ID: 502675
Sample Name:
ONENOTEM(492).EXE.METADATA
Cookbook: default.jbs
Time: 08:54:28
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

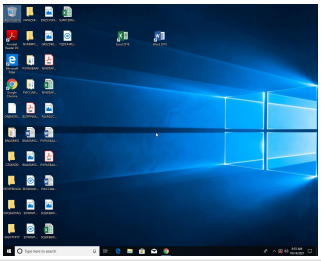
Windows Analysis Report ONENOTEM(492).EXE.METAD…

Overview

General Information

Sample Name:	ONENOTEM(492).EXE.METADATA
Analysis ID:	502675
MD5:	dd994540c02d41..
SHA1:	5e909ffe4d85440..
SHA256:	32bb2f5acc11809..

Most interesting Screenshot:



Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: 800401E3

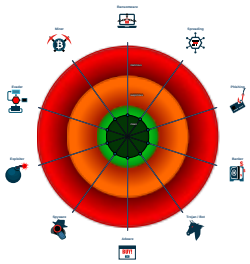
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

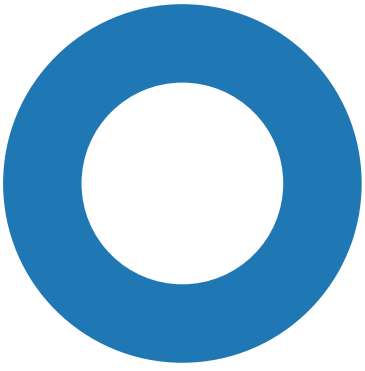
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



● System Summary

Click to jump to signature section

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

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

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

No Antivirus matches

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:	502675
Start date:	14.10.2021
Start time:	08:54:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ONENOTEM(492).EXE.METADATA
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:	2
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:	UNKNOWN
Classification:	unknown0.winMETADATA@0/0@0/0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis
Warnings:	Show All • Exclude process from analysis (whitelisted): backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 23.203.141.148 • Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • Corrupt sample or wrongly selected analyzer. Details: 80040153

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 CRLF line terminators
Entropy (8bit):	5.383346841920684
TrID:	
File name:	ONENOTEM(492).EXE.METADATA
File size:	370
MD5:	dd994540c02d41a7738c7ed8e98118d3
SHA1:	5e909ffe4d854408f6e8b6a8d4e778ab53d8c1ad
SHA256:	32bb2f5acc1180936d53772eb19df769441949427203121 e3a4efb3e983898d8

General

SHA512:	066d038aa1e03379d04b89f83b203801852caa79438816c1725ff0a52ced431978de8b2b306facba8f857bc27e52ce092750153968564d5e7504dc22e42d87c6
SSDEEP:	6:x62OjqfMK+OsL3NFAO/umT5ue2VSuNaF5ue2VSO8JBGk17I6vdYBrYjYSfy:AdGDKZImtuFSuGuFSnJBGk/vdUqYSfy
File Content Preview:	file full path = c:/System Volume Information/SystemRestore/FRStaging/Program Files/Microsoft Office/Office16/ONENOTEM(492).EXE..file creation time = 2015-31-07 07:58:06..file modification time = 2015-31-07 07:58:06..machine id = PYLUMCLIENT_EU-SANLAM_PF1

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly