ID: 756100
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 16:34:35
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

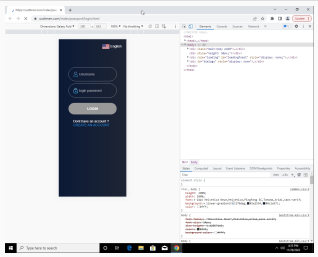
Windows Analysis Report

https://usdtmen.com

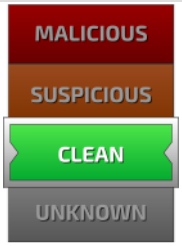
Overview

General Information

Sample URL:	http://https://usdtmen.com
Analysis ID:	756100
Infos:	



Detection

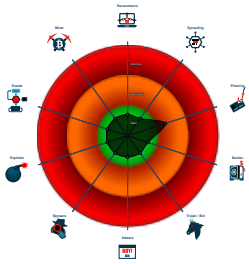


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of ...
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 7140 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://usdtmen.com/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 3268 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=1776,i,2961118636078509660,12337485403736736407,131072 --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

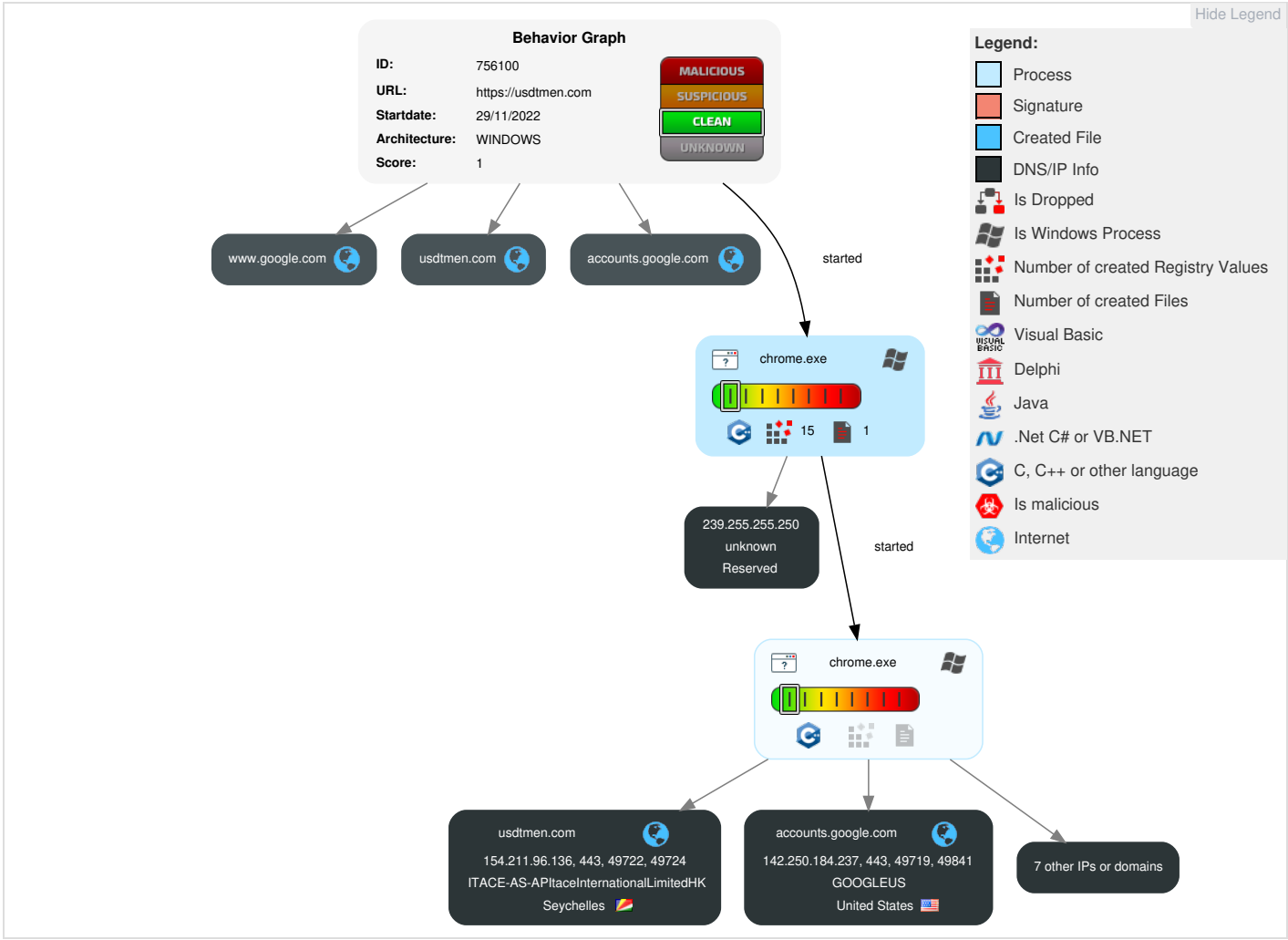
Joe Sandbox Signatures

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

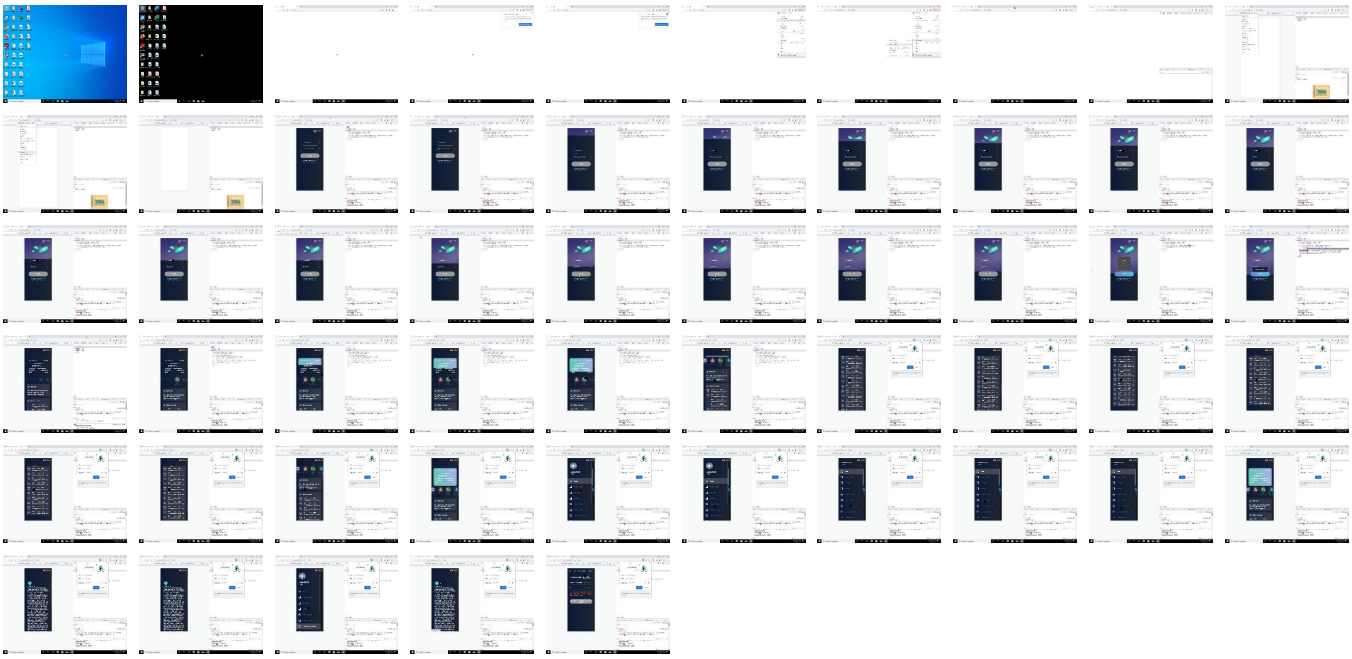
Behavior Graph

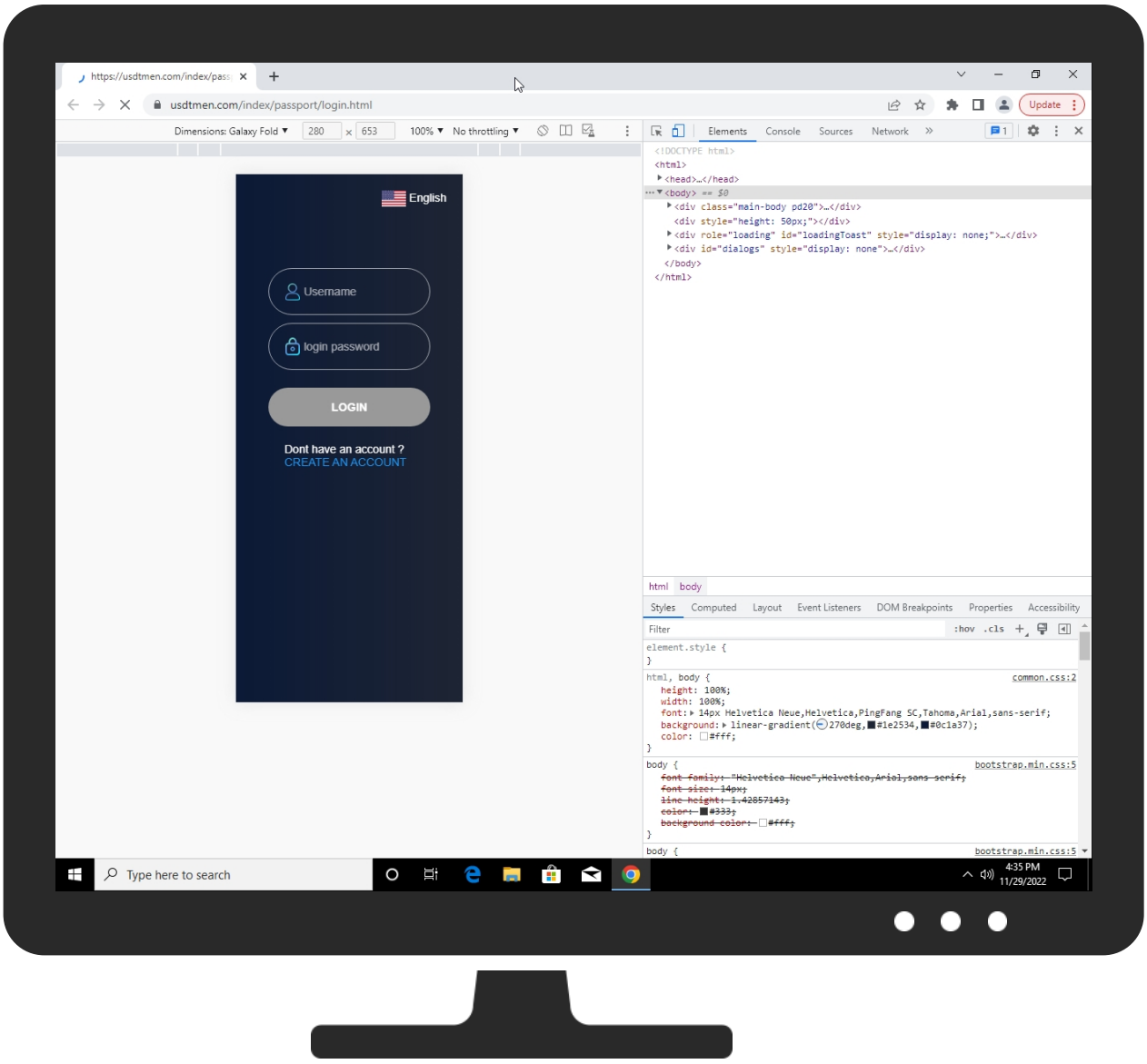


Screenshots

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://usdtmen.com/layer3.1/layer.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav1.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://usdtmen.com/image/fr.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/bg1.6c9f941a.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/records1.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/index/passport/logout.html	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/portrait.jpeg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/weui.min.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/viplevel_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/withdraw_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav2.png	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://usdtmen.com/image/records2.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav3.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/common.css	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/menu.png	0%	Avira URL Cloud	safe	
http://https://beacons2.gvt2.com/domainreliability/upload-nel	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/zepto.min.js	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav4.png	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/nav5.png	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/transfer_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/head.b8e5d31e.png	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/card.8c0955e2.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/deposit_icon.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav6.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/icons8-tether-48.png	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/nav7.png	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://https://usdtmen.com/image/pt-pt.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav9.png	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/en-us.jpg	0%	Avira URL Cloud	safe	
http://https://usdtmen.com/image/nav8.png	0%	Avira URL Cloud	safe	

Domains and IPs

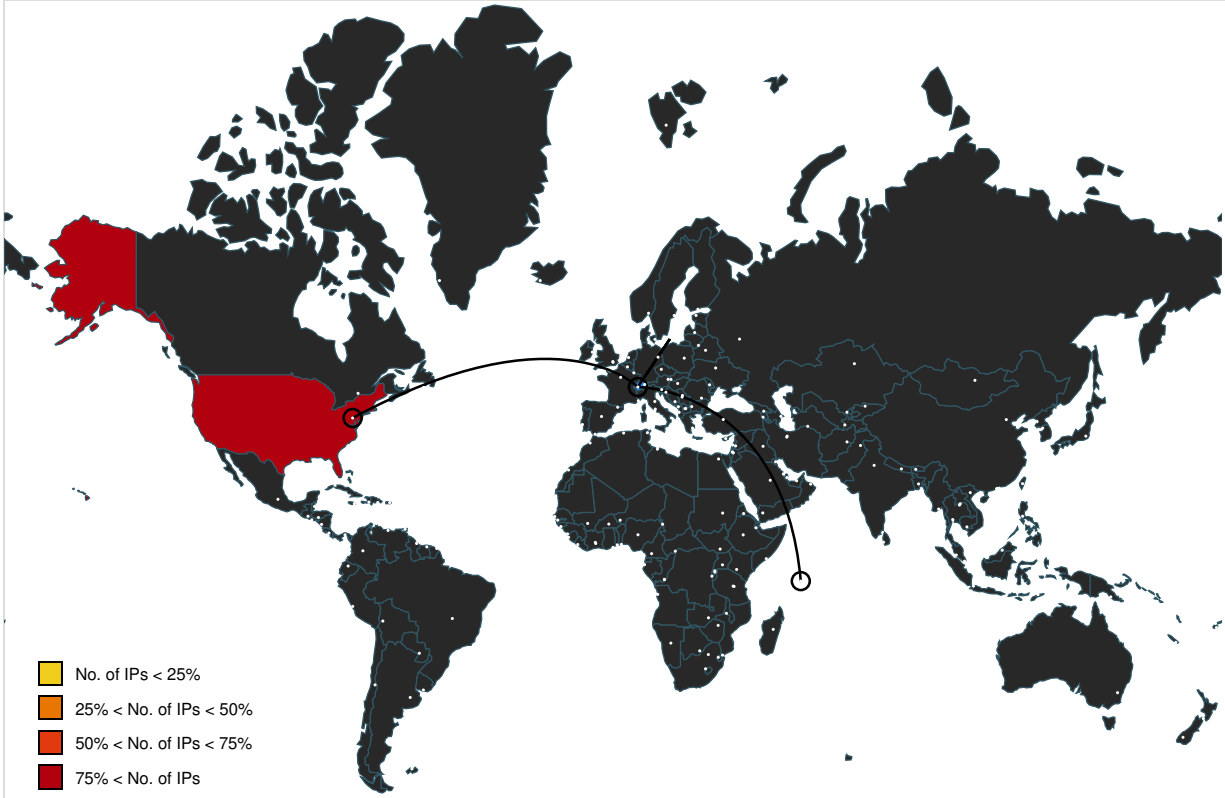
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.237	true	false		high
usdtmen.com	154.211.96.136	true	false		unknown
www.google.com	142.250.185.132	true	false		high
beacons2.gvt2.com	216.239.38.117	true	false		unknown
clients.l.google.com	142.250.186.110	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://usdtmen.com/index/order/index.html	false		unknown
http://https://usdtmen.com/layer3.1/layer.js	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/index/index.html	false		unknown
http://https://usdtmen.com/index/news/about.html	false		unknown
http://https://usdtmen.com/image/nav1.png	false	• Avira URL Cloud: 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://usdtmen.com/image/records1.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/passport/logout.html	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/portrait.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/weui.min.js	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/viplevel_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/withdraw_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/nav2.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/layer3.1/theme/default/layer.css?v=3.1.1	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/records2.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/passport/login.html	false		unknown
http://https://usdtmen.com/image/nav3.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/common.css	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/menu.png	false	• Avira URL Cloud: safe	unknown
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://usdtmen.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/zepto.min.js	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/nav4.png	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://usdtmen.com/image/nav5.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/jquery.min.js	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/es-es.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/transfer_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/password_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://usdtmen.com/image/head.b8e5d31e.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/card.8c0955e2.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/deposit_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/nav6.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/icons8-tether-48.png	false	• Avira URL Cloud: 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://usdtmen.com/image/username_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/index/index.html	false		unknown
http://https://usdtmen.com/image/bootstrap.min.css.map	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/news/about.html	false		unknown
http://https://accounts.google.com/domainreliability/upload	false		high
http://https://usdtmen.com/image/nav7.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/logo.cba20b1b.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/ar-ae.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/pt-pt.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/index/order/index.html	false		unknown
http://https://usdtmen.com/image/nav9.png	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/en-us.jpg	false	• Avira URL Cloud: safe	unknown
http://https://usdtmen.com/image/nav8.png	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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.211.96.136	usdtmen.com	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	false
142.250.185.100	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.16.196	unknown	United States		15169	GOOGLEUS	false
216.239.38.117	beacons2.gvt2.com	United States		15169	GOOGLEUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756100
Start date and time:	2022-11-29 16:34:35 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
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:	7
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:	clean1.win@28/0@15/8
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): RuntimeBroker.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.186.67, 34.104.35.123, 142.250.186.138, 172.217.18.10, 142.250.185.234, 142.250.185.138, 142.250.181.234, 172.217.16.202, 142.250.185.202, 216.58.212.138, 142.250.185.106, 172.217.16.138, 142.250.184.234, 142.250.185.74, 142.250.184.202, 142.250.186.42, 142.250.186.170, 142.250.185.170, 142.250.185.227, 142.250.186.106, 172.217.18.106, 142.250.74.202, 142.250.186.74, 216.58.212.170
- Excluded domains from analysis (whitelisted): client.wns.windows.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, slscr.update.microsoft.com, update.googleapis.com, clientservices.googleapis.com, cdn.onenote.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

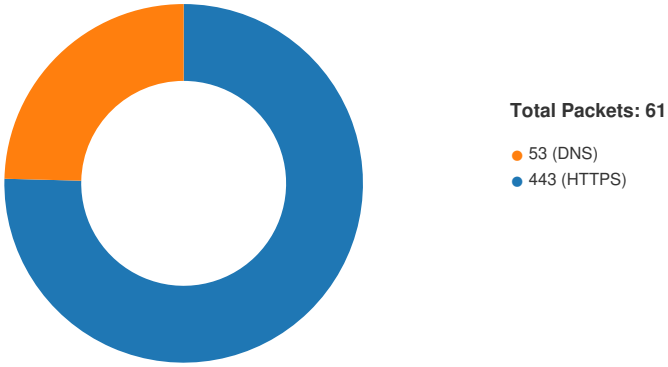
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:35:08.933305025 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:08.933347940 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:08.933442116 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:08.933768034 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:08.933856010 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:08.933995008 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:08.934210062 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:08.934231043 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:08.935841084 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:08.935878038 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.023745060 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.023804903 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.023932934 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.024252892 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.024288893 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.048182011 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.056142092 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.056159973 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.057837009 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.057976007 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.065637112 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.072374105 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.072432041 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.072983027 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.073096037 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.074866056 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.074960947 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.357707024 CET	49720	443	192.168.2.2	142.250.186.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:35:09.357788086 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.357827902 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.357842922 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.358078957 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.358206034 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.358263016 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.358475924 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.358495951 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.358618975 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.393388987 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.393544912 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.393601894 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.393650055 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.393717051 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.394799948 CET	49720	443	192.168.2.2	142.250.186.110
Nov 29, 2022 16:35:09.394829988 CET	443	49720	142.250.186.110	192.168.2.2
Nov 29, 2022 16:35:09.398066998 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.398101091 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.405095100 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.405164957 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.405186892 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.405414104 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.405481100 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.407345057 CET	49719	443	192.168.2.2	142.250.184.237
Nov 29, 2022 16:35:09.407375097 CET	443	49719	142.250.184.237	192.168.2.2
Nov 29, 2022 16:35:09.803222895 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.803695917 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.803733110 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.805032015 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.805135012 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.807235956 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.807254076 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.807353973 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.807840109 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:09.807868004 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:09.847151041 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.530600071 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:10.530754089 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:10.530853033 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.531311035 CET	49722	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.531347036 CET	443	49722	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:10.535629034 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.535711050 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:10.535847902 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.536159992 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:10.536194086 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.066715002 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.066766024 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.066839933 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.067223072 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.067240000 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.130240917 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.130584002 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.130609989 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.131877899 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.131947041 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.134362936 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.134380102 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.134484053 CET	443	49726	172.217.16.196	192.168.2.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:35:12.174340963 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.174376011 CET	443	49726	172.217.16.196	192.168.2.2
Nov 29, 2022 16:35:12.214277983 CET	49726	443	192.168.2.2	172.217.16.196
Nov 29, 2022 16:35:12.652659893 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.655206919 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:12.655265093 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.655854940 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.683619022 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:12.683653116 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.683898926 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:12.684128046 CET	49724	443	192.168.2.2	154.211.96.136
Nov 29, 2022 16:35:12.684144020 CET	443	49724	154.211.96.136	192.168.2.2
Nov 29, 2022 16:35:13.461122036 CET	443	49724	154.211.96.136	192.168.2.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:35:08.845860958 CET	56437	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:08.849659920 CET	59170	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:08.852261066 CET	60174	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:08.867503881 CET	53	59170	1.1.1.1	192.168.2.2
Nov 29, 2022 16:35:08.870886087 CET	53	60174	1.1.1.1	192.168.2.2
Nov 29, 2022 16:35:09.022564888 CET	53	56437	1.1.1.1	192.168.2.2
Nov 29, 2022 16:35:11.992185116 CET	65009	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:12.010351896 CET	53	65009	1.1.1.1	192.168.2.2
Nov 29, 2022 16:35:12.015737057 CET	60372	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:12.039489985 CET	53	60372	1.1.1.1	192.168.2.2
Nov 29, 2022 16:35:38.380709887 CET	59744	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:35:38.401396036 CET	53	59744	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:09.737880945 CET	64258	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:10.133202076 CET	53	64258	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:10.142847061 CET	53102	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:10.161789894 CET	53	53102	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:10.282659054 CET	53970	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:10.300344944 CET	53	53970	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:11.673815012 CET	60366	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:11.844702959 CET	53	60366	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:12.050575018 CET	62288	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:12.070384026 CET	53	62288	1.1.1.1	192.168.2.2
Nov 29, 2022 16:36:12.074632883 CET	53555	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:36:12.092705011 CET	53	53555	1.1.1.1	192.168.2.2
Nov 29, 2022 16:37:10.435528040 CET	63859	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:37:10.455703974 CET	53	63859	1.1.1.1	192.168.2.2
Nov 29, 2022 16:37:12.099045992 CET	51860	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:37:12.117491961 CET	53	51860	1.1.1.1	192.168.2.2
Nov 29, 2022 16:37:12.119719982 CET	52090	53	192.168.2.2	1.1.1.1
Nov 29, 2022 16:37:12.138839960 CET	53	52090	1.1.1.1	192.168.2.2

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:35:08.845860958 CET	192.168.2.2	1.1.1.1	0xc52d	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:08.849659920 CET	192.168.2.2	1.1.1.1	0xa4b2	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:08.852261066 CET	192.168.2.2	1.1.1.1	0xca57	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:11.992185116 CET	192.168.2.2	1.1.1.1	0x6cc9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:12.015737057 CET	192.168.2.2	1.1.1.1	0xcf24	Standard query (0)	www.google.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 16:35:38.380709887 CET	192.168.2.2	1.1.1.1	0x28c5	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:09.737880945 CET	192.168.2.2	1.1.1.1	0x927d	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.142847061 CET	192.168.2.2	1.1.1.1	0x4fdd	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.282659054 CET	192.168.2.2	1.1.1.1	0x1ec8	Standard query (0)	beacons2.gvt2.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:11.673815012 CET	192.168.2.2	1.1.1.1	0x963d	Standard query (0)	usdtmen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:12.050575018 CET	192.168.2.2	1.1.1.1	0x8bdd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:12.074632883 CET	192.168.2.2	1.1.1.1	0x25e6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:10.435528040 CET	192.168.2.2	1.1.1.1	0x59a3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:12.099045992 CET	192.168.2.2	1.1.1.1	0x7e09	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:12.119719982 CET	192.168.2.2	1.1.1.1	0x805c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:35:08.867503881 CET	1.1.1.1	192.168.2.2	0xa4b2	No error (0)	accounts.google.com		142.250.184.237	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:08.870886087 CET	1.1.1.1	192.168.2.2	0xca57	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:35:08.870886087 CET	1.1.1.1	192.168.2.2	0xca57	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:09.022564888 CET	1.1.1.1	192.168.2.2	0xc52d	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:12.010351896 CET	1.1.1.1	192.168.2.2	0x6cc9	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:12.039489985 CET	1.1.1.1	192.168.2.2	0xcf24	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:35:38.401396036 CET	1.1.1.1	192.168.2.2	0x28c5	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.133202076 CET	1.1.1.1	192.168.2.2	0x927d	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.161789894 CET	1.1.1.1	192.168.2.2	0x4fdd	No error (0)	accounts.google.com		142.250.184.237	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.300344944 CET	1.1.1.1	192.168.2.2	0x1ec8	No error (0)	beacons2.gvt2.com		216.239.38.117	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.300344944 CET	1.1.1.1	192.168.2.2	0x1ec8	No error (0)	beacons2.gvt2.com		216.239.32.117	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.300344944 CET	1.1.1.1	192.168.2.2	0x1ec8	No error (0)	beacons2.gvt2.com		216.239.34.117	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:10.300344944 CET	1.1.1.1	192.168.2.2	0x1ec8	No error (0)	beacons2.gvt2.com		216.239.36.117	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:11.844702959 CET	1.1.1.1	192.168.2.2	0x963d	No error (0)	usdtmen.com		154.211.96.136	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:12.070384026 CET	1.1.1.1	192.168.2.2	0x8bdd	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:36:12.092705011 CET	1.1.1.1	192.168.2.2	0x25e6	No error (0)	www.google.com		142.250.185.100	A (IP address)	IN (0x0001)	false

