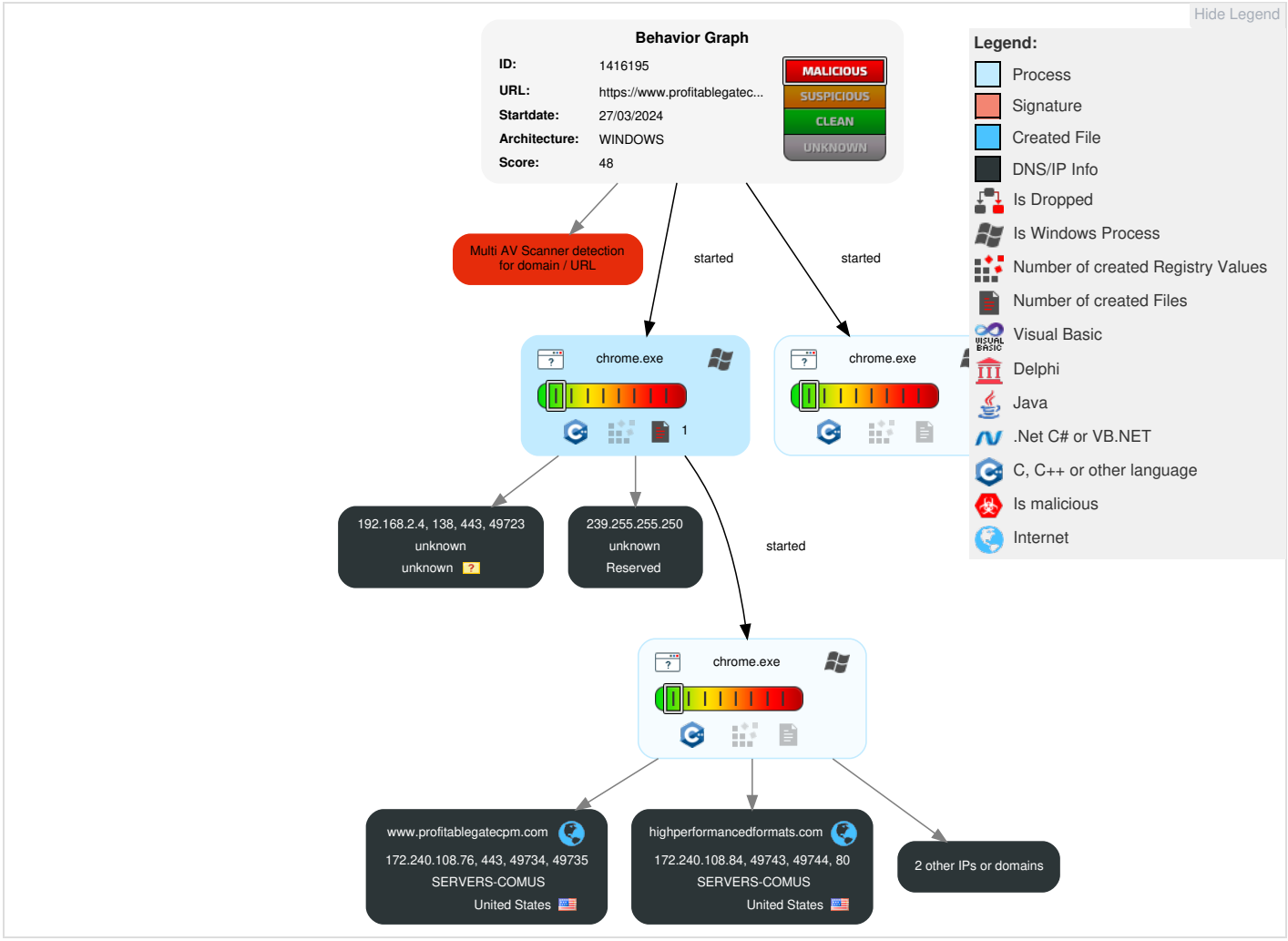
AV Detection

Multi AV Scanner detection for domain / URL

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	3 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	4 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	3 Ingress Tool Transfer	Traffic Duplication	Data Destruction

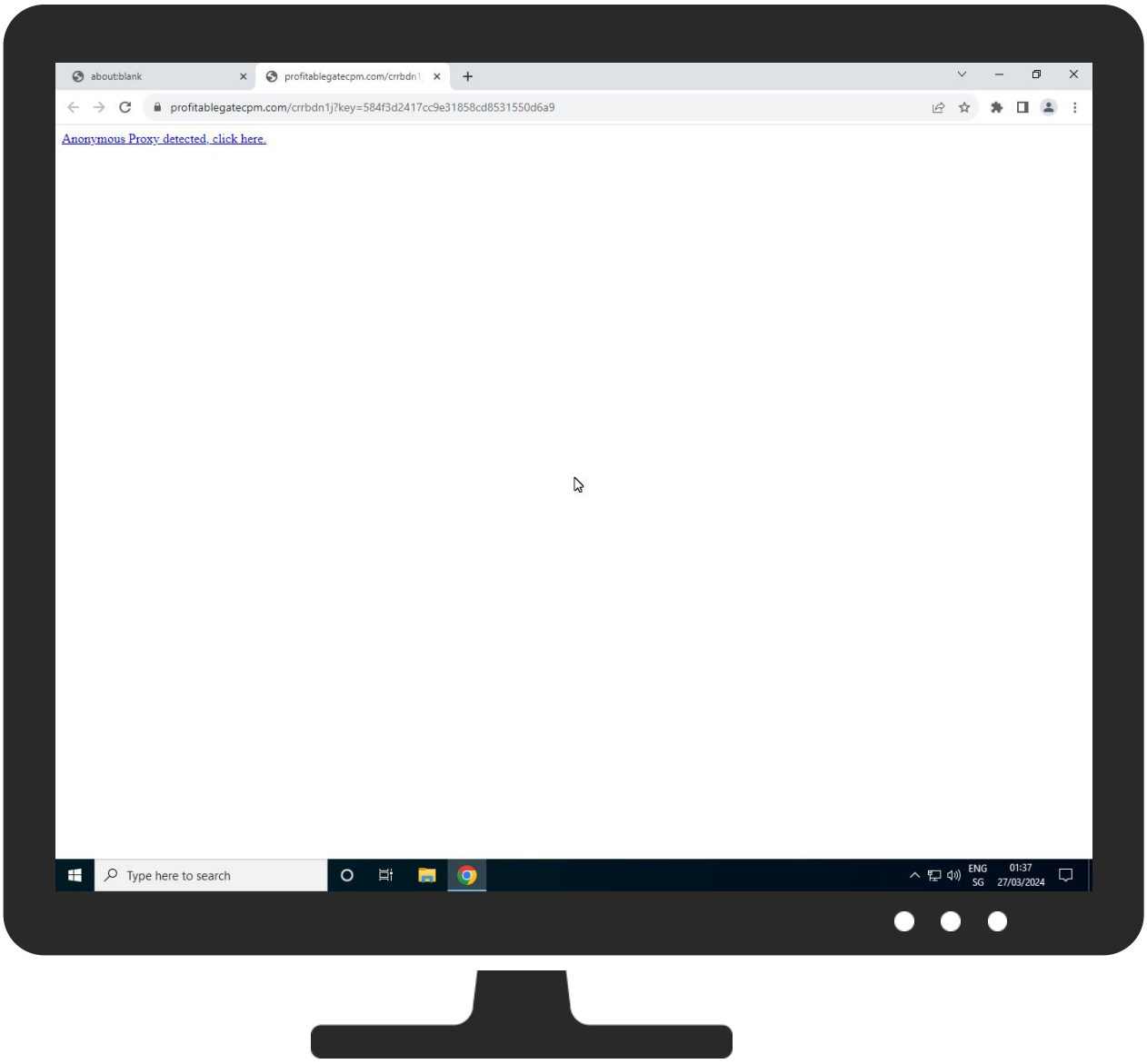
Behavior Graph



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://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9	0%	Avira URL Cloud	safe	
http://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.profitablegatecpm.com	3%	Virustotal		Browse
fp2e7a.wpc.phicdn.net	0%	Virustotal		Browse
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse
highperformancedformats.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.profitablegatecpm.com/favicon.ico	0%	Avira URL Cloud	safe	
http://highperformancedformats.com/anonymous/	0%	Avira URL Cloud	safe	
http://https://www.profitablegatecpm.com/favicon.ico	2%	Virustotal		Browse
http://highperformancedformats.com/anonymous/	4%	Virustotal		Browse

Domains and IPs

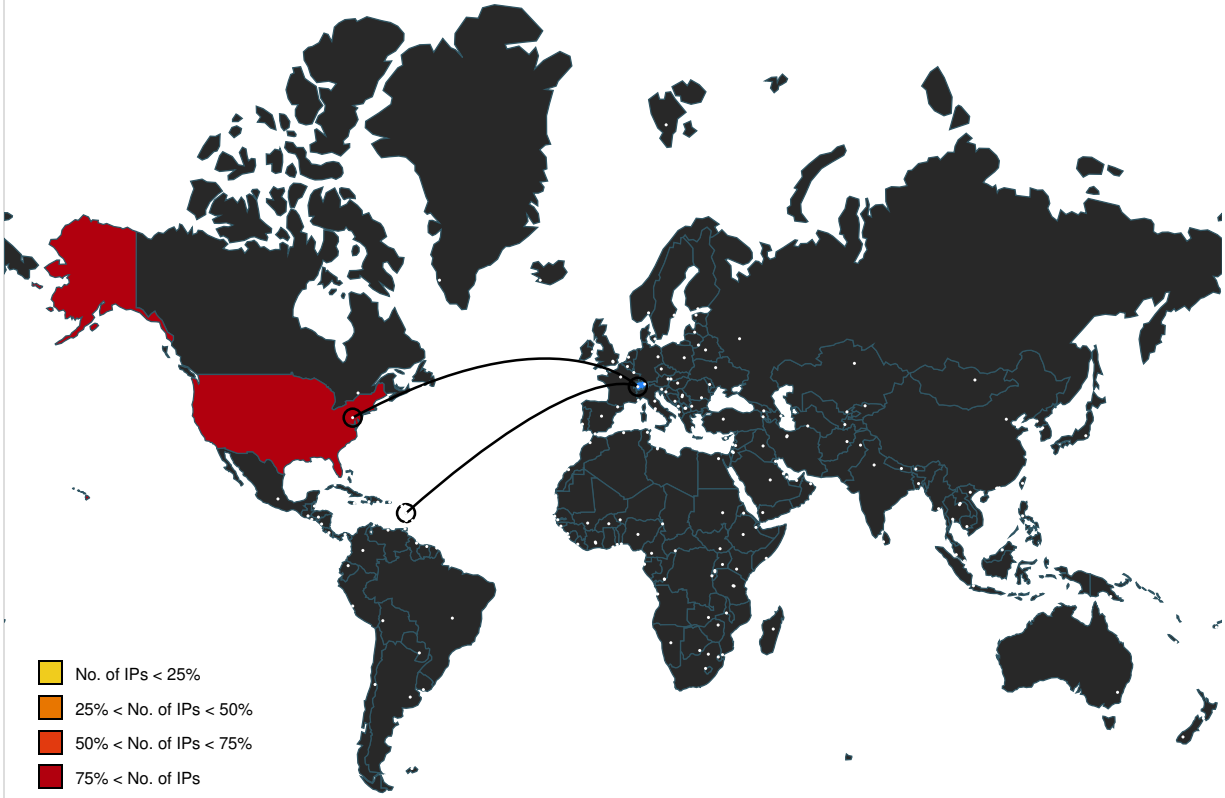
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
highperformancedformats.com	172.240.108.84	true	false	• 6%, Virustotal, Browse	unknown
www.profitablegatecpm.com	172.240.108.76	true	false	• 3%, Virustotal, Browse	unknown
www.google.com	172.253.62.99	true	false		high
fp2e7a.wpc.phicdn.net	192.229.211.108	true	false	• 0%, Virustotal, Browse	unknown
windowsupdatebg.s.llnwi.net	69.164.0.0	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.profitablegatecpm.com/favicon.ico	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9	false		unknown
http://highperformancedformats.com/anonymous/	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.240.108.76	www.profitablegatecpm.com	United States		7979	SERVERS-COMUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.243.61.227	unknown	Dominica		39572	ADVANCEDHOSTERS-ASNL	false
172.240.108.84	highperformancedformats.com	United States		7979	SERVERS-COMUS	false
172.253.62.99	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1416195
Start date and time:	2024-03-27 04:36:24 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 2m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9
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:	7
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:	MAL
Classification:	mal48.win@18/2@8/6
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: http://highperformancedformats.com/anonymous/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.253.63.84, 172.253.122.113, 172.253.122.138, 172.253.122.100, 172.253.122.102, 172.253.122.139, 172.253.122.101, 172.253.115.94, 34.104.35.123, 52.165.165.26, 69.164.0.0, 192.229.211.108, 52.165.164.15, 20.242.39.171, 172.253.63.94
- Excluded domains from analysis (whitelisted): fs.microsoft.com, accounts.google.com, slscr.update.microsoft.com, clientservices.googleapis.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, clients2.google.com, edgedl.me.gvt1.com, ocsp.digicert.com, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, update.googleapis.com, clients.l.google.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile 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

Chrome Cache Entry: 42

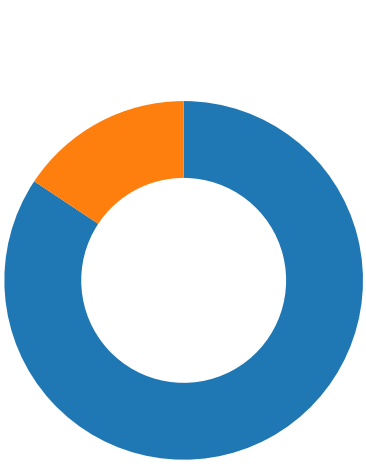
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.719823396275518
Encrypted:	false
SSDEEP:	3:uNXADiFCDRAWMO5h1KRWLRE+Vs2+ZJiNRDs7SGKy:uFAyTWLhgRW2+T+ZJas7Sdy
MD5:	16579CC322E9E105427ECFA57890EF69
SHA1:	8BB47EC30CF894AB49032D7271A45F0C778BAA05
SHA-256:	F28CE5BEFE08ED90A2E12B6B2A5E9FDAFAA6AD173503079155260AA480C66590
SHA-512:	FCF36F77D99F6594929BDED28F200BEE11FAB9B316A5E437567345B8877CFC6707BF8A116C03F07B03C0235B587E71DBD4843560564BAE07BAD2F5B6295CCE3F
Malicious:	false
Reputation:	low
URL:	http://https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9
Preview:	Anonymous Proxy detected, click here.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2024 04:37:06.651168108 CET	49678	443	192.168.2.4	104.46.162.224
Mar 27, 2024 04:37:07.448016882 CET	49675	443	192.168.2.4	173.222.162.32
Mar 27, 2024 04:37:15.791064024 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.791094065 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:15.791270971 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.791625977 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.791654110 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:15.791712046 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.791891098 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.791903973 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:15.792037964 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:15.792049885 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.098902941 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.099225044 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.099247932 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.099517107 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.099703074 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.099711895 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.100162983 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.100234032 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.100591898 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.100655079 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.101247072 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.101313114 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.102154970 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.102209091 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.102287054 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.102292061 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.153175116 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.153343916 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.153350115 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.200347900 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.200414896 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.200509071 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.205190897 CET	49734	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.205204010 CET	443	49734	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.251863003 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.256798029 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.300275087 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.353025913 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.353096962 CET	443	49735	172.240.108.76	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2024 04:37:16.353143930 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.353610039 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.353619099 CET	443	49735	172.240.108.76	192.168.2.4
Mar 27, 2024 04:37:16.353646040 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.353662968 CET	49735	443	192.168.2.4	172.240.108.76
Mar 27, 2024 04:37:16.480485916 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.480514050 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.480602026 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.480807066 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.480818987 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.652334929 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.652368069 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.652436972 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.652620077 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.652637005 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.767479897 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.768412113 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.768420935 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.769309044 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.769381046 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.769675016 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.769726038 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.769809008 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.769813061 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.821882010 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.862059116 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.862421036 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.862427950 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.863321066 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.863403082 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.864309072 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.864334106 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.864361048 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.864368916 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.864423990 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.865156889 CET	49737	443	192.168.2.4	192.243.61.227
Mar 27, 2024 04:37:16.865164042 CET	443	49737	192.243.61.227	192.168.2.4
Mar 27, 2024 04:37:16.915647030 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:16.915653944 CET	443	49738	172.253.62.99	192.168.2.4
Mar 27, 2024 04:37:16.962546110 CET	49738	443	192.168.2.4	172.253.62.99
Mar 27, 2024 04:37:17.056277037 CET	49675	443	192.168.2.4	173.222.162.32
Mar 27, 2024 04:37:18.868546963 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:18.868566036 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:18.868676901 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:18.870333910 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:18.870346069 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.070045948 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.070167065 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.076385975 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.076390982 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.076601028 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.128412962 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.153554916 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.200228930 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.254271984 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.254334927 CET	443	49741	23.221.242.90	192.168.2.4
Mar 27, 2024 04:37:19.254471064 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.254671097 CET	49741	443	192.168.2.4	23.221.242.90
Mar 27, 2024 04:37:19.254683971 CET	443	49741	23.221.242.90	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2024 04:37:14.331636906 CET	53	56607	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:14.332320929 CET	53	61536	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:14.947185993 CET	53	52837	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:15.425201893 CET	58584	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:15.425362110 CET	60679	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:15.520006895 CET	53	60679	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:15.784751892 CET	53	58584	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:16.356590033 CET	54729	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:16.356777906 CET	61688	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:16.453017950 CET	53	54729	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:16.556750059 CET	55088	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:16.556896925 CET	57192	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:16.651356936 CET	53	57192	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:16.651674986 CET	53	55088	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:16.698818922 CET	53	61688	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:28.521361113 CET	56309	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:28.521892071 CET	54708	53	192.168.2.4	1.1.1.1
Mar 27, 2024 04:37:28.616873980 CET	53	56309	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:28.860877991 CET	53	54708	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:31.982098103 CET	53	52657	1.1.1.1	192.168.2.4
Mar 27, 2024 04:37:37.187417030 CET	138	138	192.168.2.4	192.168.2.255
Mar 27, 2024 04:37:50.950275898 CET	53	52929	1.1.1.1	192.168.2.4
Mar 27, 2024 04:38:13.139796019 CET	53	59569	1.1.1.1	192.168.2.4
Mar 27, 2024 04:38:13.654031038 CET	53	56459	1.1.1.1	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 27, 2024 04:37:16.698884010 CET	192.168.2.4	1.1.1.1	c233	(Port unreachable)	Destination Unreachable
Mar 27, 2024 04:37:28.860934973 CET	192.168.2.4	1.1.1.1	c233	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 27, 2024 04:37:15.425201893 CET	192.168.2.4	1.1.1.1	0xf3d8	Standard query (0)	www.profitablegatecpm.com	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.425362110 CET	192.168.2.4	1.1.1.1	0xb267	Standard query (0)	www.profitablegatecpm.com	65	IN (0x0001)	false
Mar 27, 2024 04:37:16.356590033 CET	192.168.2.4	1.1.1.1	0xe0a	Standard query (0)	www.profitablegatecpm.com	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.356777906 CET	192.168.2.4	1.1.1.1	0x4780	Standard query (0)	www.profitablegatecpm.com	65	IN (0x0001)	false
Mar 27, 2024 04:37:16.556750059 CET	192.168.2.4	1.1.1.1	0xd59c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.556896925 CET	192.168.2.4	1.1.1.1	0x7bc9	Standard query (0)	www.google.com	65	IN (0x0001)	false
Mar 27, 2024 04:37:28.521361113 CET	192.168.2.4	1.1.1.1	0x694d	Standard query (0)	highperformancedformats.com	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.521892071 CET	192.168.2.4	1.1.1.1	0xf153	Standard query (0)	highperformancedformats.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		192.243.59.20	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		172.240.253.132	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		172.240.108.68	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		192.243.59.12	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:15.784751892 CET	1.1.1.1	192.168.2.4	0xf3d8	No error (0)	www.profitablegatecpm.com		172.240.127.234	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		172.240.108.68	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		172.240.253.132	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		192.243.59.20	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		172.240.127.234	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.453017950 CET	1.1.1.1	192.168.2.4	0xe0a	No error (0)	www.profitablegatecpm.com		192.243.59.12	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.651356936 CET	1.1.1.1	192.168.2.4	0x7bc9	No error (0)	www.google.com			65	IN (0x0001)	false
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.99	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.104	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.147	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.106	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.103	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:16.651674986 CET	1.1.1.1	192.168.2.4	0xd59c	No error (0)	www.google.com		172.253.62.105	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		192.243.59.12	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		192.243.59.20	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		172.240.127.234	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		172.240.253.132	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		172.240.108.68	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:28.616873980 CET	1.1.1.1	192.168.2.4	0x694d	No error (0)	highperformancedformats.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:30.456981897 CET	1.1.1.1	192.168.2.4	0x8e9b	No error (0)	windowsupdatebg.s.llnwi.net		69.164.0.0	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:30.764244080 CET	1.1.1.1	192.168.2.4	0xcfdb	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 27, 2024 04:37:30.764244080 CET	1.1.1.1	192.168.2.4	0xcfdb	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:37:43.699197054 CET	1.1.1.1	192.168.2.4	0xde52	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 27, 2024 04:37:43.699197054 CET	1.1.1.1	192.168.2.4	0xde52	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:38:06.043224096 CET	1.1.1.1	192.168.2.4	0x470c	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 27, 2024 04:38:06.043224096 CET	1.1.1.1	192.168.2.4	0x470c	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 27, 2024 04:38:25.886792898 CET	1.1.1.1	192.168.2.4	0xc8ba	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 27, 2024 04:38:25.886792898 CET	1.1.1.1	192.168.2.4	0xc8ba	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.profitablegatecpm.com
- https:
- fs.microsoft.com
- highperformancedformats.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: 3496, Parent PID: 2568

General

Target ID:	0
Start time:	01:37:08
Start date:	27/03/2024
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: 6008, Parent PID: 3496

General

Target ID:	2
Start time:	01:37:10
Start date:	27/03/2024

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=2428 --field-trial-handle=2376,i,12535326634719702236,3848146617297136620,262144 --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: **6544**, Parent PID: **2568**

General

Target ID:	3
Start time:	01:37:13
Start date:	27/03/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" "https://www.profitablegatecpm.com/crrbdn1j?key=584f3d2417cc9e31858cd8531550d6a9"
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