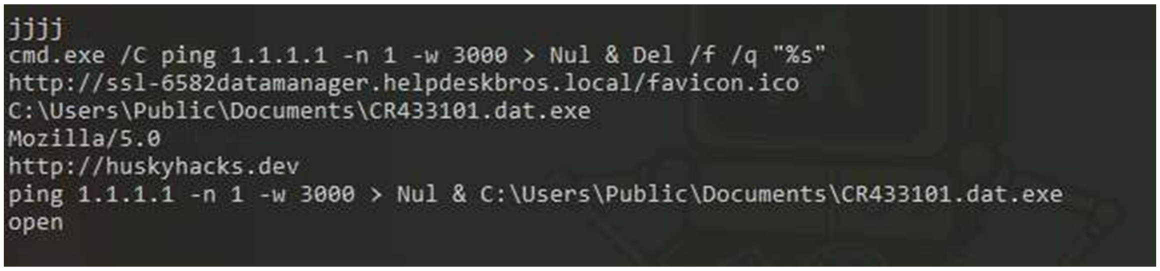
File Name : Malware.Unknown.exe.malz

Static Analysis (Report)

FLOSS (FLOSS.exe Malware.Unknown.exe.malz)



```
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
```

1. **cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 :** We could see that this is a domain based malware because it is pinging on 1.1.1.1(So we have top do Network based Analysis for POC).

2. **http://ssl-6582datamanager.helpdeskbros.local/favicon.ico :** As we can see that there are two protocols - 1st is HTTP and 2nd is ssl.(So we have to do a network based analysis)

3. **C:\Users\Public\Documents\CR433101.dat.exe** : As we can see that after executing the malware, we can see that the malware is creating a path in the documents directory and creating a new file name that is **CR433101.dat.exe** (So therefore we have to do a host based analysis for the system for POC)

4. **Nul & Del /f /q :** As we can see that there is a variable that is null and delete so that means that the program will run for a single time because -n 1 is representing that it will only run the payload for a single interval of the time with an internet connection. If the internet is not connected then the payload will execute for a single point of time and it will stop the entire the process and deleted the malware

from the system" (So therefore we have to do an host based analysis to determine whether the malware is null and delete or not)

Dynamic Analysis (Report)

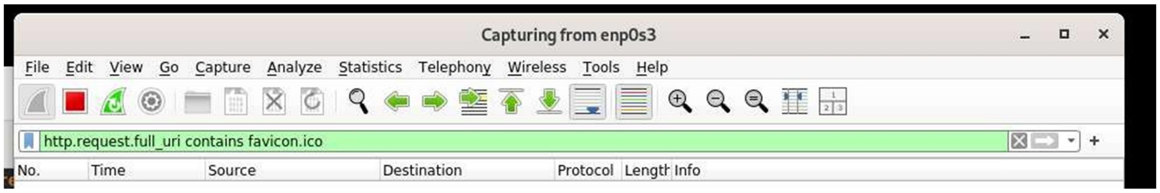
Network Based Analysis

Hypertext Transfer Protocol

Step 1: Open remnux and open inetsim. And in the another terminal open Wireshark with the command:- Sudo Wireshark.

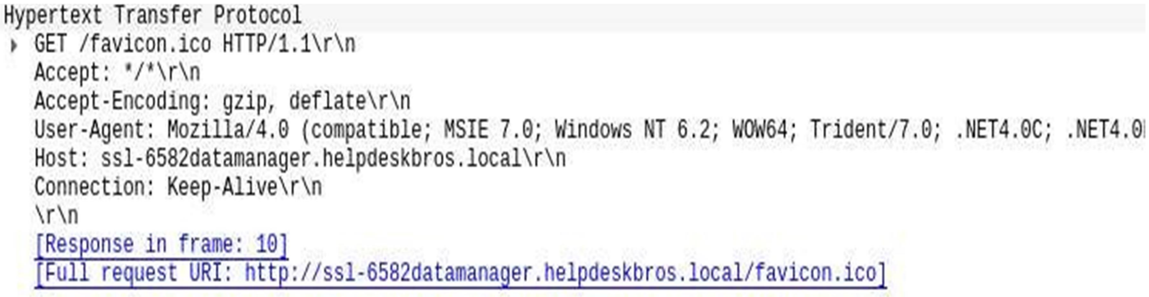
Step 2: Open flareVM and Execute the malware by removing the the malz form the File .

Step 3: Add "http.request.full_uri contains favicon.ico" in the Wireshark header (to find http connections).



```
http.request.full_uri contains favicon.ico
```

Step 4: Go to Hypertext Transfer Protocol.



```
Hypertext Transfer Protocol
 ▸ GET /favicon.ico HTTP/1.1\r\n
   Accept: */*\r\n
   Accept-Encoding: gzip, deflate\r\n
   User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0
   Host: ssl-6582datamanager.helpdeskbros.local\r\n
   Connection: Keep-Alive\r\n
   \r\n
   [Response in frame: 10]
   [Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
```

1. **GET /favicon.ico HTTP/1.1\r\n:**
    - **GET:** HTTP method used to request data from a server.
    - **/favicon.ico:** The path to the resource requested — in this case, the website's favicon (It is a domain which is proved).
    - **HTTP/1.1:** Version of the HTTP protocol being used.

2. **Host: ssl-6582datamanager.helpdeskbros.local\r\n** : Specifies the target host(domain name). ssl-6582datamanager.helpdeskbros.local is likely an internal (non-public) domain.

3. **Connection: Keep-Alive\r\n :** This tells the server or client that "Please keep the TCP connection open after this request/response."4**.[Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico] :** The wireshrak tool reconstructs and shows the full URI that was requested.

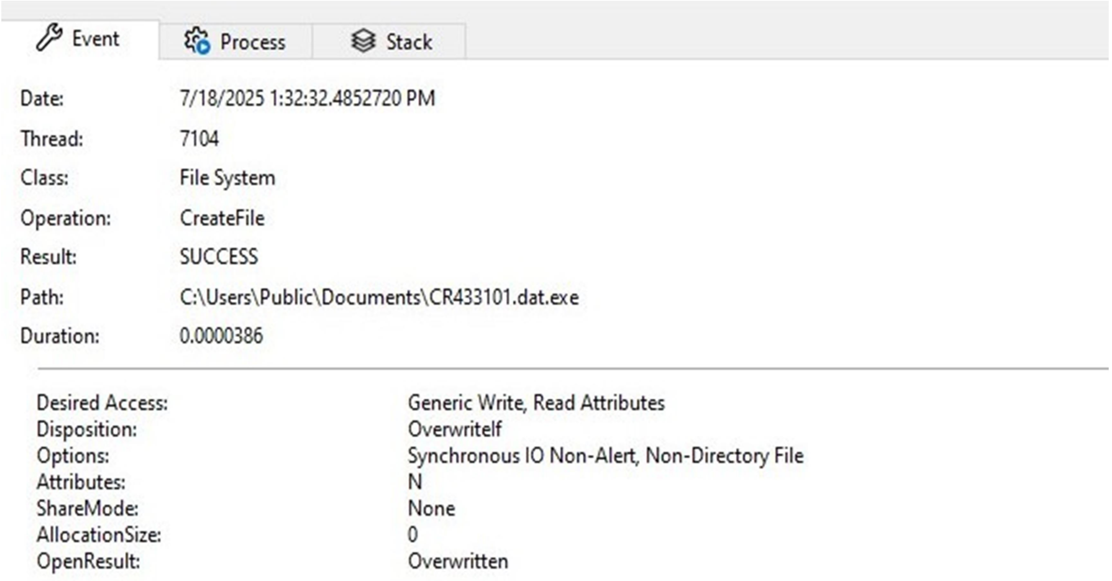
Host Based Analysis

1. CR433101.dat.exe

Step 1: Open procmon and open the Filter of procmon.

Step 2: Type Process is Malware.Unknown.exe (Press add) and ok . And type operation contains File (Press add) and ok .

Step 3: We find the File that create a new name of the malware when it executes (if we delete this File in the path the malware is Deleted)



```
Date:        7/18/2025 1:32:32.4852720 PM
Thread:      7104
Class:       File System
Operation:   CreateFile
Result:      SUCCESS
Path:        C:\Users\Public\Documents\CR433101.dat.exe
Duration:    0.0000386

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

- C:\Users\Public\Documents\CR433101.dat.exe : This is the full path to the file being accessed. The .dat.exe extension is suspicious—it may be disguising an executable file as a data file, which is a common malware tactic.

- Desired Access: **Generic Write, Read Attributes** -> The process requested permission to write to the file and read its attributes.

- Disposition: **OverwriteIf ->** Indicates the file was to be overwritten if it already existed—and created otherwise.

2. NULL And Delete :

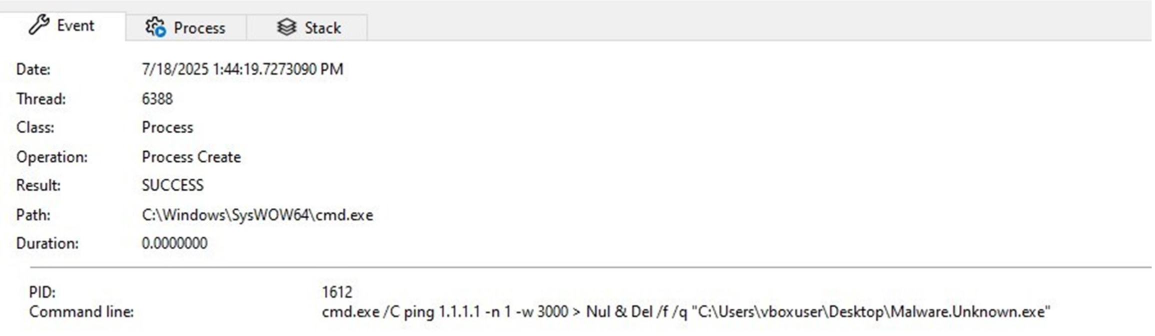
Step 1: Close inetsim Inside Remnux .

Step 2: Go to procmon and Go to the filter.

Step 3: Type Details Contains cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q then Include (Press add) and ok.

Step 4: Type Process is Malware.Unknown.exe then Include (Press add) and ok.

Step 5: Execute Malware.Unknown.exe file and it automatically delete that file. And you can see that file in procmon and investigate it by enter it.



```
Date:           7/18/2025 1:44:19.7273090 PM
Thread:         6388
Class:          Process
Operation:      Process Create
Result:         SUCCESS
Path:           C:\Windows\SysWOW64\cmd.exe
Duration:       0.0000000

PID:                    1612
Command line:           cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\vboxuser\Desktop\Malware.Unknown.exe"
```

cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\vboxuser \Desktop\Malware.Unknown.exe"

- cmd.exe /C : Tells the Command Prompt to run the following command string and then terminate.
- ping 1.1.1.1: Sends a ping to IP address 1.1.1.1 .
- -n 1: Send only 1 echo request.
- -w 3000: Wait up to 3000 milliseconds (3 seconds) for a reply.
- > Nul: Redirects output to NUL, meaning it’s discarded (silent execution).
- & : Separates two commands. The second command runs after the first one finishes (in this case, after the delay).
- Del /f /q "C:\Users\vboxuser\Desktop\Malware.Unknown.exe" : This deletes a file:

  Del: Delete command.

  /f: Force deletion, even if the file is read-only.

  /q: Quiet mode (no confirmation).

"C:\Users\vboxuser\Desktop\Malware.Unknown.exe": Path to the target file.