Tool list

Monday, July 1, 2024

1:39 PM

Basic Static Analysis:

* File hashes:
  + to get file hashes you will do SHA256sum. exe then the malware name
  + To get file hash you will type in md5sum.exe then the malware name
* VirusTotal:
  + We will utilize this to search the hashes to see if it has been used anywhere else
* Floss:
  + this is used to pull out important strings from binary and decode anything it finds
* PEStudio
  + This can be used to find everything above such as hashes, important things it found that it thinks ins malicious, etc
* PEView
  + This is used to exam the structure of the Portable executables (PE) for example if a file has MZ or 4D 5A it is a PE.

Basic Dynamic Analysis:

* Wireshark
* Inetsim
* Netcat
* TCPView
* Procmon

Malware.Unknown.exe.

Monday, July 1, 2024

9:44 AM

# File Has & VT Analysis

SHA256 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a \*Malware.Unknown.exe.malz MD5Sum 1d8562c0adcaee734d63f7baaca02f7c \*Malware.Unknown.exe.malz

# Basic Static Analysis

|  |  |
| --- | --- |
| Strings & Floss Output | jjjj  cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s" httxp://ssl-6582datamanager.helpdeskbros.local/favicon.ico  C:\Users\Public\Documents\CR433101.dat.exe  Mozilla/5.0  ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe open |

# Basic Dynamic Analysis

Utilizing the above information that was captured utilizing floss in our static analysis to help with the Dynamic analysis.

## Network Signature

|  |  |
| --- | --- |
| I will start off by using wireshark to capture outbound network request. I utilized one of the strings that was found in our static analysis "httxp://ssl-6582datamanager.helpdeskbros.local/favicon.ico".    In the screenshot you will see I filter:http.request.full\_uri contains favicon.ico. This shows when the malware is clicked on it establish a connection with favicon.ico. This is a big find. | network_capture.png |

# Host-Based Indicators

|  |  |
| --- | --- |
| Now that we finished our network signature, I will move onto the host based signature. Like we did before I will go ahead and take the information we found from running floss and use that to help with the host based indicators.    If you recall in our static analysis we found the path "C:\Users\Public\Documents\CR433101.dat.exe". This indicates the malware puts something into our path.    I utilized procmon to see if this is true. I detontated the malware and used procmon to filter to see if this was true. If you look at the screen shots you will see the evidence I collected once I ran the malware. This confirmed once the malware is detonated it puts something suspicious in the public document folder. | host_capture.png  host_capture_2.png |

# Final

Now, that I have utilized everything that we have found. I will talk about what I came up with. This malware is very unique. If the URL exist:

* It will download favicon.io
* Writes to disk:CR433101.dat.exe
* Run favicon.ico:CR433101.dat.exe

If the URL doesn’t exist:

* Delete from disk
* Do not run