JoeSandbox Cloud BASIC

ID: 613367
Sample Name: download.exe
Cookbook: default.jbs
Time: 19:06:14
Date: 21/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

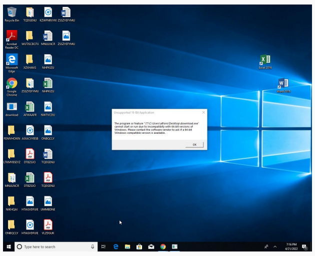
Windows Analysis Report

download.exe

Overview

General Information

Sample Name:	download.exe
Analysis ID:	613367
MD5:	4842e206e4cfff2..
SHA1:	80c9820ff2efe8a..
SHA256:	2acab1228e8935..



Errors

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

Detection

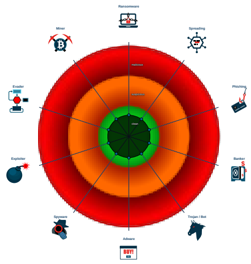
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Malware Configuration

⊘ **No configs have been found**

Yara Signatures

⊘ **No yara matches**

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

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

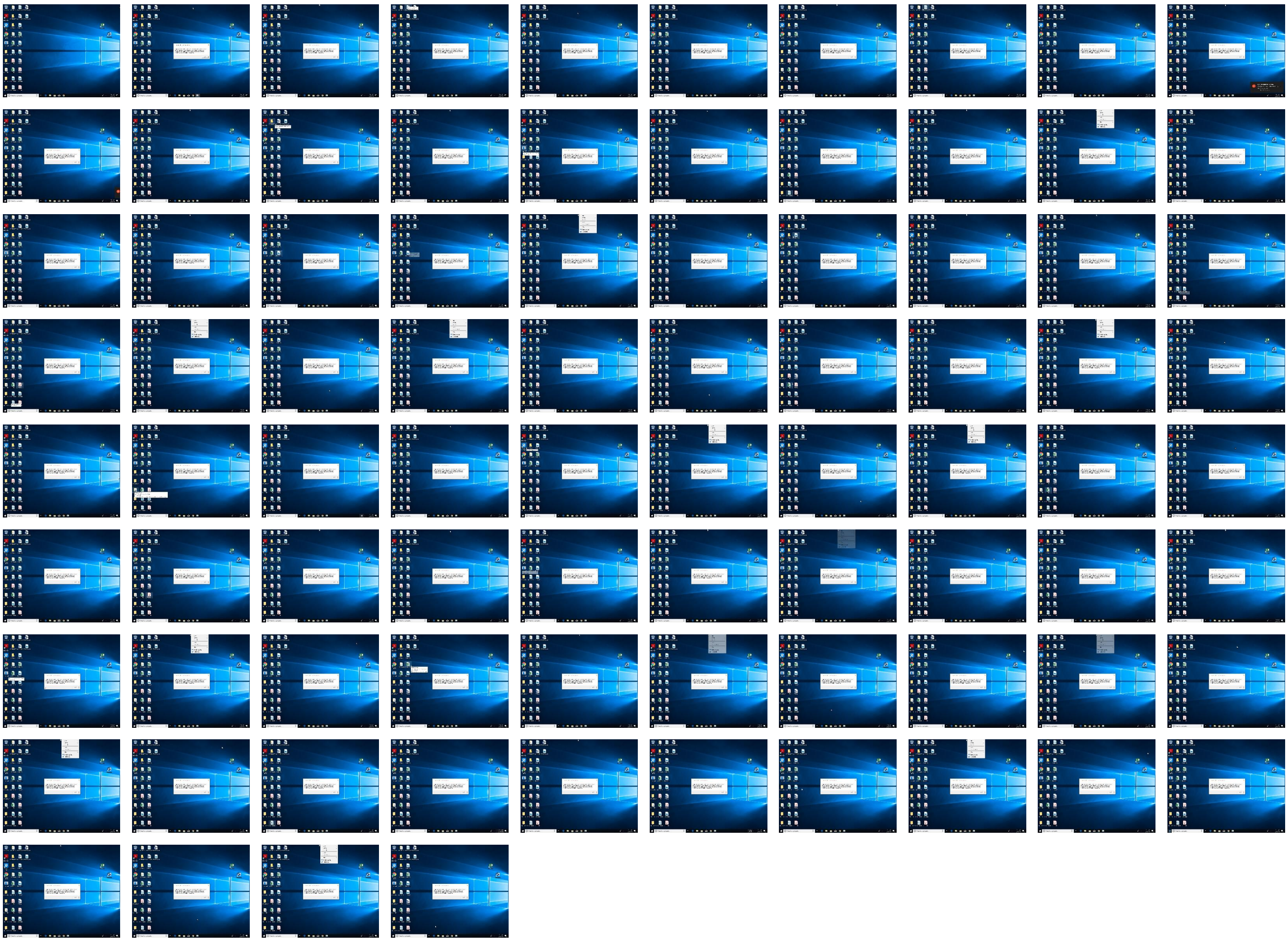
Mitre Att&ck Matrix

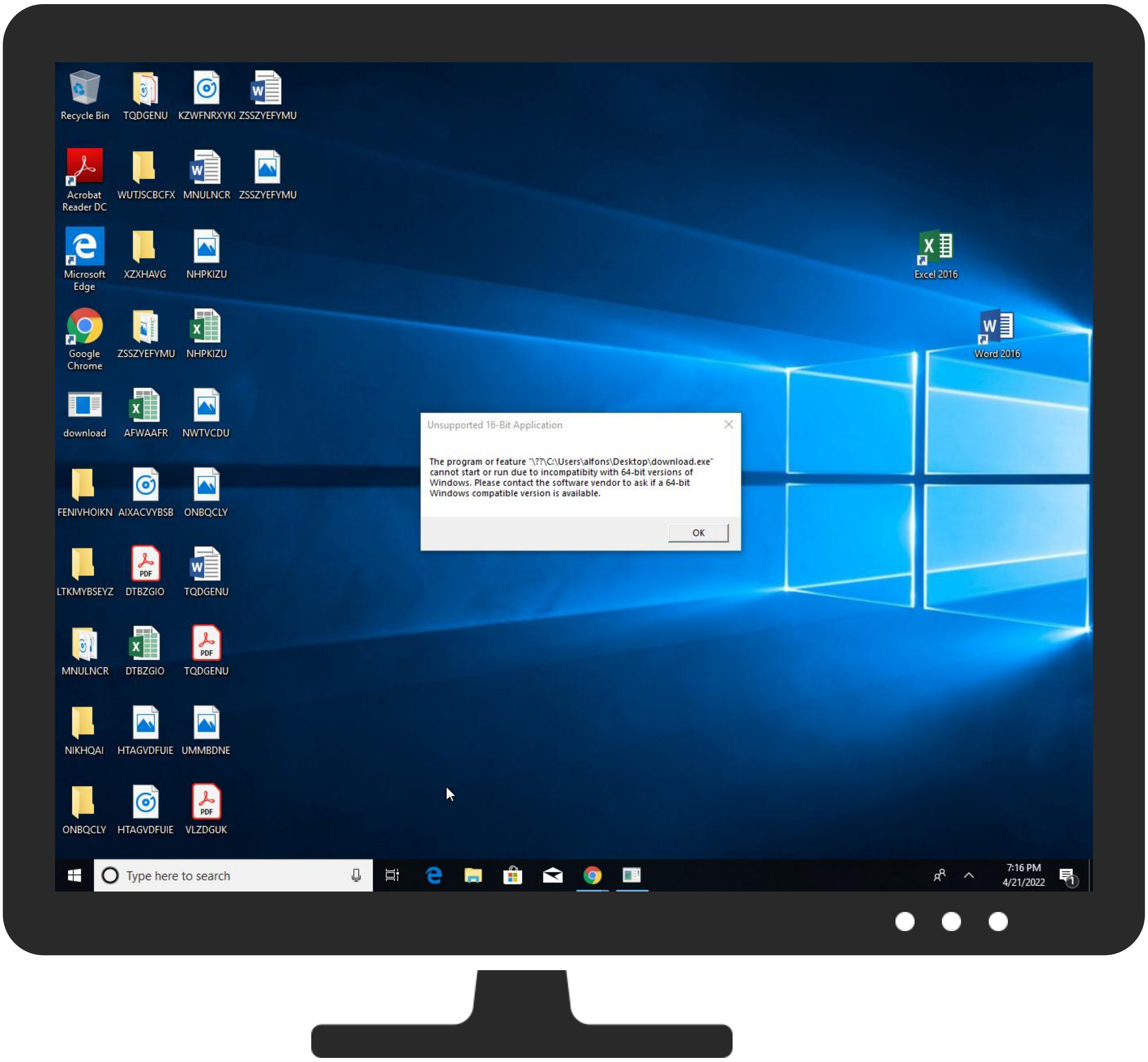
⊘ **No Mitre Att&ck techniques found**

Screenshots

Thumbnails

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





Unsupported 16-Bit Application

The program or feature "\??\C:\Users\alfons\Desktop\download.exe" cannot start or run due to incompatibity with 64-bit versions of Windows. Please contact the software vendor to ask if a 64-bit Windows compatible version is available.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
download.exe	0%	Virustotal		Browse
download.exe	0%	Metadefender		Browse
download.exe	0%	ReversingLabs		

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**

World Map of Contacted IPs

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	613367
Start date and time: 21/04/202219:06:14	2022-04-21 19:06:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	download.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:	25
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
Detection:	UNKNOWN
Classification:	unknown0.winEXE@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Errors

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

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, tile-service.weather.microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

Simulations

Behavior and APIs

⊘ **No simulations**

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **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):	1.9219280948873623
TrID:	
File name:	download.exe
File size:	5
MD5:	4842e206e4cfff2954901467ad54169e
SHA1:	80c9820ff2efe8aa3d361df7011ae6eee35ec4f0
SHA256:	2acab1228e8935d5dfdd1756b8a19698b6c8b786c90f87993ce9799a67a96e4e
SHA512:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bdcba2fdbc81d366da6c97eb76ecb6cba
SSDEEP:	3:w:w
TLSH:	
File Content Preview:	0....

File Icon

Icon Hash:	00828e8e8686b000

Network Behavior

⊘ **No network behavior found**

Statistics

⊘ **No statistics**

System Behavior

⊘ **No system behavior**

Disassembly

⊘ **No disassembly**