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*

---

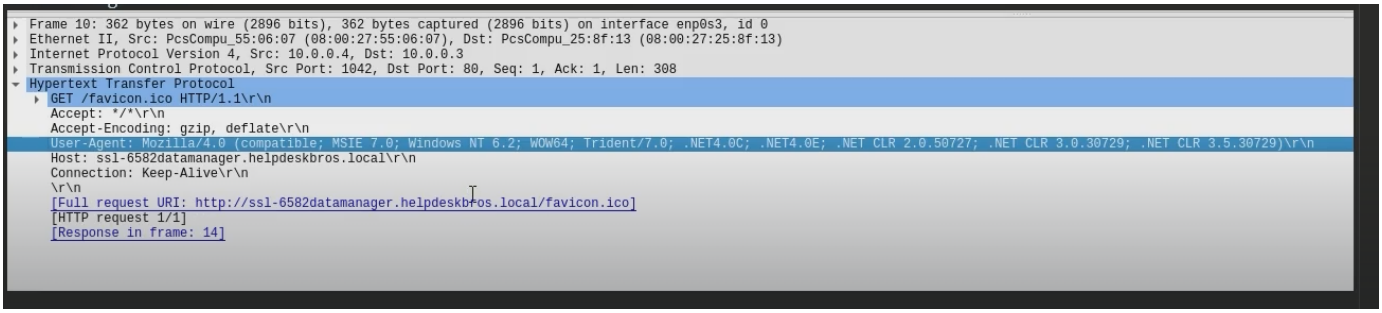
wireshark and inetsim.

- 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
```

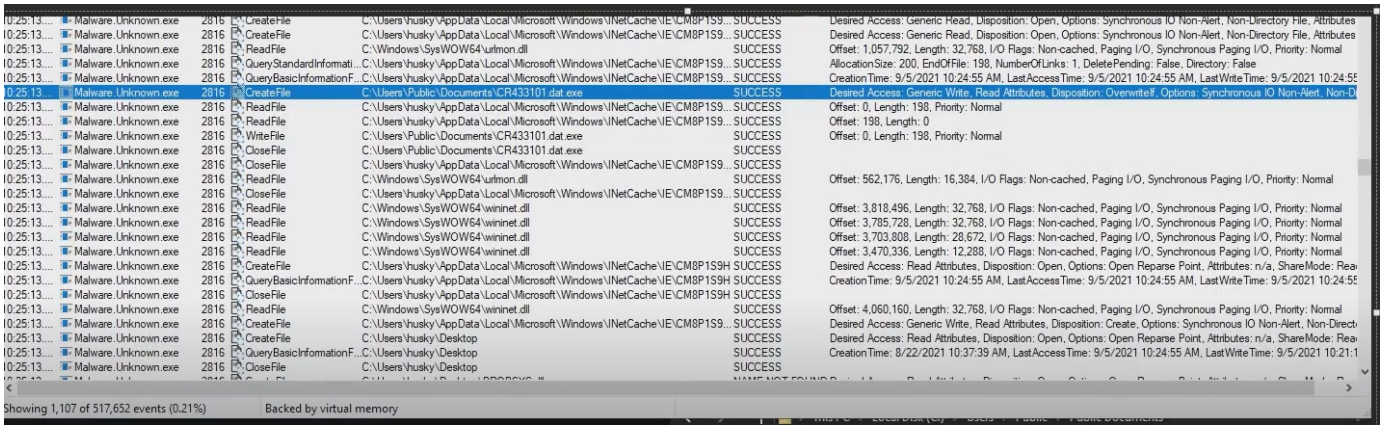


cause `favicon.ico` we find on running floss as a full string, so we confirmed that our malware does send request to the internet to download a second stage payload to further infiltrate.

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

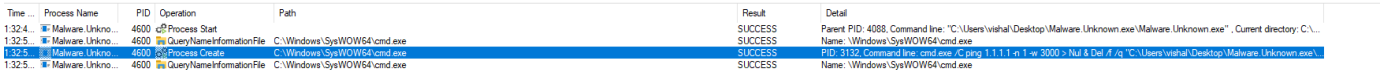
open `Procmon` , this is made by microsoft , its most imp features is filter .

- 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)



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



FInallay :

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.