ID: 796121
Sample Name: AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk
Cookbook: default.jbs
Time: 16:54:36
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk

Overview

General Information

Sample Name:	AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk
Analysis ID:	796121
MD5:	d32354771cc4…
SHA1:	3392046cc948…
SHA256:	7914acd017e4…

Errors

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

⚠ Corrupt sample or wrongly selected analyzer. Details: C0000001

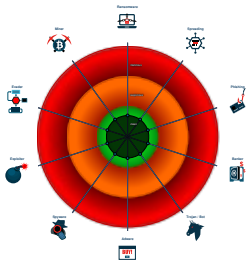
Detection

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk	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:	36.0.0 Rainbow Opal
Analysis ID:	796121
Start date and time:	2023-02-01 16:54:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk
Detection:	UNKNOWN
Classification:	unknown0.winLNK@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .lnk • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sam ple was found
- Corrupt sample or wrongly sele cted analyzer. Details: C0000001

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- VT rate limit hit for: AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk

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 Relative path, Has Working directory, Archive, ctime=Sun Apr 14 13:00:00 2019, mtime=Sun Apr 14 13:00:00 2019, atime=Sun Apr 14 13:00:00 2019, length=93986304, window=hide
Entropy (8bit):	4.242735360021169
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	AntSword.exe - #U5feb#U6377#U65b9#U5f0f.lnk
File size:	1933
MD5:	d32354771cc48a9276d61673e28b8481
SHA1:	3392046cc9485ef007fef9f5f2871e6319911402
SHA256:	7914acd017e40a017aa6815c849244871b151bcf05e618b3b2d30c51f26a6eb7
SHA512:	81d4fbc223e5a6e22556dbc10dc92f546d42e9a1330c55c820d2013ba01981fb44eaac6f69fdf99c8dd08d113f4e2927effeab88a50186951edee3c66e010c35
SSDEEP:	24:8+vffVyMzoKP4xt2Rp7YAJyAwCmdm5//tGXQGxiSfEpCRXm:8iffzTP4xt2H7BNmdmltGX7izpCRXm
TLSH:	B84101150FF30B1AF28EA7310AB0F00099703983E551CFCC9A98AB1D6D75B09A8B4F27
File Content Preview:	L.....F.... ....0.Y.....0.Y.....0.Y.....[....P.O. .:i.....+00.../C:\.....P.1.....mT!1..tools.<.....mT.1mT!1.....m.....39#.t.o.o.l.s.....Z.1.....mTZ1..AntSword..B.....mT.1mTZ1.....m.....

File Icon

Icon Hash:	aab2e3e38383a919

Static Windows Shortcut Info

General

Relative Path:	..\..\..\tools\AntSword\AntSword-Loader-v4.0.3-win32-x64\AntSword-Loader-v4.0.3-win32-x64\AntSword.exe
Command Line Argument:	
Icon location:	

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