|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 2 | 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.

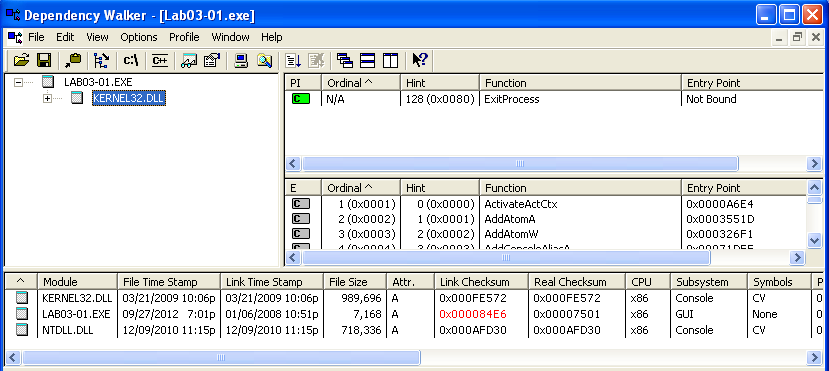
Submit your answers on MeL.

# Lab 01 [60 mins]

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

**Question 1**

What DLLs does the malware import? Could the malware be packed? KERNEL32.dll is imported. The malware looks like it may be packed as the only import function is ExitProcess.

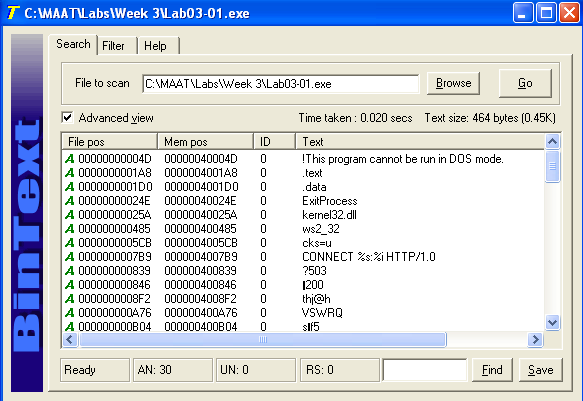


**Question 2**

What are some strings that may provide useful information for analysis (try to give 3)?

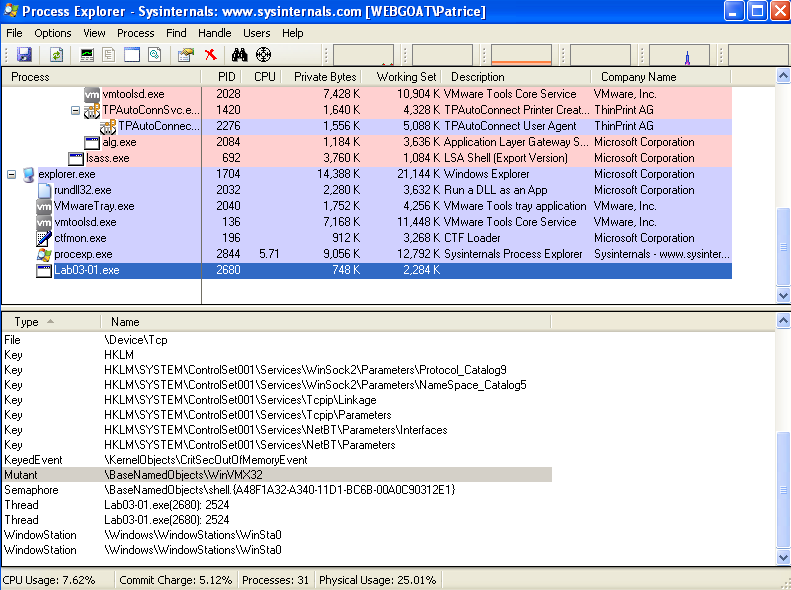
Host-based indicator: VideoDriver, WinVMX32-, admin, SOFTWARE\Microsoft\Windows\CurrentVersion\Run, AppData

Network indicator: [www.ngeeann-malwareparalysis.com](http://www.ngeeann-malwareparalysis.com), CONNECT %s%iHTTP/1.0, ws2\_32, ?503, !200



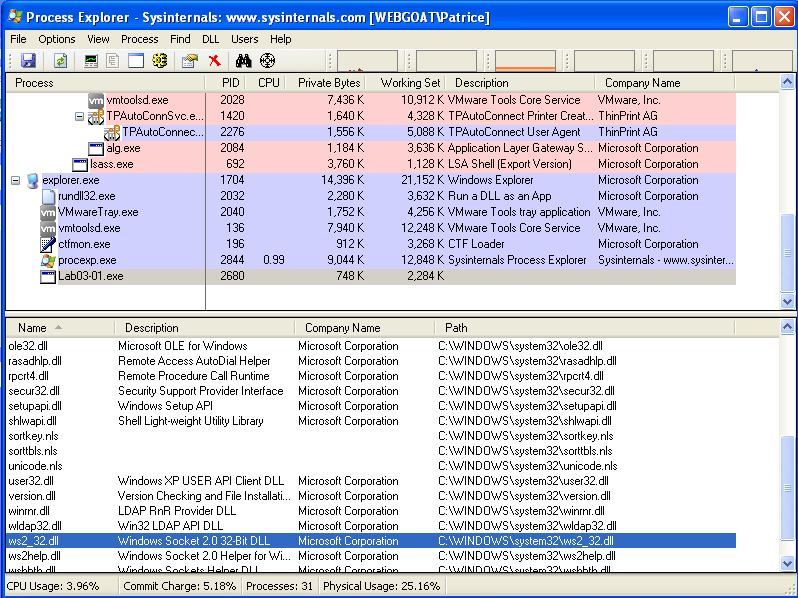
**Question 3**

Does the malware create a Mutex when it is running? Yes, it creates a mutex called \BasedNamedObjects\WinVMX32



**Question 4**

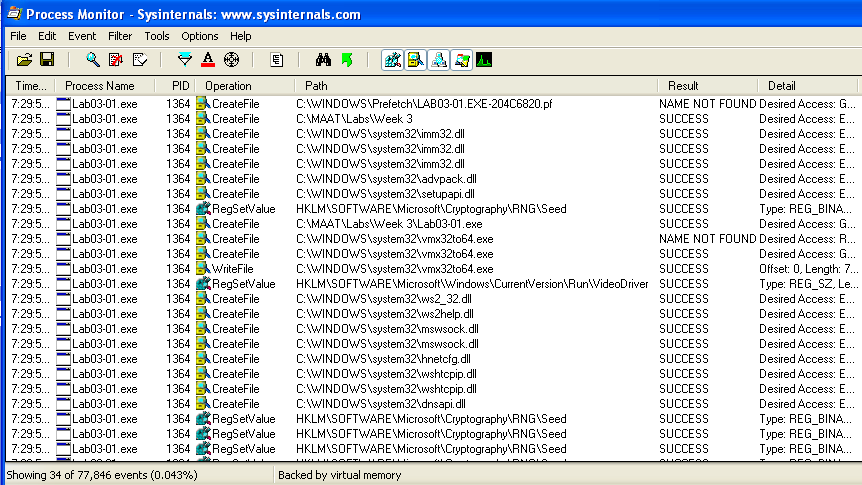
Does the malware load any new DLLs when running? yes



**Question 5**

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

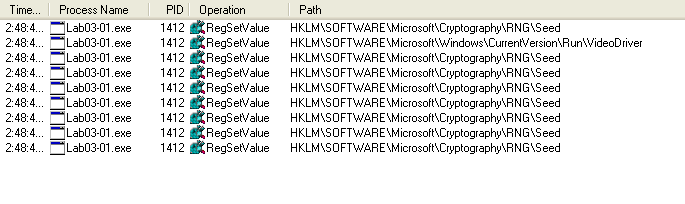
Ws2\_32.dll is created in c:\windows\system32

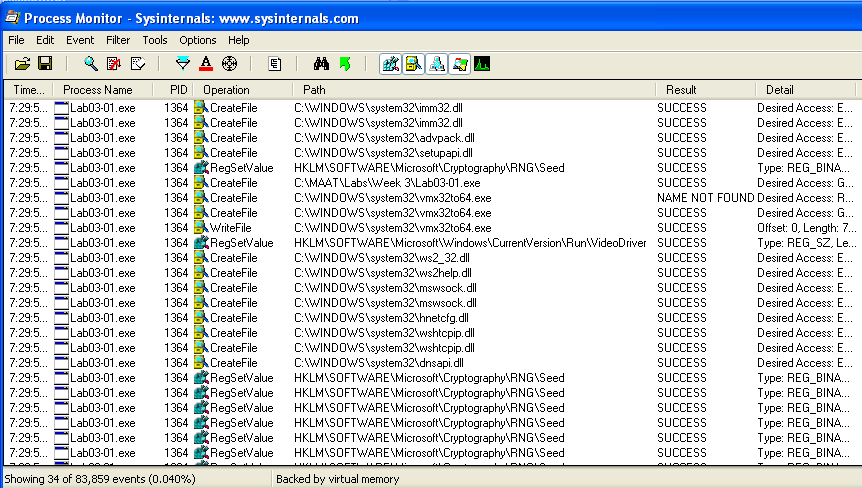


**Question 6**

What registry keys are being modified? HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed

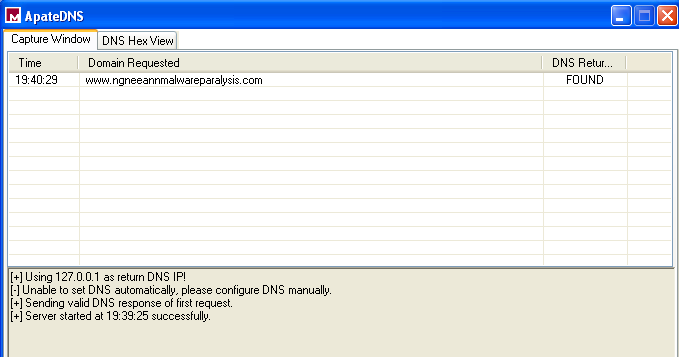
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver





**Question 7**

What DNS request is being made? www.ngeeann-malwareparalysis.com



**Question 6**

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

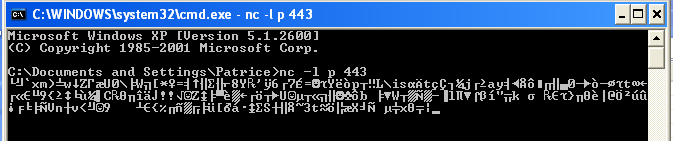
It sends a 256 bit binary string

uΓC█I].├║╙ú►└Γ∩ì╒▓g%▓ Æ#╨┼H╕Q`ü^ƒ½╕╙6«Ö─↔ß╥·≈'~┼╔ú←⌐E<▼╥n·?╧Kp╙╬Q$çW ╩▀

O±╥\⌠╢8£ ▐¡├↑¥⌐¬▬¢⌠≥╛P%.╡╩♂;h↓[&>½#↑«F→φµ┐0≡Ö<H♦¡╖u╜╡P╩∩Ç▌ {ñ╫0σ5π∞∟ì╘εΓ▬IO♫o⌐W⌡

AGU-î∟|≤→¿¥5Fá3≥/▲JΣ█8≤Oº

çΣLí√CÉ@½←←⌠p6←╪╛bσ9º├♣O↓≡µs α[¥↕è↨─z♠u!D¿ú ≤♀⌠╙╚µ║α♠τW⌡«4ƒ▼ é{r£i7iÄÅ┐z§↑┤ƒüπ



# Lab 02 [60 mins]

Refer to the files: Lab03-02.dll

**Question 1**

What are the imported & exported functions of this DLL?

Imported

RegSetValueExA

RegCreateKeyA

CloseServiceHandle

CreateServiceA

RegCloseKey

RegQueryValueExA

RegOpenKeyExA

DeleteService

OpenServiceA

SetServiceStatus

InternetReadFile

HttpQueryInfoA

HttpSendRequestA

HttpOpenRequestA

InternetConnectA

InternetOpenA

InternetCloseHandle

Exported

Install

ServiceMain

UninstallMain

installA

uninstallA

**Question 2**

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

Run RUNDLL32.exe Lab03-02.dll,install in CMD ton install

Run **net start IPRIP in CMD to run**

**Question 3**

What important functions are imported in the DLL?

CloseServiceHandle

CreateServiceA

DeleteService

OpenServiceA

SetServiceStatus

InternetReadFile

HttpQueryInfoA

HttpSendRequestA

HttpOpenRequestA

InternetConnectA

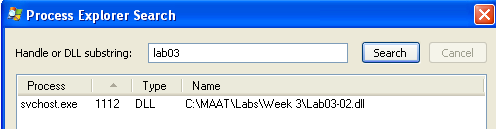
InternetOpenA

InternetCloseHandle

With those functions, it show that it create a service that access the internet

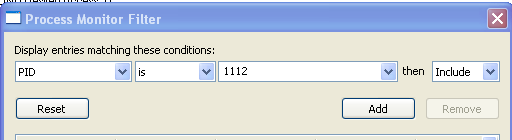
**Question 4**

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: IPRIP
* Registry Changes: HKLM/services/CurrentControlSet/Services/IPRIP

**Question 7**

What are some network-based indicators?

* Which domain name the malware is trying to connect? ngeeann-malwareparalysis.com
* Which port? 80
* What is the data being transferred? Which protocol? It sent a get request to ngeeann-malwareparalysis.com using HTTP protocol