JoeSandbox Cloud BASIC

ID: 458971
Sample Name:
SvchostInjector_x64 with SC.dll
Cookbook: default.jbs
Time: 23:28:51
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

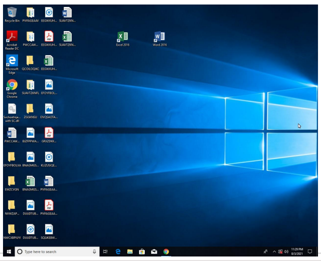
Windows Analysis Report SvchostInjector_x64 with SC.…

Overview

General Information

Sample Name:	SvchostInjector_x64 with SC.dll
Analysis ID:	458971
MD5:	4c0bbe1f536e0bf..
SHA1:	19b91d0188eb05..
SHA256:	c57a35df292b4e1.
Infos:	

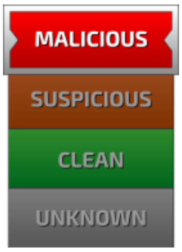
Most interesting Screenshot:



Errors

⚠ Nothing to analyse, Joe Sandbox has not found any analysis process or sample

Detection

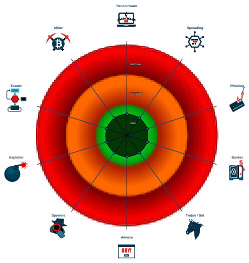


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara signature match

Classification



Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SvchostInjector_x64 with SC.dll	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x1d1fe:$xs1: WS2_32.dll • 0x1d03d:$xs2: ReflectiveLoader

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

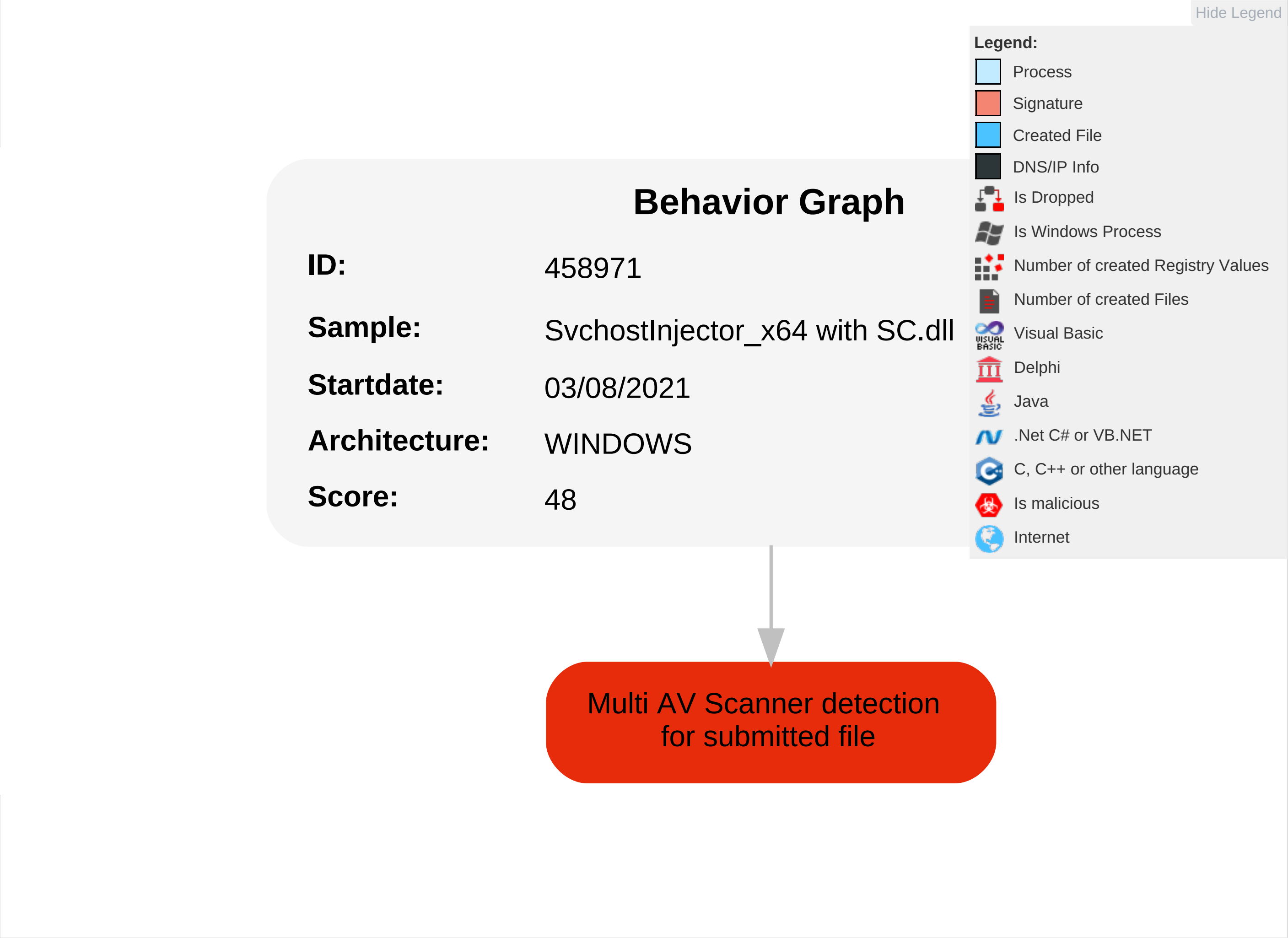
AV Detection:

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Behavior Graph



Legend:

- 🟦 Process
- 🟥 Signature
- 🟦 Created File
- ⬛ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Behavior Graph

ID: 458971

Sample: SvchostInjector_x64 with SC.dll

Startdate: 03/08/2021

Architecture: WINDOWS

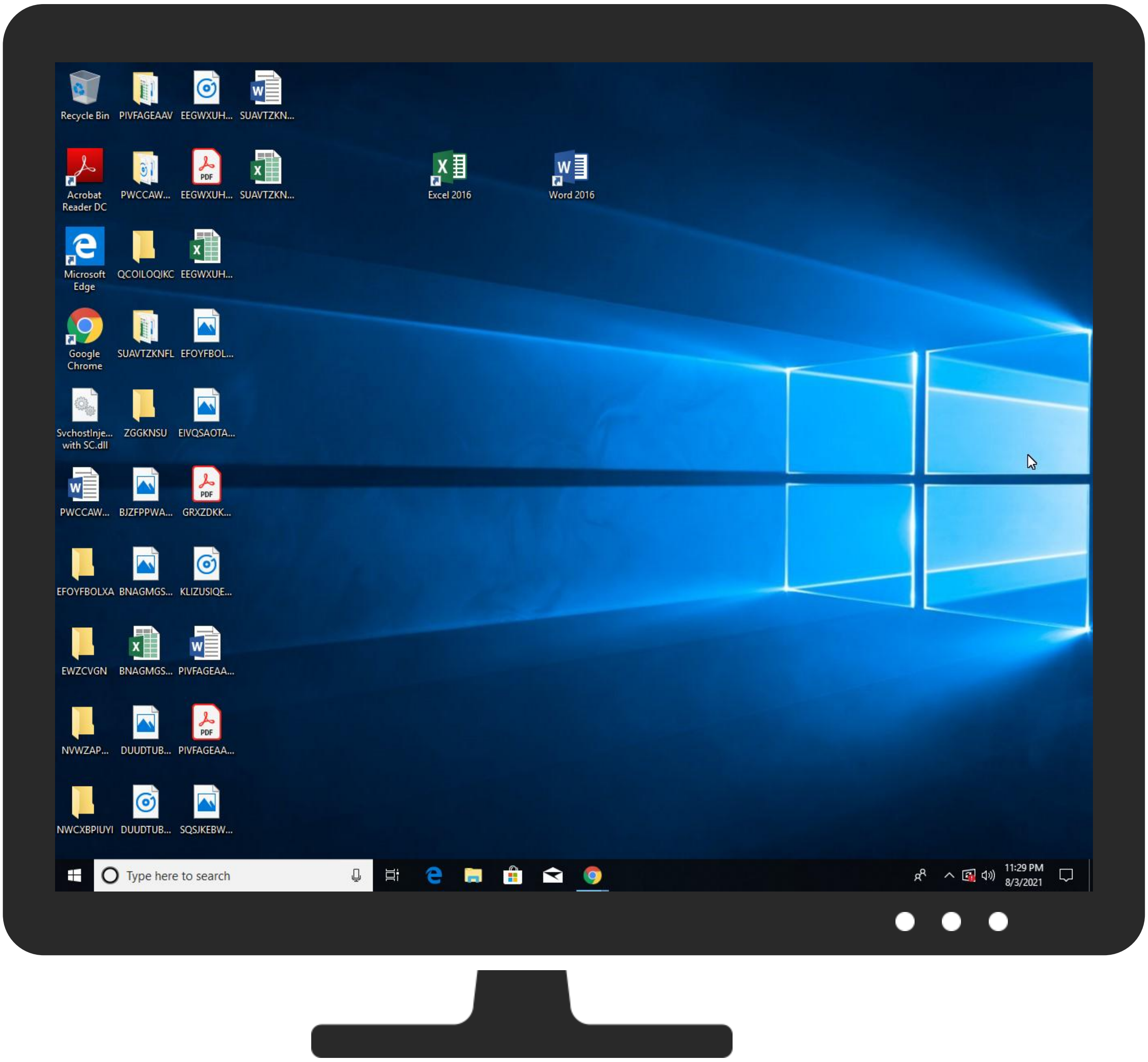
Score: 48

Multi AV Scanner detection for submitted file

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
SvchostInjector_x64 with SC.dll	16%	Virustotal		Browse
SvchostInjector_x64 with SC.dll	6%	Metadefender		Browse

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458971
Start date:	03.08.2021
Start time:	23:28:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SvchostInjector_x64 with SC.dll
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:	1
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.winDLL@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Stop behavior analysis, all processes terminated
Warnings:	Show All
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample

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:	data
Entropy (8bit):	6.002524238832623
TrID:	
File name:	SvchostInjector_x64 with SC.dll
File size:	121132
MD5:	4c0bbe1f536e0bf780b740ed6824941f
SHA1:	19b91d0188eb051f12ceb848b0f6d7b20db4813a
SHA256:	c57a35df292b4e1aabee65c4d645dad018d93965c276b563311f7833a2a5ef96
SHA512:	21d600f8a1ae0f16cf6fbf0791401536015fb2c117d97d0e79551c9ead905f851cd85fbd3d6d697ef28dd59b2bdd79509df981b747d0d7a2d81f900b39529adb
SSDEEP:	3072:tW+2/lPbvCyMnovvrCXngS99sysb3MvFf4vd:tWhNtMnYjAngU9o+Fmd
File Content Preview:	.....YI..H..#....1...I..#...A.....VH..H...H..0.D$ ....H..^.H.. H.X.D.H L.@..P.UVWATAUAVAWH.l$.H..p...E3..E.k.e. H..L.}......L.}.L.}.E.OeL.}.D.M.D.M.L.}.L.}.L.}.D.}$D.|$,.E.r.n..E.e.l..E.3.2..E...d..E.l.l..D$@Slee.D$Dp.D$XLoad.D$\Libr.D$`aryA.D$HVirt.D$

File Icon

Icon Hash:	74f0e4ecccdce0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly