ID: 800682
Cookbook: browseurl.jbs
Time: 18:06:08
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

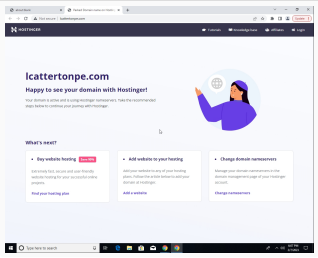
Windows Analysis Report

http://lcattertonpe.com

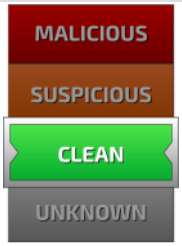
Overview

General Information

Sample URL:	http://lcattertonpe.com
Analysis ID:	800682
Infos:	



Detection

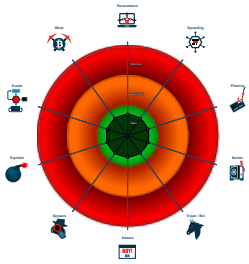


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 2888 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4544 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=1960 --field-trial-handle=1736,i,823529605349688411,4145770639965686966,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 1724 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://lcattertonpe.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

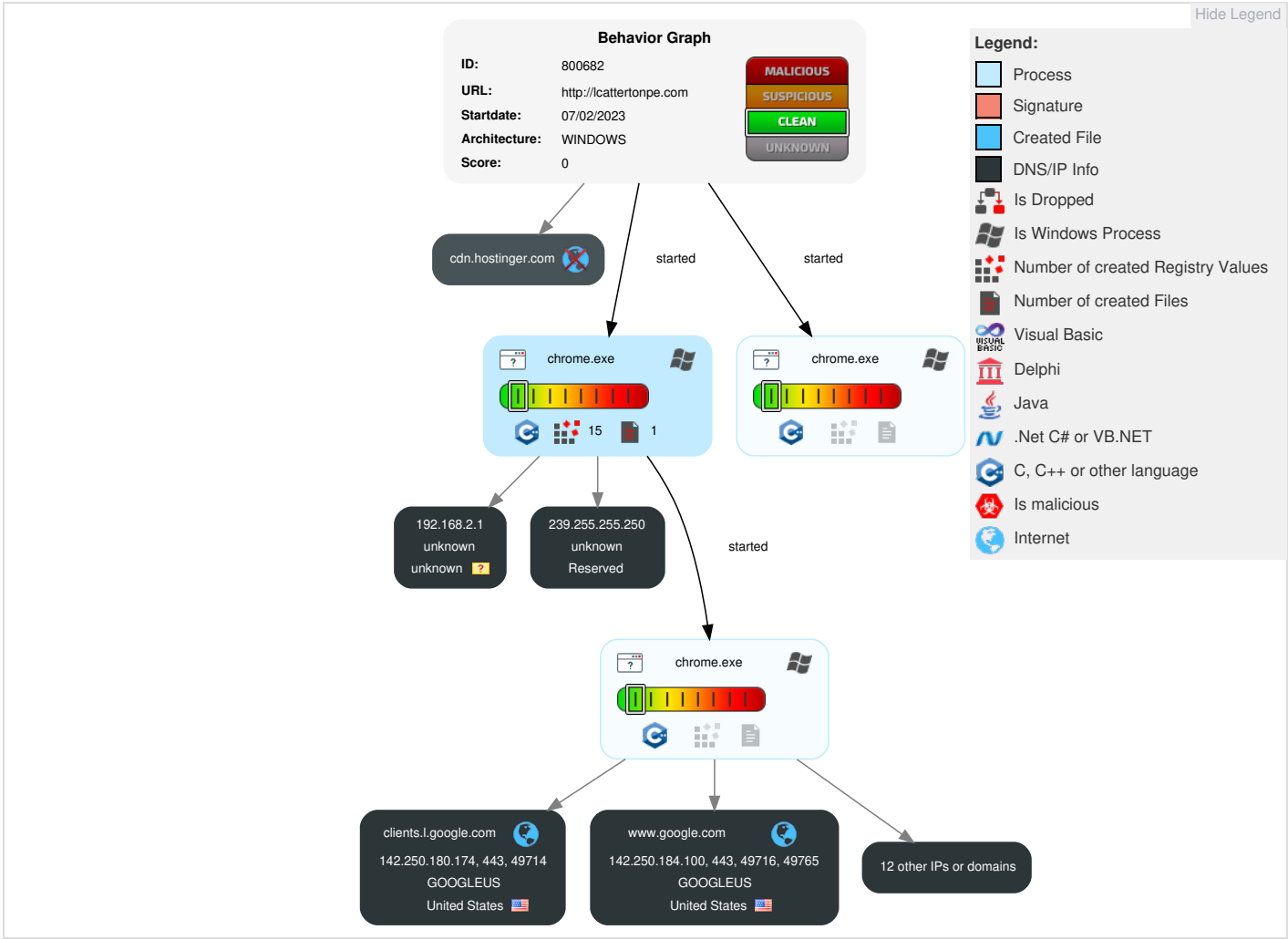
Joe Sandbox Signatures

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

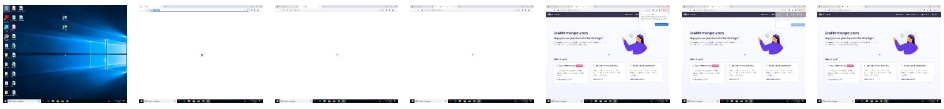
Behavior Graph

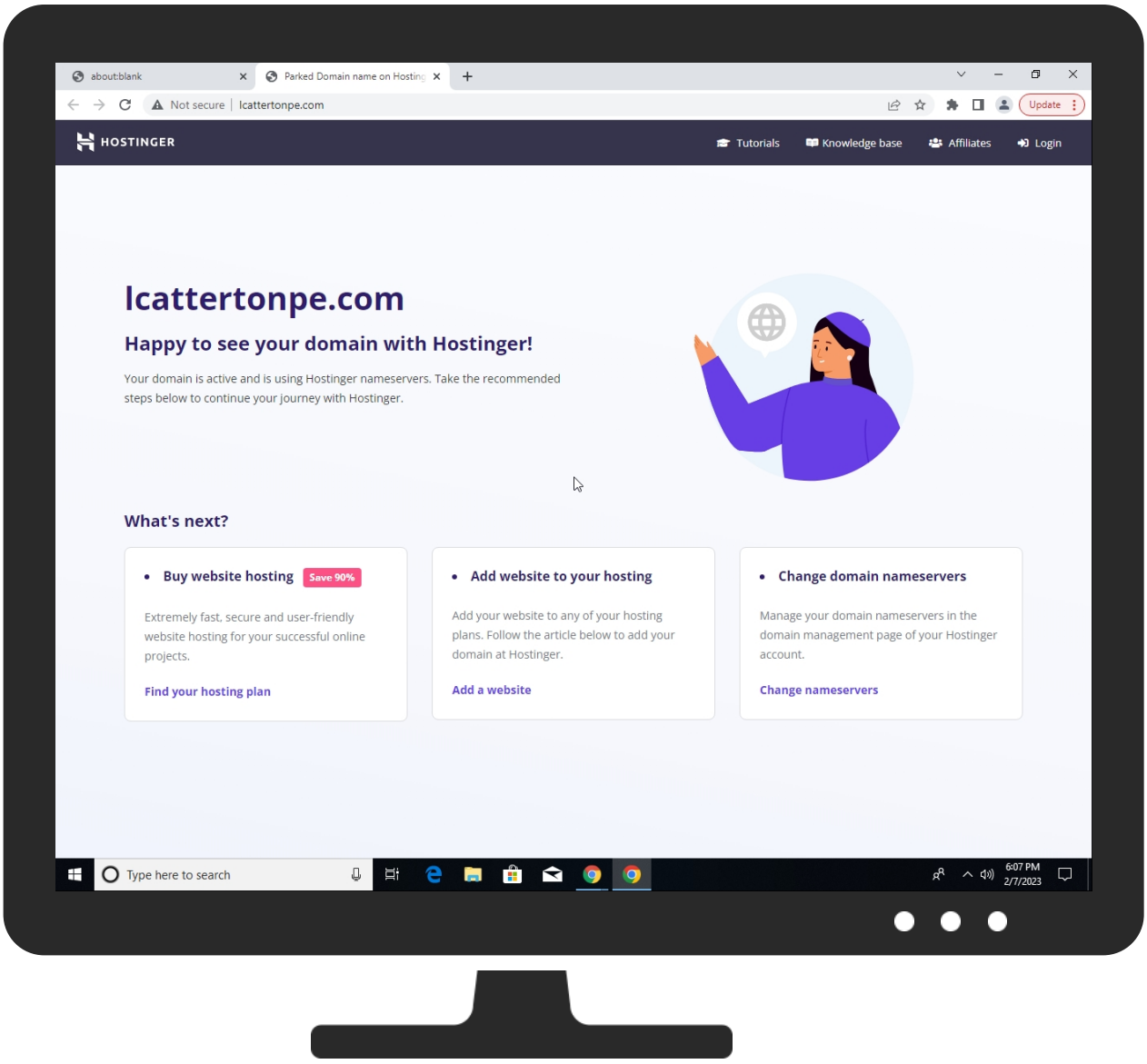


Screenshots

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://lcattertonpe.com	0%	Virustotal		Browse
http://lcattertonpe.com	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://lcattertonpe.com/favicon.ico	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-26575989-44&cid=315444834.1675822043&jid=1751296008&_u=YEBAAUAAAAAAACAAI~&z=481455849	0%	Avira URL Cloud	safe	

Domains and IPs

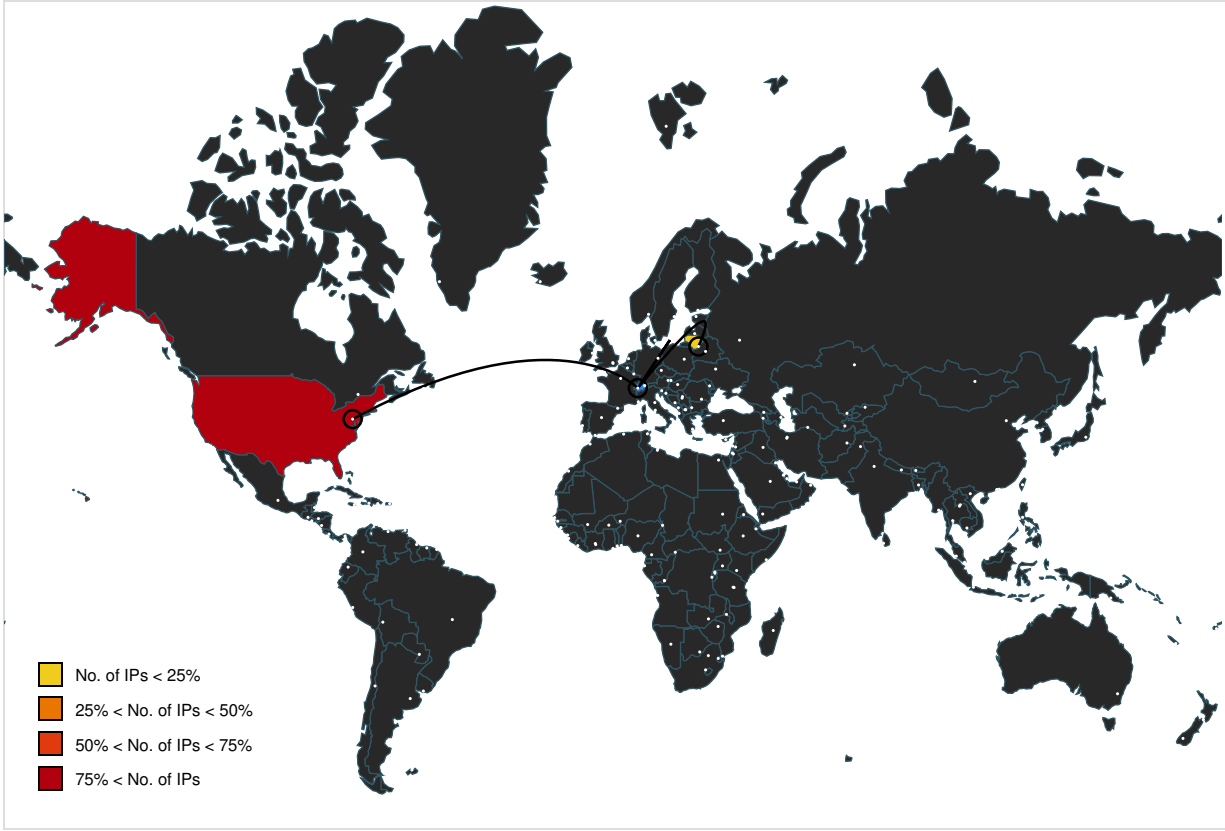
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
lcattertonpe.com	2.57.90.16	true	false		unknown
cdnjs.cloudflare.com	104.17.24.14	true	false		high
www.google.co.uk	142.251.209.3	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
stats.g.doubleclick.net	142.251.31.155	true	false		high
cpanel.hostinger.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
cdn.hostinger.com	unknown	unknown	false		high
support.hostinger.com	unknown	unknown	false		high
www.hostinger.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-26575989-44&cid=315444834.1675822043&jid=1751296008&gjid=1286070036&_gid=1283538996.1675822043&_u=YEBAAUAAAAAAACAAI~&z=612317697	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.3/webfonts/fa-brands-400.woff2	false		high
http://lcattertonpe.com/	false		unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.3/webfonts/fa-solid-900.woff2	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-26575989-44&cid=315444834.1675822043&jid=1751296008&_u=YEBAAUAAAAAAACAAI~&z=481455849	false		high
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://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.3/css/all.min.css	false		high
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-26575989-44&cid=315444834.1675822043&jid=1751296008&_u=YEBAAUAAAAAAACAAI~&z=481455849	false	• Avira URL Cloud: safe	unknown
http://lcattertonpe.com/	false		unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	false		high
http://lcattertonpe.com/favicon.ico	false	• Avira URL Cloud: safe	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
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.251.31.155	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.251.209.3	www.google.co.uk	United States		15169	GOOGLEUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false
2.57.90.16	lcattertonpe.com	Lithuania		47583	AS-HOSTINGERLT	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800682
Start date and time:	2023-02-07 18:06:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://lcattertonpe.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:	13
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@25/0@13/11
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.hostinger.com/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 142.250.180.170, 142.250.180.138, 142.250.184.67, 104.18.114.100, 104.18.113.100, 142.250.180.168, 34.104.35.123, 142.250.184.110, 142.250.180.163
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, fonts.gstatic.com, ctldl.windowsupdate.com, clientservices.googleapis.com, edgedl.me.gvt1.com, login.live.com, www.googletagmanager.com, support.hostinger.com.cdn.cloudflare.net, update.googleapis.com, cdn.hostinger.com.cdn.cloudflare.net, cpanel.hostinger.com.cdn.cloudflare.net, www.hostinger.com.cdn.cloudflare.net, www.google-analytics.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

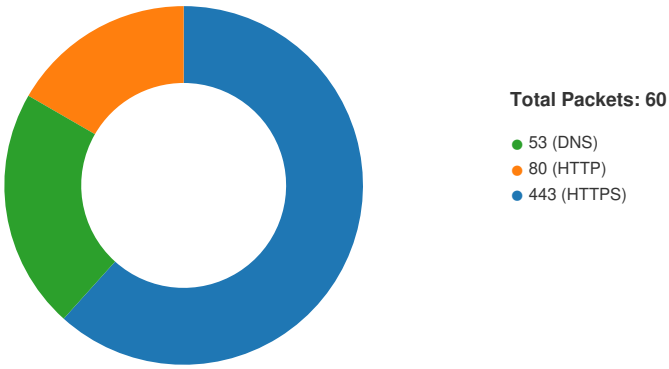
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:07:20.517294884 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.517353058 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.517474890 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.518132925 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:20.518177032 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:20.518269062 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:20.518743038 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:20.518783092 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:20.518851995 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:20.519408941 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.522578001 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.522620916 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.523626089 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:20.523653030 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:20.524456978 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:20.524486065 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:20.525861025 CET	49719	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.556240082 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.556421041 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.557173014 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.562509060 CET	80	49719	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.562674046 CET	49719	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.593693972 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593740940 CET	80	49717	2.57.90.16	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:07:20.593831062 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593858957 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593885899 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593915939 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593918085 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.593941927 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.593956947 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.593970060 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.594002962 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.594007015 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.594033957 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.594059944 CET	80	49717	2.57.90.16	192.168.2.7
Feb 7, 2023 18:07:20.594063997 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.594120026 CET	49717	80	192.168.2.7	2.57.90.16
Feb 7, 2023 18:07:20.648267984 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:20.648864985 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:20.648900032 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:20.651115894 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:20.651268959 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:20.662743092 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.675905943 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:20.695622921 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:20.695655107 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:20.696300030 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.696336985 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.697024107 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.697155952 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.697957039 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:20.697988987 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:20.698043108 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:20.698113918 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:20.835581064 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.835623980 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.835696936 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.836308956 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.836343050 CET	443	49722	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.836409092 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.837413073 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.837440968 CET	443	49722	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.839257002 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.839283943 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.887265921 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.908435106 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.908485889 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.911061049 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.911190987 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:20.911334991 CET	49724	443	192.168.2.7	104.17.24.14
Feb 7, 2023 18:07:20.911380053 CET	443	49724	104.17.24.14	192.168.2.7
Feb 7, 2023 18:07:20.911472082 CET	49724	443	192.168.2.7	104.17.24.14
Feb 7, 2023 18:07:20.914211988 CET	49724	443	192.168.2.7	104.17.24.14
Feb 7, 2023 18:07:20.914236069 CET	443	49724	104.17.24.14	192.168.2.7
Feb 7, 2023 18:07:20.946104050 CET	443	49722	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:20.967922926 CET	443	49724	104.17.24.14	192.168.2.7
Feb 7, 2023 18:07:21.002819061 CET	49724	443	192.168.2.7	104.17.24.14
Feb 7, 2023 18:07:21.002856970 CET	443	49724	104.17.24.14	192.168.2.7
Feb 7, 2023 18:07:21.003135920 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:21.003154039 CET	443	49722	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:21.004911900 CET	443	49722	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:21.004971027 CET	443	49722	104.18.10.207	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:07:21.005013943 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:21.005345106 CET	443	49724	104.17.24.14	192.168.2.7
Feb 7, 2023 18:07:21.005415916 CET	49724	443	192.168.2.7	104.17.24.14
Feb 7, 2023 18:07:21.142049074 CET	49722	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:21.145241022 CET	49716	443	192.168.2.7	142.250.184.100
Feb 7, 2023 18:07:21.145260096 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:21.145422935 CET	443	49716	142.250.184.100	192.168.2.7
Feb 7, 2023 18:07:21.145725965 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:07:21.145756960 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:21.145991087 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:07:21.146218061 CET	49721	443	192.168.2.7	104.18.10.207
Feb 7, 2023 18:07:21.146254063 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:21.146464109 CET	443	49721	104.18.10.207	192.168.2.7
Feb 7, 2023 18:07:21.146814108 CET	49715	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:07:21.146840096 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:21.147001982 CET	443	49715	216.58.209.45	192.168.2.7
Feb 7, 2023 18:07:21.147140980 CET	49722	443	192.168.2.7	104.18.10.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:07:20.453223944 CET	51007	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.457696915 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.465583086 CET	60765	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.469629049 CET	58283	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.481324911 CET	53	51007	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:20.487155914 CET	53	58283	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:20.493951082 CET	53	60765	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:20.505382061 CET	53	50513	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:20.723437071 CET	50024	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.744332075 CET	53	50024	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:20.820439100 CET	61392	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:20.844157934 CET	53	61392	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:22.005989075 CET	51526	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:22.196577072 CET	58784	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:22.209849119 CET	57970	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:22.211728096 CET	64608	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:23.276364088 CET	52750	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:23.302983046 CET	53	52750	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:23.474646091 CET	64078	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:07:23.501009941 CET	53	64078	8.8.8.8	192.168.2.7
Feb 7, 2023 18:07:27.207098961 CET	58514	53	192.168.2.7	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:07:20.453223944 CET	192.168.2.7	8.8.8.8	0xe4a6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.457696915 CET	192.168.2.7	8.8.8.8	0xa587	Standard query (0)	lcattertonpe.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.465583086 CET	192.168.2.7	8.8.8.8	0x8a08	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.469629049 CET	192.168.2.7	8.8.8.8	0x6b1b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.723437071 CET	192.168.2.7	8.8.8.8	0x8a04	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.820439100 CET	192.168.2.7	8.8.8.8	0x782f	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:22.005989075 CET	192.168.2.7	8.8.8.8	0x460a	Standard query (0)	cdn.hostinger.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:22.196577072 CET	192.168.2.7	8.8.8.8	0x5bd9	Standard query (0)	www.hostinger.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:07:22.209849119 CET	192.168.2.7	8.8.8.8	0xd893	Standard query (0)	support.hostinger.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:22.211728096 CET	192.168.2.7	8.8.8.8	0x14c	Standard query (0)	cpanel.hostinger.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.276364088 CET	192.168.2.7	8.8.8.8	0x8852	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.474646091 CET	192.168.2.7	8.8.8.8	0xba73	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:27.207098961 CET	192.168.2.7	8.8.8.8	0x3e3a	Standard query (0)	cdn.hostinger.com	A (IP address)	IN (0x0001)	false

DNS Answers

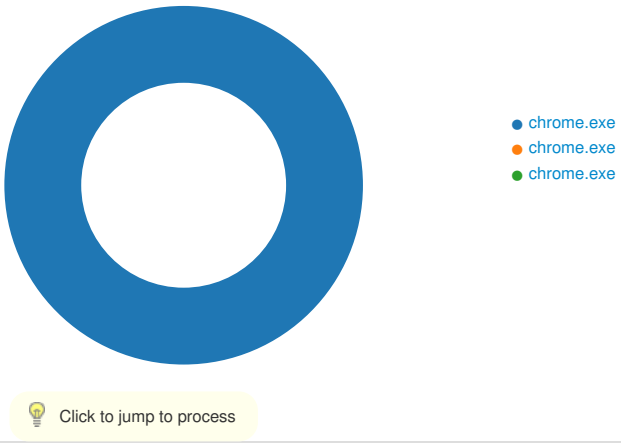
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:07:20.481324911 CET	8.8.8.8	192.168.2.7	0xe4a6	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.487155914 CET	8.8.8.8	192.168.2.7	0x6b1b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:07:20.487155914 CET	8.8.8.8	192.168.2.7	0x6b1b	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.493951082 CET	8.8.8.8	192.168.2.7	0x8a08	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.505382061 CET	8.8.8.8	192.168.2.7	0xa587	No error (0)	lcatterton pe.com		2.57.90.16	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.744332075 CET	8.8.8.8	192.168.2.7	0x8a04	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.744332075 CET	8.8.8.8	192.168.2.7	0x8a04	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.844157934 CET	8.8.8.8	192.168.2.7	0x782f	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:20.844157934 CET	8.8.8.8	192.168.2.7	0x782f	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:22.028316975 CET	8.8.8.8	192.168.2.7	0x460a	No error (0)	cdn.hostinger.com	cdn.hostinger.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:07:22.220026016 CET	8.8.8.8	192.168.2.7	0x5bd9	No error (0)	www.hostinger.com	www.hostinger.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:07:22.251935959 CET	8.8.8.8	192.168.2.7	0x14c	No error (0)	cpanel.hostinger.com	cpanel.hostinger.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:07:22.252708912 CET	8.8.8.8	192.168.2.7	0xd893	No error (0)	support.hostinger.com	support.hostinger.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:07:23.302983046 CET	8.8.8.8	192.168.2.7	0x8852	No error (0)	stats.g.doubleclick.net		142.251.31.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.302983046 CET	8.8.8.8	192.168.2.7	0x8852	No error (0)	stats.g.doubleclick.net		142.251.31.154	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.302983046 CET	8.8.8.8	192.168.2.7	0x8852	No error (0)	stats.g.doubleclick.net		142.251.31.156	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.302983046 CET	8.8.8.8	192.168.2.7	0x8852	No error (0)	stats.g.doubleclick.net		142.251.31.157	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:23.501009941 CET	8.8.8.8	192.168.2.7	0xba73	No error (0)	www.google.co.uk		142.251.209.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:07:27.227603912 CET	8.8.8.8	192.168.2.7	0x3e3a	No error (0)	cdn.hostinger.com	cdn.hostinger.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- lcattertonpe.com
  - maxcdn.bootstrapcdn.com
  - cdnjs.cloudflare.com
  - stats.g.doubleclick.net
  - www.google.com
  - www.google.co.uk
- accounts.google.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2888**, Parent PID: **1716**

General

Target ID:	0
Start time:	18:07:13
Start date:	07/02/2023
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:	0x7ff7c2920000
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: **4544**, Parent PID: **2888**

General

Target ID:	1
Start time:	18:07:14
Start date:	07/02/2023
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=1960 --field-trial-handle=1736,i,823529605349688411,4145770639965686966,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c2920000
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: **1724**, Parent PID: **1716**

General

Target ID:	2
Start time:	18:07:15
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://lcattertonpe.com
Imagebase:	0x7ff7c2920000
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