



ID: 756228
Cookbook: browseurl.jbs
Time: 20:58:49
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
HTML 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Phishing 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 8
Private 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
UDP Packets 12
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 13
Statistics 13
Behavior 13
System Behavior 14
Analysis Process: chrome.exePID: 4856, Parent PID: 1796 14
General 14
File Activities 14
Registry Activities 14
Analysis Process: chrome.exePID: 5784, Parent PID: 4856 14
General 14
File Activities 15
Analysis Process: chrome.exePID: 4440, Parent PID: 1796 15
General 15
Registry Activities 15
Disassembly 15

Copyright Joe Security LLC 2022

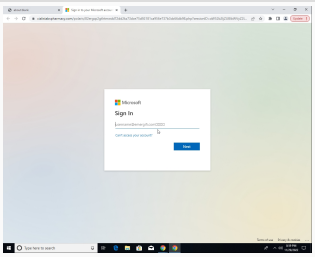
Windows Analysis Report

https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg

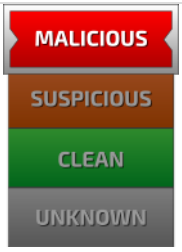
Overview

General Information

Sample URL:	http://https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg
Analysis ID:	756228
Infos:	



Detection



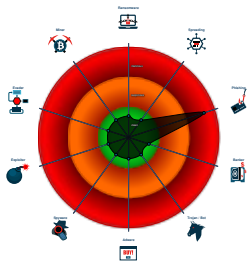
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4856 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5784 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1876 --field-trial-handle=1828,i,2187161938276056667,2480233056043708616,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4440 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
22653.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

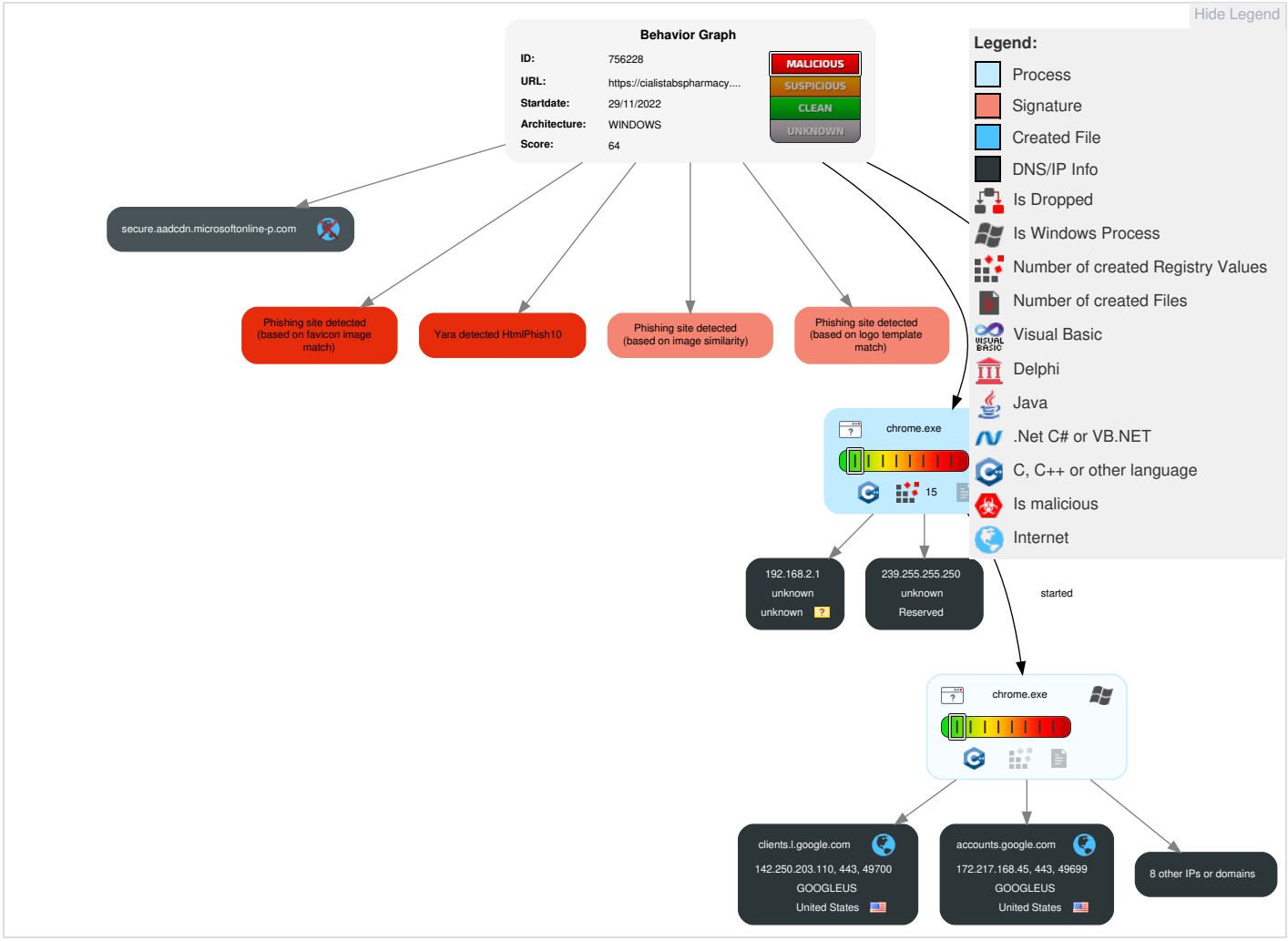
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

