ID: 876174
Cookbook: browseurl.jbs
Time: 12:27:15
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

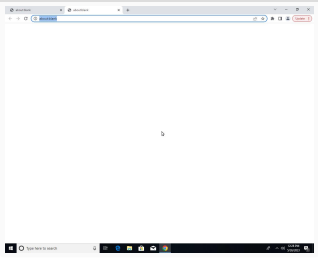
Windows Analysis Report

https://wpt158.blob.core.windows.net/wpt158/index.html

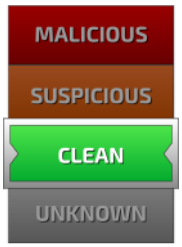
Overview

General Information

Sample URL:	http://https://wpt158.blob.core.windows.net/wpt158/index.html
Analysis ID:	876174
Infos:	



Detection

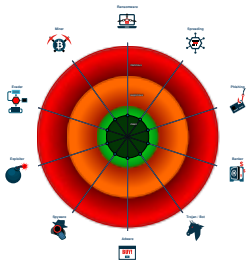


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 3460 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6016 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=1948 --field-trial-handle=1728,i,5077115762642821101,12055652744373229981,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6488 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://wpt158.blob.core.windows.net/wpt158/index.html 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

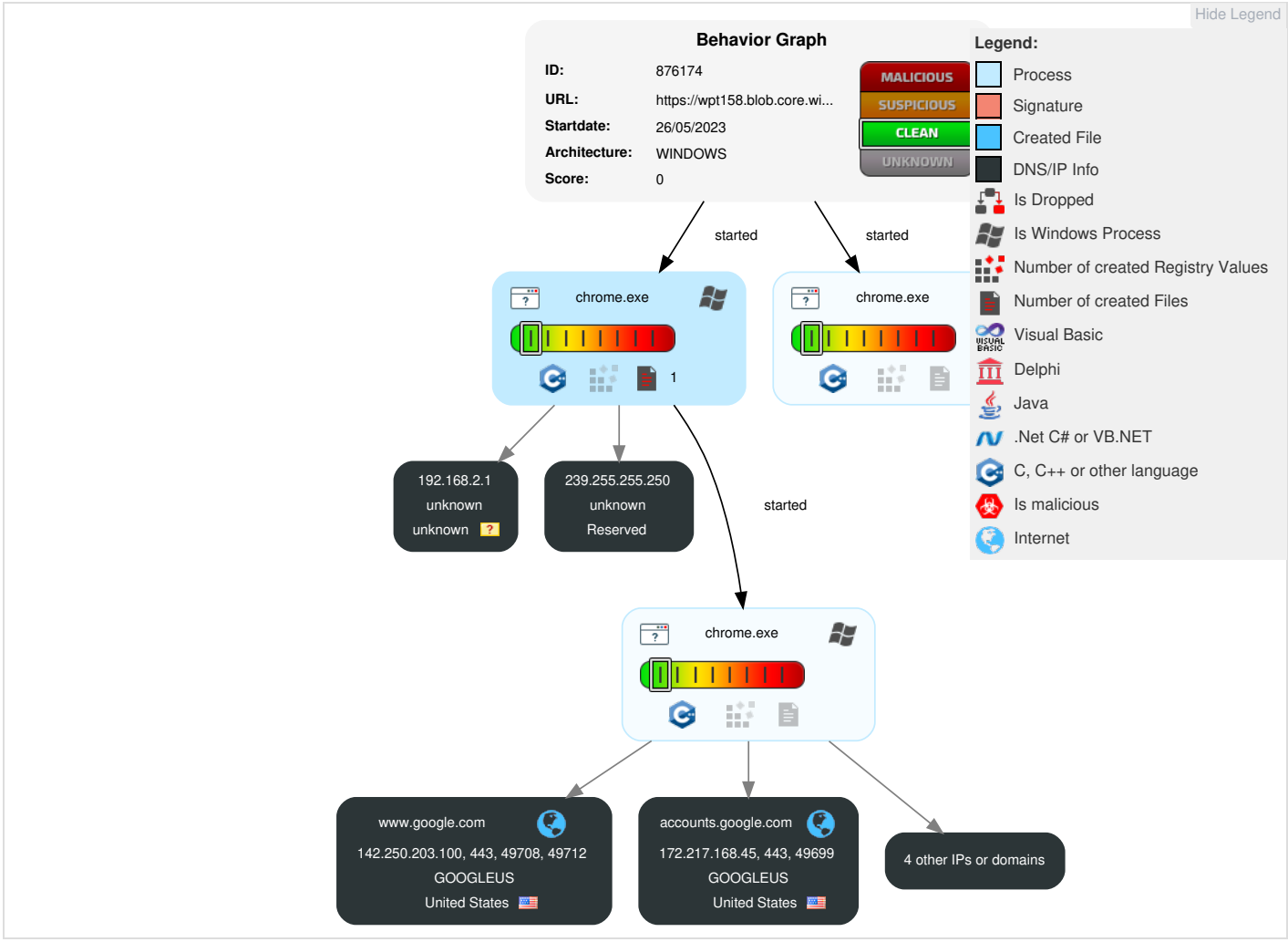
Joe Sandbox Signatures

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

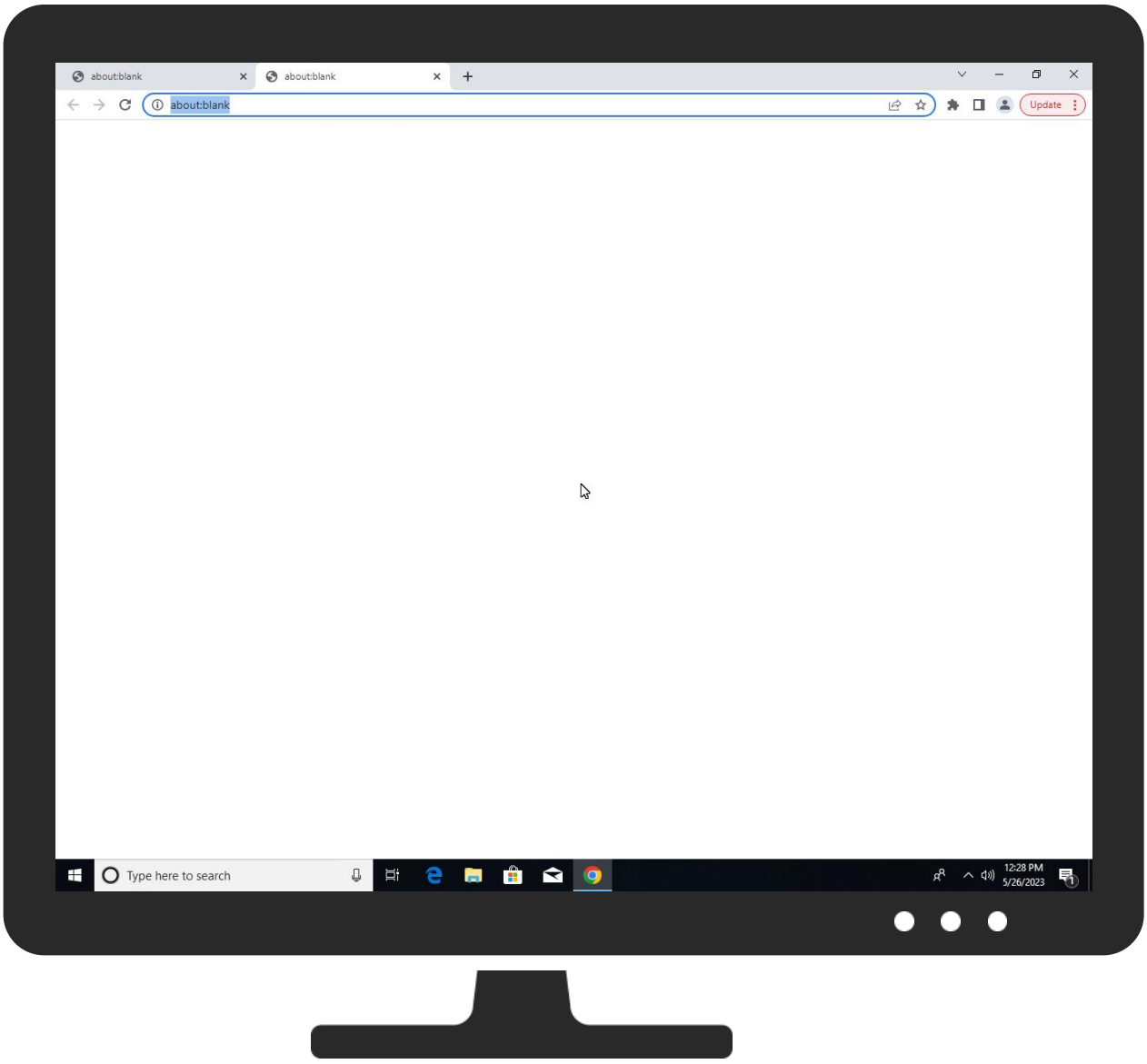
Behavior Graph



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://wpt158.blob.core.windows.net/wpt158/index.html	0%	Avira URL Cloud	safe	
http://https://wpt158.blob.core.windows.net/wpt158/index.html	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.carlitxs.com/	0%	Virustotal		Browse
http://https://www.carlitxs.com/	0%	Avira URL Cloud	safe	

Domains and IPs

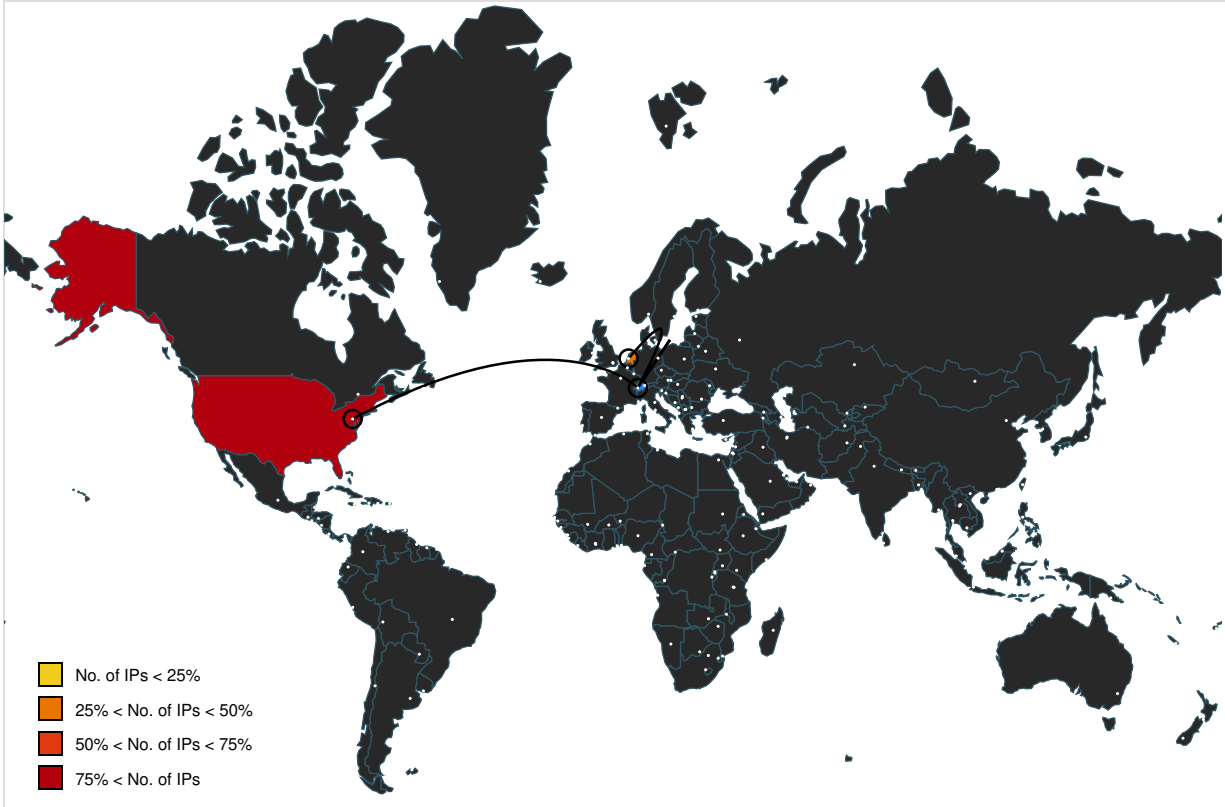
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
carlitxs.com	46.101.19.251	true	false		unknown
clients2.google.com	unknown	unknown	false		high
www.carlitxs.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
about:blank	false		low
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
http://https://www.carlitxs.com/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.101.19.251	carlitxs.com	Netherlands		14061	DIGITALOCEAN-ASNUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876174
Start date and time:	2023-05-26 12:27:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://wpt158.blob.core.windows.net/wpt158/index.html
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:	6
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@25/3@5/6
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, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.3, 34.104.35.123, 20.60.134.228
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, wpt158.blob.core.windows.net, update.googleapis.com, clientservices.googleapis.com, blob.blz23prdstr07a.store.core.windows.net
- Not all processes where analyzed, report is missing behavior information

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: 101

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	128
Entropy (8bit):	4.809876661048398
Encrypted:	false
SSDEEP:	3:qVZxZcMBqRJzYoHjJMzVJu+1zWNVYrSLbJSWacz:qzxiMMbFMRJVCNOGLUWXz
MD5:	CD0B11979210ED73ADCBE39212BC178B
SHA1:	45218289935ED7A3B9AB8FD4AD6B53913DB63CC3
SHA-256:	76FF817D7AB17AE6D2DEBB889014EB4BC5A00B1B6E1AA15B09277A8503EF98EB
SHA-512:	0FFD8D3629EBE0599AA2CD9152B4F9C8C439EF97D857DC9CACEEFA82023FF0A4713F4BDB240661A59A62119075650B85EF43E561354CCA9B16B24229AE9A48F
Malicious:	false
Reputation:	low
URL:	http://https://wpt158.blob.core.windows.net/wpt158/index.html
Preview:	<html><head>..<body>..<title></title>.....<meta http-equiv="refresh" content="0; url=https://www.carlitxs.com/">..</body></html>

Chrome Cache Entry: 102

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	5.2946249235302565
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8DHgWdzRiAU2uvxV1GIKEn/vSHpg6n:MMHdVBMHgWdzR05Gq/vT6
MD5:	969650F1C6303FEBF6C72E74B692B21D
SHA1:	0E40B5B81E18A7E58371C0202BF508EC76BC7207
SHA-256:	DBC9706456080F39816AC60124009A922E86097312545AAB3D789174693DB7B1
SHA-512:	F529AEC3E2E8DD2CF0106157FBB3C39A3E49257A0775289196485FE15CD68CCE9DCA80130A422282C65F8F217A251382B25680151EA0105A5844AC0DA68310E1
Malicious:	false
Reputation:	low
URL:	http://https://wpt158.blob.core.windows.net/favicon.ico
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>OutOfRangeInput</Code><Message>One of the request inputs is out of range..RequestId:8ad21688-601e-0069-4bbc-8fbe52000000.Time:2023-05-26T10:28:14.3042345Z</Message></Error>

Chrome Cache Entry: 103

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with no line terminators

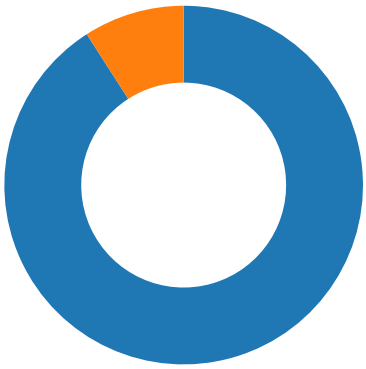
Category:	downloaded
Size (bytes):	45
Entropy (8bit):	4.430198929422622
Encrypted:	false
SSDEEP:	3:gcG4xADYFHmGUc7b:BmY9mGUYb
MD5:	639BCD7E70744BE36DB2FC48B3198536
SHA1:	FF4DC3C0BE977DE2C57722BA6E8B224AE5E1EC83
SHA-256:	EEA5E2565A62F39438758FB95DAF0342C83D4ADE8D9822BBF14CAA3F0A3847C3
SHA-512:	B4125FCE20C6FD3C5A467318F8CE43EA5A1DBDECBA57C2C8A8C6213A644A19F19FCBB087B94C0E7762BFE03029F83B03530BE736817DD718E3C3411CB2B8AF8
Malicious:	false
Reputation:	low
URL:	http://https://www.carlitxs.com/
Preview:	<script>location.href='about:blank';</script>

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:11.238286018 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.238343000 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.238416910 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.241079092 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.241112947 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.241499901 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.241548061 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.241628885 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.242100954 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.242131948 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.397882938 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.398283005 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.398350000 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.400490999 CEST	443	49699	172.217.168.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:11.400597095 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.403628111 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.447392941 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.456768990 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.456801891 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.458189964 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.458296061 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.461709976 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.461780071 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.883532047 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.883666039 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.883694887 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.883949995 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.884021044 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.884040117 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.884047031 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.884584904 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.918951035 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.919060946 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.919097900 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.919285059 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.919377089 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.920006990 CEST	49700	443	192.168.2.3	216.58.215.238
May 26, 2023 12:28:11.920039892 CEST	443	49700	216.58.215.238	192.168.2.3
May 26, 2023 12:28:11.934055090 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.934086084 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.967921972 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.968091011 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.968132973 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.968636990 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:11.968708038 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.994081020 CEST	49699	443	192.168.2.3	172.217.168.45
May 26, 2023 12:28:11.994128942 CEST	443	49699	172.217.168.45	192.168.2.3
May 26, 2023 12:28:14.267467022 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.267530918 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.267654896 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.268166065 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.268208981 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.268331051 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.268563986 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.268596888 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.268817902 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.268857956 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.370851994 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.371216059 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.371263027 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.373208046 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.373313904 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.373462915 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.373994112 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.374017954 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.375123024 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.375332117 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.375334978 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.375345945 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.375418901 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.377038956 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.377146959 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.420322895 CEST	443	49705	46.101.19.251	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:14.436851978 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.436970949 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.441572905 CEST	49705	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.441613913 CEST	443	49705	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.501338005 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.501374960 CEST	443	49706	46.101.19.251	192.168.2.3
May 26, 2023 12:28:14.713824987 CEST	49706	443	192.168.2.3	46.101.19.251
May 26, 2023 12:28:14.984357119 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:14.984430075 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:14.984560013 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:14.984882116 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:14.984920979 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.047081947 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.047827005 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:15.047869921 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.049563885 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.049695969 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:15.051877975 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:15.051994085 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.205454111 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:15.205496073 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:15.401650906 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:25.019165993 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:25.019299030 CEST	443	49708	142.250.203.100	192.168.2.3
May 26, 2023 12:28:25.019423962 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:26.315933943 CEST	49708	443	192.168.2.3	142.250.203.100
May 26, 2023 12:28:26.315987110 CEST	443	49708	142.250.203.100	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:11.210906029 CEST	56924	53	192.168.2.3	8.8.8.8
May 26, 2023 12:28:11.211236000 CEST	60625	53	192.168.2.3	8.8.8.8
May 26, 2023 12:28:11.234277964 CEST	53	56924	8.8.8.8	192.168.2.3
May 26, 2023 12:28:11.239659071 CEST	53	60625	8.8.8.8	192.168.2.3
May 26, 2023 12:28:14.234060049 CEST	57134	53	192.168.2.3	8.8.8.8
May 26, 2023 12:28:14.263858080 CEST	53	57134	8.8.8.8	192.168.2.3
May 26, 2023 12:28:14.966435909 CEST	56042	53	192.168.2.3	8.8.8.8
May 26, 2023 12:28:14.981125116 CEST	53	56042	8.8.8.8	192.168.2.3
May 26, 2023 12:29:15.026367903 CEST	58119	53	192.168.2.3	8.8.8.8
May 26, 2023 12:29:15.049537897 CEST	53	58119	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 12:28:11.210906029 CEST	192.168.2.3	8.8.8.8	0x95ec	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:11.211236000 CEST	192.168.2.3	8.8.8.8	0x52e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:14.234060049 CEST	192.168.2.3	8.8.8.8	0x87d9	Standard query (0)	www.carlitxs.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:14.966435909 CEST	192.168.2.3	8.8.8.8	0xe764	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 12:29:15.026367903 CEST	192.168.2.3	8.8.8.8	0x49d1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

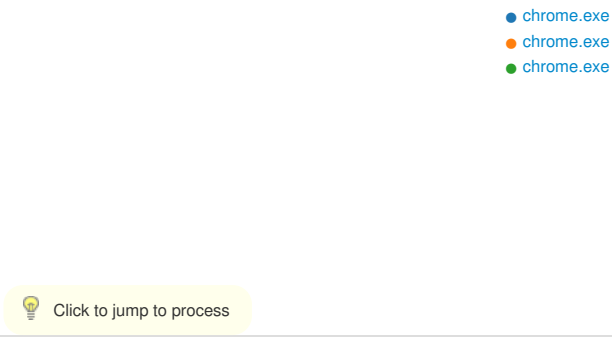
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 12:28:11.234277964 CEST	8.8.8.8	192.168.2.3	0x95ec	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:11.239659071 CEST	8.8.8.8	192.168.2.3	0x52e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 12:28:11.239659071 CEST	8.8.8.8	192.168.2.3	0x52e	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:14.263858080 CEST	8.8.8.8	192.168.2.3	0x87d9	No error (0)	www.carlitxs.com	carlitxs.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 12:28:14.263858080 CEST	8.8.8.8	192.168.2.3	0x87d9	No error (0)	carlitxs.com		46.101.19.251	A (IP address)	IN (0x0001)	false
May 26, 2023 12:28:14.981125116 CEST	8.8.8.8	192.168.2.3	0xe764	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 12:29:15.049537897 CEST	8.8.8.8	192.168.2.3	0x49d1	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- https:
  - www.carlitxs.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **3460**, Parent PID: **5308**

General

Target ID:	0

Start time:	12:28:08
Start date:	26/05/2023
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:	0x7ff614650000
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

Analysis Process: chrome.exe PID: **6016**, Parent PID: **3460**

General

Target ID:	1
Start time:	12:28:09
Start date:	26/05/2023
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=1948 --field-trial-handle=1728,i,5077115762642821101,12055652744373229981,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **6488**, Parent PID: **5308**

General

Target ID:	2
Start time:	12:28:12
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://wpt158.blob.core.windows.net/wpt158/index.html
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly