ID: 491731
Sample Name: techsmith-smart-player.min.js
Cookbook: default.jbs
Time: 20:54:22
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

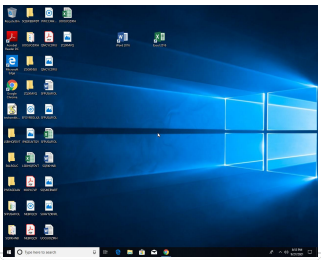
Windows Analysis Report techsmith-smart-player.min.js

Overview

General Information

Sample Name:	techsmith-smart-player.min.js
Analysis ID:	491731
MD5:	31b067a1e7db6f5.
SHA1:	feddeec3efe8f5c…
SHA256:	9d50de298d630f2.
Infos:	

Most interesting Screenshot:



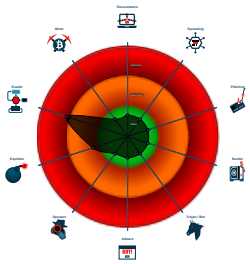
Detection

Score:	22
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Potential obfuscated javascript found
- Program does not show much activi…
- Java / VBScript file with very long s…
- Monitors certain registry keys / valu…
- Found WSH timer for Javascript or V…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 2208 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\techsmith-smart-player.min.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

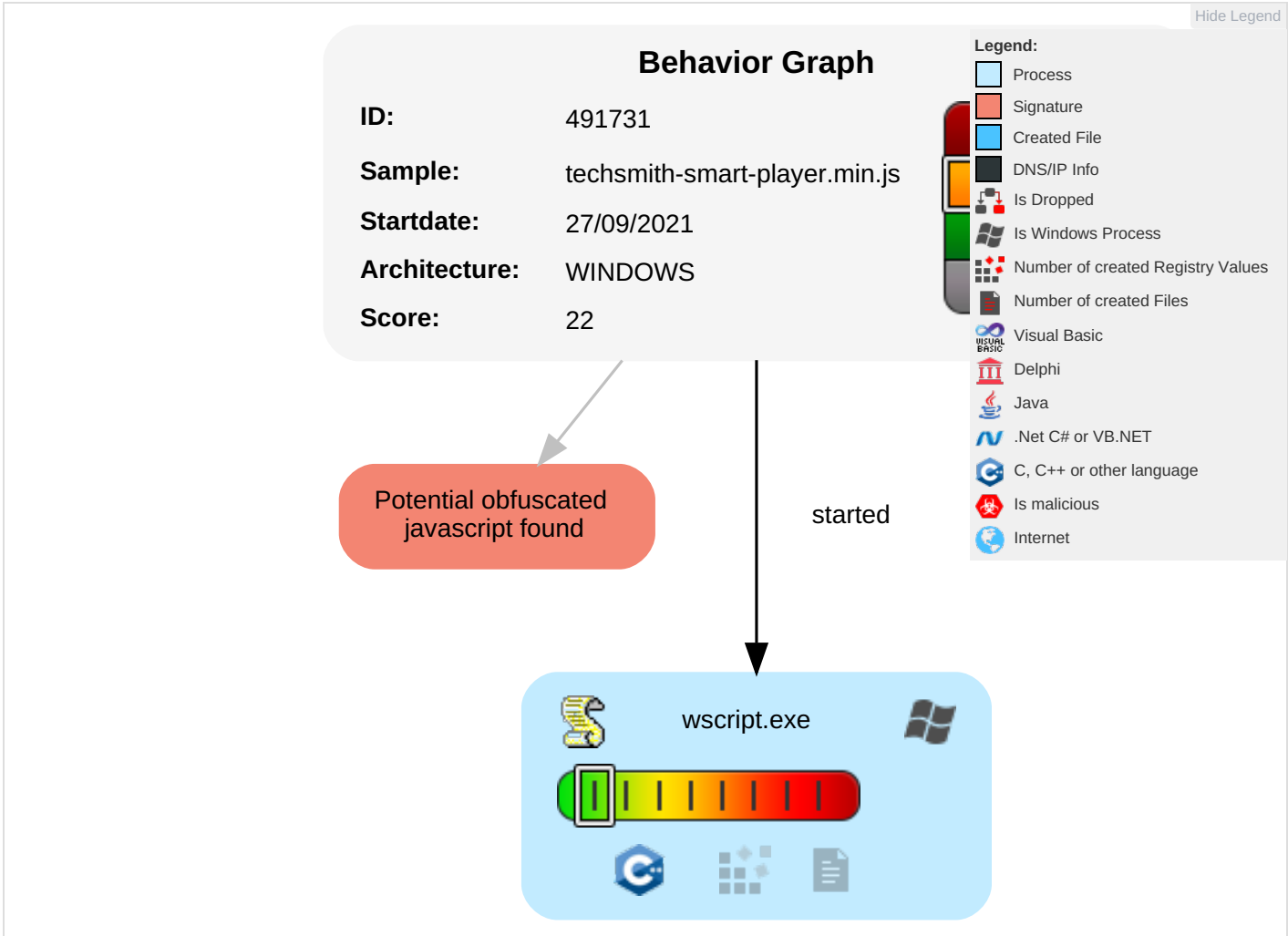
Data Obfuscation:

Potential obfuscated javascript found

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	Scripting 1 2	Path Interception	Path Interception	Scripting 1 2	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

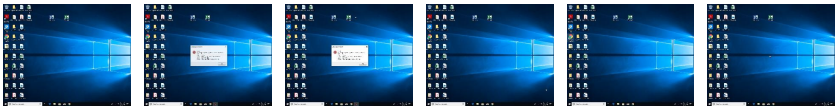
Behavior Graph



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
techsmith-smart-player.min.js	0%	Virustotal		Browse
techsmith-smart-player.min.js	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491731
Start date:	27.09.2021
Start time:	20:54:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	techsmith-smart-player.min.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:	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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus22.evad.winJS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .js • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.534536421918308
TrID:	• Java Script (8502/1) 68.00% • Digital Micrograph Script (4001/1) 32.00%
File name:	techsmith-smart-player.min.js
File size:	648978
MD5:	31b067a1e7db6f55f3727e7a820ab510
SHA1:	feddeec3efe8f5cbc7a517575088b234e2d47272
SHA256:	9d50de298d630f270c794af5b28be40ad0bb392e96efa0a224658f896fc3f04a
SHA512:	61de2b2d460e8a9371d6c1b3788df3cf03799045d251834b727e830074193d52e109579e90c5663da833bc5fe5cfd2309b1d2793d9322a85159be7e6b0914386
SSDEEP:	12288:72n29MkPfvEb/7/DpxO1RfrrJg003l+9b:7S26KfvEr7/DiDrNg0089b
File Content Preview:	/*! TechSmith Smart Player v5.6.2 */....!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("un

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: wscript.exe PID: 2208 Parent PID: 3424

General

Start time:	20:55:19
Start date:	27/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\techsmith-smart-player.min.js'
Imagebase:	0x7ff7edc40000
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

Show Windows behavior

Disassembly

Code Analysis