ID: 1485878
Cookbook: urldownload.jbs
Time: 09:20:50
Date: 01/08/2024
Version: 40.0.0 Tourmaline

Table of Contents

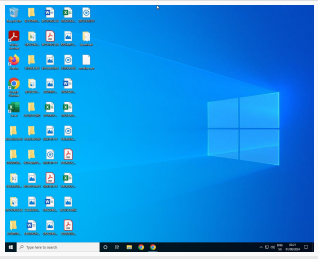
Windows Analysis Report

https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c124171768917...

Overview

General Information

Sample URL:	http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Analysis ID:	1485878
Infos:	



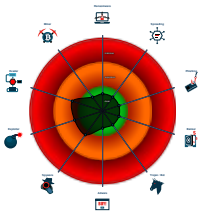
Detection

Score:	23
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Sigma detected: WScript or CScript…
- Found WSH timer for Javascript or V…
- Queries the volume information (nam…
- Sample execution stops while proce…
- Sigma detected: Usage Of Web Req…
- Sigma detected: WSF/JSE/JS/VBA…
- Very long cmdline option found, this…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 5456 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c124171768917 6015" > cmdline.out 2>&1 MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - conhost.exe (PID: 5352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - wget.exe (PID: 7128 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- wscript.exe (PID: 4428 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\download\vcd15cbe7772f49c399c6a5babf22c1241717689176015.js" MD5: A47CBE969EA935BDD3AB568BB126BC80)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

System Summary

Sigma detected: WScript or CScript Dropper

Sigma detected: Usage Of Web Request Commands And Cmdlets

Sigma detected: WSF/JSE/JS/VBA/VBE File Execution Via Cscript/Wscript

Snort Signatures

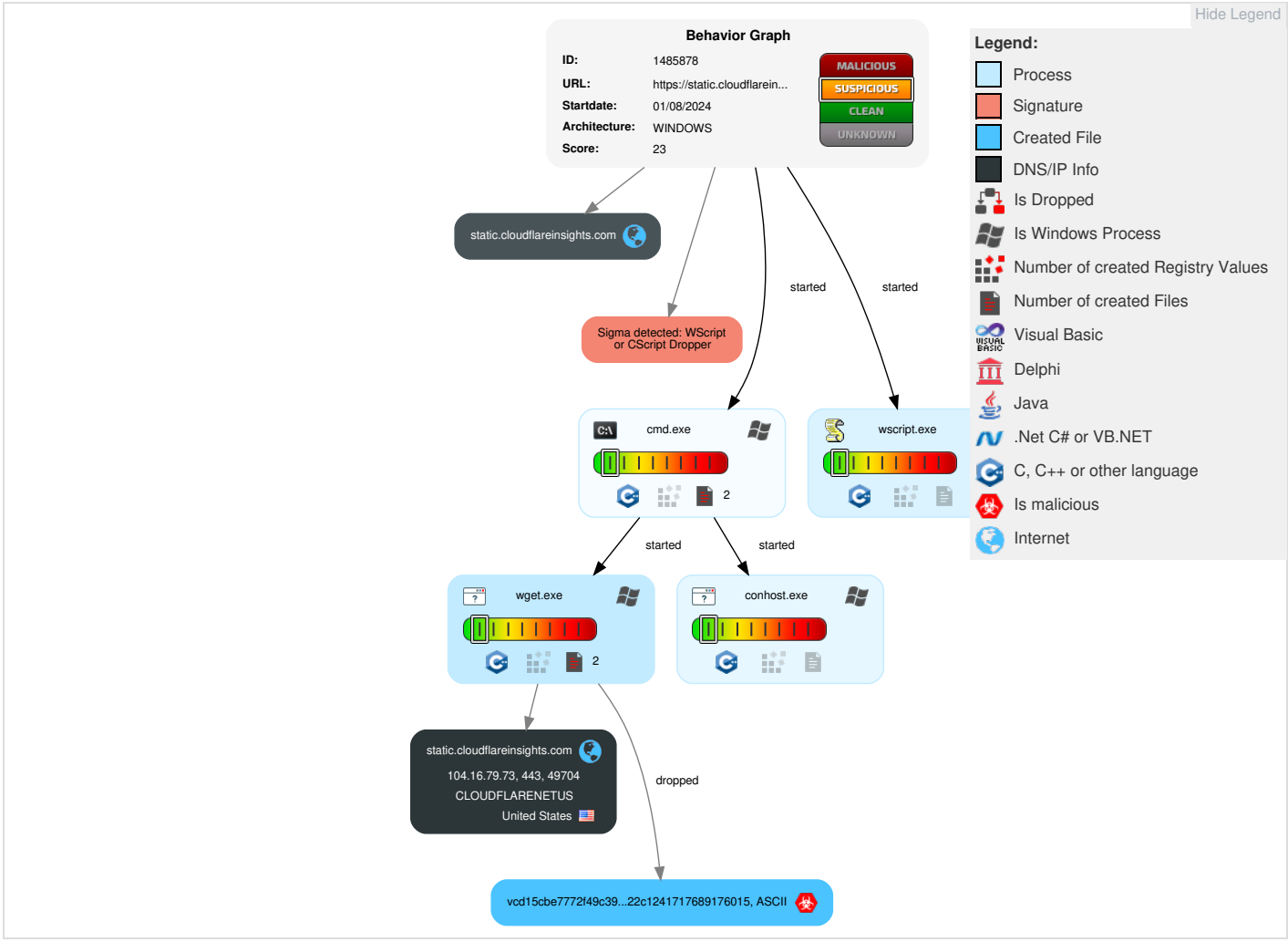
No Snort rule has matched

Joe Sandbox Signatures

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	1 Command and Scripting Interpreter	1 Scripting	1 Process Injection	1 Masqueradi ng	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 DLL Side-Loading	1 Process Injection	LSASS Memory	1 2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	2 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	Query Registry	SMB/Windo ws Admin Shares	Data from Network Shared Drive	3 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuratio n Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

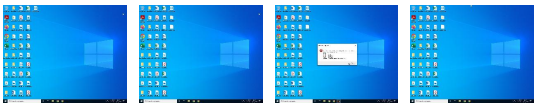
Behavior Graph



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://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c124171768917601 5	0%	URL Reputation	safe	
http:// https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c124171768917601 5	0%	URL Reputation	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c12417176891760 15le	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c12417176891760 15Dr	0%	Avira URL Cloud	safe	
http://https://cloudflareinsights.com/cdn-cgi/rum	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c12417176891760 15p	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5bab	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
static.cloudflareinsights.com	104.16.79.73	true	false		unknown

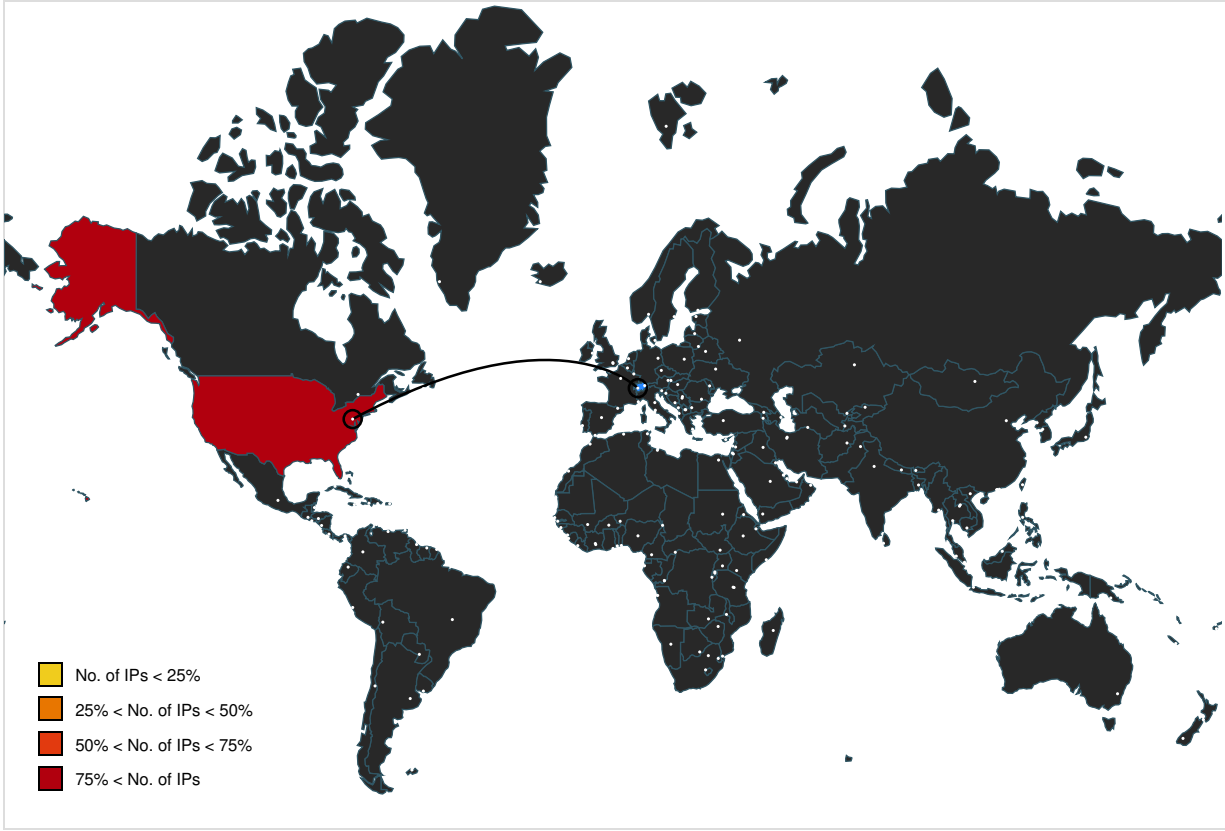
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c12417176891 76015	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.cloudflareinsights.com/beacon.min.js/vcd1 5cbe7772f49c399c6a5babf22c1241717689176015Dr	wget.exe, 00000002.00000002.2011259464.0 000000000A60000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cloudflareinsights.com/cdn-cgi/rum	wscript.exe, 00000004.00000003.202543929 8.00000175AD131000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.cloudflareinsights.com/beacon.min.js/vcd1 5cbe7772f49c399c6a5babf22c1241717689176015le	wget.exe, 00000002.00000002.2011259464.0 000000000A60000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.cloudflareinsights.com/beacon.min.js/vcd1 5cbe7772f49c399c6a5bab	wget.exe, 00000002.00000002.2011342362.0 000000000B48000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.cloudflareinsights.com/beacon.min.js/vcd1 5cbe7772f49c399c6a5babf22c1241717689176015p	wget.exe, 00000002.00000003.2011058625.0 000000002B64000.00000004.00000020.000200 00.00000000.sdmp, wget.exe, 00000002.000 00002.2011452577.0000000002B65000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.79.73	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1485878
Start date and time:	2024-08-01 09:20:50 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 1m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus23.win@5/2@1/1
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- Not all processes where analyzed, report is missing behavior information
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.

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

C:\Users\user\Desktop\cmdline.out

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	740
Entropy (8bit):	5.217996856827452
Encrypted:	false
SSDEEP:	12:HRfBk+hnNT3DUmnh2hDlh2hST1De5RhK3WRi9bV3JRbK3DUmDfBiV3JRbK3DUmu:xfCSB3kxePg3WRYPbSXBQPbSi
MD5:	14AF87B34206E4F708B3BF657EABB7A6
SHA1:	542EBB944A56E6D8F3693C4D5F813B9305893687
SHA-256:	F571C14904F9753491BCA13DC24D27D3BD55A5BF47BA3AD48BDBFD346C05B9F7
SHA-512:	2132DCD26D45615818E48ED7690C28D3F523DBAD7FEA712D3E84586F7BCC2B91145BB3066657C694B5489CCB72C427CFE0371A7BE79900D449C6BCE840C6EEF
Malicious:	false
Reputation:	low

