|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 2/3 | 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

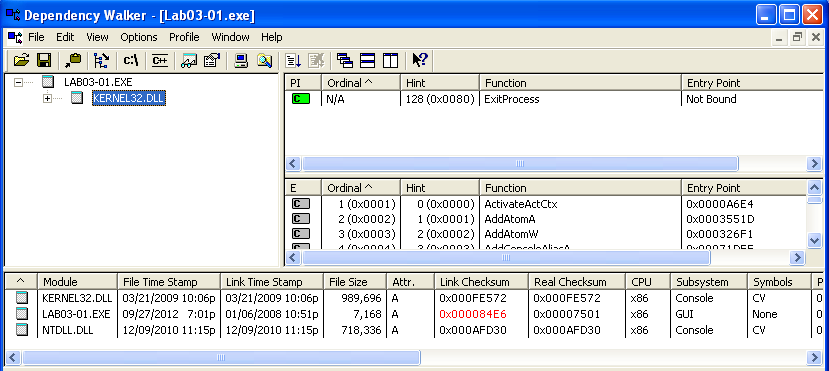
Note: Perform basic dynamic analysis in a new and clean VM snapshot every time.

# Lab 01 [60 mins]

Refer to the files: lab03-01.exe. Use Dynamic Analysis to answer the following questions.

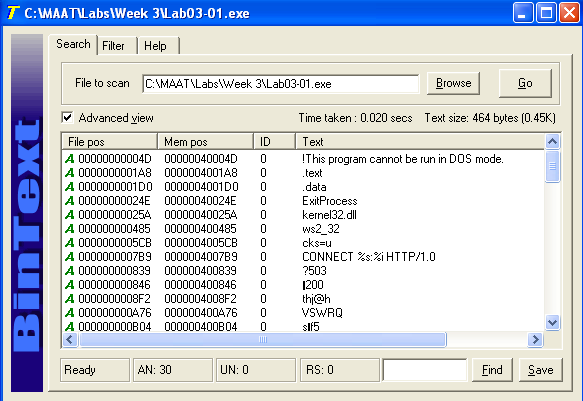
**Question 1**

What DLLs does the malware import? Could the malware be packed?



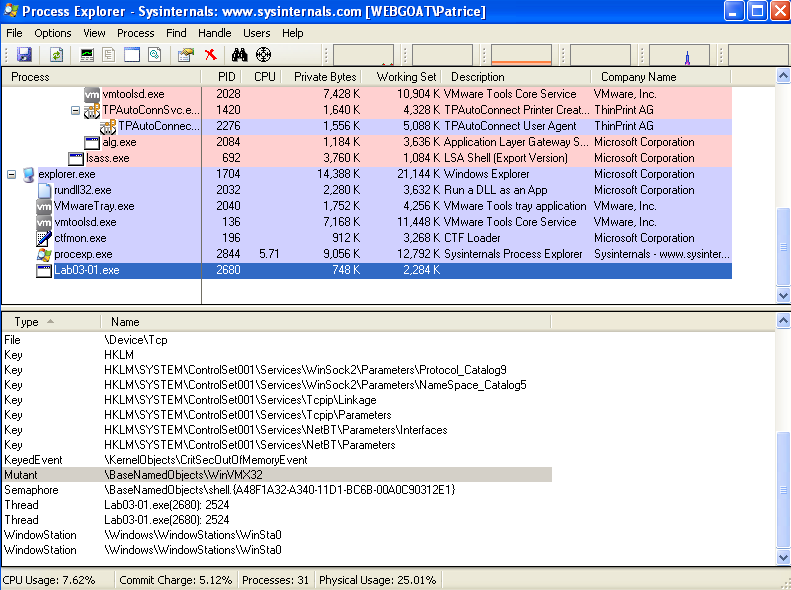
**Question 2**

What are some strings that may provide useful information for analysis?



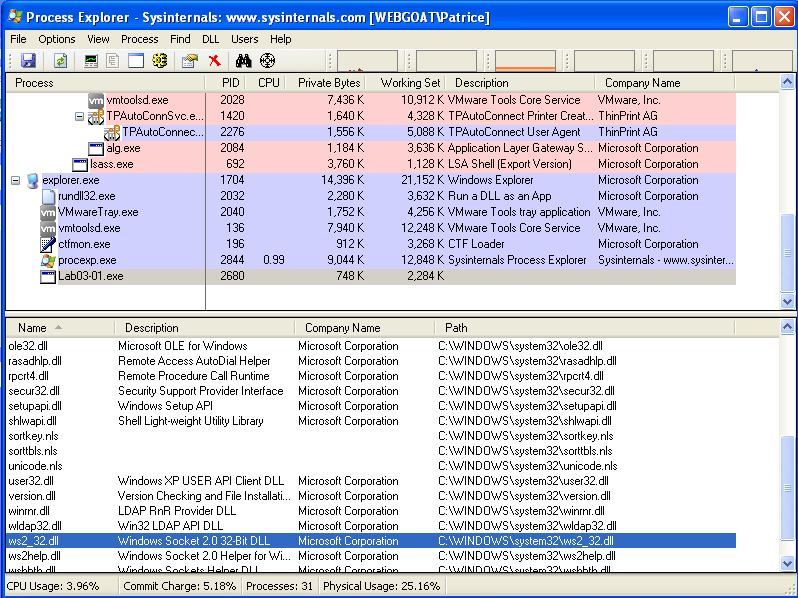
**Question 3**

Does the malware create an Mutex when it is running?



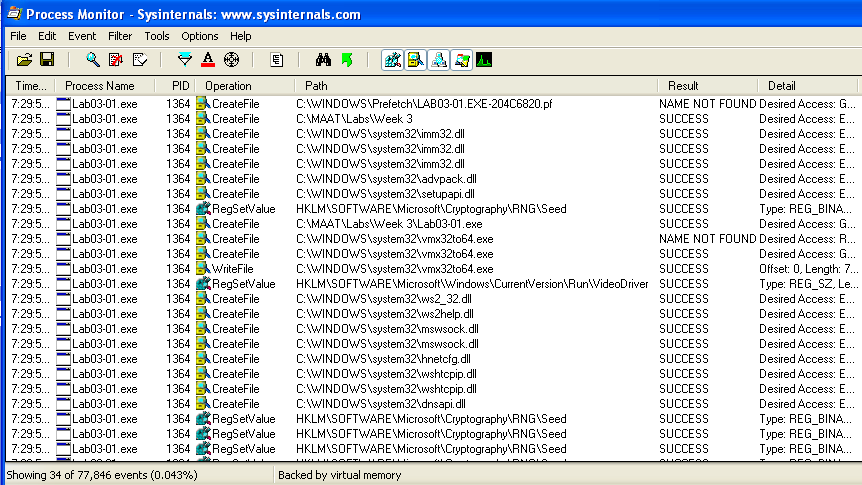
**Question 4**

Does the malware load any new DLLs when running?



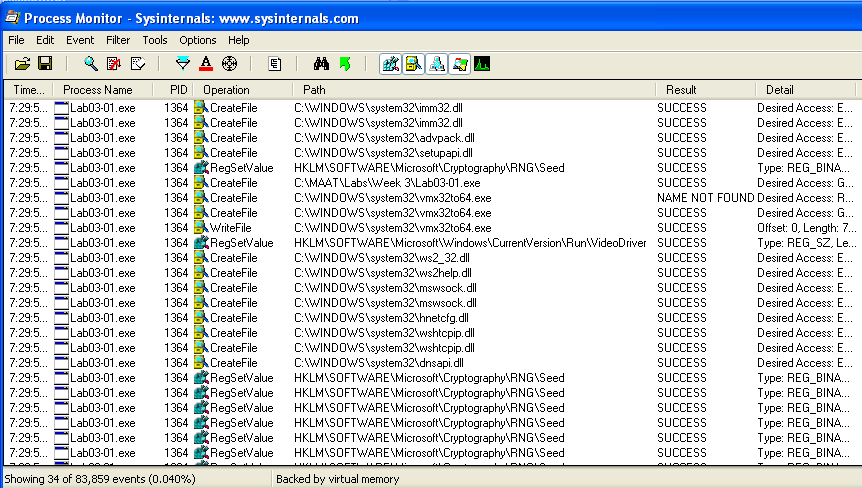
**Question 5**

Does the malware create any file? If so, what is the filename & location of the file?



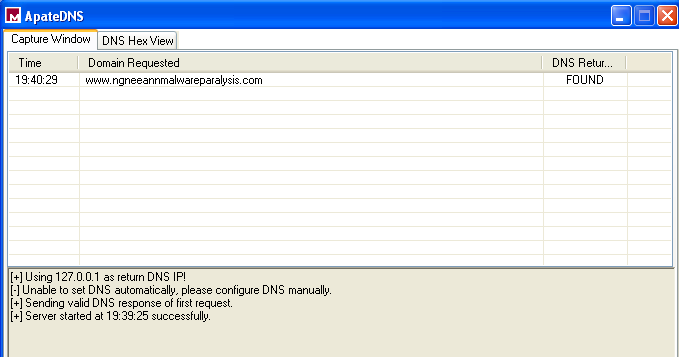
**Question 6**

What registry keys are being modified?



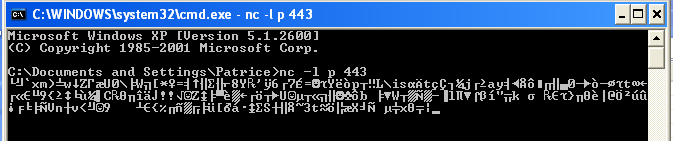
**Question 7**

What DNS request is being made?



**Question 8**

Use netcat to listen to port 443. What data is being transferred?



# Lab 02 [60 mins]

Refer to the files: Lab03-02.dll

**Question 1**

What are the imported & exported functions of this DLL?

**Question 2**

How do you install the malware? How do you run it after installing it?

**Question 3**

What important functions are imported in the DLL?

**Question 4**

Using Process Explorer, find the process under which the malware is running?

**Question 5**

Set a filter in Process Monitor to monitor the operations of the process identified in Question 4.

**Question 6**

What are some host-based indicators?

* Service Name
* Registry Changes

**Question 7**

What are some network-based indicators?

* Which domain name the malware is trying to connect?
* Which port?
* What is the data being transferred? Which protocol?

# Lab 03 [Practice]

Refer to the files: Lab03-03.exe

**Question 1**

What are the imported DLLs of this malware?

**Question 2**

Is the malware packed?

**Question 3**

What happened when you execute the malware? What does the malware do before it exits?

**Question 4**

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

**Question 5**

Does the malware create any file?

**Question 6**

What do you think is the purpose of the malware?