ANALYSIS REPORT OF Dropper.DOWNLOAD_FROM_URL.EXE

Thursday, June 29, 2023 1:52 PM

Hashes

Sha256 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
MD5sum 1d8562c0adcaee734d63f7baaca02f7c
Sha1 be138820e72435043b065fbf3a786be274b147ab

```
C:\Users\vboxuser\Desktop\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz
λ sha256sum.exe Malware.Unknown.exe
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a *Malware.Unknown.exe

C:\Users\vboxuser\Desktop\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz
λ md
md   md5sum.exe   MDEServer.exe   MDMAgent.exe   MDMAppInstaller.exe   MdmDiagnosticsTool.exe   MdRes.exe   MdSche
C:\Users\vboxuser\Desktop\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz
λ md5sum.exe Malware.Unknown.exe
1d8562c0adcaee734d63f7baaca02f7c *Malware.Unknown.exe

C:\Users\vboxuser\Desktop\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz
λ sha1sum.exe Malware.Unknown.exe
be138820e72435043b065fbf3a786be274b147ab *Malware.Unknown.exe

C:\Users\vboxuser\Desktop\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz
λ
```

- **VT Scan**

  https://www.virustotal.com/gui/file/92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

Static Analysis

Output of floss or string

```
8,808

------------------------------
| FLOSS UTF-16LE STRINGS (8) |
------------------------------
jjjj
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
open
```

jjjj
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
open

PEVIEW

property	value
sha256	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
sha1	BE138820E72435043B065FBF3A786BE274B147AB
md5	1D8562C0ADCAEE734D63F7BAACA02F7C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	12288 bytes
entropy	5.719
signature	Microsoft Visual C++
tooling	Visual Studio 2008
file-type	executable
cpu	32-bit
subsystem	**console**
file-version	n/a
description	n/a
stamps	
compiler-stamp	Sat Sep 04 18:11:12 2021
debugger-stamp	Sat Sep 04 18:11:12 2021
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
file-names	
export	n/a
debug	DownloadFromURL.pdb
version	n/a
manifest	n/a
.NET	n/a

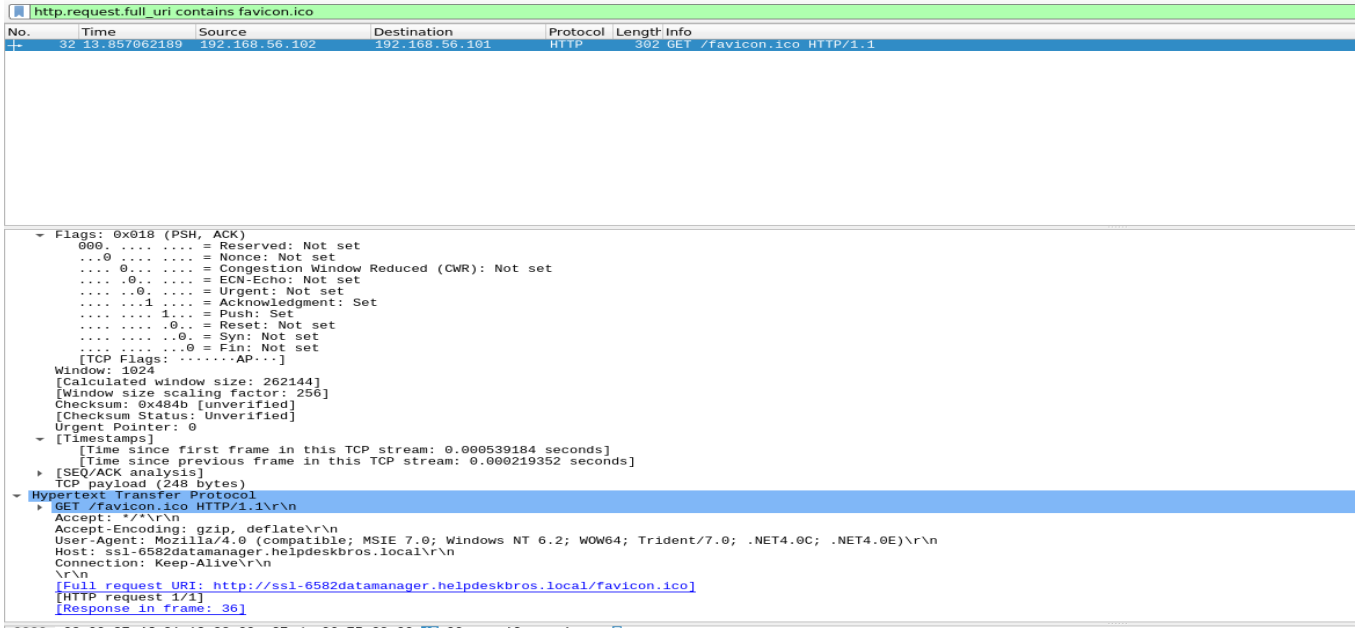
Windows API call

- DownloadFromUrl
- URLDownloadToFileW
- ShellExec
- InternetOpenURLA

Dynamic Analysis

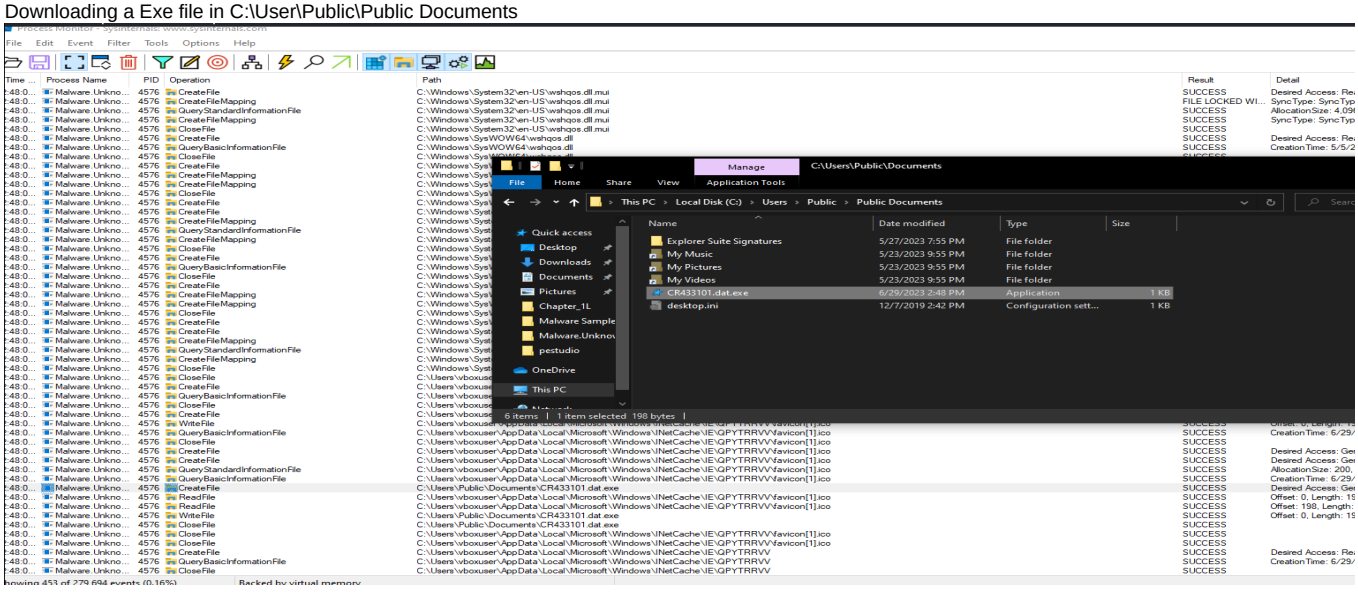
- cmd popped but no other indicator

Network signature

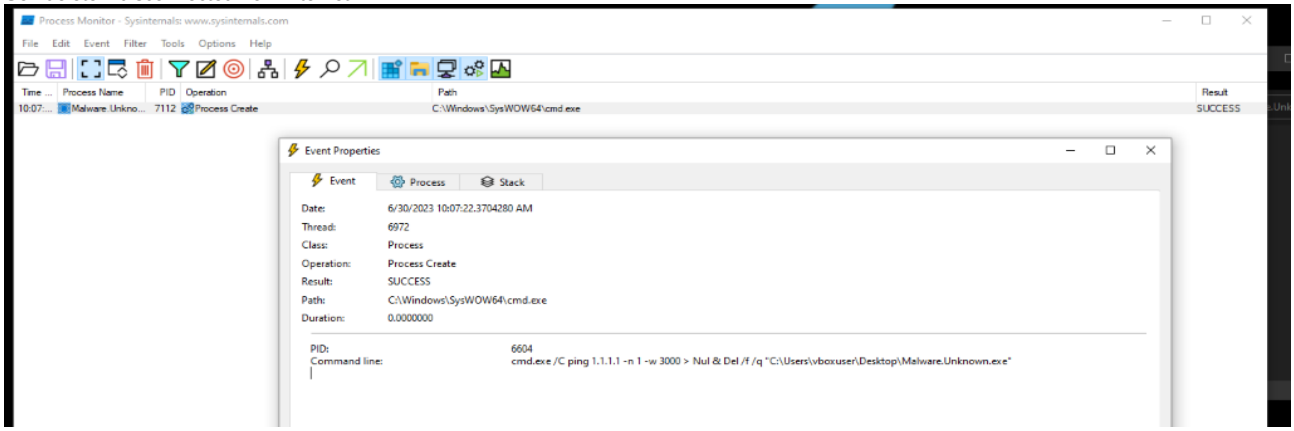


Host Based Signature

Downloading a Exe file in C:\User\Public\Public Documents



- Self-delete if disconnected from internet



- Program Execution Flow:
  - If URL exists:
    - Download favicon.ico(CR433101.dat.exe)
    - Run favicon.ico(CR433101.dat.exe)
  - If URL Doesn't exit:
    - Delete from disk
    - Don't run

Summary

Hashes:

SHA256: 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

MD5: 1d8562c0adcaee734d63f7baaca02f7c

SHA1: be138820e72435043b065fbf3a786be274b147ab

Static Analysis:

FLOSS or string output shows several strings including command execution, URLs, and file paths.

PEVIEW analysis shows various properties and signatures of the file.

Windows API calls include DownloadFromUrl, URLDownloadToFileW, ShellExec, and InternetOpenURLA.

Dynamic Analysis:

There is no clear indicator of malicious behavior in the dynamic analysis. The "cmd" process was popped, but no other significant indicators were observed.

Network Signature:

A network request was made for the favicon.ico file on a local domain.

The full request URI and details of the TCP stream are provided.

Host-Based Signature:

A file named "CR433101.dat.exe" was downloaded in the "C:\Users\Public\Documents" directory.

Program Execution Flow:

If the URL exists, the file "favicon.ico" (renamed as "CR433101.dat.exe") is downloaded and executed.

If the URL doesn't exist, the file is deleted from disk, and no execution occurs.

Based on the available information, it seems that the file "CR433101.dat.exe" (renamed from "favicon.ico") is being downloaded and executed from a specifi
and intent of the file.