ID: 528757
Sample Name:
1JXnBACf4L.exe
Cookbook: default.jbs
Time: 18:37:10
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

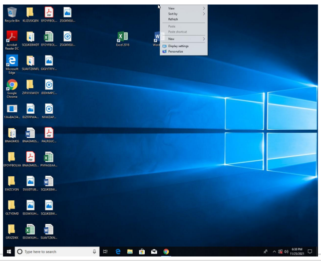
Windows Analysis Report 1JXnBACf4L.exe

Overview

General Information

Sample Name:	1JXnBACf4L.exe
Analysis ID:	528757
MD5:	55639d8c8ae909..
SHA1:	43474904bc2ae4..
SHA256:	d975e34edbe0b4..
Tags:	exe

Most interesting Screenshot:

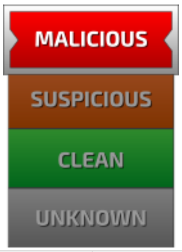


Errors

⚠ No process behavior to analyse as no analysis process or sample was found

⚠ Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

Detection

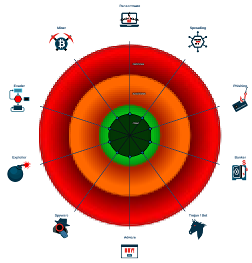


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- PE file contains section with special…
- Uses 32bit PE files
- PE file contains more sections than …
- Sample file is different than original …
- PE file contains an invalid checksum
- PE file overlay found
- Entry point lies outside standard sec…
- PE file contains sections with non-s…

Classification



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

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

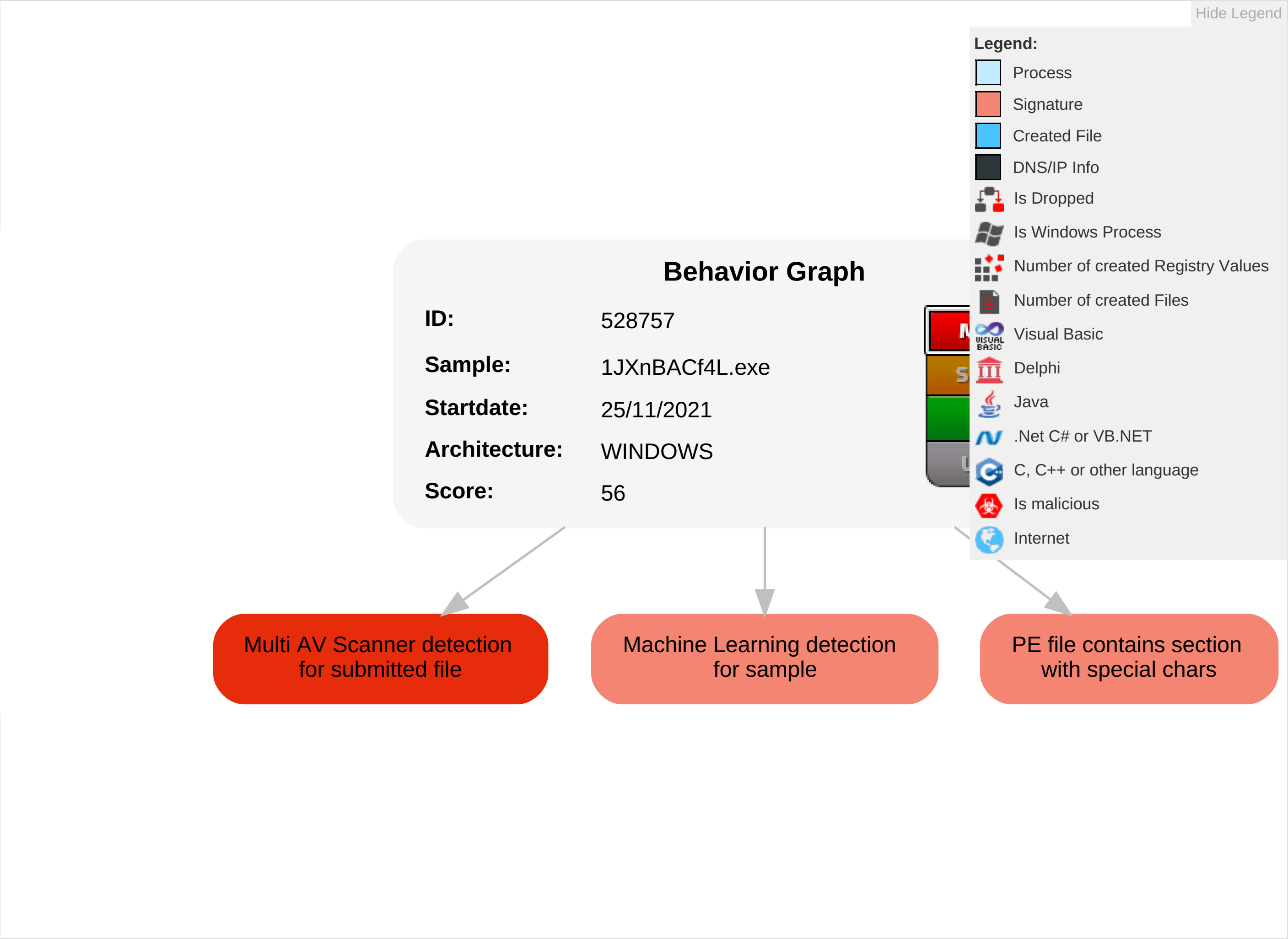
PE file contains section with special chars

Copyright Joe Security LLC 2021

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	Windows Management Instrumentation	Path Interception	Path Interception	Software Packing 2	OS Credential Dumping	System Service Discovery	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



Behavior Graph

ID: 528757

Sample: 1JXnBACf4L.exe

Startdate: 25/11/2021

Architecture: WINDOWS

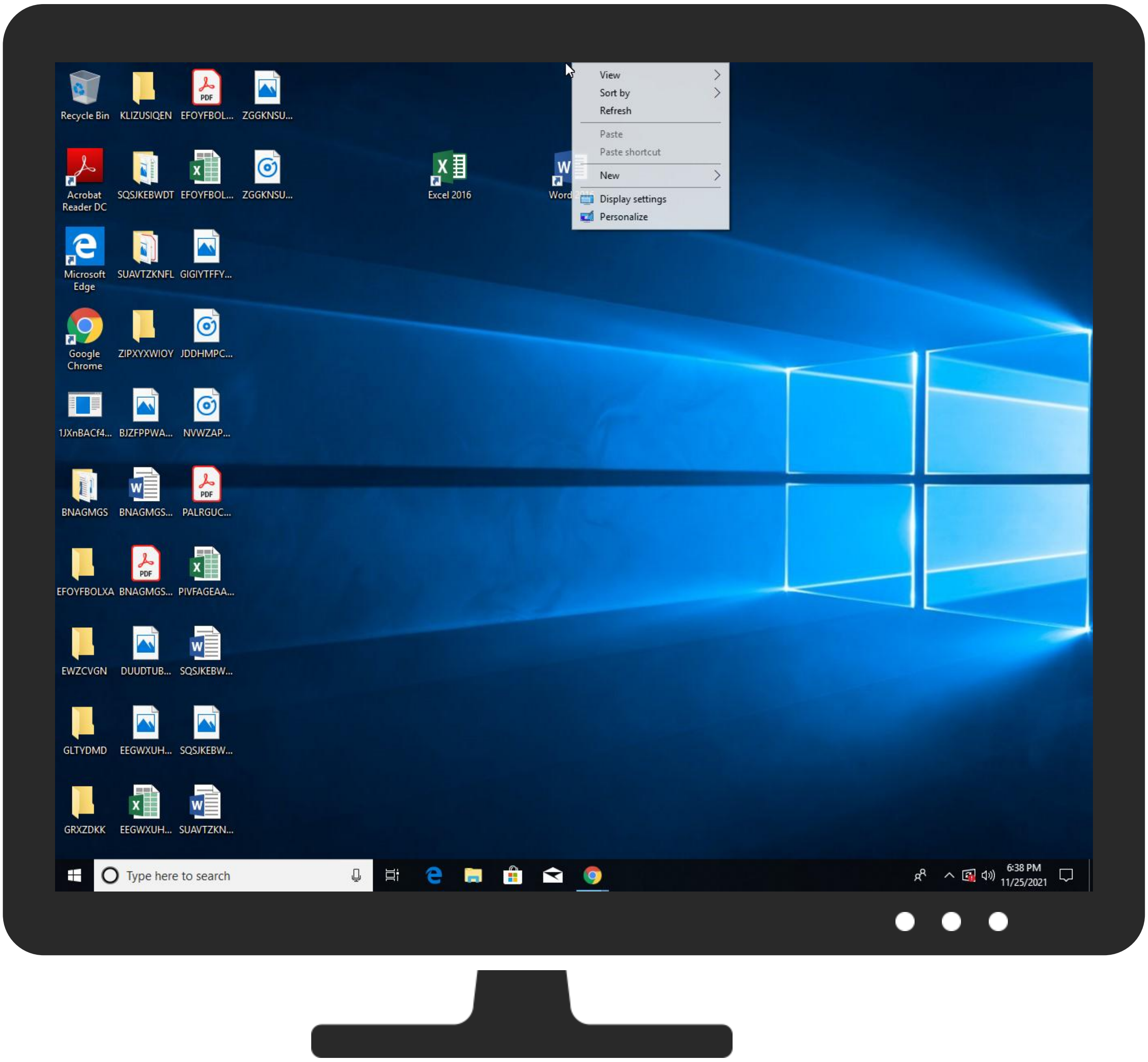
Score: 56

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1JXnBACf4L.exe	26%	Virustotal		Browse
1JXnBACf4L.exe	100%	Joe Sandbox ML		

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:	34.0.0 Boulder Opal
Analysis ID:	528757
Start date:	25.11.2021
Start time:	18:37:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1JXnBACf4L.exe
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:	mal56.winEXE@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	• No process behavior to analyse as no analysis process or sample was found • Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

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:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.937653870615833
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	1JXnBACf4L.exe
File size:	332271
MD5:	55639d8c8ae9090875ac0a663f0a8f57
SHA1:	43474904bc2ae4f7dc2a3a6de33fb70bf11fb906
SHA256:	d975e34edbe0b4371e2ea6f82bf56289486b4f5d43a6fb069def7360b813ab19
SHA512:	760a002c88a501f20bd4751770ac642bbc89c58d5ee350d02e1663c94a179f923da40b019c926a9326f2366fd0d341de39a1a817cc866a8ac9aff2e2a09120eb
SSDEEP:	6144:IADrRaW+IlIUM2VmrI09qJdkfwsgF9f4fetvB87mRMc0P48LyYxH:DvRL+0MjrI0EVF9YcB8UM3FFH
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........R.ZQ3e.Q3e.Q3e.XK..A3e..[a.]3e..[f.T3e..[`.M3e..[d.U3e.EXd.@3e.Q3d..3e..Zl.]3e..Z..P3e.Q3..P3e..Zg.P3e.RichQ3e.........PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x7d4108
Entrypoint Section:	.boot
Digitally signed:	false
Imagebase:	0x400000

Copyright Joe Security LLC 2021

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6196E78F [Thu Nov 18 23:53:51 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	62887e1cbeeea4bcc9666b312e1861a8

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x10a87	0x8129	False	1.00063511266	data	7.97271005667	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x12000	0x5ac8	0x185f	False	1.00176310306	data	7.92650297366	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x18000	0x960	0x12d	False	1.0365448505	data	7.12254688974	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x19000	0x4e8	0x271	False	1.0176	data	7.6271406474	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x1a000	0xe84	0xd8d	False	1.00317094263	data	7.86809864864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.imports	0x1b000	0x1000	0x600	False	0.3671875	data	3.89574962759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x1c000	0x1000	0x200	False	0.056640625	data	0.181201876782	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x1000	0x600	False	0.40625	data	3.71175649169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.winlice	0x1e000	0x3b6000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.boot	0x3d4000	0x293e00	0x293e00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x668000	0x1000	0x10	False	0	empty	0.0	IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly

Copyright Joe Security LLC

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal