PROJ 14: Malware Behavior

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

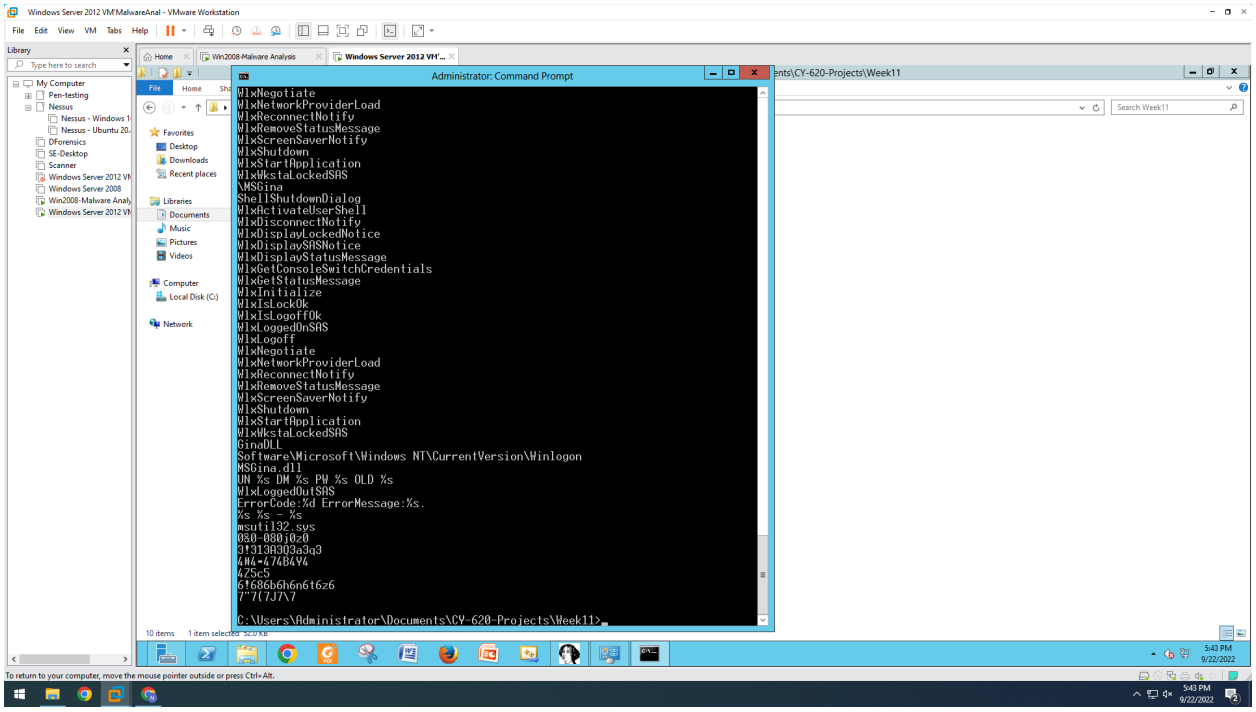
Nikhil Patel

11/15/2022

Introduction: In this lab, we will Lab11-1 file and examine its behavior using PEview, Process Monitor & Hash Calc.

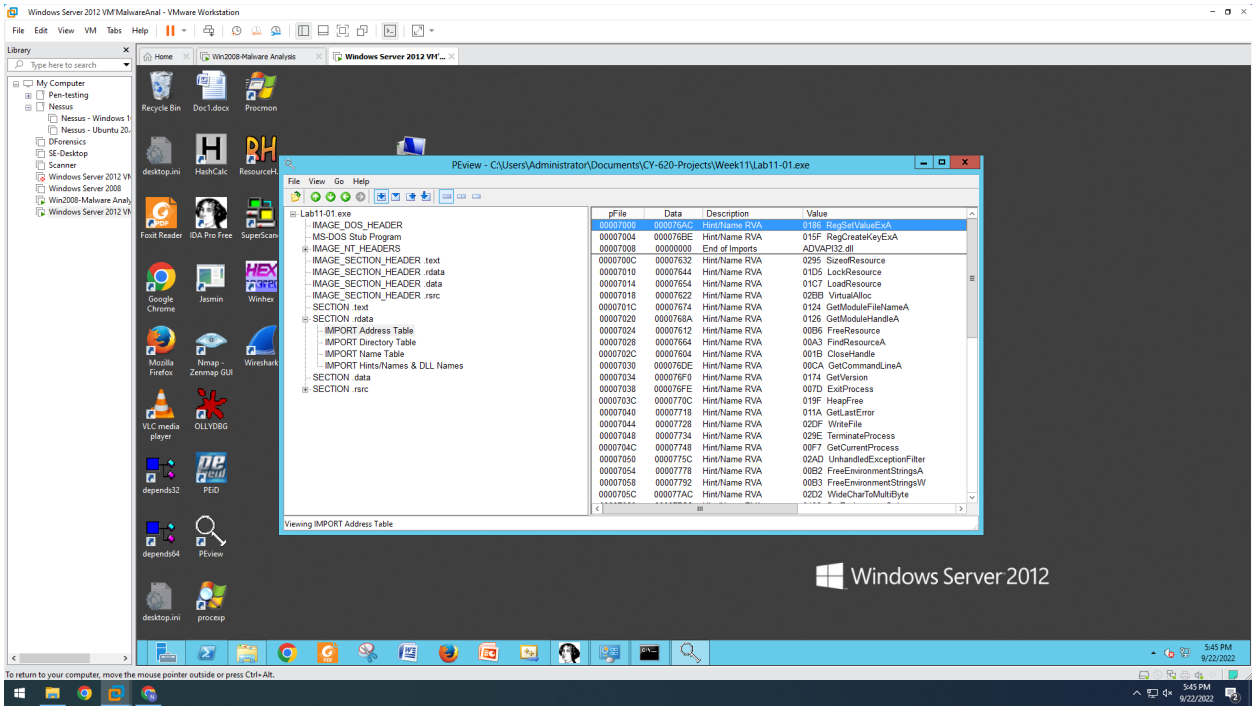
Procedure :

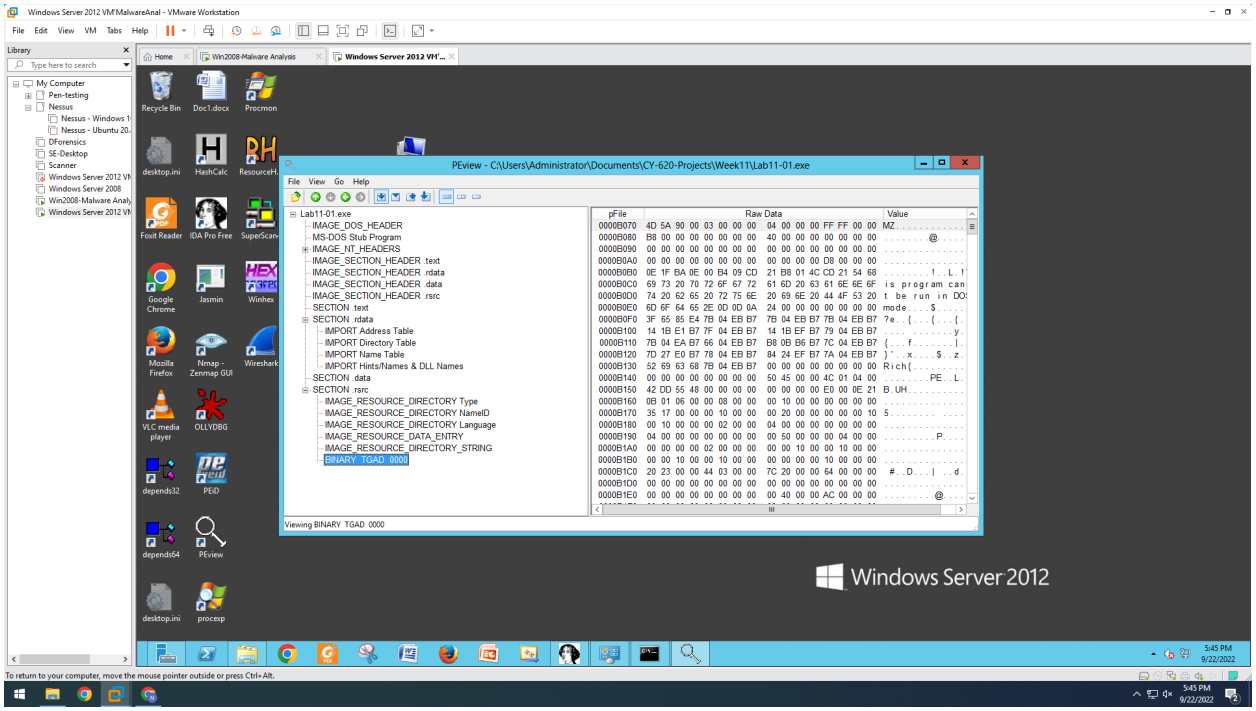
Static Analysis with Strings



Static Analysis with PEview

- Open the file named Lab 11-01.exe in preview.
- Then go to Import Address Table in Section. rdata.
- Take a ScreenShot and then go to Section. Rsrc.
- And then Binary TGAD 0000 and take a screenshot of the first value.


Windows Server 2012 VM MalwareAnal - VMware Workstation
PEview - C:\Users\Administrator\Documents\CY-620-Projects\Week11\Lab11-01.exe
Lab11-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .rsrc
pFile Data Description Value
00007000 000076AC Hint/Name RVA 0186 RegSetValueExA
00007004 000076BE Hint/Name RVA 015F RegCreateKeyExA
00007008 00000000 End of Imports ADVAPI32.dll
Viewing IMPORT Address Table
Windows Server 2012

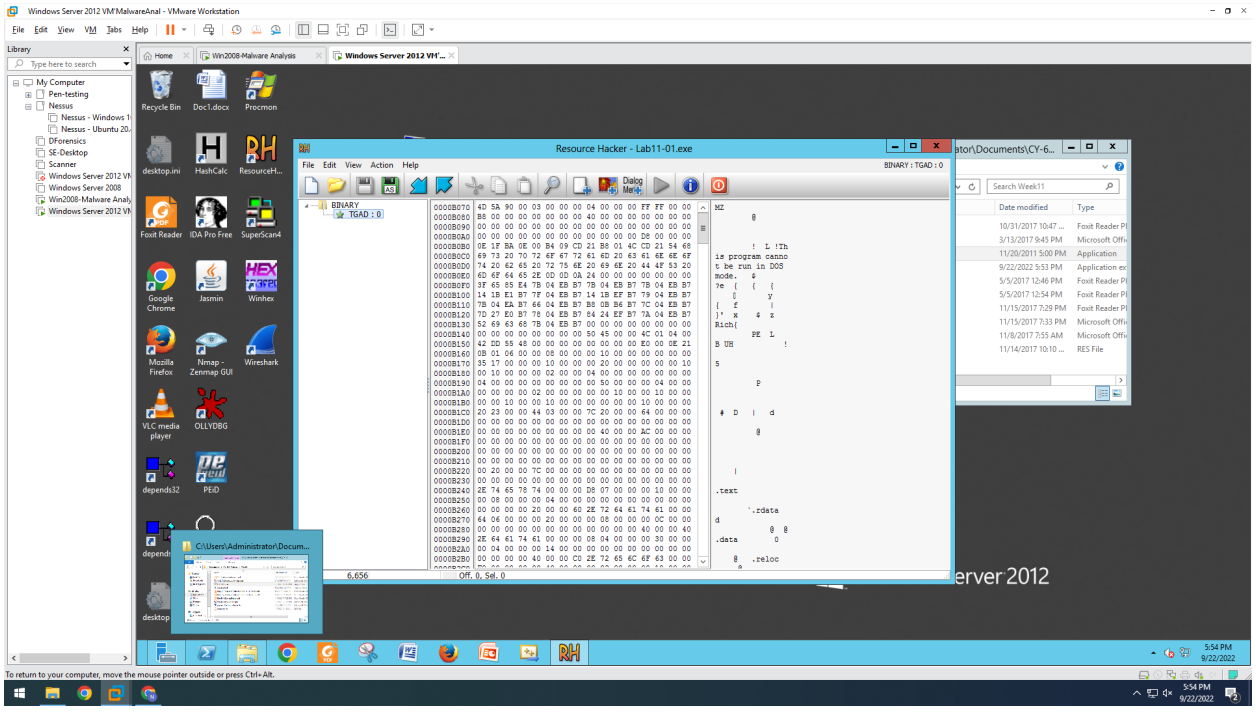

Windows Server 2012 VM MalwareAnal - VMware Workstation
PEview - C:\Users\Administrator\Documents\CY-620-Projects\Week11\Lab11-01.exe
Lab11-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .rsrc
IMAGE_RESOURCE_DIRECTORY Type
IMAGE_RESOURCE_DIRECTORY NameID
IMAGE_RESOURCE_DIRECTORY Language
IMAGE_RESOURCE_DATA_ENTRY
IMAGE_RESOURCE_DIRECTORY_STRING
BINARY_TGAD_0000
pFile Raw Data Value
Viewing BINARY_TGAD_0000
Windows Server 2012

Dynamic Analysis with Procmon

- Open Process Monitor and click on filter > “reset filter”.
- CLick on filter > filter and then filter for process name “lab 11-01.exe”.
- Take a screenshot of the page that appeared.

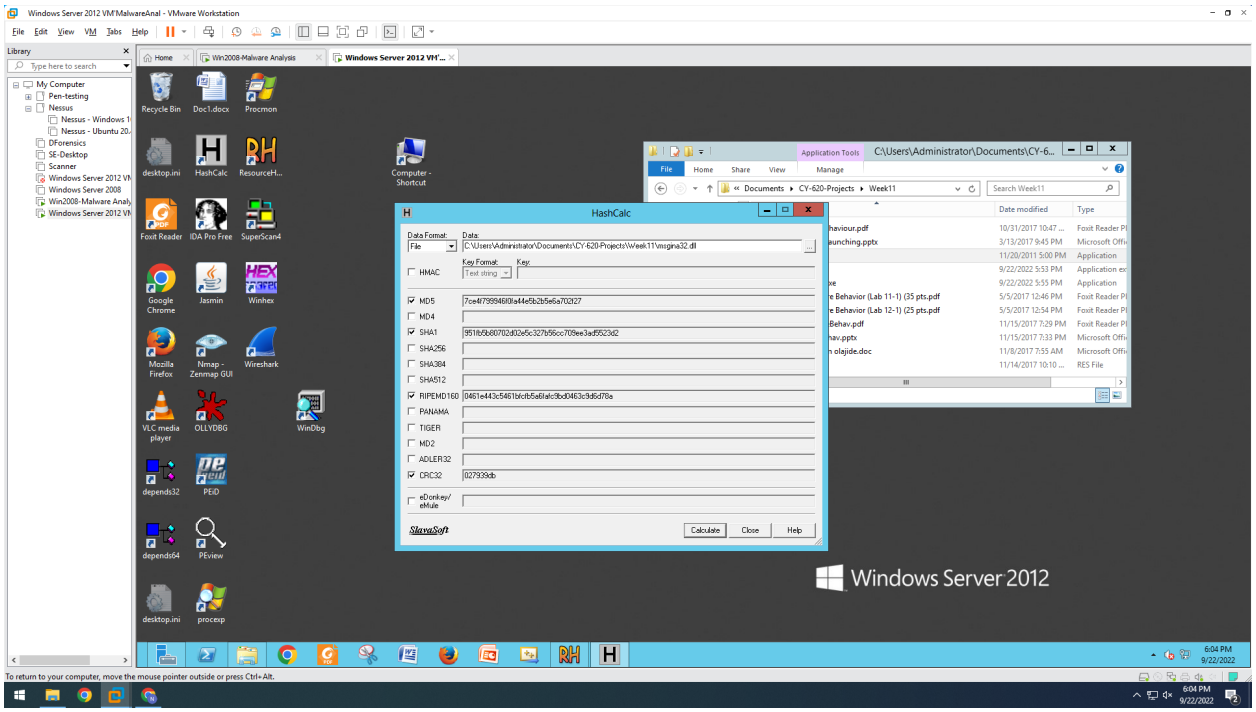
Resource Hacker

- Open Lab 11-01.exe in the resource hacker and the Binary TGAD 0 starts with MZ and contains the telltale text.
- Take a screenshot and save it.



Hash Calc

- Open msgina32.dll file in the hash calculator.
- And the result you will see on the screen.
- Take a screenshot of the page.



Conclusion: To conclude with the lab, we learned how to examine the malware behavior using the PEview, Process Monitor & Hash Calculator.