Lab 1 Solutions - The Case of Remcos RAT

Lab 1 - The case of Remcos RAT

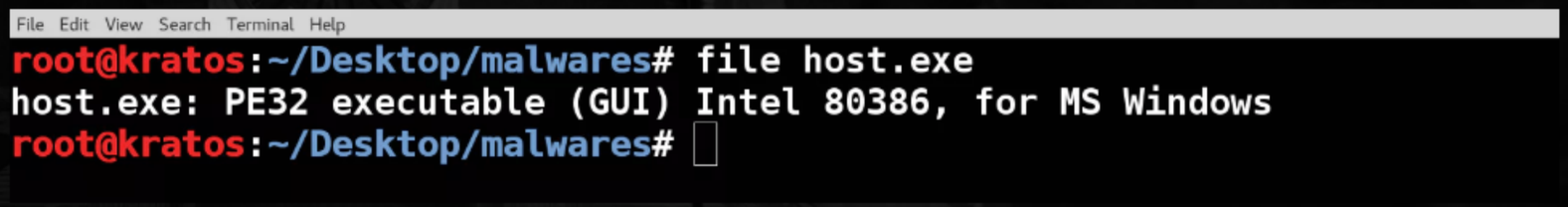
While examining a system the system admin noticed an unusual process running on the server. The system admin has collected the file (***host.exe***) associated with that process and sent it you for further analysis. Analyze the file and answer the below questions

- What is the file type?
- Determine the cryptographic hash
- Is the file packed/obfuscated?
- Are there any interesting strings?
- Which malware imports suggest the use of network activity?
- Is the file malicious?

Answers

01. What is the File type?

File Type can be determined using ***file*** utility on Linux based systems and another alternative to file utility is using ***pestudio*** on Windows systems. In this case, the file is a PE file indicating that the target is Windows operating system