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	1 Process Injection	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	Rootkit	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

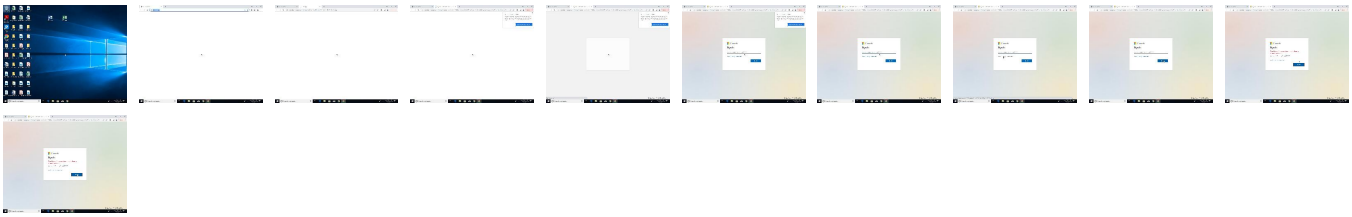
Behavior Graph

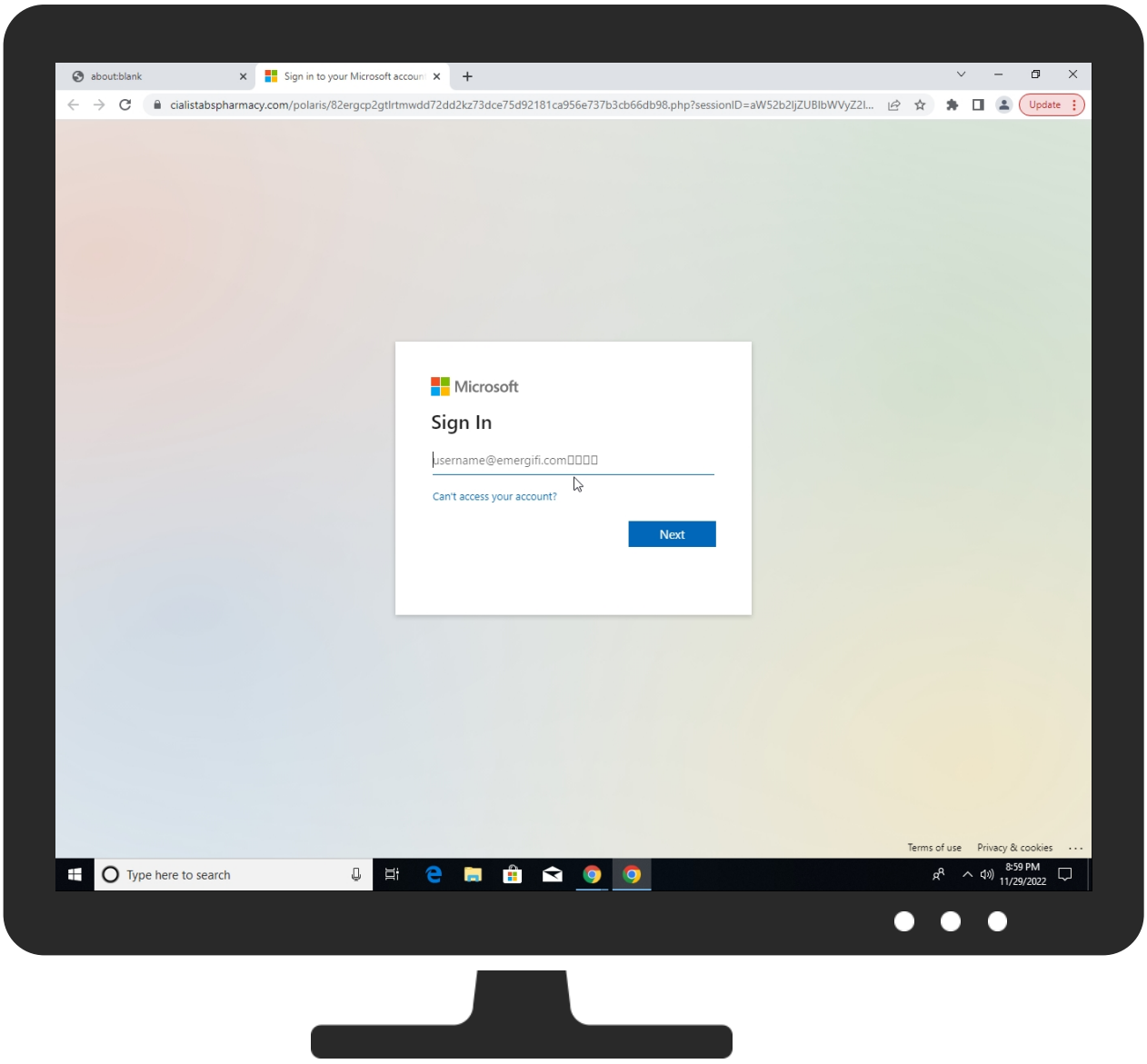


Screenshots

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://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cialistabspharmacy.com/polaris/82ergcp2gtlrtmwdd72dd2kz73dce75d92181ca956e737b3cb66db98.php?sessionID=aW52b2ljZUBlbWVyZ2lmaS5jb20dDwMFAg==	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

