ID: 1395948
Cookbook: browseurl.jbs
Time: 09:23:48
Date: 21/02/2024
Version: 40.0.0 Tourmaline

Table of Contents

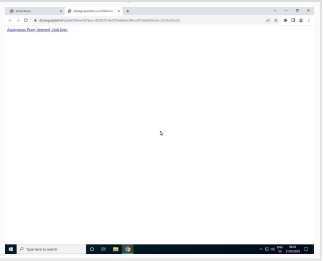
Windows Analysis Report

http://zwgaleriamlodych.pl

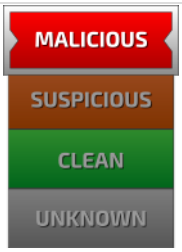
Overview

General Information

Sample URL:	http://zwgaleriamlodych.pl
Analysis ID:	1395948
Infos:	



Detection

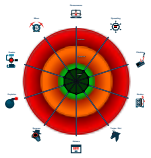


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dom…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3320 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 5228 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=2384 --field-trial-handle=2308,i,2546780249924042766,14441408258148433188,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6508 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://zwgaleriamlodych.pl 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

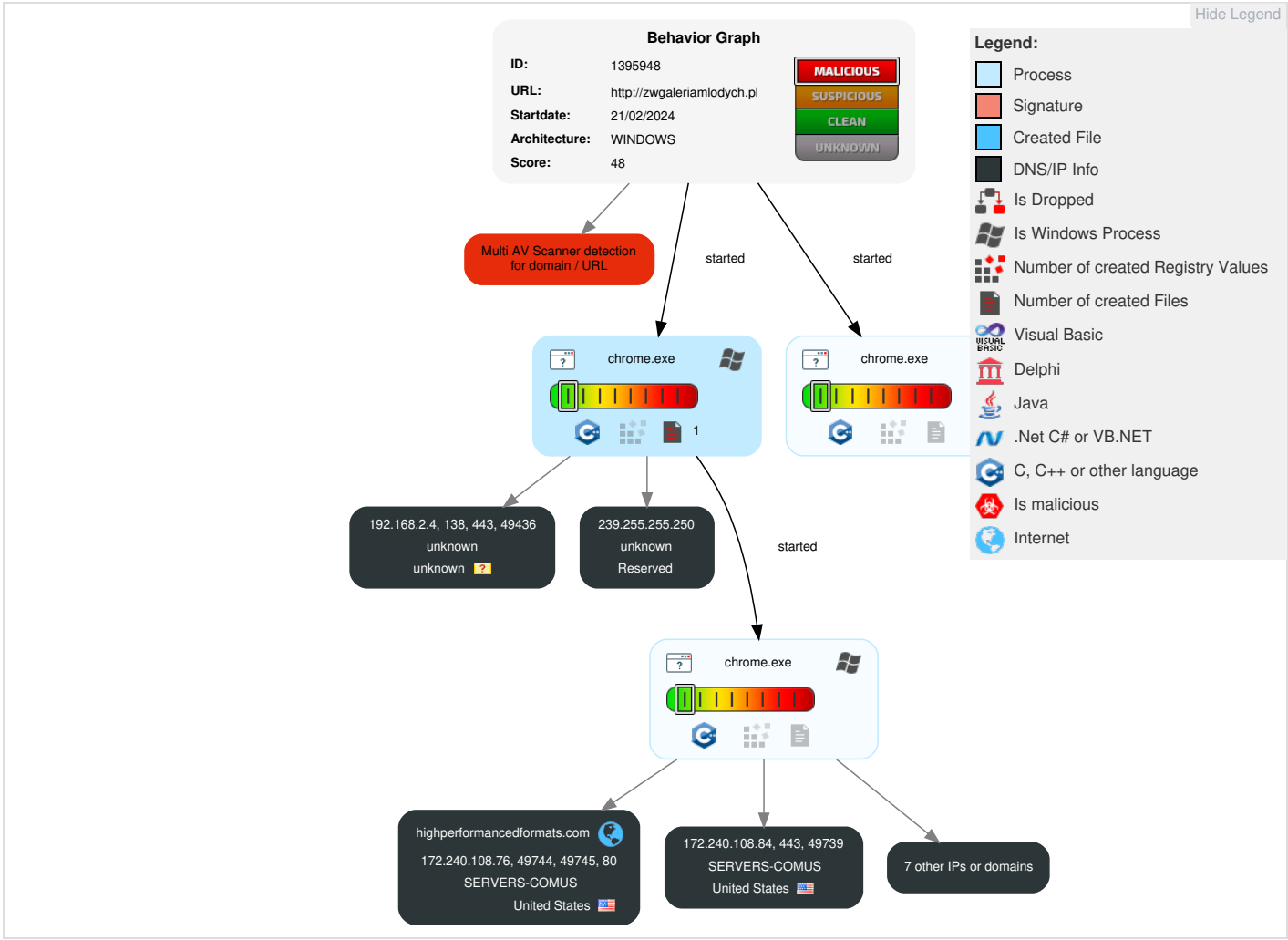
AV Detection

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 Masquerading	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	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	4 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	5 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

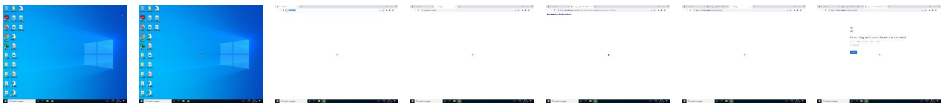
Behavior Graph

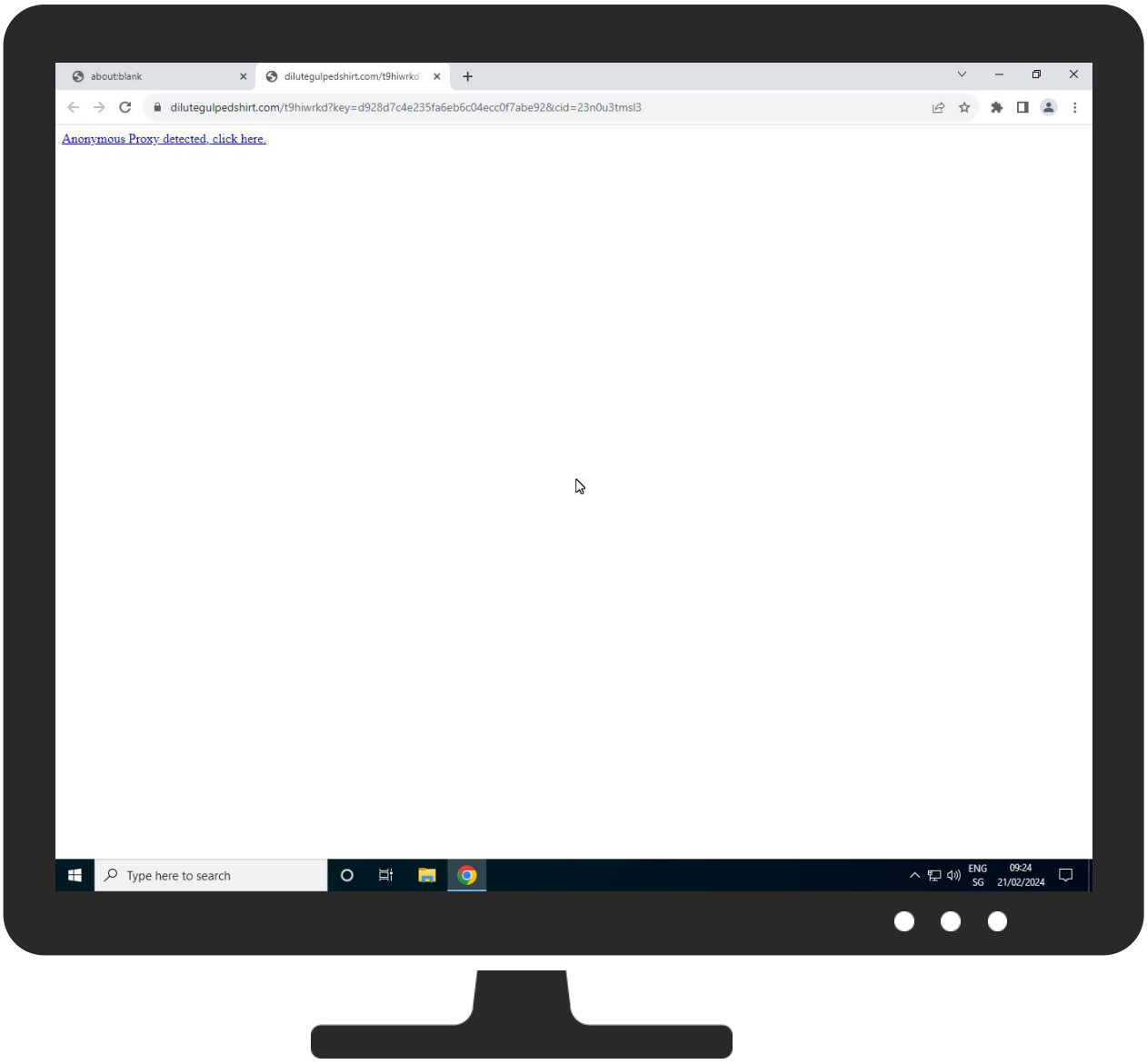


Screenshots

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://zwgaleriamlodych.pl	0%	Avira URL Cloud	safe	
http://zwgaleriamlodych.pl	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dilutegulpedshirt.com	1%	Virustotal		Browse
fp2e7a.wpc.phicdn.net	0%	Virustotal		Browse
highperformancedformats.com	7%	Virustotal		Browse
zwgaleriamlodych.pl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://zwgaleriamlodych.pl/	0%	Avira URL Cloud	safe	
http://highperformancedformats.com/anonymous/	0%	Avira URL Cloud	safe	
http://https://dilutegulpedshirt.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://zwgaleriamlodych.pl/	0%	Virustotal		Browse
http://highperformancedformats.com/anonymous/	3%	Virustotal		Browse

Domains and IPs

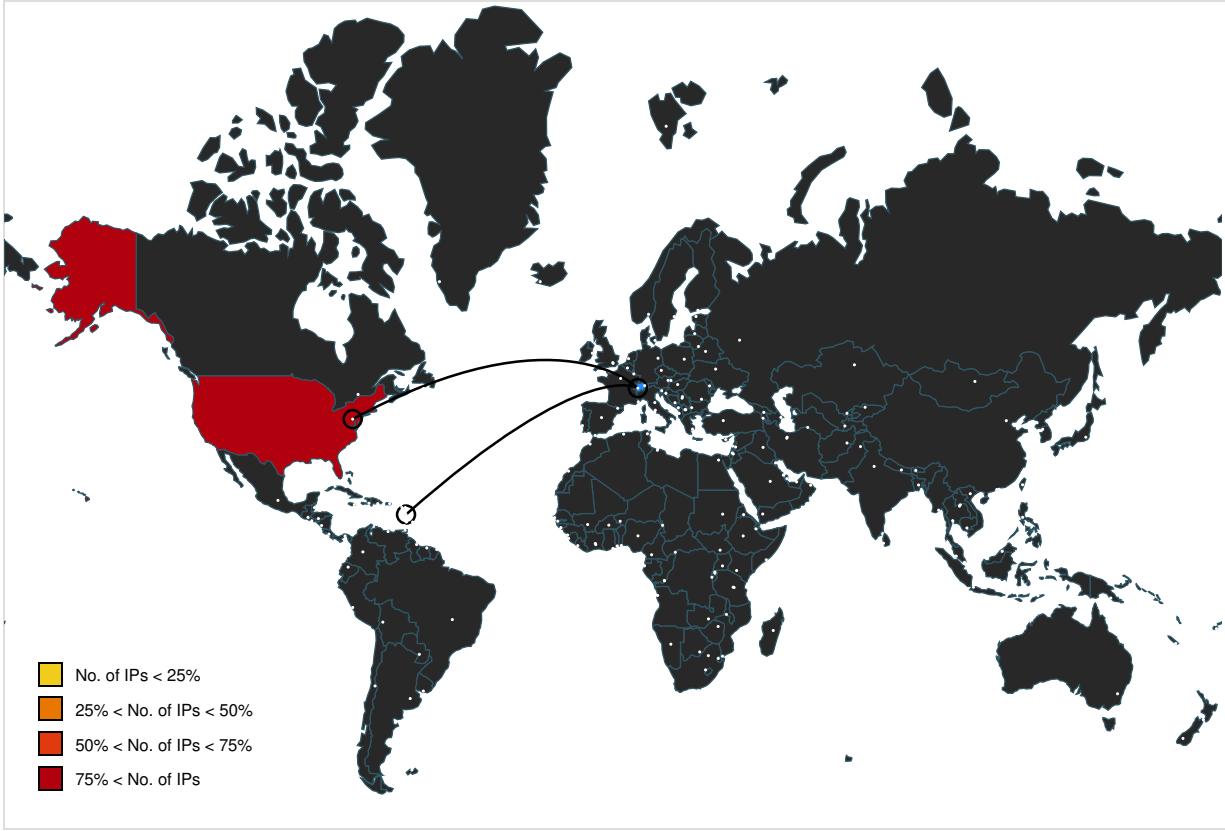
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dilutegulpedshirt.com	192.243.61.227	true	false	• 1%, Virustotal, Browse	unknown
accounts.google.com	172.253.122.84	true	false		high
highperformancedformats.com	172.240.108.76	true	false	• 7%, Virustotal, Browse	unknown
www.google.com	142.251.35.164	true	false		high
clients.l.google.com	142.250.65.174	true	false		high
zwgaleriamlodych.pl	172.67.160.242	true	false	• 0%, Virustotal, Browse	unknown
fp2e7a.wpc.phicdn.net	192.229.211.108	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://zwgaleriamlodych.pl/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	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=117.0.5938.132&lang=en-US&acceptformat=crx3,puff&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26brand%3DONGR%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://dilutegulpedshirt.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://dilutegulpedshirt.com/t9hiwrkd?key=d928d7c4e235fa6eb6c04ecc0f7abe92&cid=23n0u3tmsl3	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://highperformancedformats.com/anonymous/	false	• 3%, 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	highperformancedformats.com	United States		7979	SERVERS-COMUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.65.174	clients.l.google.com	United States		15169	GOOGLEUS	false
192.243.61.227	dilutegulpedshirt.com	Dominica		39572	ADVANCEDHOSTERS-ASNL	false
172.240.108.84	unknown	United States		7979	SERVERS-COMUS	false
104.21.9.178	unknown	United States		13335	CLOUDFLARENETUS	false
142.251.35.164	www.google.com	United States		15169	GOOGLEUS	false
172.253.122.84	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1395948
Start date and time:	2024-02-21 09:23:48 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://zwgaleriamlodych.pl
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@19/2@16/9
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): 142.250.65.195, 34.104.35.123, 13.85.23.86, 104.102.251.17, 104.102.251.57, 192.229.211.108, 52.165.164.15, 20.3.187.198, 142.251.40.227
- Excluded domains from analysis (whitelisted): fs.microsoft.com, slscr.update.microsoft.com, clientservices.googleapis.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.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, 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: 41

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

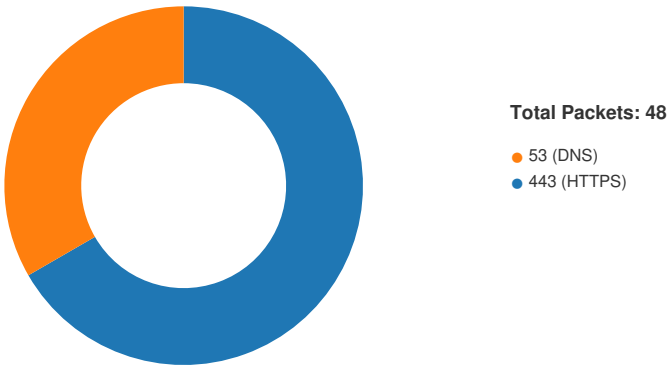
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.719823396275518
Encrypted:	false
SSDEEP:	3:uNXADiFCDRAWMO5h1KRWLRE+Vs2+ZJiNRDs7SGKy:uFAyTWLhgRW2+T+ZJas7Sdy
MD5:	16579CC322E9E105427ECFA57890EF69
SHA1:	8BB47EC30CF894AB49032D7271A45F0C778BAA05
SHA-256:	F28CE5BEFE08ED90A2E12B6B2A5E9FDAFAA6AD173503079155260AA480C66590
SHA-512:	FCF36F77D99F6594929BDED28F200BEE11FAB9B316A5E437567345B8877CFC6707BF8A116C03F07B03C0235B587E71DBD4843560564BAE07BAD2F5B6295CCE3F
Malicious:	false
Reputation:	low
URL:	http://https://dilutegulpedshirt.com/t9hiwrkd?key=d928d7c4e235fa6eb6c04ecc0f7abe92&cid=23n0u3tmsl3
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
Feb 21, 2024 09:24:36.143358946 CET	49675	443	192.168.2.4	173.222.162.32
Feb 21, 2024 09:24:42.209597111 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.209681988 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.209758043 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.210087061 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.210109949 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.210161924 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.210534096 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.210566998 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.210803032 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.210815907 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.413261890 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.414351940 CET	49731	443	192.168.2.4	142.250.65.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2024 09:24:42.414361954 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.414804935 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.414859056 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.415807962 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.415854931 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.426202059 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.426259995 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.426382065 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.426388979 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.429553032 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.430176020 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.430231094 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.431695938 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.431768894 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.436444044 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.436537027 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.440104008 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.440120935 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.485451937 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.522351980 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.613079071 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.613236904 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.613291025 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.618107080 CET	49731	443	192.168.2.4	142.250.65.174
Feb 21, 2024 09:24:42.618122101 CET	443	49731	142.250.65.174	192.168.2.4
Feb 21, 2024 09:24:42.646348000 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.646761894 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:42.646841049 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.647708893 CET	49730	443	192.168.2.4	172.253.122.84
Feb 21, 2024 09:24:42.647747993 CET	443	49730	172.253.122.84	192.168.2.4
Feb 21, 2024 09:24:43.693319082 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.693402052 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.693501949 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.693700075 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.693717957 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.897238970 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.897588015 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.897607088 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.899080992 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.899147987 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.900043964 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.900126934 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:43.900249004 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:43.900257111 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:44.049365044 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:44.303739071 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:44.304162025 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:44.304239988 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:44.308173895 CET	49734	443	192.168.2.4	104.21.9.178
Feb 21, 2024 09:24:44.308196068 CET	443	49734	104.21.9.178	192.168.2.4
Feb 21, 2024 09:24:44.399168015 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.399208069 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.399279118 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.399602890 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.399651051 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.707329035 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.707763910 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.707819939 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.709606886 CET	443	49735	192.243.61.227	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2024 09:24:44.709693909 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.710772991 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.710869074 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.710987091 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.711003065 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.766478062 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.809854031 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.810112000 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.810306072 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.811184883 CET	49735	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.811218977 CET	443	49735	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.887384892 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.887479067 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:44.887559891 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.887871981 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:44.887904882 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.181703091 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.181988955 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:45.182018995 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.182740927 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.183116913 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:45.183151007 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:45.183213949 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.235363007 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:45.277672052 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.277854919 CET	443	49738	192.243.61.227	192.168.2.4
Feb 21, 2024 09:24:45.278012991 CET	49738	443	192.168.2.4	192.243.61.227
Feb 21, 2024 09:24:45.279342890 CET	49738	443	192.168.2.4	192.243.61.227

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2024 09:24:42.117466927 CET	61942	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:42.117759943 CET	52498	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:42.118524075 CET	52973	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:42.118746042 CET	58056	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:42.188942909 CET	53	50871	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:42.205507994 CET	53	61942	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:42.206618071 CET	53	52973	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:42.206737041 CET	53	52498	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:42.206865072 CET	53	58056	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:42.752068043 CET	53	59546	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:43.500464916 CET	57342	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:43.500746965 CET	56957	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:43.590240955 CET	53	57342	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:43.590987921 CET	53	56957	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:43.592792034 CET	51596	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:43.593051910 CET	64358	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:43.681495905 CET	53	51596	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:43.692238092 CET	53	64358	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:44.309912920 CET	54590	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:44.310506105 CET	59526	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:44.398276091 CET	53	54590	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:44.398387909 CET	53	59526	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:45.283561945 CET	60947	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:45.283848047 CET	64092	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:45.372205973 CET	53	60947	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:45.494402885 CET	56800	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:45.495861053 CET	52675	53	192.168.2.4	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2024 09:24:45.582165003 CET	53	56800	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:45.584068060 CET	53	52675	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:45.631890059 CET	53	64092	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:56.515297890 CET	51785	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:56.518250942 CET	65311	53	192.168.2.4	1.1.1.1
Feb 21, 2024 09:24:56.864346027 CET	53	51785	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:56.866496086 CET	53	65311	1.1.1.1	192.168.2.4
Feb 21, 2024 09:24:59.809118032 CET	53	49436	1.1.1.1	192.168.2.4
Feb 21, 2024 09:25:01.943603039 CET	138	138	192.168.2.4	192.168.2.255
Feb 21, 2024 09:25:18.606254101 CET	53	51486	1.1.1.1	192.168.2.4
Feb 21, 2024 09:25:41.358896971 CET	53	50571	1.1.1.1	192.168.2.4
Feb 21, 2024 09:25:41.386491060 CET	53	52421	1.1.1.1	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 21, 2024 09:24:45.631989002 CET	192.168.2.4	1.1.1.1	c22f	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 21, 2024 09:24:42.117466927 CET	192.168.2.4	1.1.1.1	0xb600	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:42.117759943 CET	192.168.2.4	1.1.1.1	0x7397	Standard query (0)	clients2.google.com	65	IN (0x0001)	false
Feb 21, 2024 09:24:42.118524075 CET	192.168.2.4	1.1.1.1	0x7d25	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:42.118746042 CET	192.168.2.4	1.1.1.1	0x3e5e	Standard query (0)	accounts.google.com	65	IN (0x0001)	false
Feb 21, 2024 09:24:43.500464916 CET	192.168.2.4	1.1.1.1	0xcf7a	Standard query (0)	zwgaleriamlodych.pl	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.500746965 CET	192.168.2.4	1.1.1.1	0x91de	Standard query (0)	zwgaleriamlodych.pl	65	IN (0x0001)	false
Feb 21, 2024 09:24:43.592792034 CET	192.168.2.4	1.1.1.1	0xed88	Standard query (0)	zwgaleriamlodych.pl	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.593051910 CET	192.168.2.4	1.1.1.1	0x9b2b	Standard query (0)	zwgaleriamlodych.pl	65	IN (0x0001)	false
Feb 21, 2024 09:24:44.309912920 CET	192.168.2.4	1.1.1.1	0x91f0	Standard query (0)	dilutegulpedshirt.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.310506105 CET	192.168.2.4	1.1.1.1	0x5c0e	Standard query (0)	dilutegulpedshirt.com	65	IN (0x0001)	false
Feb 21, 2024 09:24:45.283561945 CET	192.168.2.4	1.1.1.1	0x4be0	Standard query (0)	dilutegulpedshirt.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.283848047 CET	192.168.2.4	1.1.1.1	0xe477	Standard query (0)	dilutegulpedshirt.com	65	IN (0x0001)	false
Feb 21, 2024 09:24:45.494402885 CET	192.168.2.4	1.1.1.1	0x352b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.495861053 CET	192.168.2.4	1.1.1.1	0x40ee	Standard query (0)	www.google.com	65	IN (0x0001)	false
Feb 21, 2024 09:24:56.515297890 CET	192.168.2.4	1.1.1.1	0x6d47	Standard query (0)	highperformancedformats.com	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.518250942 CET	192.168.2.4	1.1.1.1	0x9b8e	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
Feb 21, 2024 09:24:42.205507994 CET	1.1.1.1	192.168.2.4	0xb600	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:24:42.205507994 CET	1.1.1.1	192.168.2.4	0xb600	No error (0)	clients.l.google.com		142.250.65.174	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 21, 2024 09:24:42.206618071 CET	1.1.1.1	192.168.2.4	0x7d25	No error (0)	accounts.google.com		172.253.122.84	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:42.206737041 CET	1.1.1.1	192.168.2.4	0x7397	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:24:43.590240955 CET	1.1.1.1	192.168.2.4	0xcf7a	No error (0)	zwgaleriamlodych.pl		172.67.160.242	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.590240955 CET	1.1.1.1	192.168.2.4	0xcf7a	No error (0)	zwgaleriamlodych.pl		104.21.9.178	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.590987921 CET	1.1.1.1	192.168.2.4	0x91de	No error (0)	zwgaleriamlodych.pl			65	IN (0x0001)	false
Feb 21, 2024 09:24:43.681495905 CET	1.1.1.1	192.168.2.4	0xed88	No error (0)	zwgaleriamlodych.pl		104.21.9.178	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.681495905 CET	1.1.1.1	192.168.2.4	0xed88	No error (0)	zwgaleriamlodych.pl		172.67.160.242	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:43.692238092 CET	1.1.1.1	192.168.2.4	0x9b2b	No error (0)	zwgaleriamlodych.pl			65	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		192.243.59.20	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		172.240.253.132	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		192.243.59.12	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		172.240.108.92	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:44.398276091 CET	1.1.1.1	192.168.2.4	0x91f0	No error (0)	dilutegulpedshirt.com		172.240.108.68	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		172.240.108.68	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		192.243.59.20	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		172.240.253.132	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		172.240.108.92	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.372205973 CET	1.1.1.1	192.168.2.4	0x4be0	No error (0)	dilutegulpedshirt.com		192.243.59.12	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.582165003 CET	1.1.1.1	192.168.2.4	0x352b	No error (0)	www.google.com		142.251.35.164	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:45.584068060 CET	1.1.1.1	192.168.2.4	0x40ee	No error (0)	www.google.com			65	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		172.240.108.76	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		192.243.61.227	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		192.243.59.13	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		172.240.108.84	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		172.240.108.92	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		172.240.253.132	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:24:56.864346027 CET	1.1.1.1	192.168.2.4	0x6d47	No error (0)	highperformancedformats.com		192.243.61.225	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:25:00.207549095 CET	1.1.1.1	192.168.2.4	0x62ee	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:25:00.207549095 CET	1.1.1.1	192.168.2.4	0x62ee	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:25:14.933439016 CET	1.1.1.1	192.168.2.4	0xea2e	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:25:14.933439016 CET	1.1.1.1	192.168.2.4	0xea2e	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:25:33.668837070 CET	1.1.1.1	192.168.2.4	0xeb0a	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:25:33.668837070 CET	1.1.1.1	192.168.2.4	0xeb0a	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 21, 2024 09:25:54.199307919 CET	1.1.1.1	192.168.2.4	0x2482	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 21, 2024 09:25:54.199307919 CET	1.1.1.1	192.168.2.4	0x2482	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- zwgaleriamlodych.pl
- dilutegulpedshirt.com
- https:
- fs.microsoft.com
- highperformancedformats.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: **3320**, Parent PID: **1908**

General

Target ID:	0
Start time:	09:24:38
Start date:	21/02/2024
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: **5228**, Parent PID: **3320**

General	
Target ID:	1
Start time:	09:24:40
Start date:	21/02/2024
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=2384 --field-trial-handle=2308,i,2546780249924042766,14441408258148433188,262144 --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: **6508**, Parent PID: **1908**

General	
Target ID:	3
Start time:	09:24:42
Start date:	21/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://zwgaleriamlodych.pl
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