

JoeSandbox Cloud BASIC



ID: 528750

Sample Name:

eLVD8YyLgN.exe

Cookbook: default.jbs

Time: 18:30:23

Date: 25/11/2021

Version: 34.0.0 Boulder Opal


Table of Contents

Table of Contents	2
Windows Analysis Report eLVD8YyLgN.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	3
Mitre Att&ck Matrix	3
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
General Information	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	7
Static PE Info	7
General	7
Entrypoint Preview	8
Data Directories	8
Sections	8
Network Behavior	8
Code Manipulations	8
Statistics	8
System Behavior	8
Disassembly	8

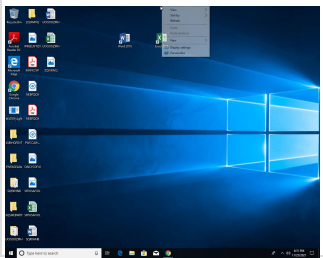
Windows Analysis Report eLVD8YyLgN.exe

Overview

General Information

Sample Name:	eLVD8YyLgN.exe
Analysis ID:	528750
MD5:	6518d0ae2e7013..
SHA1:	3457cd0c31d835..
SHA256:	c14c596d56885c...
Tags:	

Most interesting Screenshot:



Errors

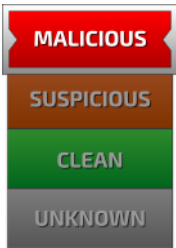
 No process behavior to analyse as no analysis process or sample was found

Malware Configuration

analyzer. Details: %1 is not a valid Win32 application.

No configs have been found

Detection

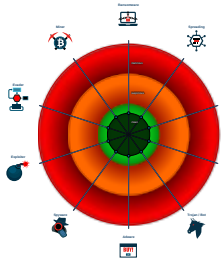


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Machine Learning detection for samp...
- PE file overlay found
- Uses 32bit PE files
- PE file does not import any functions
- PE file contains an invalid checksum

Classification



Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

[Click to jump to signature section](#)

AV Detection:



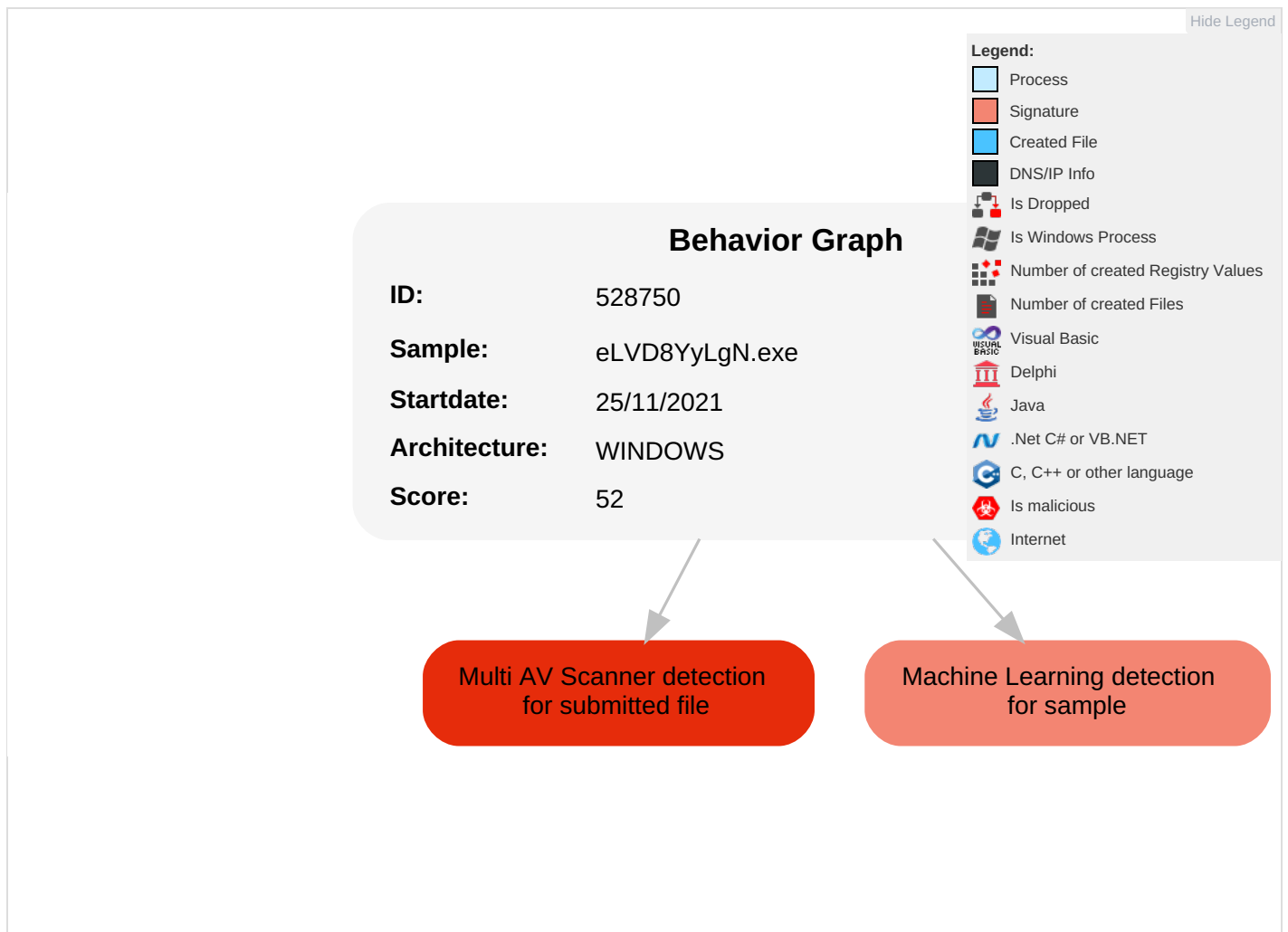
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

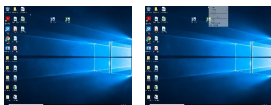
Behavior Graph



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
eLVD8YyLgN.exe	12%	Virustotal		Browse
eLVD8YyLgN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.home.r-hs.de/philippinen/antivirus/sig/signature.db0This	0%	Avira URL Cloud	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:	34.0.0 Boulder Opal
Analysis ID:	528750
Start date:	25.11.2021
Start time:	18:30:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eLVD8YyLgN.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:	3
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:	<ul style="list-style-type: none">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.winEXE@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	<ul style="list-style-type: none">• 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):	4.4133402742573375
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.15%Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%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:	eLVD8YyLgN.exe
File size:	235257
MD5:	6518d0ae2e70133d19f94681d640590b
SHA1:	3457dc0d31d8355b9395245b2f3a093c394b4e43
SHA256:	c14c596d56885c5a21913cb8b33bef299ab564fd81fe05836ceb4f7192a1c0d7
SHA512:	c240e656d5fb4d059903b9b8e92dcb286eb9e271b423f1190272fdb9c96bcefdeea80c5c5047baab37ca571675b7f4f3e2e45f41347a66cdf5f9554deb6c910a
SSDEEP:	1536:8RWdX8T3mkA1mMB0hECRFaCfCd7NFOb0Fz87ylyZvd+TzeMGQtb6XMuZXKMRm4Sc:8RWp8CIYECRFaXd7NAAFz1ysGso
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$.....&...b...b..b.....c.....B.....c...Richb.....PE.L.....a.....`.....(.....p....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4028a0

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x619805F0 [Fri Nov 19 20:15:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x55a38	0x56000	False	0.323925748721	data	4.43879142147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x57000	0x614c	0x1000	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x6424	0x7000	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly