ID: 756095
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 16:31:55
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

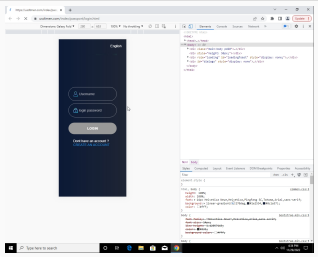
Windows Analysis Report

https://usdtmen.com

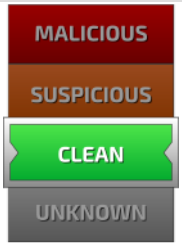
Overview

General Information

Sample URL:	http://https://usdtmen.com
Analysis ID:	756095
Infos:	



Detection

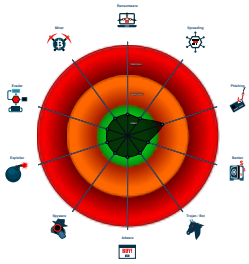


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 3188 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://usdtmen.com/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6160 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=2040 --field-trial-handle=1768,i,5818765958052219750,8192306715576805166,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **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

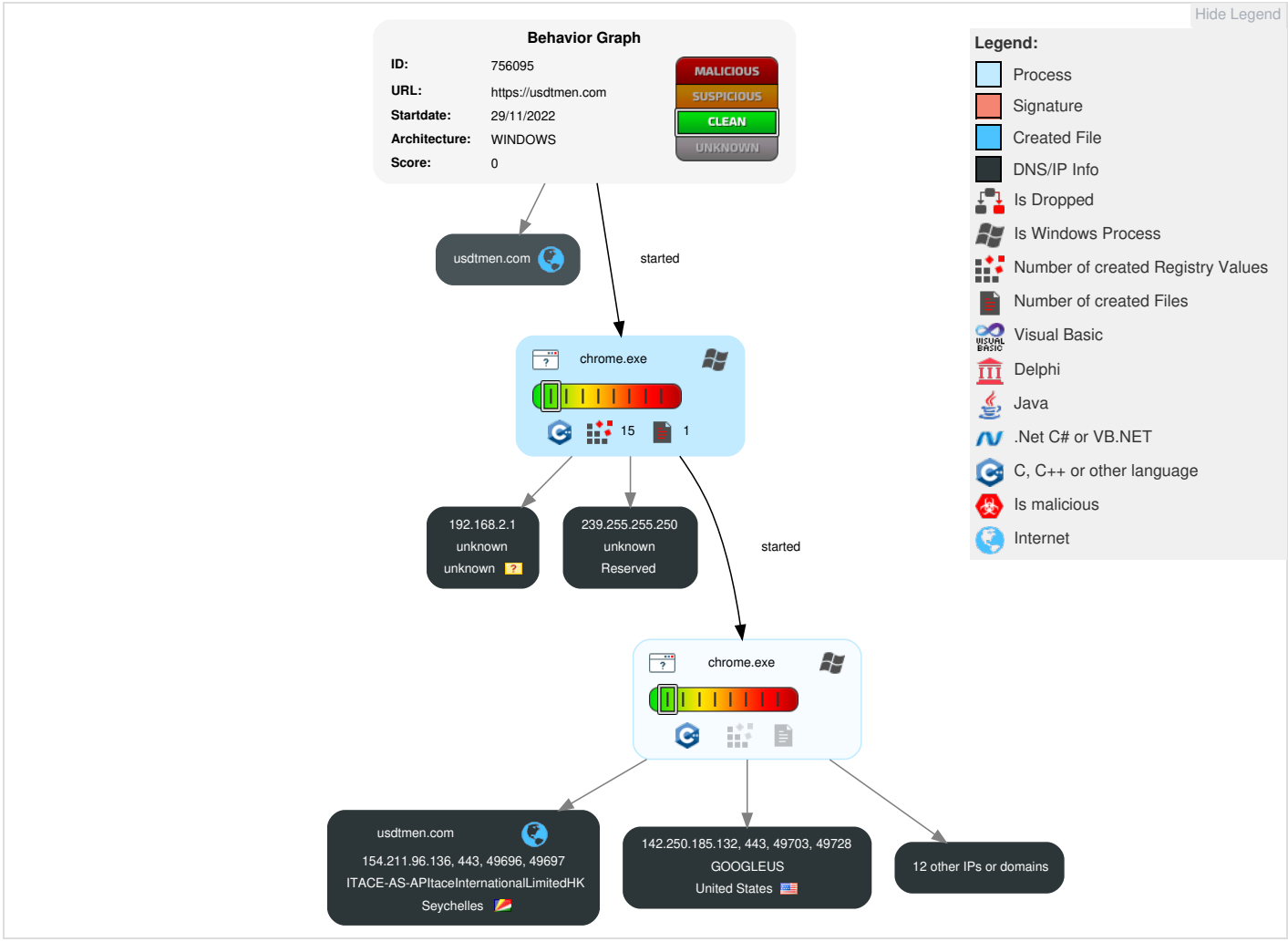
Joe Sandbox Signatures

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

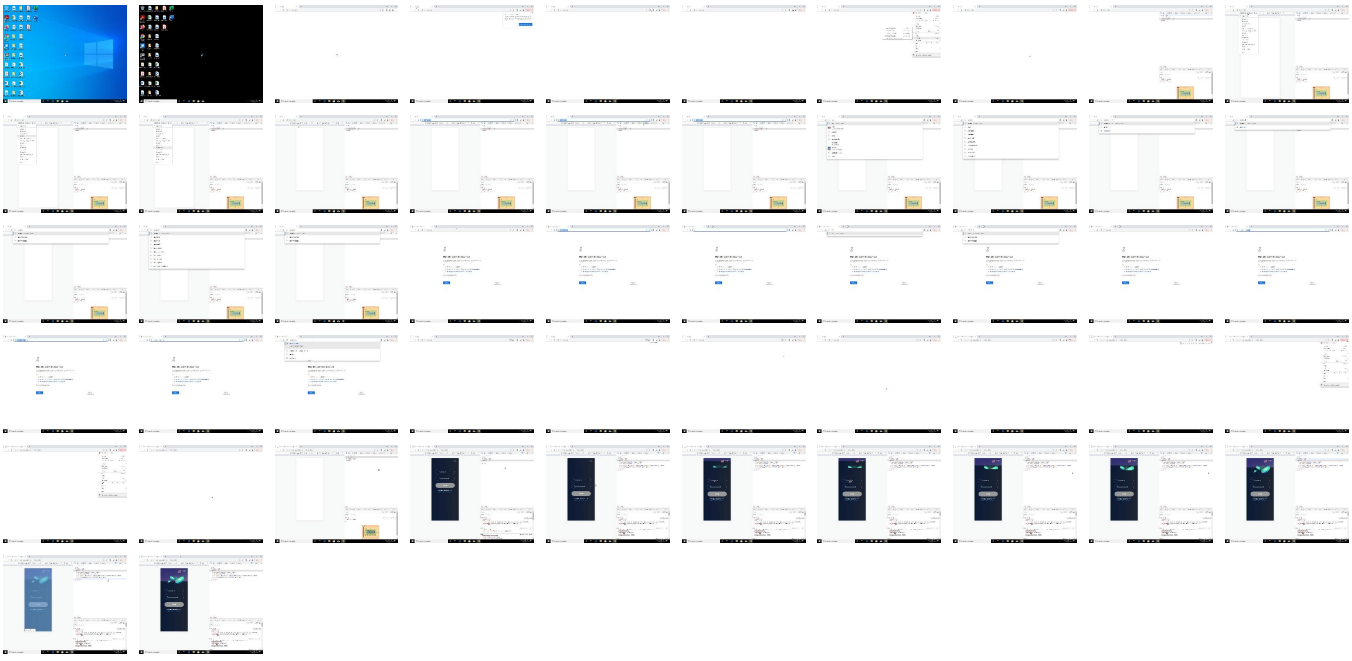
Behavior Graph

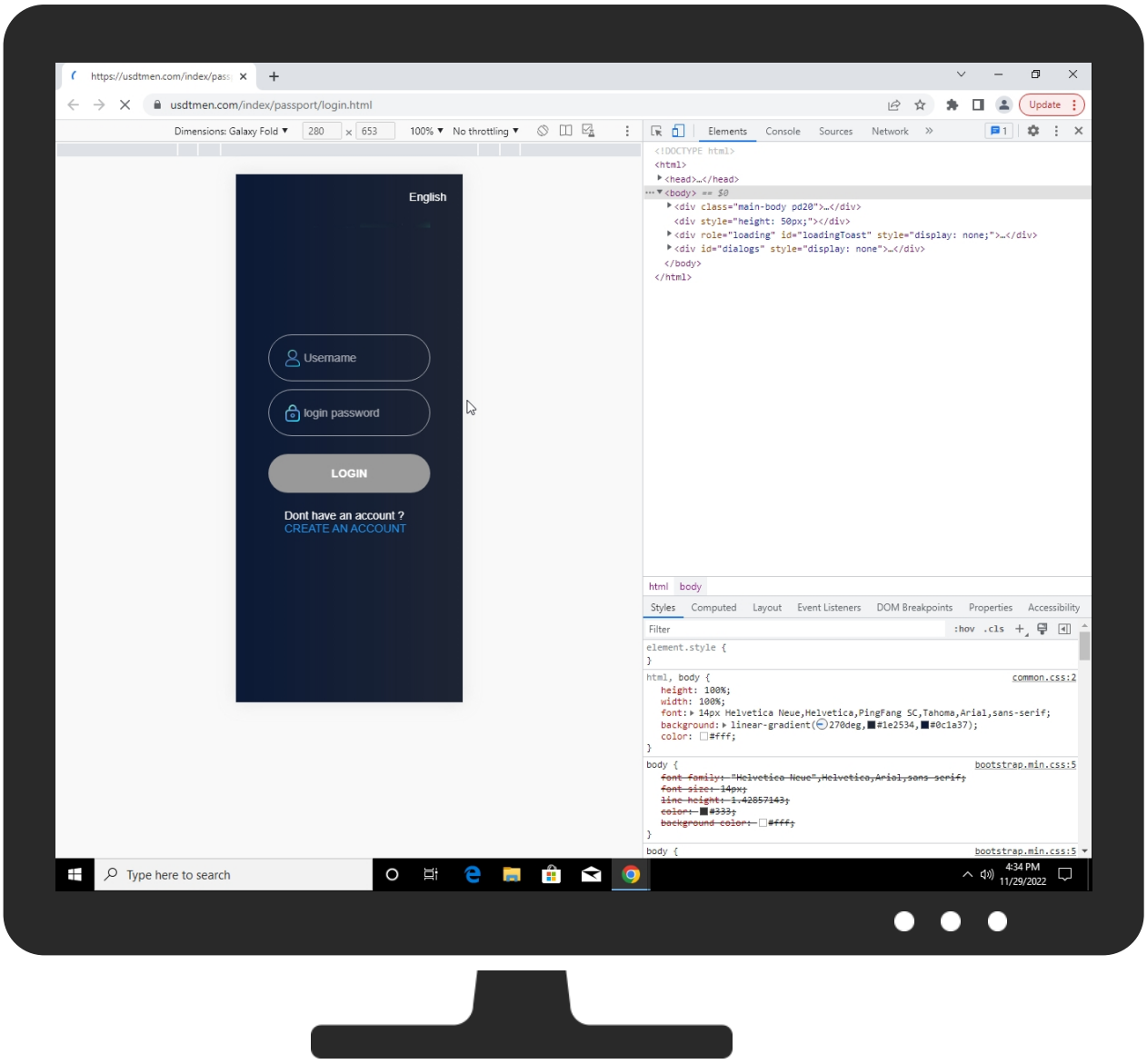


Screenshots

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://usdtmen.com	1%	Virustotal		Browse
http://https://usdtmen.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://https://beacons.gcp.gvt2.com/domainreliability/upload	0%	URL Reputation	safe	
http://https://beacons.gvt2.com/domainreliability/upload	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://usdtmen.com/index/passport/logout.html	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/weui.min.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/bg1.6c9f941a.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/fr.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/layer3.1/layer.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/common.css	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/layer3.1/theme/default/layer.css?v=3.1.1	0%	Avira URL Cloud	safe	
http://https://beacons2.gvt2.com/domainreliability/upload-nel	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/index/passport/logout.html	3%	Virustotal		Browse
http://https://usdtmen.com/image/zepto.min.js	0%	Avira URL Cloud	safe	
http://https://e2c27.gcp.gvt2.com/nel/	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/weui.css	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/iconfont.css	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/jquery.min.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/es-es.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/password_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/bootstrap.min.css	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/common.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/ko.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/username_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/bootstrap.min.css.map	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/logo.cba20b1b.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/ar-ae.jpg	0%	Avira URL Cloud	safe	
http://usdtmen.com/	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/pt-pt.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/en-us.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.186.109	true	false		high
beacons-handoff.gcp.gvt2.com	142.251.143.67	true	false		unknown
usdtmen.com	154.211.96.136	true	false		unknown
e2c27.gcp.gvt2.com	35.227.159.135	true	false		unknown
www.google.com	142.250.186.100	true	false		high
beacons2.gvt2.com	172.217.13.227	true	false		unknown
clients.l.google.com	142.250.185.206	true	false		high
beacons.gvt2.com	216.58.212.163	true	false		unknown
clients2.google.com	unknown	unknown	false		high
www.usdtmen.com	unknown	unknown	false		unknown
beacons.gcp.gvt2.com	unknown	unknown	false		unknown

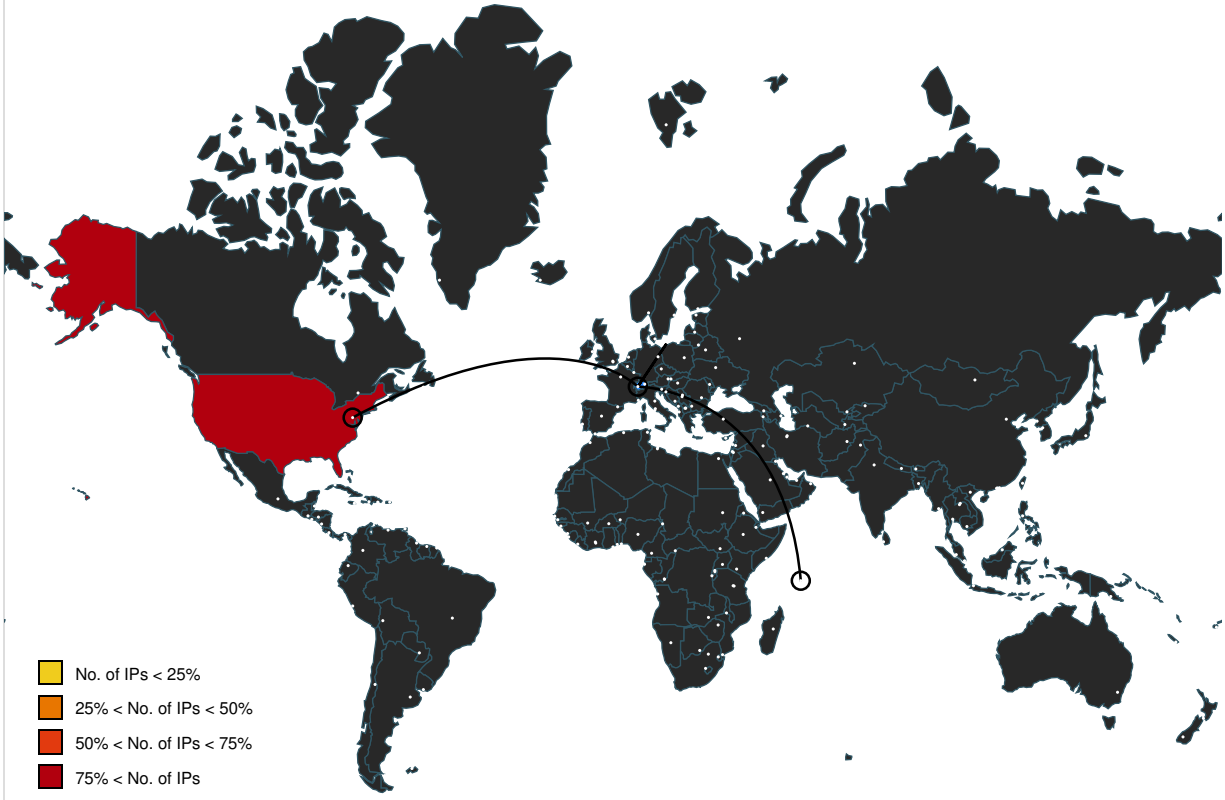
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=USDTME&oit=1&cp=6&gs_rn=42&psi=qRYiebaDLQ80oWlb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usd&oit=1&cp=3&gs_rn=42&psi=qRYiebaDLQ80oWlb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=wwusdtmen.com&oit=3&cp=2&gs_rn=42&psi=qRYiebaDLQ80oWlb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=USDT&oit=1&cp=4&gs_rn=42&psi=qRYiebaDLQ80oWlb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://usdtmen.com/layer3.1/layer.js	false	• Avira URL Cloud: safe	unknown
http://https://beacons.gcp.gvt2.com/domainreliability/upload	false	• URL Reputation: safe	unknown
http://https://usdtmen.com/image/fr.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/bg1.6c9f941a.png	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=USDTMEN&oit=1&cp=7&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/index/passport/logout.html	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen%3ECO&oit=4&cp=10&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/weui.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen.com&oit=3&cp=0&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen%3E&oit=4&cp=8&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/layer3.1/theme/default/layer.css?v=3.1.1	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/passport/login.html	false		unknown
http://https://usdtmen.com/image/common.css	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=U&oit=1&cp=1&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://beacons2.gvt2.com/domainreliability/upload-nel	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/passport/login.html	false		unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtm&oit=1&cp=5&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/zepto.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen%3ECOM&oit=4&cp=11&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://e2c27.gcp.gvt2.com/nel/	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/weui.css	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/iconfont.css	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdt&oit=1&cp=4&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/jquery.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen&oit=1&cp=7&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/es-es.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/password_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=u&oit=1&cp=1&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://usdtmen.com/image/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://beacons.gvt2.com/domainreliability/upload	false	• URL Reputation: safe	unknown
http://https://usdtmen.com/image/common.js	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/ko.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmen%3EC&oit=4&cp=9&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=USD&oit=1&cp=3&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=&oit=0&gs_rn=42&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=us&oit=1&cp=2&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtme&oit=1&cp=6&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://usdtmen.com/image/username_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/bootstrap.min.css.map	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/logo.cba20b1b.png	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtmeN&oit=1&cp=7&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/ar-ae.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=US&oit=1&cp=2&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://usdtmen.com/image/pt-pt.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/en-us.jpg	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=104.0.5112.102&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://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=USDTM&oit=1&cp=5&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=wusdtmen.com&oit=3&cp=1&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://usdtmen.com/	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=usdtme%3C&oit=4&cp=7&gs_rn=42&psi=qRYiebaDLQ80oWIb&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
154.211.96.136	usdtmen.com	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	false
142.250.185.132	unknown	United States		15169	GOOGLEUS	false
142.250.186.109	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
35.227.159.135	e2c27.gcp.gvt2.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.13.227	beacons2.gvt2.com	United States		15169	GOOGLEUS	false
142.251.143.67	beacons-handoff.gcp.gvt2.com	United States		15169	GOOGLEUS	false
216.58.212.163	beacons.gvt2.com	United States		15169	GOOGLEUS	false
172.217.18.100	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756095
Start date and time:	2022-11-29 16:31:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://https://usdtmen.com
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	11
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@46/0@26/12
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): SIHClient.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe, WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 216.58.212.131, 34.104.35.123, 142.250.185.78, 142.250.185.227, 142.250.186.74, 142.250.181.234, 172.217.18.106, 142.250.186.138, 142.250.184.202, 172.217.23.106, 142.250.185.170, 142.250.186.106, 142.250.185.234, 172.217.16.202, 142.250.185.202, 172.217.18.10, 142.250.186.42, 142.250.186.170, 142.250.74.202, 216.58.212.138
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, slscr.update.microsoft.com, encrypted-tbn0.gstatic.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.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

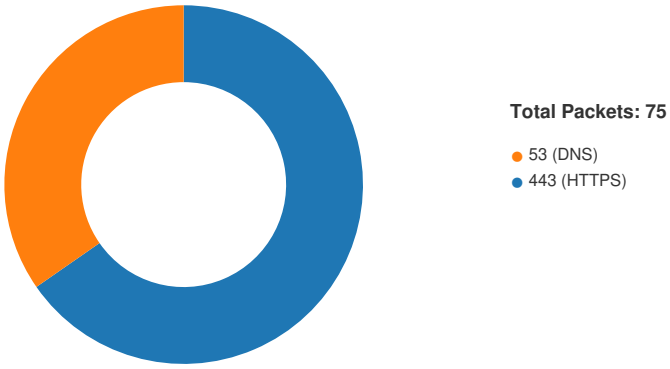
No created / dropped files found

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 16:32:24.708003044 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.708069086 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.708170891 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.709017038 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:24.709076881 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:24.709172010 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:24.710900068 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.710937023 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.711082935 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:24.711122036 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:24.807111025 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.807537079 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.807569027 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.808891058 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.809051991 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.811466932 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:24.812520027 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:24.812593937 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:24.812896013 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:24.812937021 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:24.814241886 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:24.814347982 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:24.864588976 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.864680052 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:24.864778042 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.868828058 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.868891954 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:24.869621038 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.869697094 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:24.869796991 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.870282888 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:24.870317936 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.112036943 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.112126112 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.112443924 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.112585068 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:25.112657070 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.112723112 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.112760067 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.112907887 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.113239050 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:25.113274097 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.141805887 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.142009974 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:25.142059088 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.142101049 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.142169952 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:25.153376102 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.155416965 CET	49694	443	192.168.2.3	142.250.185.206
Nov 29, 2022 16:32:25.155456066 CET	443	49694	142.250.185.206	192.168.2.3
Nov 29, 2022 16:32:25.162925005 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.163044930 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.163091898 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.163386106 CET	443	49695	142.250.186.109	192.168.2.3
Nov 29, 2022 16:32:25.163472891 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.164813995 CET	49695	443	192.168.2.3	142.250.186.109
Nov 29, 2022 16:32:25.164843082 CET	443	49695	142.250.186.109	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:32:25.611713886 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.612323999 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:25.612380981 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.613661051 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.613925934 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:25.625515938 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:25.625571966 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.625761032 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:25.625778913 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.625838041 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.666445017 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:25.666507959 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:25.766500950 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.333307028 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.333479881 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.333652973 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.334096909 CET	49696	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.334134102 CET	443	49696	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.625600100 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.637968063 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.638020992 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.640913963 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.641068935 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.651804924 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.651832104 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.652049065 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.652206898 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:26.652234077 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:26.767512083 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.743208885 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:27.743351936 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:27.743583918 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.799185038 CET	49697	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.799241066 CET	443	49697	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:27.803515911 CET	49699	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.803599119 CET	443	49699	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:27.803699017 CET	49699	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.804119110 CET	49699	443	192.168.2.3	154.211.96.136
Nov 29, 2022 16:32:27.804153919 CET	443	49699	154.211.96.136	192.168.2.3
Nov 29, 2022 16:32:28.408863068 CET	49703	443	192.168.2.3	142.250.185.132
Nov 29, 2022 16:32:28.408904076 CET	443	49703	142.250.185.132	192.168.2.3
Nov 29, 2022 16:32:28.408998013 CET	49703	443	192.168.2.3	142.250.185.132
Nov 29, 2022 16:32:28.409378052 CET	49703	443	192.168.2.3	142.250.185.132

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:32:24.675823927 CET	62586	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:32:24.676929951 CET	64208	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:32:24.677033901 CET	49405	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:32:24.694432974 CET	53	62586	1.1.1.1	192.168.2.3
Nov 29, 2022 16:32:24.695607901 CET	53	49405	1.1.1.1	192.168.2.3
Nov 29, 2022 16:32:24.850765944 CET	53	64208	1.1.1.1	192.168.2.3
Nov 29, 2022 16:32:28.347985029 CET	58968	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:32:28.365712881 CET	53	58968	1.1.1.1	192.168.2.3
Nov 29, 2022 16:32:28.383533955 CET	60752	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:32:28.401398897 CET	53	60752	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:07.758765936 CET	49753	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:08.083023071 CET	53	49753	1.1.1.1	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:33:08.126359940 CET	53744	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:08.147835970 CET	53	53744	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:09.346384048 CET	54957	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:09.405230045 CET	53	54957	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:11.070312023 CET	62677	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:11.638418913 CET	53	62677	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:14.836524010 CET	62507	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:14.893490076 CET	53	62507	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:19.956929922 CET	57517	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:20.132723093 CET	53	57517	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:23.238204956 CET	64040	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:23.407876968 CET	53	64040	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:23.476464033 CET	55241	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:23.646177053 CET	53	55241	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:24.804167032 CET	52387	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:24.834027052 CET	53	52387	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:28.402385950 CET	51807	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:28.420521021 CET	53	51807	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:28.424760103 CET	60310	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:28.442527056 CET	53	60310	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:29.899596930 CET	57646	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:29.962117910 CET	53	57646	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:33.938812017 CET	54880	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:34.335639954 CET	53	54880	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:36.911083937 CET	62304	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:37.082370996 CET	53	62304	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:50.214030027 CET	61115	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:50.270365000 CET	53	61115	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:55.175709009 CET	49243	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:55.193550110 CET	53	49243	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:55.353043079 CET	59424	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:55.353043079 CET	63769	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:55.372543097 CET	53	59424	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:55.372581959 CET	53	63769	1.1.1.1	192.168.2.3
Nov 29, 2022 16:33:56.519668102 CET	63858	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:33:56.537300110 CET	53	63858	1.1.1.1	192.168.2.3
Nov 29, 2022 16:34:00.010442972 CET	60408	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:34:00.185385942 CET	53	60408	1.1.1.1	192.168.2.3
Nov 29, 2022 16:34:03.454722881 CET	50401	53	192.168.2.3	1.1.1.1
Nov 29, 2022 16:34:03.479424953 CET	53	50401	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:32:24.675823927 CET	192.168.2.3	1.1.1.1	0x1946	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:24.676929951 CET	192.168.2.3	1.1.1.1	0x308e	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:24.677033901 CET	192.168.2.3	1.1.1.1	0x1a2e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:28.347985029 CET	192.168.2.3	1.1.1.1	0xd789	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:28.383533955 CET	192.168.2.3	1.1.1.1	0x9f1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:07.758765936 CET	192.168.2.3	1.1.1.1	0x3fc2	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:08.126359940 CET	192.168.2.3	1.1.1.1	0xce86	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:09.346384048 CET	192.168.2.3	1.1.1.1	0x6284	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:11.070312023 CET	192.168.2.3	1.1.1.1	0xda2d	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:33:14.836524010 CET	192.168.2.3	1.1.1.1	0x3a39	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:19.956929922 CET	192.168.2.3	1.1.1.1	0xf446	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:23.238204956 CET	192.168.2.3	1.1.1.1	0x2445	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:23.476464033 CET	192.168.2.3	1.1.1.1	0xd13	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:24.804167032 CET	192.168.2.3	1.1.1.1	0x6d02	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:28.402385950 CET	192.168.2.3	1.1.1.1	0xab35	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:28.424760103 CET	192.168.2.3	1.1.1.1	0xc80a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:29.899596930 CET	192.168.2.3	1.1.1.1	0x2ce1	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:33.938812017 CET	192.168.2.3	1.1.1.1	0x380d	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:36.911083937 CET	192.168.2.3	1.1.1.1	0xae51	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:50.214030027 CET	192.168.2.3	1.1.1.1	0xce88	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.175709009 CET	192.168.2.3	1.1.1.1	0x6e2f	Standard query (0)	beacons.gcp.gvt2.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.353043079 CET	192.168.2.3	1.1.1.1	0x3170	Standard query (0)	e2c27.gcp.gvt2.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.353043079 CET	192.168.2.3	1.1.1.1	0x279b	Standard query (0)	beacons2.gvt2.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:56.519668102 CET	192.168.2.3	1.1.1.1	0xb794	Standard query (0)	beacons.gvt2.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:00.010442972 CET	192.168.2.3	1.1.1.1	0xc869	Standard query (0)	www.usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:03.454722881 CET	192.168.2.3	1.1.1.1	0x81d6	Standard query (0)	usdtmen.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 16:32:24.694432974 CET	1.1.1.1	192.168.2.3	0x1946	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:32:24.694432974 CET	1.1.1.1	192.168.2.3	0x1946	No error (0)	clients.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:24.695607901 CET	1.1.1.1	192.168.2.3	0x1a2e	No error (0)	accounts.google.com		142.250.186.109	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:24.850765944 CET	1.1.1.1	192.168.2.3	0x308e	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:28.365712881 CET	1.1.1.1	192.168.2.3	0xd789	No error (0)	www.google.com		142.250.186.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:32:28.401398897 CET	1.1.1.1	192.168.2.3	0x9f1	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:28.420521021 CET	1.1.1.1	192.168.2.3	0xab35	No error (0)	www.google.com		142.250.186.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:28.442527056 CET	1.1.1.1	192.168.2.3	0xc80a	No error (0)	www.google.com		172.217.18.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:34.335639954 CET	1.1.1.1	192.168.2.3	0x380d	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:37.082370996 CET	1.1.1.1	192.168.2.3	0xae51	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.193550110 CET	1.1.1.1	192.168.2.3	0x6e2f	No error (0)	beacons.gcp.gvt2.com	beacons-handoff.gcp.gvt2.com		CNAME (Canonical name)	IN (0x0001)	false

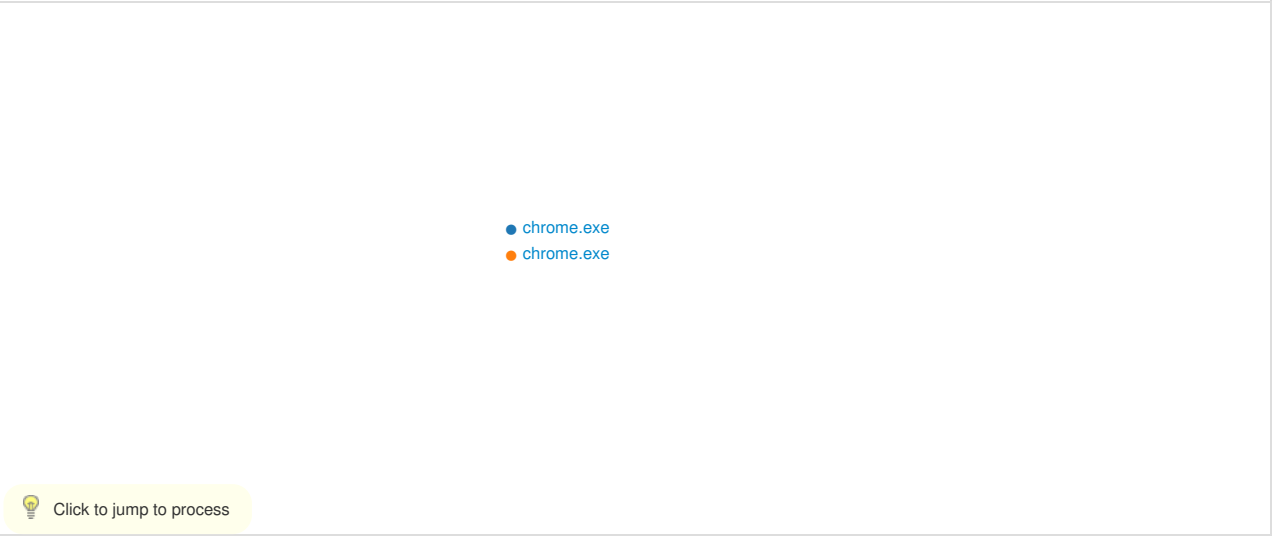
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:33:55.193550110 CET	1.1.1.1	192.168.2.3	0x6e2f	No error (0)	beacons-handoff.gcp.gvt2.com		142.251.143.67	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.372543097 CET	1.1.1.1	192.168.2.3	0x3170	No error (0)	e2c27.gcp.gvt2.com		35.227.159.135	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:55.372581959 CET	1.1.1.1	192.168.2.3	0x279b	No error (0)	beacons2.gvt2.com		172.217.13.227	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:33:56.537300110 CET	1.1.1.1	192.168.2.3	0xb794	No error (0)	beacons.gvt2.com		216.58.212.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:03.479424953 CET	1.1.1.1	192.168.2.3	0x81d6	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- usdtmen.com
- www.google.com
- https:
- beacons.gcp.gvt2.com
- e2c27.gcp.gvt2.com
- beacons2.gvt2.com
- beacons.gvt2.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **3188**, Parent PID: **2540**

General

Target ID:	0
Start time:	16:32:21
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 --single-argument https://usdtmen.com/
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: **6160**, Parent PID: **3188**

General

Target ID:	1
Start time:	16:32:22
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=2040 --field-trial-handle=1768,i,5818765958052219750,8192306715576805166,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Disassembly

No disassembly