Joe Sandbox Cloud BASIC

ID: 491729
Sample Name: config_xml.js
Cookbook: default.jbs
Time: 20:56:37
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

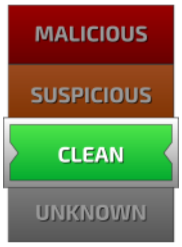
Windows Analysis Report config_xml.js

Overview

General Information

Sample Name:	config_xml.js
Analysis ID:	491729
MD5:	21ec939eb873ed..
SHA1:	4b88725c8b4f09e.
SHA256:	cc6f27e54cac322..
Infos:	

Detection

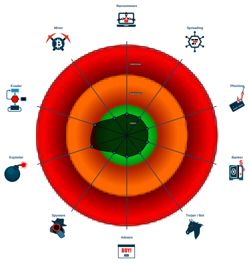


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Program does not show much activi…
- Java / VBScript file with very long s…
- Found WSH timer for Javascript or V…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6372 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\config_xml.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

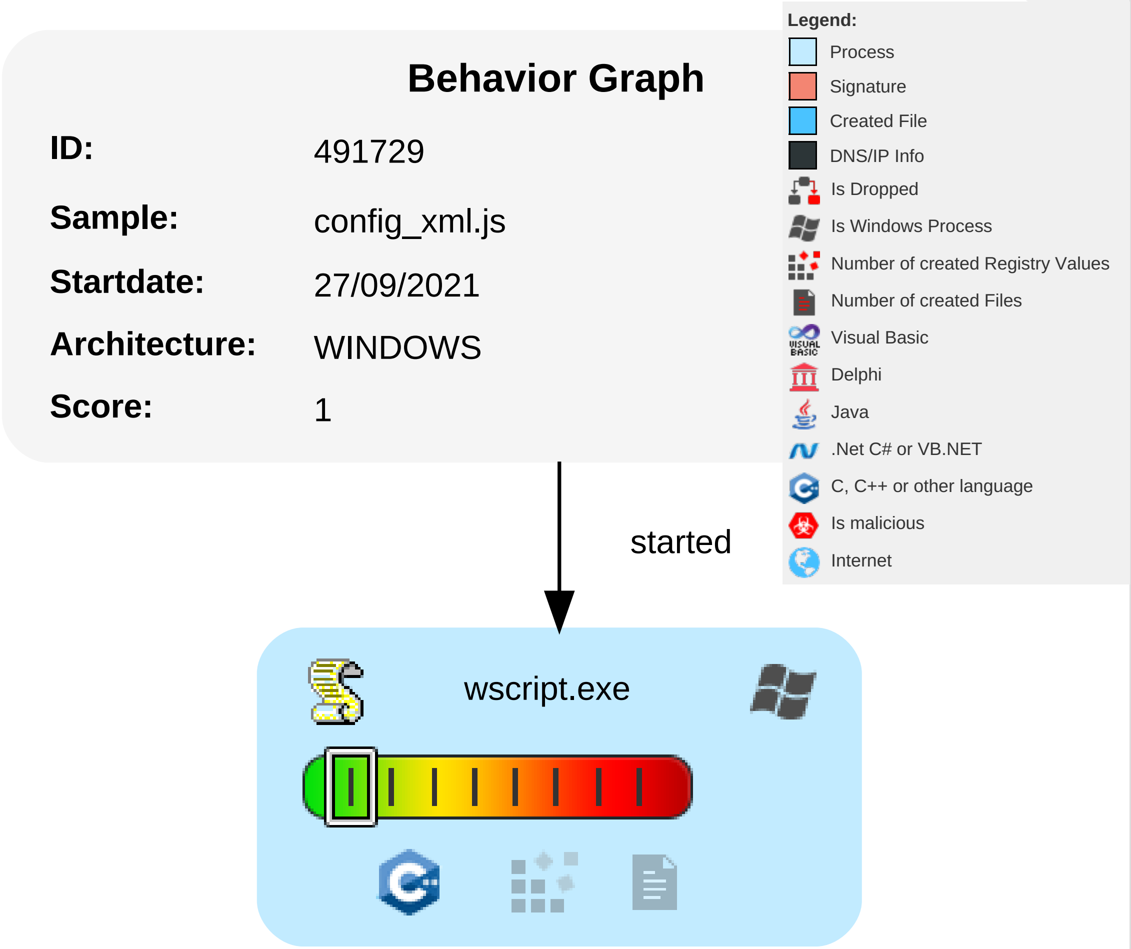
There are no malicious signatures, click here to show all signatures.

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	Scripting 2	Path Interception	Path Interception	Scripting 2	OS Credential Dumping	System Information Discovery 2	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	Application Window Discovery	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

Hide Legend



Behavior Graph

ID: 491729

Sample: config_xml.js

Startdate: 27/09/2021

Architecture: WINDOWS

Score: 1

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.ad	0%	URL Reputation	safe	

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:	491729
Start date:	27.09.2021
Start time:	20:56:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	config_xml.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:	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:	CLEAN
Classification:	clean1.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:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.377651253467105
TrID:	
File name:	config_xml.js
File size:	5604
MD5:	21ec939eb873eda0ac91bf0c4dbb2a6e
SHA1:	4b88725c8b4f09edccf7cc70557c26c6a5d34ccf
SHA256:	cc6f27e54cac322380736bc5c7153a4ac07ce4466f69e06d780dba9e8b27a2b8
SHA512:	24752b9d8c9886c4dc5125ad2fee1dc4fc4662506a75fba58f10485b723b7268d6a4888f8fab9512724231f5dc3af9bb9d0aa809ad13379d556fefcaee1619e1

General

SSDEEP:	96:o0wHkvZV1Nc6oN8tRuq9LjYtCrTcU5E9B5Jvhuk/tCaRItvo6ya25FG9+Igghe:7wHkhV1N9s8tRuc1AHSrylgh
File Content Preview:	var TSC = TSC || {};....TSC.embedded_config_xml = '<x:xmpmeta tsc:version="2.0.1" xmlns:x="adobe:ns:meta/" xmlns:tsc="http://www.techsmith.com/xmp/tsc/">\.. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:xmp="http://ns.adobe.com/

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: wscript.exe PID: 6372 Parent PID: 3424

General

Start time:	20:57:32
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\config_xml.js'
Imagebase:	0x7ff7f7de0000
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