ID: 679454
Sample Name: AutoUpdater.js
Cookbook: default.jbs
Time: 20:10:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report AutoUpdater.js 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Memory Dumps 3
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 4
Networking 4
HIPS / PFW / Operating System Protection Evasion 4
Mitre Att&ck Matrix 4
Behavior Graph 5
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
Public IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 10
File Icon 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
UDP Packets 11
DNS Queries 11
DNS Answers 11
HTTP Request Dependency Graph 11
HTTPS Proxied Packets 11
Statistics 12
System Behavior 12
Analysis Process: wscript.exePID: 5700, Parent PID: 3968 12
General 12
File Activities 12
Disassembly 12

Copyright Joe Security LLC 2022

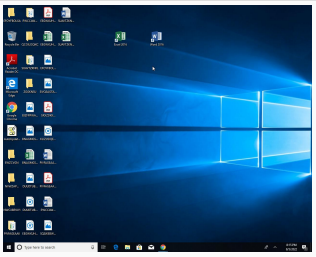
Windows Analysis Report

AutoUpdater.js

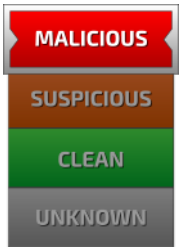
Overview

General Information

Sample Name:	AutoUpdater.js
Analysis ID:	679454
MD5:	c249583badbaef..
SHA1:	6fec191fc99d6d4..
SHA256:	376180cf80a620..
Tags:	js
Infos:	HTTP YARA



Detection

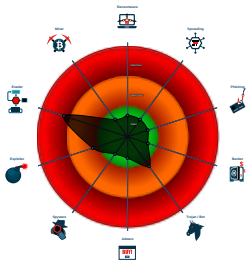


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- JA3 SSL client fingerprint seen in co…
- Yara signature match
- Java / VBScript file with very long s…
- Uses a known web browser user age…
- IP address seen in connection with …
- Found WSH timer for Javascript or V…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5700 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\AutoUpdater.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
Process Memory Space: wscript.exe PID: 5700	apt_CN_Tetris_JS_advanced_1	Unique code from Jetriz, Swid & Jeniva of the Tetris framework	@imp0rtp3 (modified by Florian Roth)	• 0x105b:$b1: a0_0x • 0x1067:$b1: a0_0x • 0x1071:$b1: a0_0x • 0x107b:$b1: a0_0x • 0x1087:$b1: a0_0x • 0x1096:$b1: a0_0x • 0x15d4:$b1: a0_0x • 0x15e4:$b1: a0_0x • 0x15f0:$b1: a0_0x • 0x15fb:$b1: a0_0x • 0x1605:$b1: a0_0x • 0x1611:$b1: a0_0x • 0x161e:$b1: a0_0x • 0x169a:$b1: a0_0x • 0x16a8:$b1: a0_0x • 0x16b4:$b1: a0_0x • 0x16c0:$b1: a0_0x • 0x196f:$b1: a0_0x • 0x19be:$b1: a0_0x • 0x1fee:$b1: a0_0x • 0x2135:$b1: a0_0x

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Networking

System process connects to network (likely due to code injection or exploit)

HIPS / PFW / Operating System Protection Evasion

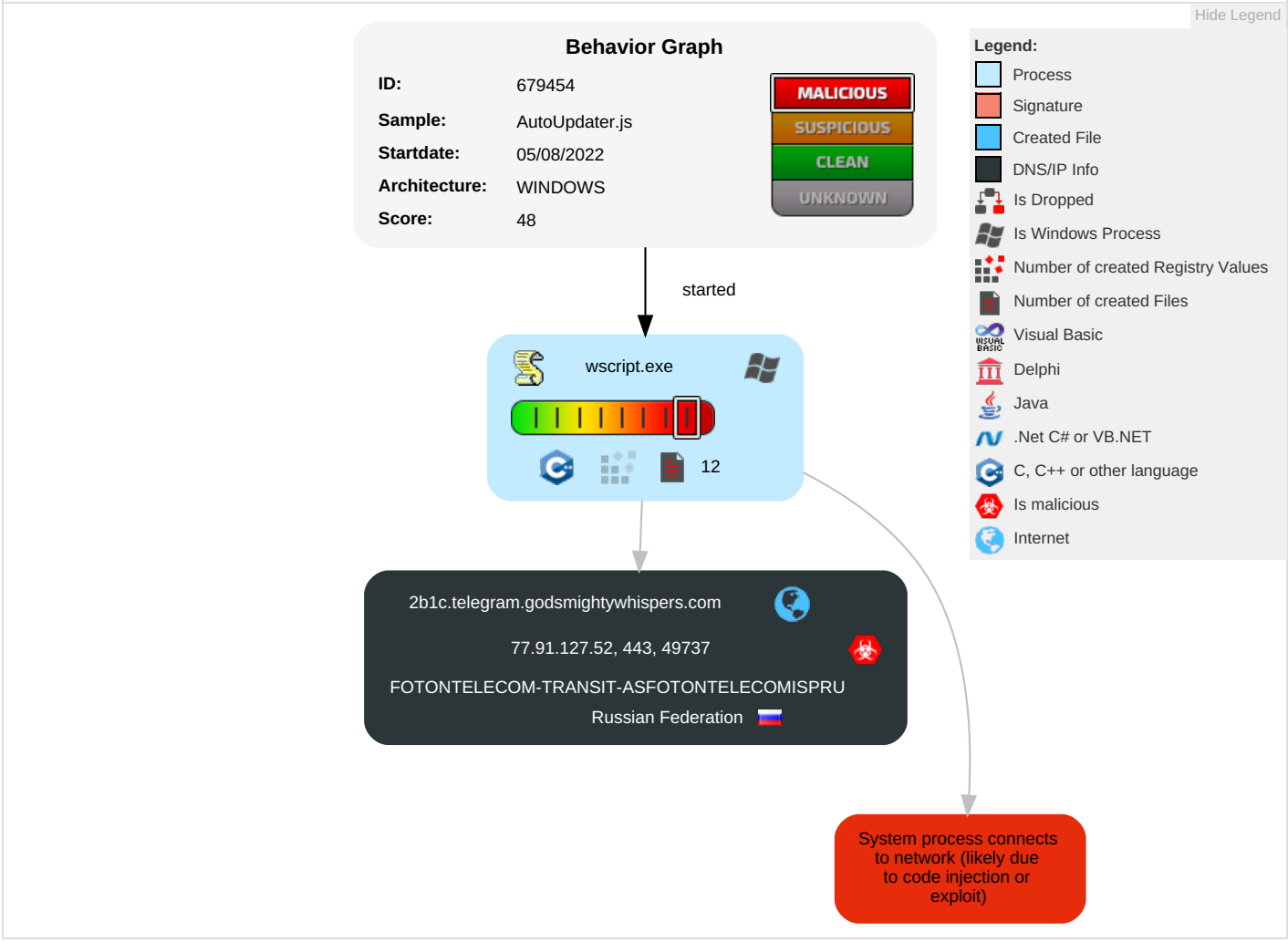
System process connects to network (likely due to code injection or exploit)

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	2 Scripting	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	1 Security Software 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	2 Scripting	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 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)	1 Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Copyright Joe Security LLC 2022

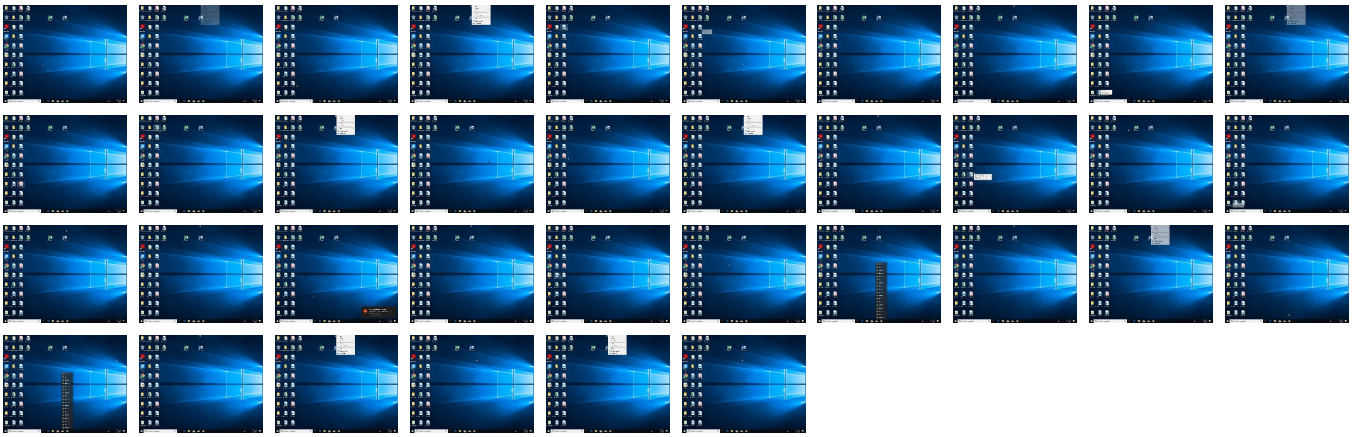
Behavior Graph



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
AutoUpdater.js	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://2b1c.telegram.godsmightywhispers.com/updateResource~	0%	Avira URL Cloud	safe	
http://https://2b1c.telegram.godsmightywhispers.com/updateResource	0%	Avira URL Cloud	safe	
http://https://2b1c.telegram.godsmightywhispers.com/.	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://2b1c.telegram.godsmightywhispers.com/	0%	Avira URL Cloud	safe	
http://https://2b1c.telegram.godsmightywhispers.com/updateResource$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
2b1c.telegram.godsmightywhispers.com	77.91.127.52	true	true		unknown

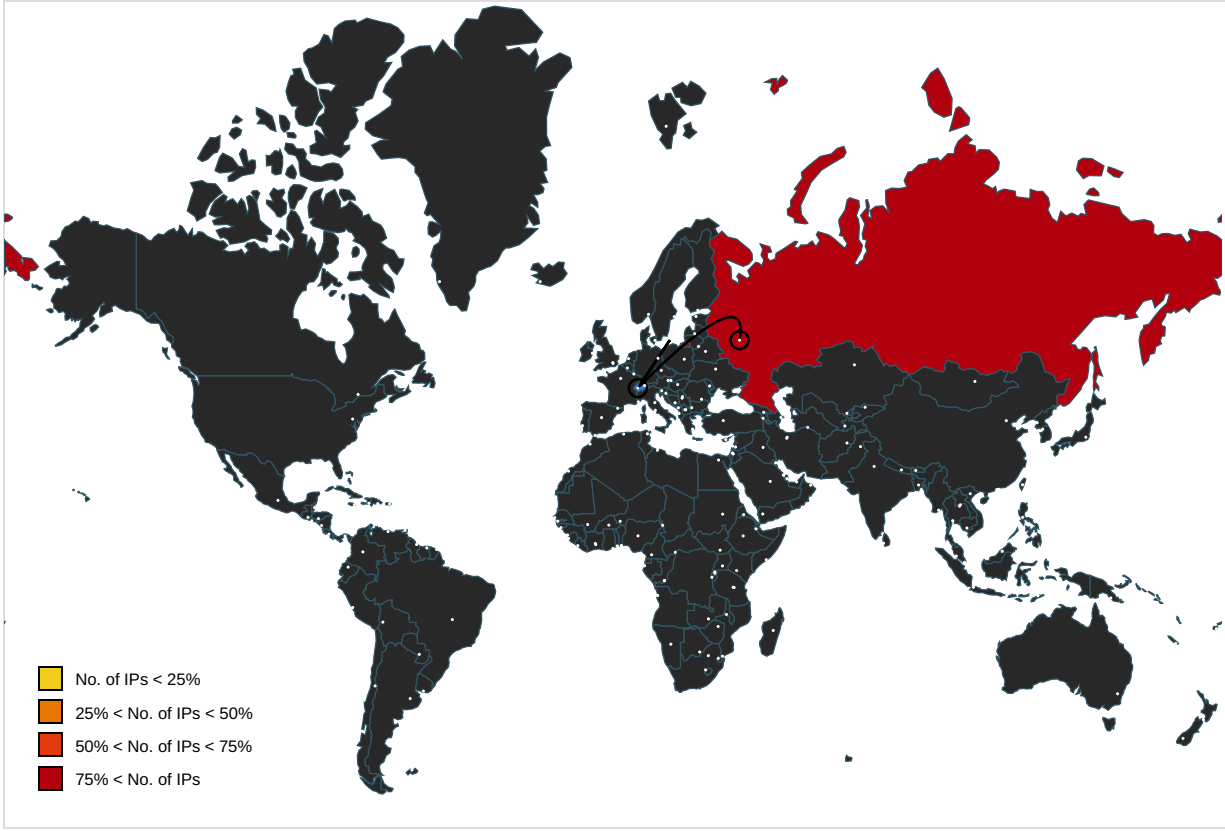
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://2b1c.telegram.godsmightywhispers.com/updateResource	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2b1c.telegram.godsmightywhispers.com/updateResource~	wscript.exe, 00000000.00000002.297436981.0000019F6DEF8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296673454.0000019F6DEDB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296707627.0000019F6DEF3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2b1c.telegram.godsmightywhispers.com/.	wscript.exe, 00000000.00000002.297436981.0000019F6DEF8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296673454.0000019F6DEDB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296707627.0000019F6DEF3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2b1c.telegram.godsmightywhispers.com/	wscript.exe, 00000000.00000002.297436981.0000019F6DEF8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296673454.0000019F6DEDB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.296707627.0000019F6DEF3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2b1c.telegram.godsmightywhispers.com/updateResource$	wscript.exe, 00000000.00000003.296699224.0000019F6DF14000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.297453139.0000019F6DF14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.91.127.52	2b1c.telegram.godsmightywhispers.com	Russian Federation		42861	FOTONTELECOM-TRANSIT-ASFOTONTELECOMISPRU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679454
Start date and time: 05/08/202220:10:08	2022-08-05 20:10:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AutoUpdater.js
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	29
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:	MAL
Classification:	mal48.evad.winJS@1/0@1/1
EGA Information:	Failed

Copyright Joe Security LLC 2022

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey 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

General

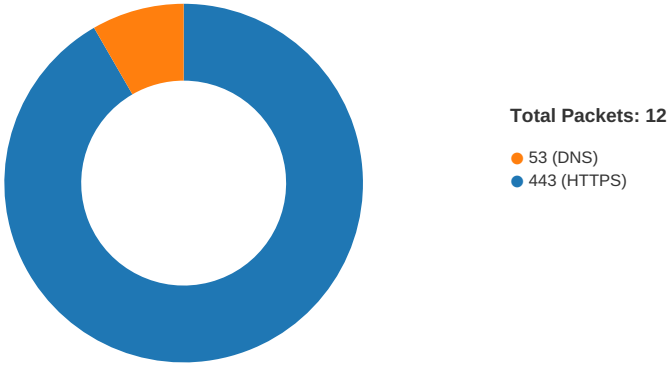
File type:	ASCII text, with very long lines, with no line terminators
Entropy (8bit):	5.281095567126216
TrID:	
File name:	AutoUpdater.js
File size:	8508
MD5:	c249583badbaef9a09e430a433a35914
SHA1:	6fec191fc99d6d4bf85ece108d0cdb191d2a9fcf
SHA256:	376180cf80a62085441a0b2a19e9b0fb2abdf3e1020955cfc4bd549e4bcc6726
SHA512:	64bd4c7ba9f05a7a30d373e99605ce851d6ec8e635343053e26d6f1bedb96aa2e7e6b25cb2923fcb5a3bfdb38d261f860b3e8226c5d2f0c5958c5025c899011d
SSDEEP:	96:HtmNoqutXY7vRcbWdtBu+TZmfNLXMRMgRXftIkwZQQsvo2imAJPfrtvK6IeO61RG:Np92Dg+GUhOQ6VJ3rtvKSv14ySsJrEQM
TLSH:	74027496A7E06CC01297AFF3131665D6F4259C9E3790040EF541BBB4FE91D11EB96E30
File Content Preview:	(function(_0x1f1fa8,_0x760f46){var a0_0x27f9cd= {_0x202319:0x2a,_0xf0c758:0x2f,_0x379c8b:'t3Y7',_0x2265b0:0x1f,_0x11a50c:0x1c,_0x2b0c5b:0x21,_0x5b4906:0x3a,_0x4fcc6b:0x18,_0x1c2c1b:0x30,_0x44afb1:0x50 ,_0x32bb71:'cG(L',_0x2d1ef6:'vp)t',_0xe7012:0x3be,_0x16c

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:11:11.205722094 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.205777884 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:11.205869913 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.232745886 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.232774019 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:11.335408926 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:11.335513115 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.613723993 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.613791943 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:11.614442110 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:11.614528894 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.621592999 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:11.622116089 CEST	49737	443	192.168.2.3	77.91.127.52

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:11:11.622178078 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:34.745378971 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:34.745501041 CEST	443	49737	77.91.127.52	192.168.2.3
Aug 5, 2022 20:11:34.745522022 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:34.745636940 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:34.746159077 CEST	49737	443	192.168.2.3	77.91.127.52
Aug 5, 2022 20:11:34.746182919 CEST	443	49737	77.91.127.52	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:11:11.013549089 CEST	64851	53	192.168.2.3	8.8.8.8
Aug 5, 2022 20:11:11.129642963 CEST	53	64851	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 20:11:11.013549089 CEST	192.168.2.3	8.8.8.8	0xa3a1	Standard query (0)	2b1c.telegram.godsmightywhispers.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 20:11:11.129642963 CEST	8.8.8.8	192.168.2.3	0xa3a1	No error (0)	2b1c.telegram.godsmightywhispers.com		77.91.127.52	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 2b1c.telegram.godsmightywhispers.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49737	77.91.127.52	443	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 18:11:11 UTC	0	OUT	POST /updateResource HTTP/1.1 Accept: */* Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 2b1c.telegram.godsmightywhispers.com Content-Length: 44 Connection: Keep-Alive Cache-Control: no-cache
2022-08-05 18:11:11 UTC	0	OUT	Data Raw: 6a 38 37 53 4e 6c 38 45 57 51 4b 43 51 7a 4c 2b 58 70 65 49 32 35 4b 34 67 65 45 41 79 42 69 30 30 77 2f 54 6c 6b 4d 70 4a 41 3d 3d Data Ascii: j87SNl8EWQKCQzL+XpeI25K4geEAyBi00w/TlkMpJA==
2022-08-05 18:11:34 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.23.0 Date: Fri, 05 Aug 2022 18:11:34 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET,POST,OPTIONS Cache-Control: no-cache, no-store

Copyright Joe Security LLC 2022

Statistics

No statistics

System Behavior

Analysis Process: wscript.exe PID: 5700, Parent PID: 3968

General

Target ID:	0
Start time:	20:11:07
Start date:	05/08/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\AutoUpdater.js"
Imagebase:	0x7ff693d70000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly

Copyright Joe Security LLC 2022