ID: 796693
Sample Name: shortcut.lnk
Cookbook: default.jbs
Time: 04:14:09
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

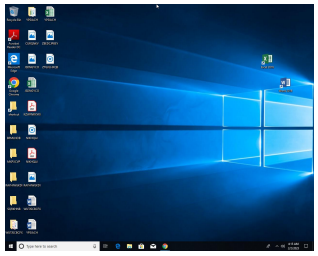
Windows Analysis Report

shortcut.lnk

Overview

General Information

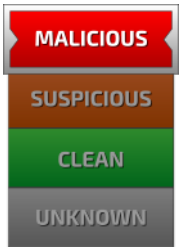
Sample Name:	shortcut.lnk
Analysis ID:	796693
MD5:	465f6c16be1f5…
SHA1:	078286bef60b2..
SHA256:	0b9e2923f442b..
Tags:	lnk



Errors

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

Detection

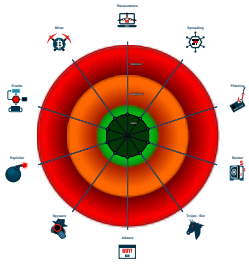


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…

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

AV Detection

Antivirus / Scanner detection for submitted sample

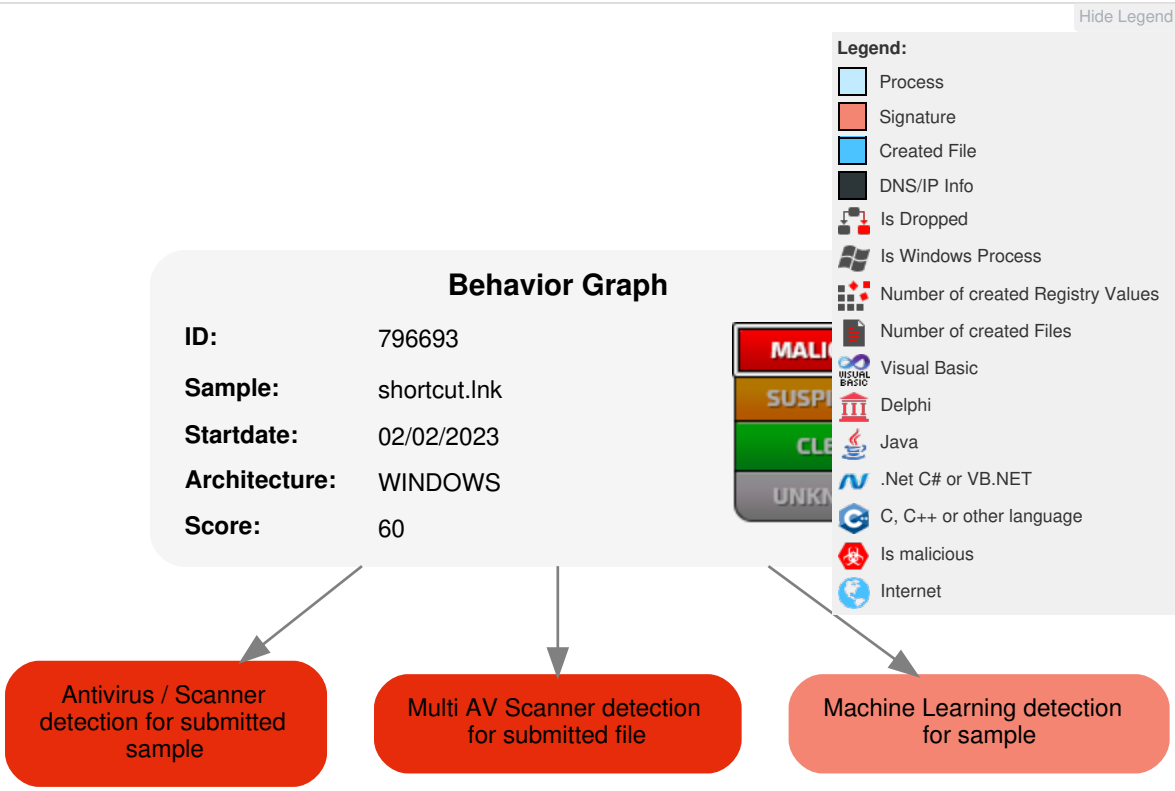
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

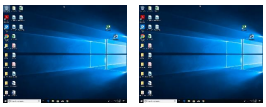
Behavior Graph



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
shortcut.lnk	42%	ReversingLabs	Shortcut.Backdoor.Andromeda	
shortcut.lnk	42%	Virustotal		Browse
shortcut.lnk	100%	Avira	LNK/Runner.VPMK	
shortcut.lnk	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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796693
Start date and time:	2023-02-02 04:14:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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
Sample file name:	shortcut.lnk
Detection:	MAL
Classification:	mal60.winLNK@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .lnk • Stop behavior analysis, all processes terminated

Errors

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

Warnings

- Exclude process from analysis (whitelisted): rundll32.exe

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:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Working directory, Has command line arguments, Icon number=3, Archive, ctime=Sat Dec 7 08:09:32 2019, mtime=Sun Jan 29 13:41:19 2023, atime=Sat Dec 7 08:09:32 2019, length=61440, window=hide
Entropy (8bit):	3.187898363479202
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	shortcut.lnk
File size:	1842
MD5:	465f6c16be1f568f5f1c3c2fb3252fb9
SHA1:	078286bef60b2973471ff6db532493213933ed49
SHA256:	0b9e2923f442b718fca90af4fc50a4a7ca77089b98b1bffb9abb5e091ff44162
SHA512:	dfb12eb2a2fe039d29a5d37e2997ed95770649d46987d420e593edd9de6699a3103ce9fa3f6fac406672f11777228221a1dddecab84f8e1a60c98d8aa08d1896
SSDEEP:	24:84obBJcUA0+BTRYlMa2JM9eAVpccgQ68CluXhxexhxLabTkCm:87JcHhT+lz2JFAV4QAlaoLasC
TLSH:	2231CB250BD31269D172C239BDBA230FCB15F88BC5469F2E84C0E54A7C51501BD69F7B
File Content Preview:	L.....F.... ....I.....A....3...I.....E....P.O. .:i.....+00.../C:\.....V.1.....3U....Windows.@.....OwH=V.u.....r..W.i.n.d.o.w.s.....Z.1.....3U....System32..B.....OwH=V.u.....

File Icon

Icon Hash:	30b4b4b464696d0d

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	Shell32.dll,ShellExec_RunDLL "RCYCLR\.com" "Recovery"

General	
Icon location:	%WINDIR%\System32\Shell32.dll

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly