|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 3 | Basic Dynamic Analysis - Practical | 120 mins |

**Lesson Objectives**

Perform Basic Dynamic Analysis on unknown Portable Executable with the following tools:

* Process Monitor
* Process Explorer
* Regshot
* ApateDNS
* Netcat
* CaptureBAT

Note: Perform basic dynamic analysis in a new and clean VM snapshot everytime.

Submit your answers on MeL.

# Lab 01 [60 mins]

Refer to the files: Lab03-03.exe

**Question 1**

What are the imported DLLs of this malware? KERNEL32.dll

**Question 2**

Is the malware packed? No

**Question 3**

What happened when you execute the malware? What does the malware do before it exits? It created svchost.exe in C:\WINDOWS\system32\svchost.exe

**Question 4**

Using Process Explorer, examine the Strings in the malware, on disk and in memory

Image

Software\Microsoft\Windows NT\CurrentVersion\Svchost

\Registry\Machine\System\CurrentControlSet\Control\SercurePipeServers\

Svchost.exe

KERNEL32.dll

Memory

Microsoft Visual C++ Runtime Library

CreateFileA

Practicalmalwareanalysis.log

C:\\WINDOWS\system32\svchost.exe

SetWindowsHookExA

UnhookWindowsHookEx

**Question 5**

Does the malware create any file?

Yes, it creates Practicalmalwareanalysis.log

**Question 6**

What do you think is the purpose of the malware?

It is a Keylogger

# Lab 02 [60 mins]

Analyse the malware found in the file Lab03-04.exe using basic dynamic analysis

tools.

**Question 1**

What happens when you run this file? It start a Process that did some reading of the system registry. Before it end process, it run a CMD command "C:\WINDOWS\system32\cmd.exe" /c del C:\MAAT\Labs\WEEK3~1\COPYOF~1.EXE >> NUL which delete itself

**Question 2**

What is causing the roadblock in dynamic analysis?

The program close too fast, not allowing us to do much dynamic analysis. There is also not much information we can get from static analysis too.

**Question 3**

Are there other ways to run this program? We can use ollydbg or IDAPro where we can run the program in debugger mode where we can set break point