ID: 528753
Sample Name:
ouO9N7aFZl.exe
Cookbook: default.jbs
Time: 18:35:21
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report ouO9N7aFZl.exe

Overview

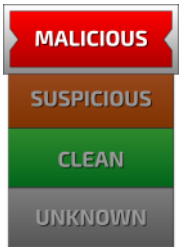
General Information

Sample Name:	ouO9N7aFZl.exe
Analysis ID:	528753
MD5:	546d1e802d7c2e..
SHA1:	6c85b22d9349c9..
SHA256:	06e57daff1fec75…
Tags:	exe

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

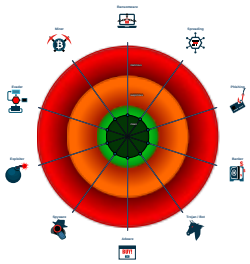


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- PE file overlay found
- Uses 32bit PE files
- PE file contains strange resources

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

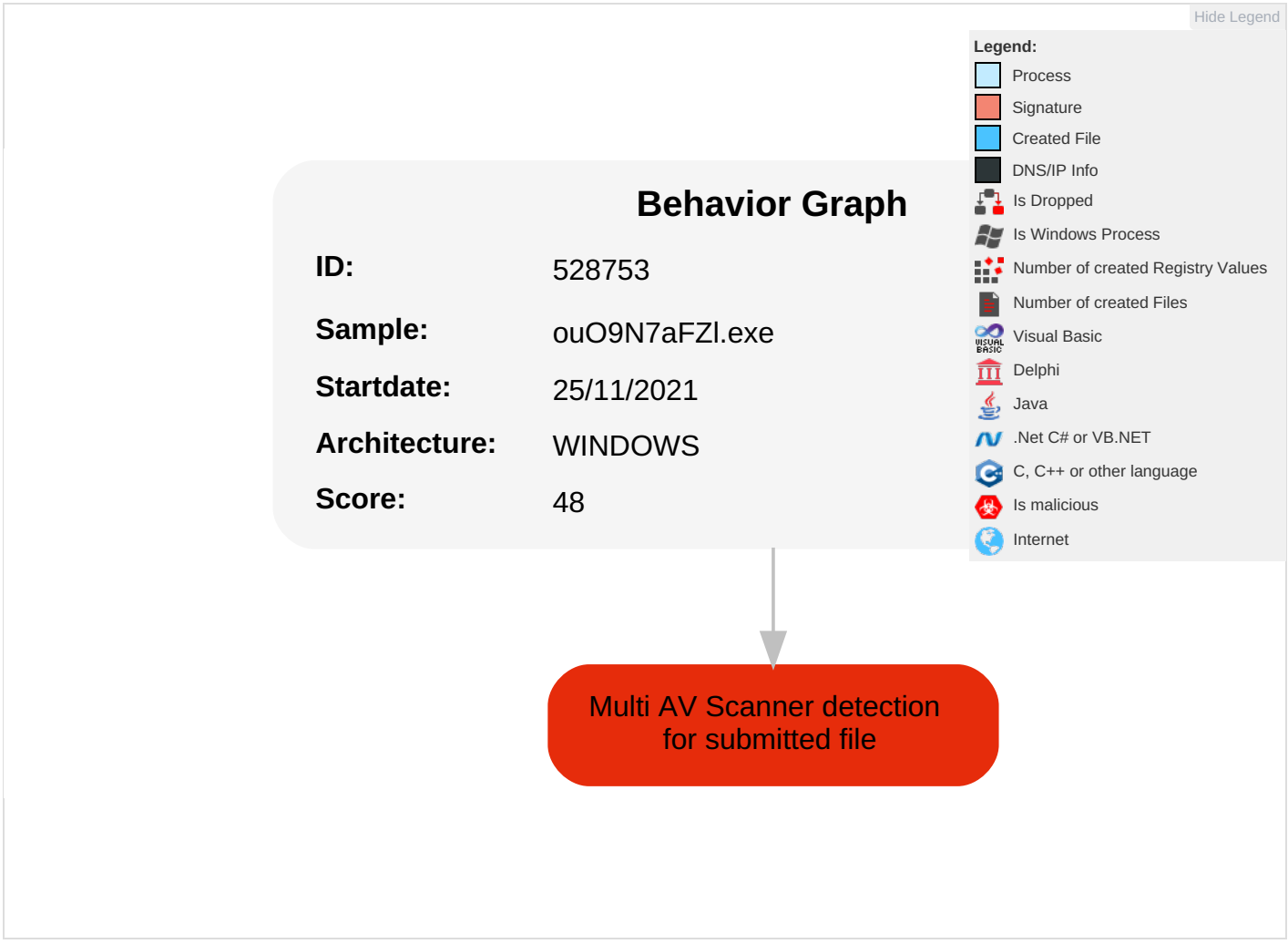
AV Detection:

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ouO9N7aFZl.exe	29%	Virustotal		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:	34.0.0 Boulder Opal
Analysis ID:	528753
Start date:	25.11.2021
Start time:	18:35:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ouO9N7aFZl.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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.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):	6.772197524298749
TrID:	• Win32 Executable (generic) a (10002005/4) 97.12% • Win32 Executable Borland Delphi 6 (262906/60) 2.55% • Win32 Executable Delphi generic (14689/80) 0.14% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	ouO9N7aFZl.exe
File size:	574087
MD5:	546d1e802d7c2e76569de1ec3c1e0a3b
SHA1:	6c85b22d9349c9937ec074f8df4aaf1f6232d395
SHA256:	06e57daff1fec75764f9c282cb99a09e9e33e07df95a8c0082647776fc6d336c
SHA512:	80c99c51c83906769bfc37019426e29a65869361bea810888bc78a6acc2b11fb8cc9b0260037ceeb91f0a886cd8eec0187db4bd65f47e1c45289cc5c3b8db9bb
SSDEEP:	12288:JN7qAaluiiivQxUVi9MpvAw642f/2KvWu17uV:DOFuofI8K/r+I7U
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x451330
Entrypoint Section:	CODE
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	51bdd5c24a2d998f177313ae325d417a

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x50378	0x50400	False	0.533869377921	data	6.52996506528	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x52000	0x119c	0x1200	False	0.450086805556	data	4.1649939827	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x54000	0xc45	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x55000	0x2058	0x2200	False	0.352711397059	data	4.76658957514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x58000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x59000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x5a000	0x5a94	0x5c00	False	0.646229619565	data	6.674071652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0xe1000	0xe1000	False	0.539179546146	data	6.38060718271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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