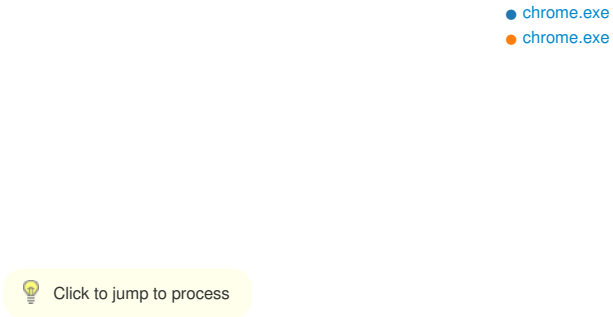
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:37:10.455703974 CET	1.1.1.1	192.168.2.2	0x59a3	No error (0)	accounts.google.com		142.250.186.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:12.117491961 CET	1.1.1.1	192.168.2.2	0x7e09	No error (0)	www.google.com		172.217.18.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:37:12.138839960 CET	1.1.1.1	192.168.2.2	0x805c	No error (0)	www.google.com		172.217.16.132	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- usdtmen.com
- https:
- beacons2.gvt2.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 7140, Parent PID: 6700

General

Target ID:	0
Start time:	16:35:04
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:	0x7ff600460000

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: **3268**, Parent PID: **7140**

General

Target ID:	1
Start time:	16:35:06
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=1776,i,2961118636078509660,12337485403736736407,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff600460000
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