ID: 756102
Cookbook: browseurl.jbs
Time: 16:35:45
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

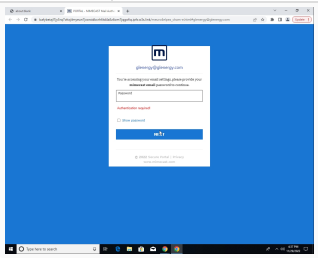
Windows Analysis Report

https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_ch...

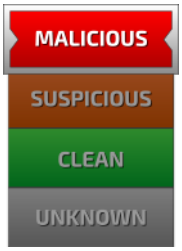
Overview

General Information

Sample URL:	http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com
Analysis ID:	756102
Infos:	



Detection

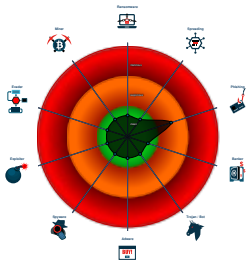


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- URL contains potential PII (phishing…
- HTML body contains low number of …
- Invalid T&C link found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6012 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3536 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=1808 --field-trial-handle=1780,i,4275831116974464191,11394012430591457211,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5524 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

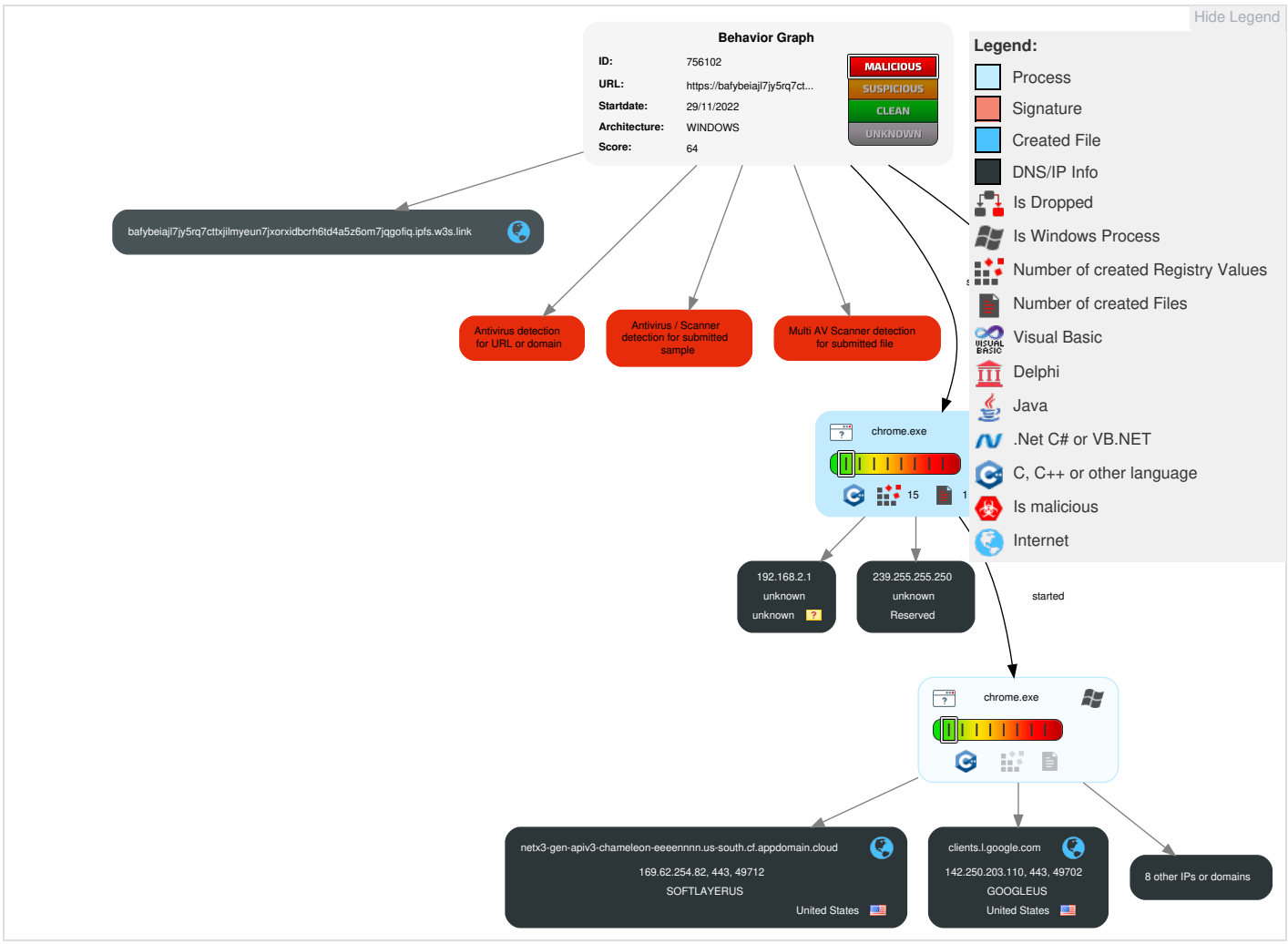
Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

