ID: 796593
Sample Name: Epic Privacy Browser.lnk
Cookbook: default.jbs
Time: 00:34:58
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

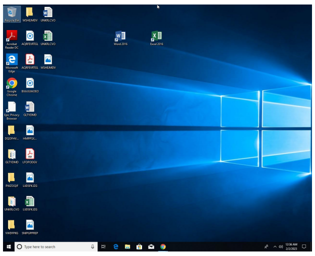
Windows Analysis Report

Epic Privacy Browser.lnk

Overview

General Information

Sample Name:	Epic Privacy Browser.lnk
Analysis ID:	796593
MD5:	c60b17da68fad..
SHA1:	368cbaf2aa7e5..
SHA256:	778712d44739..
Tags:	lnk



Errors

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

⚠ Corrupt sample or wrongly selected analyzer. Details: C000007B

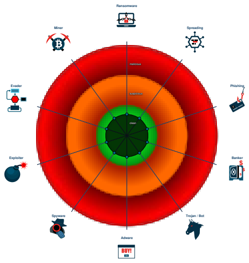
Detection

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.

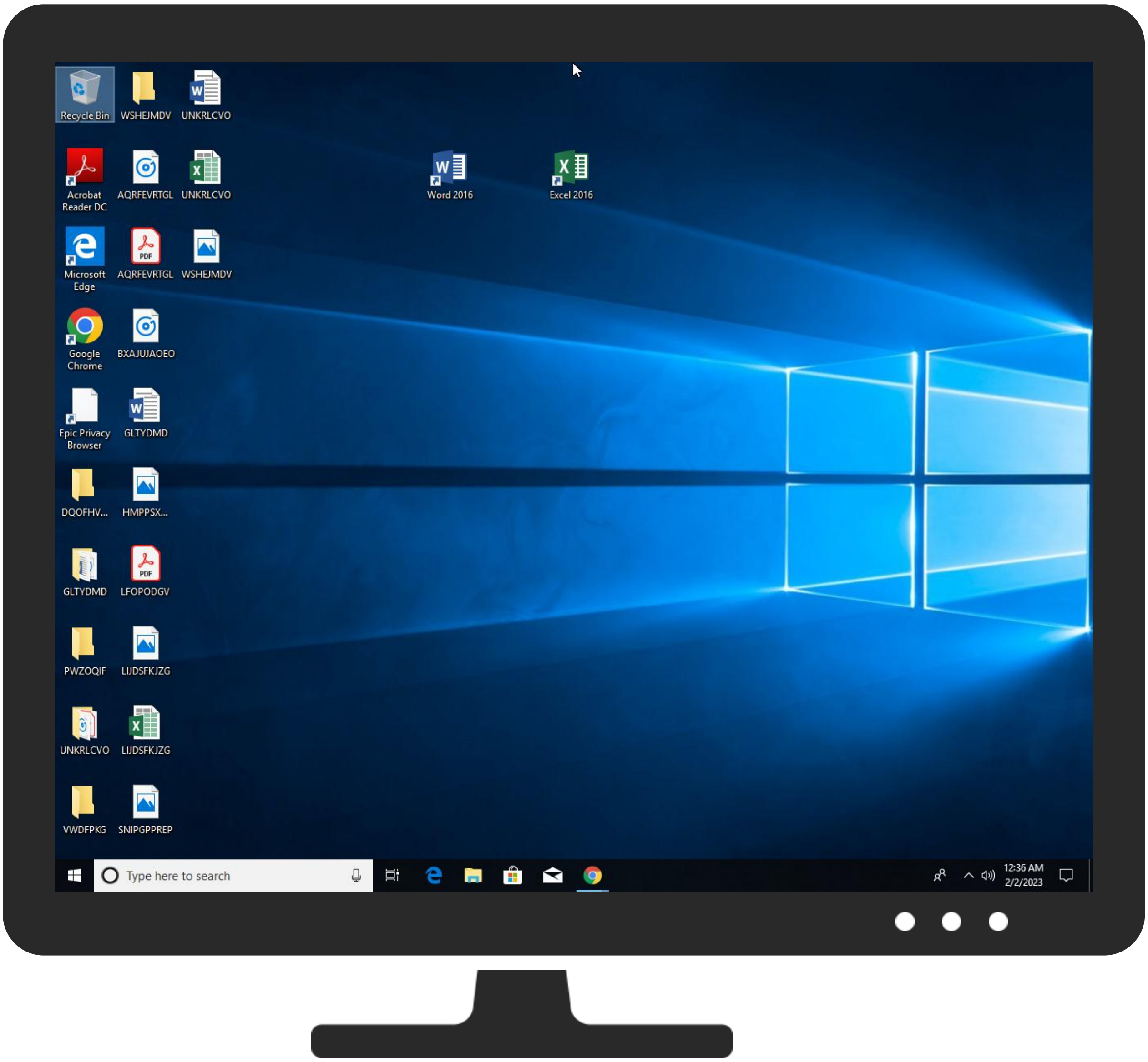
Mitre Att&ck Matrix

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

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
Epic Privacy Browser.lnk	0%	ReversingLabs		
Epic Privacy Browser.lnk	0%	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**

World Map of Contacted IPs

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796593
Start date and time:	2023-02-02 00:34:58 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 27s
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:	0
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:	Epic Privacy Browser.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: C00000BB

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**

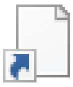
Static File Info

General

File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Working directory, Icon number=0, Archive, ctime=Thu Dec 1 02:22:36 2022, mtime=Thu Dec 1 02:22:36 2022, atime=Sun Aug 14 10:08:19 2022, length=2212864, window=hide
Entropy (8bit):	3.9222373748794426
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	Epic Privacy Browser.lnk
File size:	2349
MD5:	c60b17da68fad886be8bc335763eda29
SHA1:	368cbaf2aa7e594c80d309a9336f25c313eb7633
SHA256:	778712d44739c782b88ec1f2c4fa36e37486401e4027bf09cdb8b920bba3cff1
SHA512:	ea2e0131217490bd840966f058dcf56681b1e06682e60ac2e46a41e0b7dd71c82cd3295feaf6e022d670baa8d1cf88eebca3151855b8ae6677d775dc02653f2e

SSDEEP:	48:8wlqmDRe0Q9lnvy0Dk+ZQ9NqkzcvgWjE6:8nm9eHVyzDbzt
TLSH:	4D4151517BEA1B02F2FB763706F772215DBE3C58B755852E1150C1161E32C189C9C72B
File Content Preview:	L.................F.@.. ......(4......(4...c..(......!.....................:.:..DG..Yr?.D..U..k0.&...&.......z}J81q.._...z......(4.......t...CFSF..1......Q*,..AppData...t.Y^...H.g.3.. (......gVA.G..k...@........QX*.U.......]........................A.p.p.D

File Icon



Icon Hash:	74f0e4e4e4e1e1ed

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	
Icon location:	C:\Users\DaoThu\AppData\Local\Epic Privacy Browser\Application\epic.exe

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**