Preview:	--2024-08-01 03:21:37-- https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015..Resolving static.cloudflareinsights.com (static.cloudflareinsights.com)... 104.16.79.73, 104.16.80.73..Connecting to static.cloudflareinsights.com (static.cloudflareinsights.com)|104.16.79.73|:443... connected...HTTP request sent, awaiting response... 200 OK..Length: 19948 (19K) [text/javascript]..Saving to: 'C:/Users/user/Desktop/download/vcd15cbe7772f49c399c6a5babf22c1241717689176015'.... 0K .... 100% 385K=0.05s....2024-08-01 03:21:37 (385 KB/s) - 'C:/Users/user/Desktop/download/vcd15cbe7772f49c399c6a5babf22c1241717689176015' saved [19948/19948]....

C:\Users\user\Desktop\download\vcd15cbe7772f49c399c6a5babf22c1241717689176015

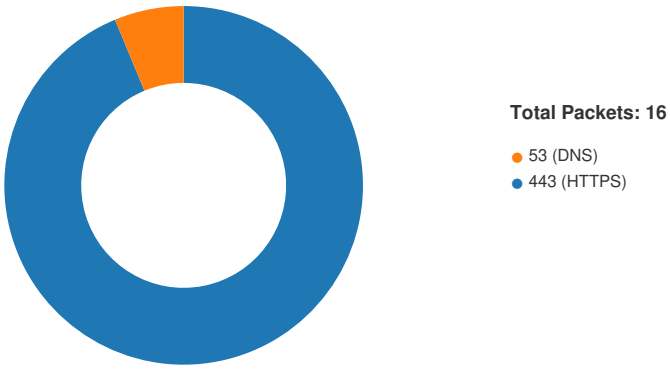
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with very long lines (19948), with no line terminators
Category:	dropped
Size (bytes):	19948
Entropy (8bit):	5.261902742187293
Encrypted:	false
SSDEEP:	384:XriNpnjyMkg8XMtExRN1w29JIOzahXtO2nJ65:GijgSWuanfJ65
MD5:	EC18AF6D41F6F278B6AED3BDABFFA7BC
SHA1:	62C9E2CAB76B888829F3C5335E91C320B22329AE
SHA-256:	8A18D13015336BC184819A5A768447462202EF3105EC511BF42ED8304A7ED94F
SHA-512:	669B0E9A545057ACBDD3B4C8D1D2811EAF4C776F679DA1083E591FF38AE7684467ABACEF5AF3D4AABD9FB7C335692DBCA0DEF63DDAC2CD28D8E14E95680C3511
Malicious:	**true**
Reputation:	low
Preview:	!function(){var e={343:function(e){"use strict";for(var t=[],n=0;n<256;++n)t[n]=(n+256).toString(16).substr(1);e.exports=function(e,n){var r=n||0,i=t;return[i[e[r++]],i[e[r++]],i[e[r++]],i[e[r++]],"-",i[e[r++]],i[e[r++]],"-",i[e[r++]],i[e[r++]],"-",i[e[r++]],i[e[r++]],"-",i[e[r++]],i[e[r++]],i[e[r++]],i[e[r++]],i[e[r++]],i[e[r++]]].join("")}},944:function(e){"use strict";var t="undefined"!=typeof crypto&&crypto.getRandomValues&&crypto.getRandomValues.bind(crypto)||"undefined"!=typeof msCrypto&&"function"==typeof window.msCrypto.getRandomValues&&msCrypto.getRandomValues.bind(msCrypto);if(t){var n=new Uint8Array(16);e.exports=function(){return t(n),n}}else{var r=new Array(16);e.exports=function(){for(var e,t=0;t<16;t++)0==(3&t)&&(e=4294967296*Math.random()),r[t]=e>>>((3&t)<<3)&255;return r}},508:function(e,t,n){"use strict";var r=n(944),i=n(343);e.exports=function(e,t,n){var o=t&&n||0;"string"==typeof e&&(t="binary"===e?new Array(16):null,e=null);var a=(e=e||{}).random||(e.rng||r)();if(

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2024 09:21:37.932367086 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:37.932452917 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:37.932728052 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:37.934487104 CEST	49704	443	192.168.2.5	104.16.79.73

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2024 09:21:37.934523106 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.435611963 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.435810089 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.437731028 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.437751055 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.438106060 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.439141035 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.484503984 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751213074 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751328945 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751393080 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.751413107 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751508951 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751585960 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.751594067 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751677036 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751769066 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751836061 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.751843929 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751895905 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.751903057 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.751979113 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.752051115 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.752058029 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.755826950 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.755918980 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.755938053 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.755949974 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.756091118 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.756097078 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.756242990 CEST	443	49704	104.16.79.73	192.168.2.5
Aug 1, 2024 09:21:38.756517887 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.827277899 CEST	49704	443	192.168.2.5	104.16.79.73
Aug 1, 2024 09:21:38.827305079 CEST	443	49704	104.16.79.73	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2024 09:21:37.918056011 CEST	59359	53	192.168.2.5	1.1.1.1
Aug 1, 2024 09:21:37.927730083 CEST	53	59359	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Aug 1, 2024 09:21:37.918056011 CEST	192.168.2.5	1.1.1.1	0xc577	Standard query (0)	static.cloudflareinsights.com	A (IP address)	IN (0x0001)	false

DNS Answers

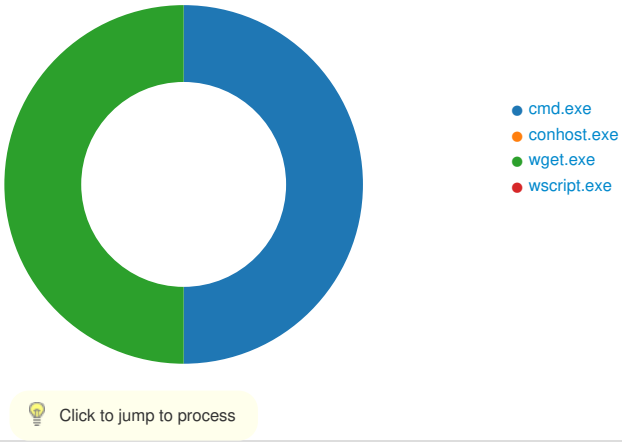
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Aug 1, 2024 09:21:37.927730083 CEST	1.1.1.1	192.168.2.5	0xc577	No error (0)	static.cloudflareinsights.com		104.16.79.73	A (IP address)	IN (0x0001)	false
Aug 1, 2024 09:21:37.927730083 CEST	1.1.1.1	192.168.2.5	0xc577	No error (0)	static.cloudflareinsights.com		104.16.80.73	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- static.cloudflareinsights.com

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **5456**, Parent PID: **5748**

General

Target ID:	0
Start time:	03:21:36
Start date:	01/08/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf2 2c1241717689176015" > cmdline.out 2>&1
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: **5352**, Parent PID: **5456**

General

Target ID:	1
Start time:	03:21:36
Start date:	01/08/2024
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wget.exe PID: 7128, Parent PID: 5456

General

Target ID:	2
Start time:	03:21:37
Start date:	01/08/2024
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015"
Imagebase:	0x400000
File size:	3'895'184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download \vcd15cbe7772f49c399c6a5babf22c1241717689176015	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 4428, Parent PID: 1028

General

Target ID:	4
Start time:	03:21:39
Start date:	01/08/2024
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\download\vcd15cbe7772f49c399c6a5babf22c1241717689176015.js"
Imagebase:	0x7ff62f600000
File size:	170'496 bytes
MD5 hash:	A47CBE969EA935BDD3AB568BB126BC80
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly