

Week-9 IOT Exercise-1
Lakshminath Reddy Alamuru
SUID: 367982169

Downloading the virtual box with windows 11 which is taking time. As I have linux machine virtual box.

Task-1

Downloaded the key.7z file and extracted the file with passwords malware.
 Then opened the file from PEview and provided the screenshots after navigating to import address table in rdata section

Windows11 [Running]

PEview - C:\Users\laksh\Downloads\key.exe

File View Go Help

Viewing IMPORT Address Table

pFile	Data	Description	Value
00021000	0002F93E	Hint/Name RVA	02A8 RegSetValueExA
00021004	0002F930	Hint/Name RVA	028A RegOpenKeyA
00021008	0002F922	Hint/Name RVA	025B RegCloseKey
0002100C	00000000	End of Imports	ADVAPI32.dll
00021010	0002FEC8	Hint/Name RVA	034E HeapSize
00021014	0002FED4	Hint/Name RVA	0611 WriteConsoleW
00021018	0002FC46	Hint/Name RVA	0462 RaiseException
0002101C	0002F95E	Hint/Name RVA	057D Sleep
00021020	0002F966	Hint/Name RVA	00A8 CopyFileA
00021024	0002F972	Hint/Name RVA	0207 GetConsoleWindow
00021028	0002F986	Hint/Name RVA	0261 GetLastError
0002102C	0002F996	Hint/Name RVA	05FE WideCharToMultiBy
00021030	0002F9AC	Hint/Name RVA	0131 EnterCriticalSection
00021034	0002F9C4	Hint/Name RVA	03BD LeaveCriticalSection
00021038	0002F9DC	Hint/Name RVA	0110 DeleteCriticalSection

File View Go Help

pFile	Data	Description	Value
00021120	0002FDFE	Hint/Name RVA	017B FindFirstFileExW
00021124	0002FE12	Hint/Name RVA	018C FindNextFileW
00021128	0002FE22	Hint/Name RVA	038B IsValidCodePage
0002112C	0002FE34	Hint/Name RVA	01B2 GetACP
00021130	0002FE3E	Hint/Name RVA	0297 GetOEMCP
00021134	0002FE4A	Hint/Name RVA	0237 GetEnvironmentStr
00021138	0002FE64	Hint/Name RVA	01AA FreeEnvironmentStr
0002113C	0002FE7E	Hint/Name RVA	0514 SetEnvironmentVaria
00021140	0002FE98	Hint/Name RVA	054A SetStdHandle
00021144	0002FEA8	Hint/Name RVA	02B4 GetProcessHeap
00021148	00000000	End of Imports	KERNEL32.dll
0002114C	0002F902	Hint/Name RVA	0121 GetAsyncKeyState
00021150	0002F8F4	Hint/Name RVA	0380 ShowWindow
00021154	00000000	End of Imports	USER32.dll

User32.dll, give the hints of getasynckeysstate, showwindow.

PEview - C:\Users\laksh\Downloads\key.exe

Raw Data | **Value**

```

53 68 6F 77 57 69 6E 64 6F 77 00 00 21 01 ..ShowWindow...!
74 41 73 79 6E 63 4B 65 79 53 74 61 74 65 GetAsyncKeyState
55 53 45 52 33 32 2E 64 6C 6C 00 00 5B 02 ..USER32.dll...[.
67 43 6C 6F 73 65 4B 65 79 00 8A 02 52 65 RegCloseKey...Re
70 65 6E 4B 65 79 41 00 A8 02 52 65 67 53 gOpenKeyA...RegS
56 61 6C 75 65 45 78 41 00 00 41 44 56 41 etValueExA..ADVA
33 32 2E 64 6C 6C 00 00 7D 05 53 6C 65 65 P132.dll...}.Slee
A8 00 43 6F 70 79 46 69 6C 65 41 00 07 02 p...CopyFileA...
74 43 6F 6E 73 6F 6C 65 57 69 6E 64 6F 77 GetConsoleWindow
61 02 47 65 74 4C 61 73 74 45 72 72 6F 72 ...a.GetLastError
FE 05 57 69 64 65 43 68 61 72 54 6F 4D 75 ...WideCharToMu
69 42 79 74 65 00 31 01 45 6E 74 65 72 43 ItiByte.1.EnterC
74 69 63 61 6C 53 65 63 74 69 6F 6E 00 00 critcalSection..
4C 65 61 76 65 43 72 69 74 69 63 61 6C 53 ..LeaveCriticalSection
74 69 6F 6E 00 00 10 01 44 65 6C 65 74 65 ection....Delete

```

Viewing IMPORT Hints/Names & DLL Names

> This PC

PEview - C:\Users\laksh\Downloads\key.exe

Raw Data | **Value**

```

74 43 75 72 72 65 6E 74 50 72 6F 63 65 73 GetCurrentProces
8C 05 54 65 72 6D 69 6E 61 74 65 50 72 6F s...TerminatePro
73 73 00 00 86 03 49 73 50 72 6F 63 65 73 cess....IsProces
72 46 65 61 74 75 72 65 50 72 65 73 65 6E sorFeaturePresen
4D 04 51 75 65 72 79 50 65 72 66 6F 72 6D t.M.QueryPerform
63 65 43 6F 75 6E 74 65 72 00 18 02 47 65 anceCounter...Ge
75 72 72 65 6E 74 50 72 6F 63 65 73 73 49 tCurrentProcessI
1C 02 47 65 74 43 75 72 72 65 6E 74 54 68 d...GetCurrentTh
61 64 49 64 00 00 63 03 49 6E 69 74 69 61 readId..c.Initia
7A 65 53 4C 69 73 74 48 65 61 64 00 7F 03 lizeSListHead...
44 65 62 75 67 67 65 72 50 72 65 73 65 6E lsDebuggerPresen
D0 02 47 65 74 53 74 61 72 74 75 70 49 6E t...GetStartupIn
57 00 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C foW KERNEL32.dll
62 04 52 61 69 73 65 45 78 63 65 70 74 69 ...b.RaiseExcepti
00 00 03 04 52 74 6C 55 6E 77 69 6E 64 00 on....RtlUnwind.

```

Viewing IMPORT Hints/Names & DLL Names

> This PC

> CD Drive (D:) CC

PEview - C:\Users\laksh\Downloads\key.exe

Raw Data | **Value**

```

53 68 6F 77 57 69 6E 64 6F 77 00 00 21 01 ..ShowWindow...!
74 41 73 79 6E 63 4B 65 79 53 74 61 74 65 GetAsyncKeyState
55 53 45 52 33 32 2E 64 6C 6C 00 00 5B 02 ..USER32.dll...[.
67 43 6C 6F 73 65 4B 65 79 00 8A 02 52 65 RegCloseKey...Re
70 65 6E 4B 65 79 41 00 A8 02 52 65 67 53 gOpenKeyA...RegS
56 61 6C 75 65 45 78 41 00 00 41 44 56 41 etValueExA..ADVA
33 32 2E 64 6C 6C 00 00 7D 05 53 6C 65 65 P132.dll...}.Slee
A8 00 43 6F 70 79 46 69 6C 65 41 00 07 02 p...CopyFileA...
74 43 6F 6E 73 6F 6C 65 57 69 6E 64 6F 77 GetConsoleWindow
61 02 47 65 74 4C 61 73 74 45 72 72 6F 72 ...a.GetLastError

```

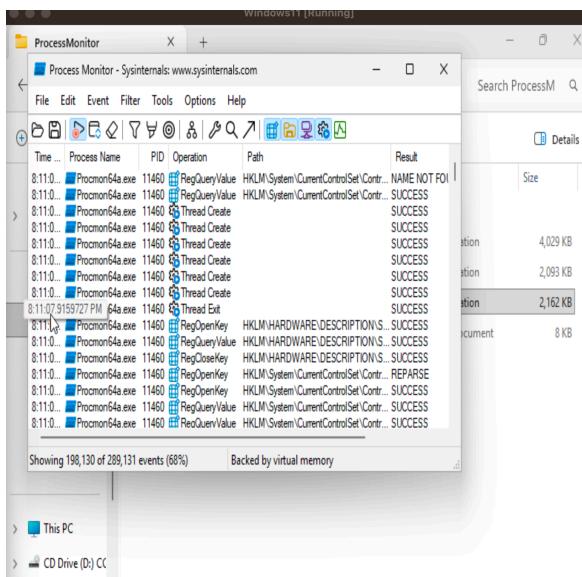
User32.dll is windows UI/input API

GetAsyncKeyState often signals key polling (possible keylogger/hotkey/anti-analysis) when called repeatedly in tight loops and followed by writes or network send.
ShowWindow manipulates window visibility (e.g., SW_HIDE)

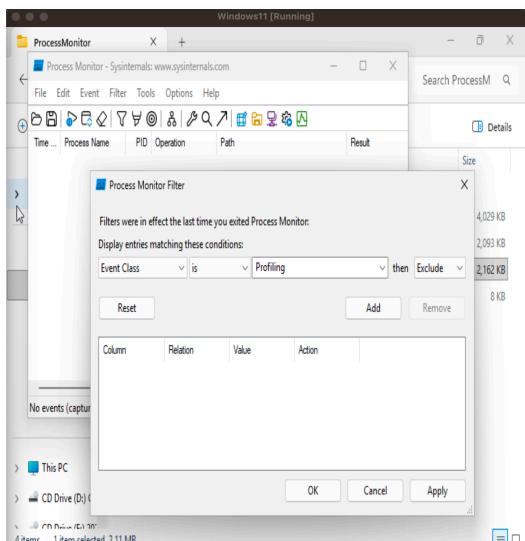
ADVAPI32.dll gives regopenkey, regclosekey
Kernel.dll gives getprocessheap , setsthandle which is more about the kernel related hints that can provide.

Task-2

I have downloaded the application for process monitor.



I have removed all the processes, and showed the screenshot below



Learnings:

Got the greater understanding on the PEview, process monitor application. Which gave me the better understanding on the dynamic malware analysis.