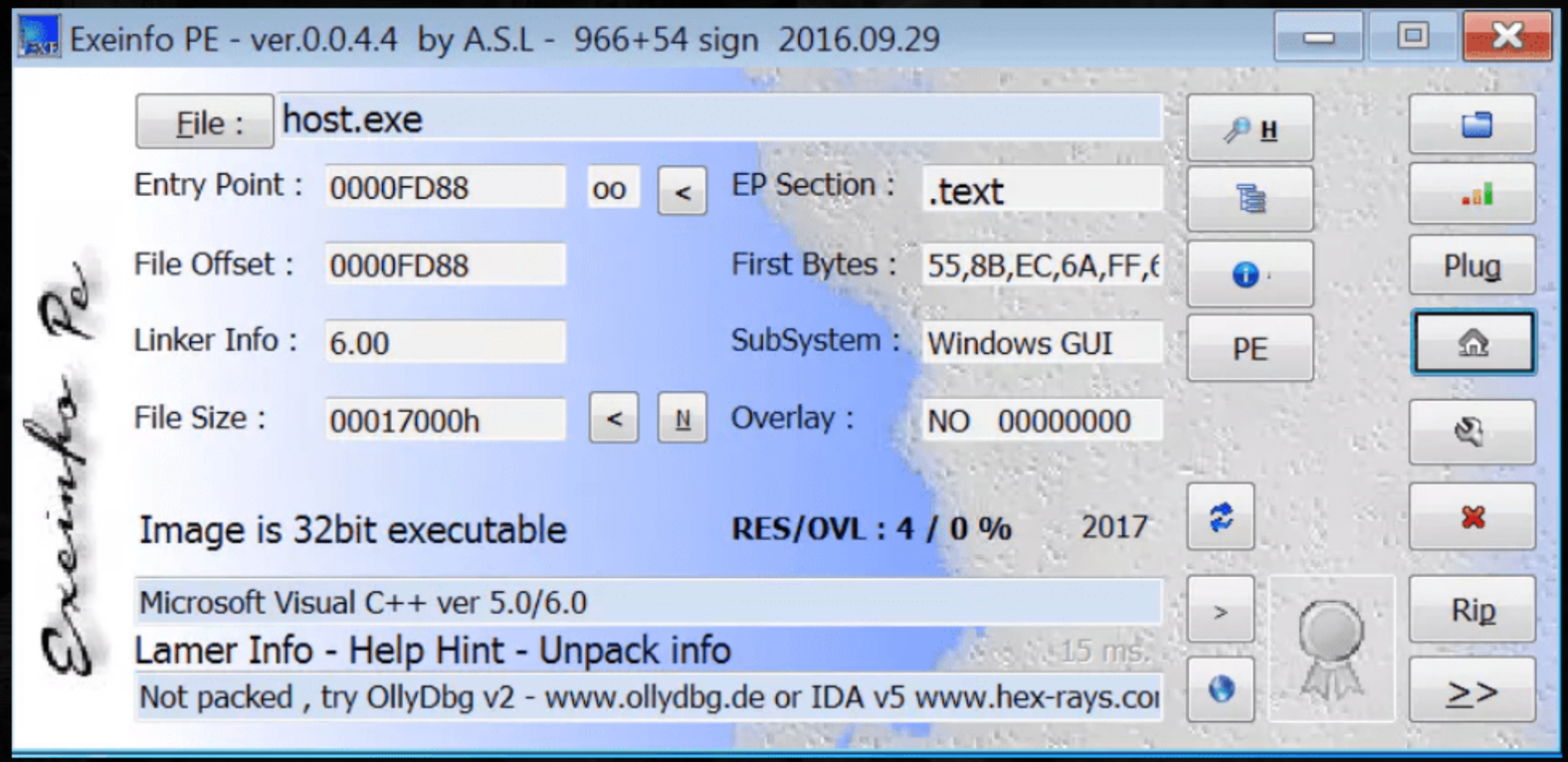
02. Determine the Cryptographic Hash

The screenshot shows the cryptographic hashes associated with the sample, these cryptographic hashes can be used as a unique identifier throughout the course of analysis. On Windows system, ***pestudio*** can be used to determine the cryptographic hash

```
File  Edit  View  Search  Terminal  Help
root@kratos:~/Desktop/malwares# md5sum host.exe
4a21e5957aeda4467dad810e29bf2cfa  host.exe
root@kratos:~/Desktop/malwares# sha256sum host.exe
ebf5b7798713eef8e2fb453b94dfab6b3535e283d54bc003c11710300dd8ddb3  host.exe
root@kratos:~/Desktop/malwares# sha1sum host.exe
f06ccfb42a4f4918e880e57581ff47f6e53411e7  host.exe
```

03. Is the file packed/obfuscated?

Loading the file in ***Exeinfo*** PE tool does not show any indication of the file being packed or obfuscated.



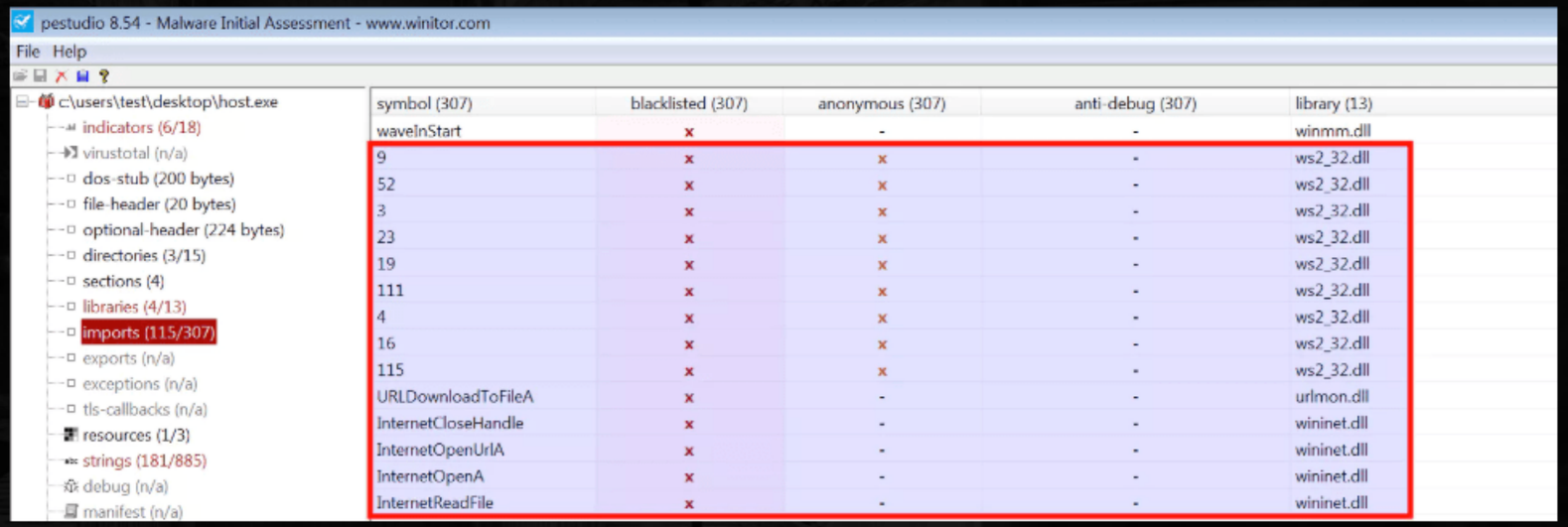
04. Are there any interesting strings?

Extracting strings from the strings utility show references to interesting strings. There are a lot of strings which is of interest, one of the strings shown below has references to the ***Run registry key*** indicating that probably malware is going to persist by adding an entry in this registry key. The below strings also show reference to a domain and a unique string ***"REMCOS V"*** this can be a good host-based indicator.

```
|dmc|
[DataStart]
[DataStart]0000
%02i:%02i:%02i:%03i [KeepAlive]
Enabled! (Timeout: %i seconds)
[Firefox StoredLogins not found]
\AppData\Roaming\Mozilla\Firefox\Profiles\
[Firefox cookies found, cleared!]
\cookies.sqlite
[Firefox Cookies not found]
[IE cookies cleared!]
Software\Microsoft\Windows\CurrentVersion\Run\
exit
\install.bat
Remcos Mutex Inj
Connected to C&C!
%02i:%02i:%02i:%03i [INFO]
Initializing connection to C&C...
 * Breaking-Security.Net
 * REMCOS v
```

05. Which malware imports suggest the use of network activity?

The file imports various functions from ***ws2_32.dll***, ***urlmon.dll*** & ***wininet.dll*** which provides network functionality. Malware importing these functions suggest the use of network activity.



06. Is the file malicious?

Submitting the file to ***VirusTotal*** confirms it to be malicious and one of the AV vendor (Avast) identifies this malware as ***Remcos RAT***

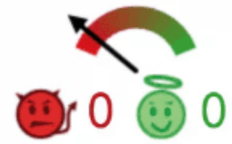
virustotal

SHA256: ebf5b7798713eef8e2fb453b94dfab6b3535e283d54bc003c11710300dd8ddb3

File name: host.exe

Detection ratio: 39 / 58

Analysis date: 2017-03-11 11:27:25 UTC (1 minute ago)



Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
ALYac	Generic.Malware.SL!B.B21311F3	20170311
AVG	Agent5.AWOO	20170311
Ad-Aware	Generic.Malware.SL!B.B21311F3	20170311
AhnLab-V3	Backdoor/Win32.Farfli.C1564294	20170310
Antiy-AVL	Trojan/Win32.AGeneric	20170311
Arcabit	Generic.Malware.SL!B.B21311F3	20170311
Avast	Win32:RemcosRAT-A [Trj]	20170311
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9999	20170311