

Basics Dynamic Analysis

Dynamic // Heuristic // Behavioral Analysis

There are gonna two indicators as **Host/Network indicators**

host : *when something happend on host // Delete*

Network : *Internet thing*

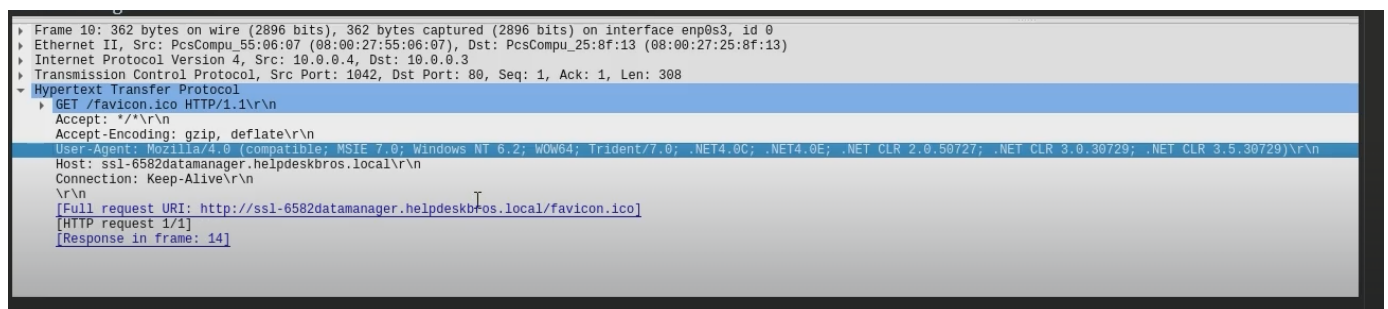
wireshark and inetsim.

- To check for any **network indicators**.

Turn on your `inetsim` and open `wireshark` ,start capturing the traffic to analyze.

Filter Used :

```
tcp.port == 80 && http.request.full_uri contains favicon.ico
```



cause `favicon.ico` we find on running floss as a full string, so we confirmed that our malware does send request to the internet to download a second stage payload to further infiltrate.

To check for any **host-based indicators**.

open `Procmon` , this is made by microsoft , its most imp features is filter .

- Put Process name in the filter.
- Add other filter if you want.
- Run your malware.
- It will Capture what your malware did from the very starting
- You can select files in operations.(will give you all interactions with any files)

10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes
10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Offset: 1,057,792, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	QueryStandardInformation...	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	AllocationSize: 200, EndOfFile: 198, NumberOfLinks: 1, DeletePending: False, Directory: False
10/25/13...	Malware.Unknown.exe	2816	QueryBasicInformationF...	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	CreationTime: 9/5/2021 10:24:55 AM, LastAccessTime: 9/5/2021 10:24:55 AM, LastWriteTime: 9/5/2021 10:24:55
10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Non-D
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	Offset: 0, Length: 198, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	Offset: 198, Length: 0
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Offset: 0, Length: 198, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Offset: 562,176, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Offset: 3,818,496, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,785,728, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,703,808, Length: 28,672, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,470,336, Length: 12,288, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9H	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Rea
10/25/13...	Malware.Unknown.exe	2816	QueryBasicInformationF...	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9H	SUCCESS	CreationTime: 9/5/2021 10:24:55 AM, LastAccessTime: 9/5/2021 10:24:55 AM, LastWriteTime: 9/5/2021 10:24:55
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9H	SUCCESS	
10/25/13...	Malware.Unknown.exe	2816	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 4,060,160, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\husky\AppData\Local\Microsoft\Windows\NetCache\IE\CM8P1S9...	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options: Synchronous IO Non-Alert, Non-Direct
10/25/13...	Malware.Unknown.exe	2816	CreateFile	C:\Users\husky\Desktop	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Rea
10/25/13...	Malware.Unknown.exe	2816	QueryBasicInformationF...	C:\Users\husky\Desktop	SUCCESS	CreationTime: 8/22/2021 10:37:39 AM, LastAccessTime: 9/5/2021 10:24:55 AM, LastWriteTime: 9/5/2021 10:21:1
10/25/13...	Malware.Unknown.exe	2816	CloseFile	C:\Users\husky\Desktop	SUCCESS	

we found a file path , which we also did find in the floss .

From every thing we can confirm that , malware is downloading a second stage payload and writing it to the disk to execute further operations

Time ...	Process Name	PID	Operation	Path	Result	Detail
1:32:4...	Malware.Unknown...	4600	Process Start		SUCCESS	Parent PID: 4088, Command line: "C:\Users\visual\Desktop\Malware.Unknown.exe\Malware.Unknown.exe", Current directory: C:\...
1:32:5...	Malware.Unknown...	4600	QueryNameInformationFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Name: \Windows\SysWOW64\cmd.exe
1:32:5...	Malware.Unknown...	4600	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 3132, Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > nul & Del /f /q "C:\Users\visual\Desktop\Malware.Unknown.exe\...
1:32:5...	Malware.Unknown...	4600	QueryNameInformationFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Name: \Windows\SysWOW64\cmd.exe

Finally :

We know the program flow.

- If URL Exits
 - Download Favicon.ico
 - write to disk (CR433101.dat.exe)
 - Run Favicon.ico (CR433101.dat.exe)
- If URL Doesn't exits.
 - Delete from disk
 - Do not run.