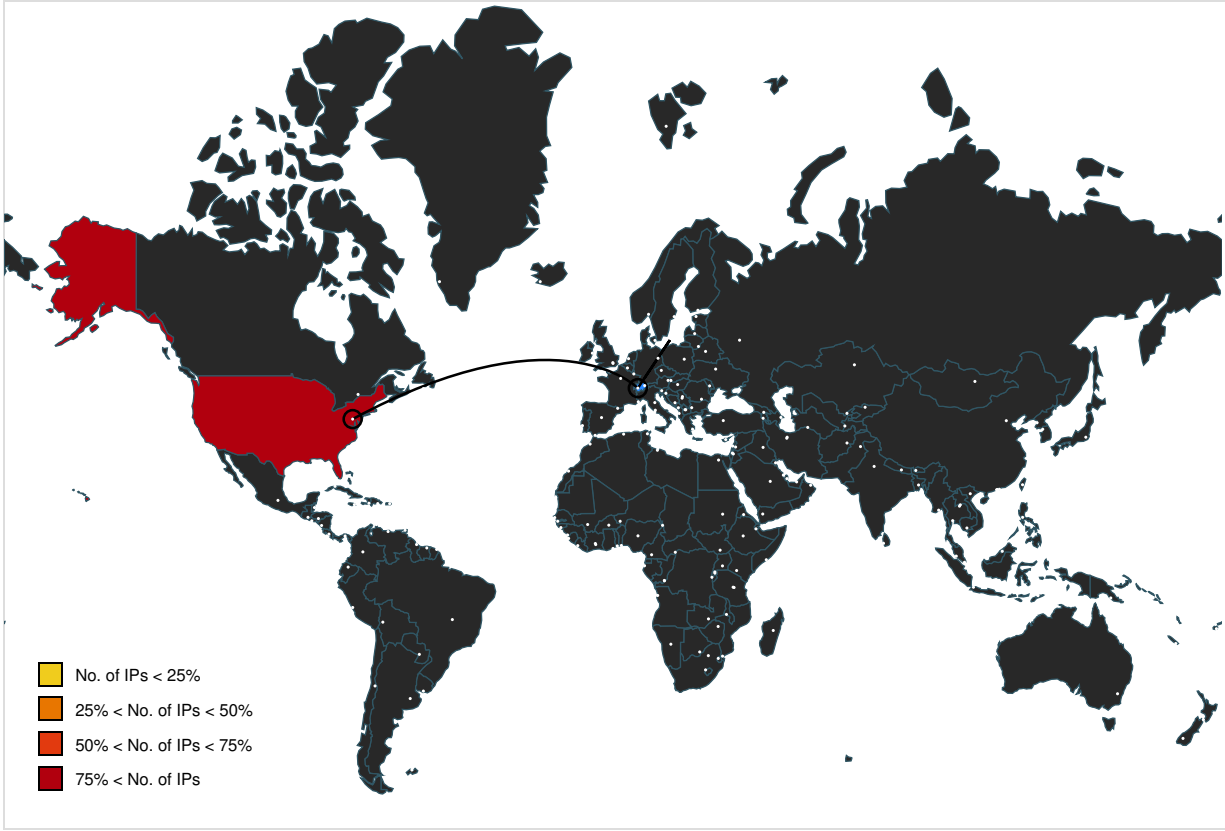
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
www.google.com	172.217.168.68	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
cialistabspharmacy.com	184.168.106.3	true	false		unknown
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
cdn.jsdelivr.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cialistabspharmacy.com/polaris/82ergcp2gtlrtmwdd72dd2kz73dce75d92181ca956e737b3cb66db98.php?sessionID=aW52b2ljZUBlbWVyZ2lmaS5jb20dDwMFAg%3D%3D&websrc=Vu8j5MDuFXclw8caZsLSg55YePOh7Ob1bLax6UMeEfDH2KtK69Kqs79wEmhs2ylwjZ5CaLnlzZH3RFD01GRVFKvyr8is3O7T3wD2KhSkVmVTPRktolOwAxUy8ttkICXaNsewe6s7gIXCnTs9cFBweAi5HyNNk7t3OORb0C2z5SzegFUu1LFDMJ0HgsH9nle2lluf8j3Z2tuFqdtL42gYt9mPkPe2erCcOkDBHoEZqhkbWne5873SqeBR3vAlzZBbCNKcAQfs58EVSFpqYqLnoSLVyiSjACshGsaLBSaNAS07le&dispatch=273&id=726371	true		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-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg	false		unknown
http://https://cialistabspharmacy.com/polaris/82ergcp2gtlrtmwdd72dd2kz73dce75d92181ca956e737b3cb66db98.php?sessionID=aW52b2ljZUBlbWVyZ2lmaS5jb20dDwMFAg==	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/axios/0.21.1/axios.min.js	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://cialistabspharmacy.com/polaris/82ergcp2gtlrtmwdd72dd2kz73dce75d92181ca956e737b3cb66db98.php?sessionID=aW52b2ljZUBlbWVyZ2lmaS5jb20dDwMFAg%3D%3D&websrc=Vu8j5MDuFXclw8caZsLSg55YePOh7Ob1bLax6UMeEfDH2KtK69Kqs79wEmhs2ylwjZ5CaLnlzZH3RFD01GRVFKvyr8is3O7T3wD2KhSkVmVTPRktolOwAxUy8ttkICXaNsewe6s7gIXCnTs9cFBweAi5HyNNk7t3OORb0C2z5SzegFUu1LFDMJ0HgsH9nle2lluf8j3Z2tuFqdtL42gYt9mPkPe2erCcOkDBHoEZqhkbWne5873SqeBR3vAlzZBbCNKcAQfs58EVSFpqYqLnoSLVyiSjACshGsaLBSaNAS07le&dispatch=273&id=726371	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
184.168.106.3	cialistabspharmacy.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
104.17.25.14	cdnjs.cloudflare.com	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:	756228
Start date and time:	2022-11-29 20:58:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg
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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2022

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.phis.win@23/0@9/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 104.16.86.20, 104.16.88.20, 104.16.85.20, 104.16.87.20, 104.16.89.20, 96.16.150.76, 172.217.168.42, 172.217.168.74, 142.250.203.106, 216.58.215.234, 172.217.168.10
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, cdn.jsdelivr.net.cdn.cloudflare.net, edgedl.me.gvt1.com, content-autofill.googleapis.com, lgincdn.trafficmanager.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, lgincdnvzeuno.ec.azureedge.net, e13761.dscg.akamaiedge.net, clientservices.googleapis.com, lgincdnvzeuno.azureedge.net
- 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

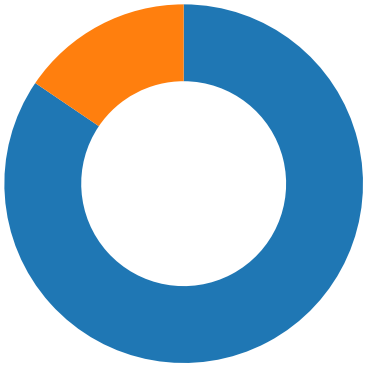
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 58

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:59:41.843067884 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:41.843147039 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:41.843231916 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:41.843532085 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:41.843596935 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:41.843672991 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:41.844242096 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:41.844266891 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:41.844451904 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:41.844485044 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:41.971976042 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:41.978758097 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:42.012360096 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:42.021476030 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:42.031418085 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:42.031439066 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:42.031645060 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:42.031696081 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:42.033921957 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:42.034025908 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:42.034800053 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:42.034902096 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:42.037800074 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:42.037888050 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:43.503597975 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.503678083 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.503997087 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.504014969 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.504060030 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.504308939 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:43.504370928 CET	443	49700	142.250.203.110	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:59:43.504736900 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:43.504766941 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:43.504792929 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:43.558389902 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.558428049 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.580784082 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.580909967 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.580946922 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.581175089 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.581249952 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.589349031 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:43.589380980 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:43.689444065 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:43.872733116 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:43.872801065 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:43.872932911 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:43.877302885 CET	49699	443	192.168.2.4	172.217.168.45
Nov 29, 2022 20:59:43.877342939 CET	443	49699	172.217.168.45	192.168.2.4
Nov 29, 2022 20:59:43.885545015 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:43.885608912 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.111474991 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:44.111622095 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:44.111756086 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:44.112951994 CET	49700	443	192.168.2.4	142.250.203.110
Nov 29, 2022 20:59:44.112987041 CET	443	49700	142.250.203.110	192.168.2.4
Nov 29, 2022 20:59:44.676935911 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.707285881 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:44.707348108 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.710585117 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.710758924 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:44.717650890 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:44.717689037 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.717832088 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:44.717868090 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.718086958 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.789486885 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:44.789530993 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:44.889523983 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.192882061 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.193026066 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.193119049 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.201554060 CET	49702	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.201606035 CET	443	49702	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.205714941 CET	49704	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.205792904 CET	443	49704	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.205930948 CET	49704	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.206311941 CET	49704	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.206342936 CET	443	49704	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.304317951 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.304384947 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.304517031 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.312937021 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.312997103 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.382834911 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.383321047 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.383385897 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.385241032 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.385445118 CET	49705	443	192.168.2.4	172.217.168.68

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:59:45.387926102 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.387974024 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.388104916 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.559623003 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.559678078 CET	443	49705	172.217.168.68	192.168.2.4
Nov 29, 2022 20:59:45.730473042 CET	443	49704	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.757577896 CET	49705	443	192.168.2.4	172.217.168.68
Nov 29, 2022 20:59:45.758435011 CET	49704	443	192.168.2.4	184.168.106.3
Nov 29, 2022 20:59:45.758495092 CET	443	49704	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.759740114 CET	443	49704	184.168.106.3	192.168.2.4
Nov 29, 2022 20:59:45.767420053 CET	49704	443	192.168.2.4	184.168.106.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:59:41.770828009 CET	58565	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:41.773571968 CET	52239	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:41.790349960 CET	53	58565	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:41.801201105 CET	53	52239	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:41.949896097 CET	61007	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:41.970788956 CET	53	61007	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:45.236793041 CET	55570	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:45.256650925 CET	53	55570	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:45.281066895 CET	64906	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:45.300988913 CET	53	64906	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:46.876437902 CET	61088	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:46.879719973 CET	58729	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:46.901210070 CET	53	58729	8.8.8.8	192.168.2.4
Nov 29, 2022 20:59:47.639122963 CET	56022	53	192.168.2.4	8.8.8.8
Nov 29, 2022 20:59:52.022222042 CET	54521	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 20:59:41.770828009 CET	192.168.2.4	8.8.8.8	0xc313	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:41.773571968 CET	192.168.2.4	8.8.8.8	0x62f7	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:41.949896097 CET	192.168.2.4	8.8.8.8	0x992e	Standard query (0)	cialistabspharmacy.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:45.236793041 CET	192.168.2.4	8.8.8.8	0x2ff1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:45.281066895 CET	192.168.2.4	8.8.8.8	0x5ad6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:46.876437902 CET	192.168.2.4	8.8.8.8	0x173b	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:46.879719973 CET	192.168.2.4	8.8.8.8	0x471e	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:47.639122963 CET	192.168.2.4	8.8.8.8	0xa5ea	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:52.022222042 CET	192.168.2.4	8.8.8.8	0xa8c0	Standard query (0)	secure.aadcdn.microsoftonline-p.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
Nov 29, 2022 20:59:41.790349960 CET	8.8.8.8	192.168.2.4	0xc313	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:41.801201105 CET	8.8.8.8	192.168.2.4	0x62f7	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

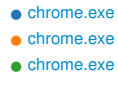
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 20:59:41.801201105 CET	8.8.8.8	192.168.2.4	0x62f7	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:41.970788956 CET	8.8.8.8	192.168.2.4	0x992e	No error (0)	cialistabspharmacy.com		184.168.106.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:45.256650925 CET	8.8.8.8	192.168.2.4	0x2ff1	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:45.300988913 CET	8.8.8.8	192.168.2.4	0x5ad6	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:46.375910997 CET	8.8.8.8	192.168.2.4	0xbf56	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:46.899960041 CET	8.8.8.8	192.168.2.4	0x173b	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:46.901210070 CET	8.8.8.8	192.168.2.4	0x471e	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:46.901210070 CET	8.8.8.8	192.168.2.4	0x471e	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:47.661205053 CET	8.8.8.8	192.168.2.4	0xa5ea	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:51.864490032 CET	8.8.8.8	192.168.2.4	0x2767	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:52.041032076 CET	8.8.8.8	192.168.2.4	0xa8c0	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

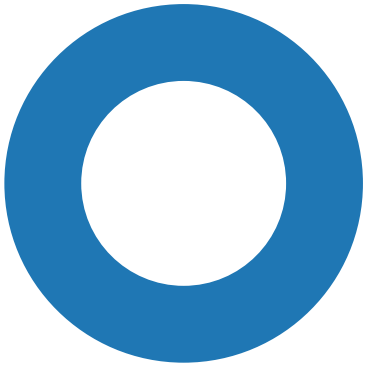
- accounts.google.com
- clients2.google.com
- cialistabspharmacy.com
- https:
  - logincdn.msauth.net
  - cdnjs.cloudflare.com

Statistics

Behavior



Copyright Joe Security LLC 2022



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **4856**, Parent PID: **1796**

General

Target ID:	0
Start time:	20:59:37
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:	0x7ff683680000
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

Registry Activities

Analysis Process: chrome.exe PID: **5784**, Parent PID: **4856**

General

Target ID:	1
Start time:	20:59:38
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1876 --field-trial-handle=1828,i,2187161938276056667,2480233056043708616,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8

Imagebase:	0x7ff683680000
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: **4440**, Parent PID: **1796**

General

Target ID:	2
Start time:	20:59:39
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://cialistabspharmacy.com/polaris/?aW52b2ljZUBlbWVyZ2lmaS5jb20=&d=DwMFAg
Imagebase:	0x7ff683680000
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