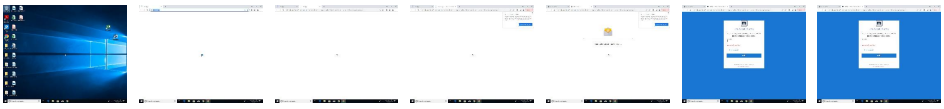
Behavior Graph

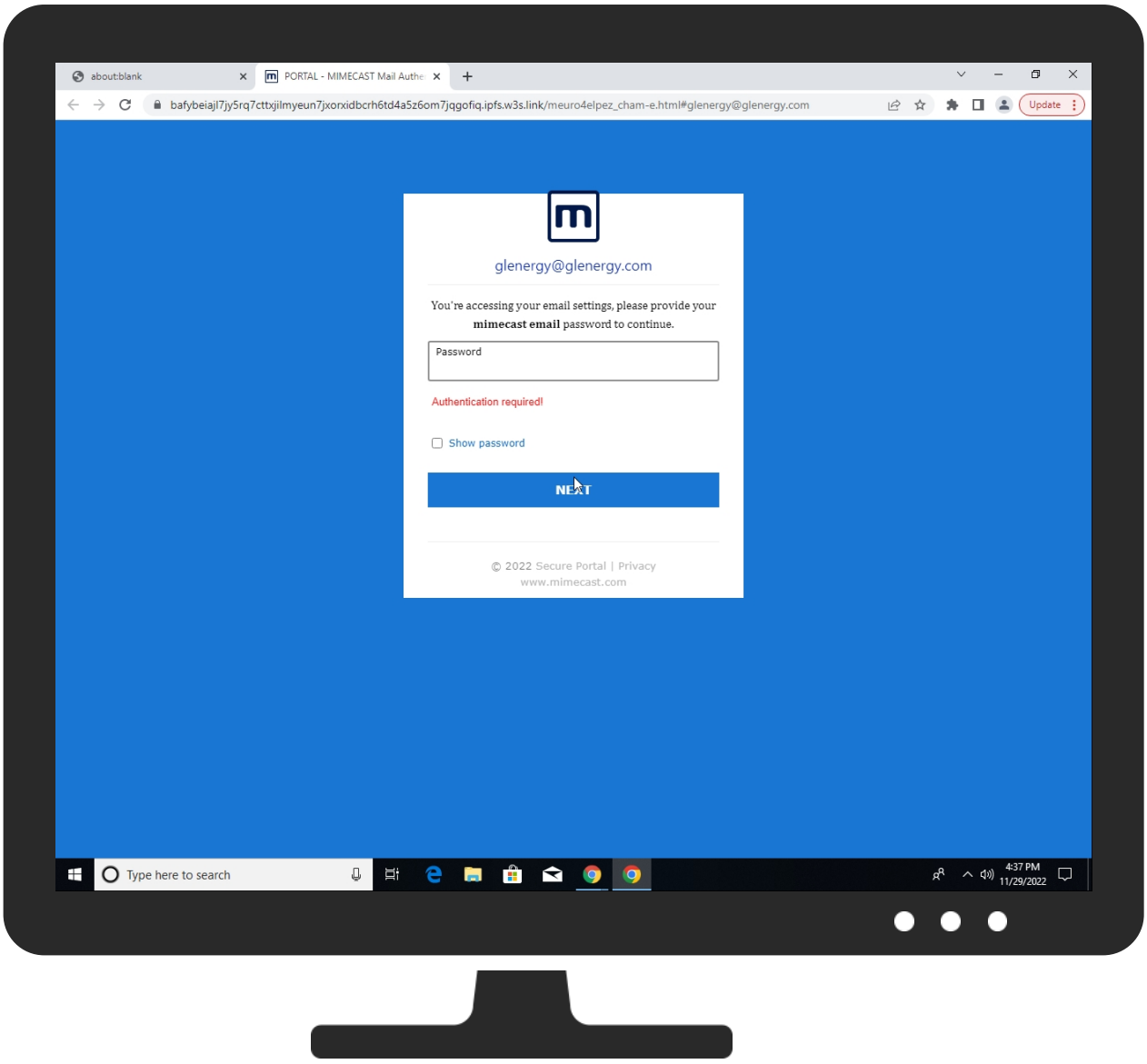


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http:// https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com	13%	Virustotal		Browse
http:// https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http:// https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html	100%	Avira URL Cloud	phishing	
http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/images/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud/?getemailinfo=glenergy@glenergy.com&linkbox=meuro4elpez&url=https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html	0%	Avira URL Cloud	safe	

Domains and IPs

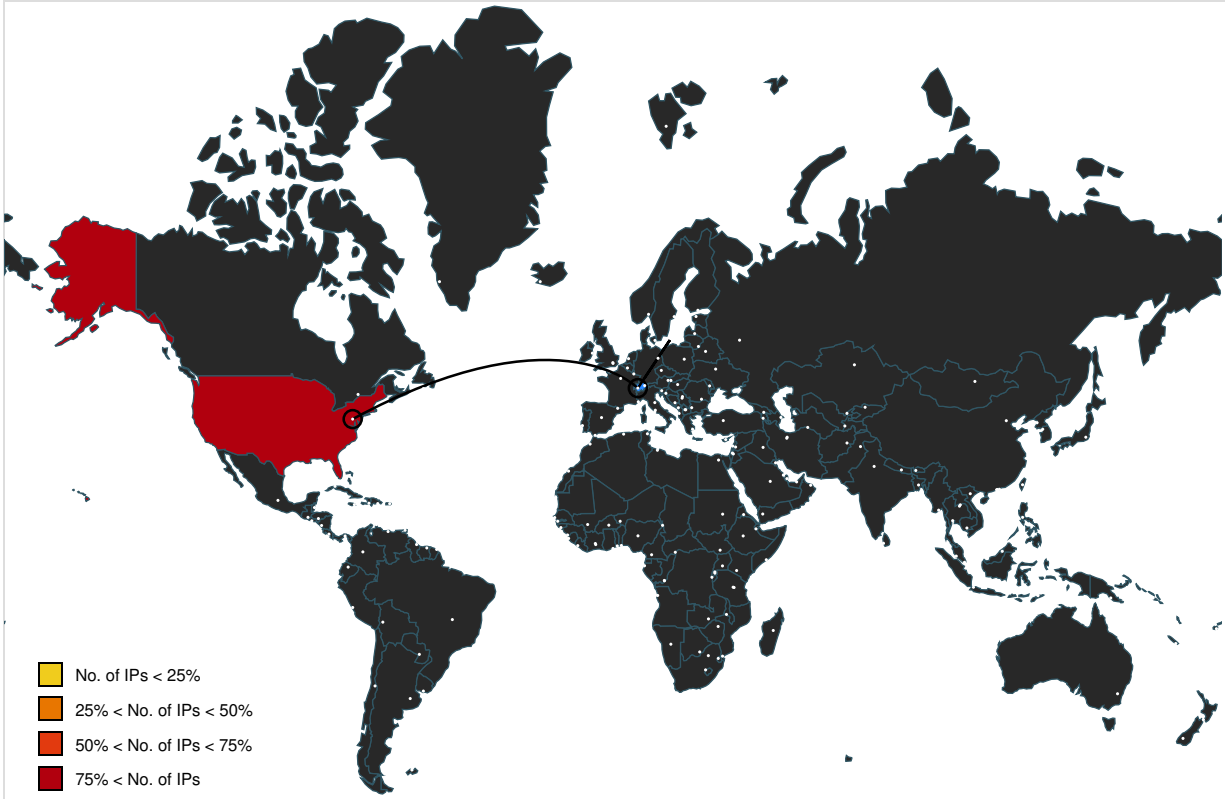
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
cs837.wac.edgecastcdn.net	192.229.133.221	true	false		high
www.google.com	172.217.168.36	true	false		high
netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud	169.62.254.82	true	false		unknown
bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link	104.18.22.52	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
www.w3schools.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html	false	• Avira URL Cloud: phishing	unknown
http://https://netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud/?getemailinfo=glenergy@glenergy.com&linkbox=meuro4elpez&url=https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html	false	• 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=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://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/images/favicon.ico	false	• Avira URL Cloud: phishing	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://www.w3schools.com/w3css/4/w3.css	false		high
http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
169.62.254.82	netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud	United States		36351	SOFTLAYERUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
192.229.133.221	cs837.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.22.52	bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756102
Start date and time:	2022-11-29 16:35:45 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_chame.html#glenergy@glenergy.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.win@25/0@8/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 172.217.168.42, 172.217.168.74, 142.250.203.106, 216.58.215.234, 172.217.168.10, 142.250.203.100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, t3.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

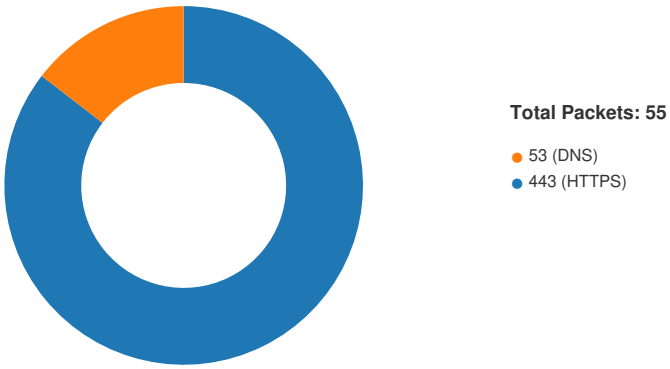
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:36:52.192600012 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.192656040 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.192776918 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.194288015 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.194344044 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.194437027 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.196091890 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.196149111 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.196240902 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.201035976 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.201085091 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.201178074 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.202960968 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.202987909 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.204045057 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.204076052 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.204351902 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.204386950 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.204926968 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.204958916 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.208432913 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.208477020 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.208551884 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.209290028 CET	49708	443	192.168.2.5	104.18.22.52

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:36:52.209307909 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.321921110 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.325030088 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.325063944 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.326003075 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.326103926 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.327344894 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.327424049 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.384345055 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.386132002 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.394582987 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.394614935 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.394946098 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.394985914 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.397383928 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.397505999 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.397625923 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.397706985 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.417339087 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.417450905 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.418498993 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.418534040 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.418817043 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.418845892 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.420460939 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.420552969 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.420677900 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.420768023 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.919751883 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:52.919816017 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.919995070 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:52.920667887 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.920722961 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.920762062 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.920792103 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.920878887 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.920979977 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.921164989 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.921190023 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.921345949 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.921514988 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.921545029 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.921663046 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.921690941 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.921727896 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.921926022 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:52.921950102 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:52.921996117 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.922015905 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:52.977283955 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.977473021 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.977760077 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.983900070 CET	49704	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.983939886 CET	443	49704	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.990854025 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:52.990871906 CET	443	49705	172.217.168.45	192.168.2.5
Nov 29, 2022 16:36:52.990888119 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:52.990914106 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:53.023339987 CET	443	49702	142.250.203.110	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:36:53.023557901 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:53.023638964 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:53.023931026 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:53.023940086 CET	443	49706	172.217.168.36	192.168.2.5
Nov 29, 2022 16:36:53.036806107 CET	49702	443	192.168.2.5	142.250.203.110
Nov 29, 2022 16:36:53.036827087 CET	443	49702	142.250.203.110	192.168.2.5
Nov 29, 2022 16:36:53.090918064 CET	49705	443	192.168.2.5	172.217.168.45
Nov 29, 2022 16:36:53.125768900 CET	49706	443	192.168.2.5	172.217.168.36
Nov 29, 2022 16:36:53.285386086 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285465002 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285511017 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285554886 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285552025 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:53.285593987 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285614014 CET	49708	443	192.168.2.5	104.18.22.52
Nov 29, 2022 16:36:53.285649061 CET	443	49708	104.18.22.52	192.168.2.5
Nov 29, 2022 16:36:53.285681963 CET	49708	443	192.168.2.5	104.18.22.52

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:36:52.025835991 CET	49724	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:52.029284000 CET	61452	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:52.030622959 CET	65323	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:52.032983065 CET	51484	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:52.048765898 CET	53	61452	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:52.049890041 CET	53	65323	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:52.053812981 CET	53	49724	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:52.055362940 CET	53	51484	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:53.394701004 CET	60975	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:53.410052061 CET	59220	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:53.416220903 CET	53	60975	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:53.431782007 CET	53	59220	8.8.8.8	192.168.2.5
Nov 29, 2022 16:36:53.944679022 CET	55068	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:36:53.975847006 CET	53	55068	8.8.8.8	192.168.2.5
Nov 29, 2022 16:37:04.987277985 CET	65513	53	192.168.2.5	8.8.8.8
Nov 29, 2022 16:37:05.012047052 CET	53	65513	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:36:52.025835991 CET	192.168.2.5	8.8.8.8	0x1d4e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.029284000 CET	192.168.2.5	8.8.8.8	0x79e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.030622959 CET	192.168.2.5	8.8.8.8	0xd880	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.032983065 CET	192.168.2.5	8.8.8.8	0x106c	Standard query (0)	bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.394701004 CET	192.168.2.5	8.8.8.8	0x6c54	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.410052061 CET	192.168.2.5	8.8.8.8	0xc65b	Standard query (0)	www.w3schools.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.944679022 CET	192.168.2.5	8.8.8.8	0xc9e9	Standard query (0)	netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:37:04.987277985 CET	192.168.2.5	8.8.8.8	0xad5c	Standard query (0)	bafybeiajl 7jy5rq7ctt xjilmyeun7 jxorxidbcr h6td4a5z6o m7jqgofiq. ipfs.w3s.link	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
Nov 29, 2022 16:36:52.048765898 CET	8.8.8.8	192.168.2.5	0x79e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:36:52.048765898 CET	8.8.8.8	192.168.2.5	0x79e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.049890041 CET	8.8.8.8	192.168.2.5	0xd880	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.053812981 CET	8.8.8.8	192.168.2.5	0x1d4e	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.055362940 CET	8.8.8.8	192.168.2.5	0x106c	No error (0)	bafybeiajl 7jy5rq7ctt xjilmyeun7 jxorxidbcr h6td4a5z6o m7jqgofiq. ipfs.w3s.link		104.18.22.52	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:52.055362940 CET	8.8.8.8	192.168.2.5	0x106c	No error (0)	bafybeiajl 7jy5rq7ctt xjilmyeun7 jxorxidbcr h6td4a5z6o m7jqgofiq. ipfs.w3s.link		104.18.23.52	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.416220903 CET	8.8.8.8	192.168.2.5	0x6c54	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.416220903 CET	8.8.8.8	192.168.2.5	0x6c54	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.431782007 CET	8.8.8.8	192.168.2.5	0xc65b	No error (0)	www.w3schools.com	cs837.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:36:53.431782007 CET	8.8.8.8	192.168.2.5	0xc65b	No error (0)	cs837.wac.edgecastcdn.net		192.229.133.221	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.975847006 CET	8.8.8.8	192.168.2.5	0xc9e9	No error (0)	netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud		169.62.254.82	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.975847006 CET	8.8.8.8	192.168.2.5	0xc9e9	No error (0)	netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud		169.46.89.154	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:53.975847006 CET	8.8.8.8	192.168.2.5	0xc9e9	No error (0)	netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud		169.47.124.25	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:05.012047052 CET	8.8.8.8	192.168.2.5	0xad5c	No error (0)	bafybeiajl 7jy5rq7ctt xjilmyeun7 jxorxidbcr h6td4a5z6o m7jqgofiq. ipfs.w3s.link		104.18.22.52	A (IP address)	IN (0x0001)	false

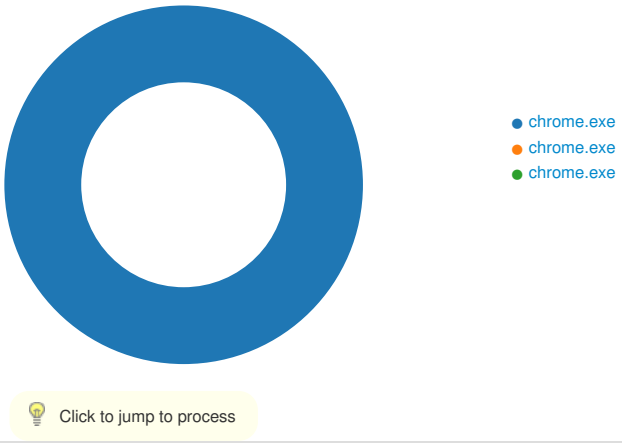
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:37:05.012047052 CET	8.8.8.8	192.168.2.5	0xad5c	No error (0)	bafybeiajl 7jy5rq7ctt xjilmyeun7 jxorxidbcr h6td4a5z6o m7jqgofiq. ipfs.w3s.link		104.18.23.52	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link
- clients2.google.com
- https:
  - www.w3schools.com
  - cdnjs.cloudflare.com
  - netx3-gen-apiv3-chameleon-eeeennnn.us-south.cf.appdomain.cloud

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6012**, Parent PID: **4520**

General

Target ID:	0
Start time:	16:36:44
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes

MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **3536**, Parent PID: **6012**

General

Target ID:	1
Start time:	16:36:46
Start date:	29/11/2022
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=1808 --field-trial-handle=1780,i,4275831116974464191,11394012430591457211,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5524**, Parent PID: **4520**

General

Target ID:	2
Start time:	16:36:47
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://bafybeiajl7jy5rq7cttxjilmyeun7jxorxidbcrh6td4a5z6om7jqgofiq.ipfs.w3s.link/meuro4elpez_cham-e.html#glenergy@glenergy.com
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes

MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly