Module 12: Malware Forensics

Scenario

Malicious software or malware is the most prevalent threat to the IT industry. These malicious programs usually consist of codes developed by cybercriminals that are designed to gain unauthorized access to computing systems or network and steal sensitive data. Investigators should be aware of these malware programs as they need to use different malware forensics techniques to identify the method used by the malware for propagation and examine its impact on the system properties and network.

Attackers also use various methods to hide the presence of malware to avert forensics investigations. They embed malicious code in PDF files and Office documents to perform an attack. As an investigator performing malware analysis, you must be able to spot the suspicious file/documents in the suspect machine and collect it as a sample. You must know how to perform static analysis to look for known traces of malware, such as presence of malicious code, strings, or executables in the file, or execute them in a controlled environment to study their behavior and functionality in real-time using dynamic malware analysis methods. You can also use online resources to identify and examine malicious elements within a file.

Lab Objectives

The objectives of the lab are to explain the process of analyzing suspicious files and documents via both static and dynamic malware analysis methods to examine their functionality and impact on system properties and network as well as scanning them over online databases to look for malicious elements in them. Accomplishing these tasks will include:

- Examining a suspicious executable file using static analysis techniques
- Performing analysis on an Emotet variant
- Analyzing a suspicious Microsoft Word document

Overview of Malware Forensics

Malware forensics refers to the method of identifying and examining hidden malicious code or strings in any file or document via both static and dynamic analysis techniques. Malware analysis helps investigators get a general overview of the functionality and impact of a malicious specimen over system properties and network. Forensic examination performed on a malware sample shows how a malware works, what changes it makes to the system,

the process it creates to run and persist on the suspect system, and what IP addresses or ports it gets connected to.

Lab Tasks

Recommended labs to assist you in malware analysis:

- Performing static analysis on a suspicious file
- Performing system behaviour analysis
- Forensic examination of a suspicious Microsoft Office document

Lab 1: Performing Static Analysis on a Suspicious File

Lab Scenario

Jacob, employed at an accounting firm, noticed that his computer has been behaving strangely for past few days. It often becomes unresponsive and restarts on its own. At times, applications also start to run even when he has not opened them. Suspecting something fishy, Jacob discussed this problem with his manager, who, in turn, got in touch with a digital forensic agency.

Robert, a forensic investigator, contacted Jacob and examined his Office system. Robert learnt that Jacob often visits different websites and downloads files from various online sources for professional purposes. Robert browsed through all the websites that Jacob has visited in the last 2 weeks and examined all the files downloaded and used on the system. After the examination, Robert collected one executable file that looked suspicious. Robert now needs to use various static malware analysis techniques to see if the file has any malicious functionality embedded in it.

Lab Objectives

Static analysis is the process of scanning a file for the presence of malicious code or strings and verifying its impact on the system and network properties without running it on the machine.

This lab will help you understand how to check any file for the presence of malicious codes or strings without executing the program. The objectives of this lab are as follows:

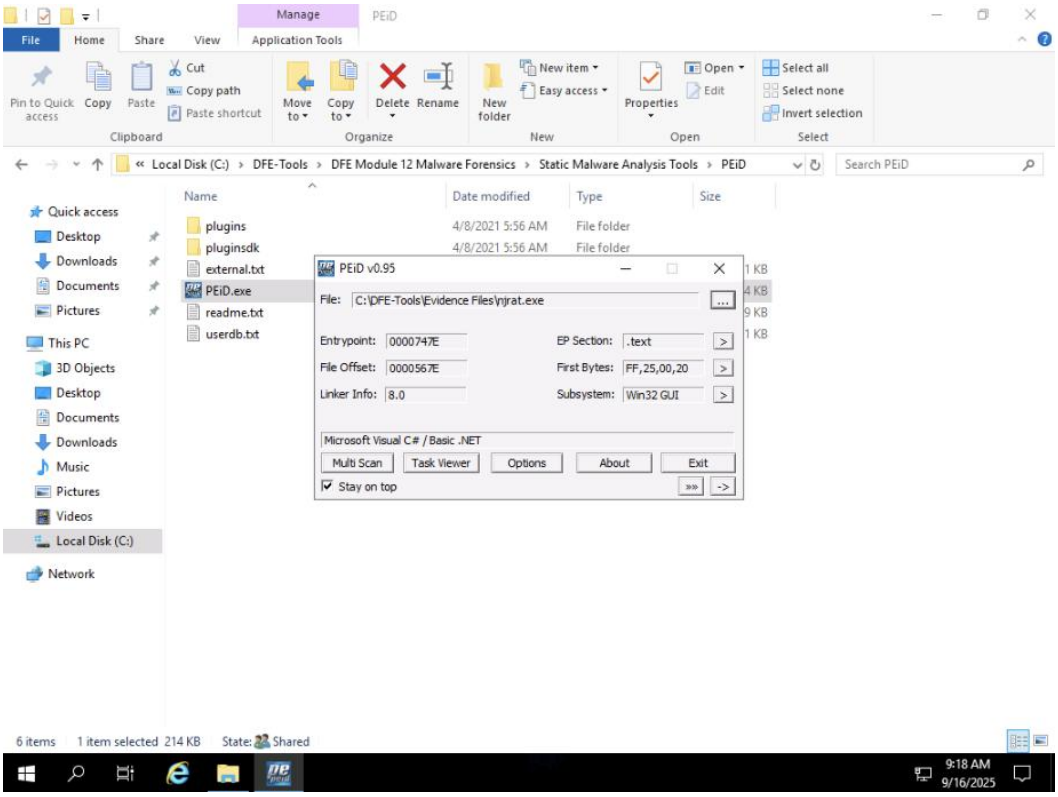
- Scanning the file to find any hidden or encrypted program or code
- Examining the file for the presence of suspicious elements
- Extracting and analyzing its PE headers

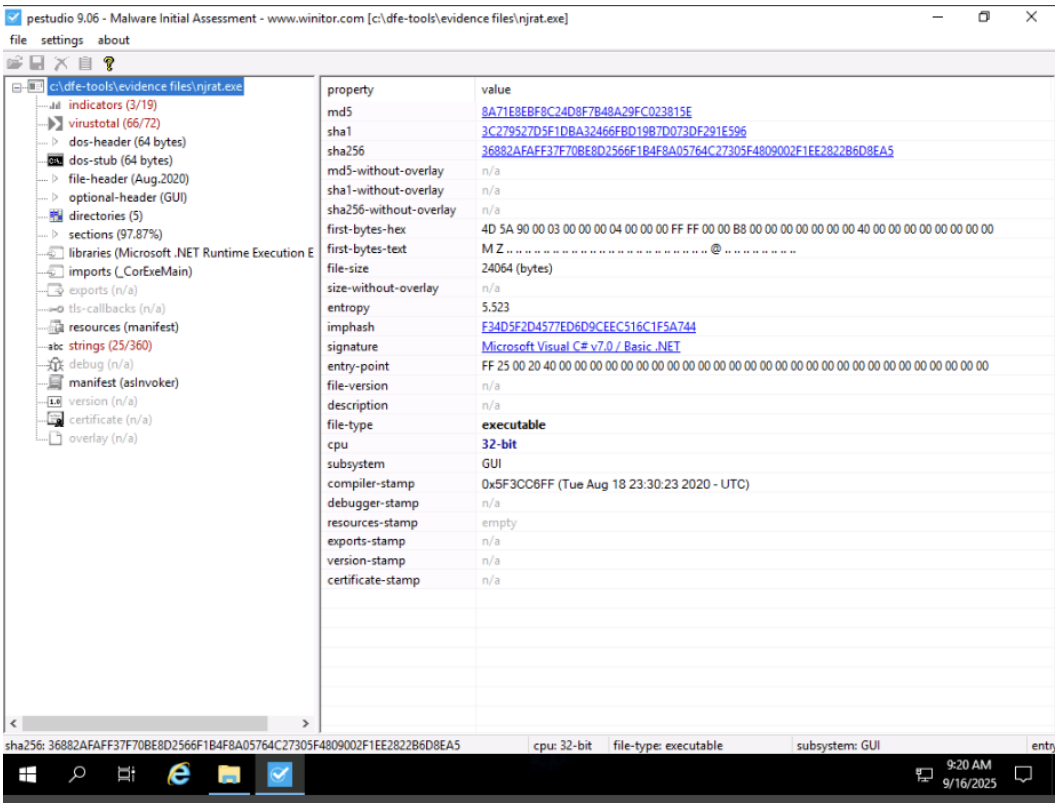
- Identifying malicious strings embedded within the file
- Finding linked libraries and dependencies of the file

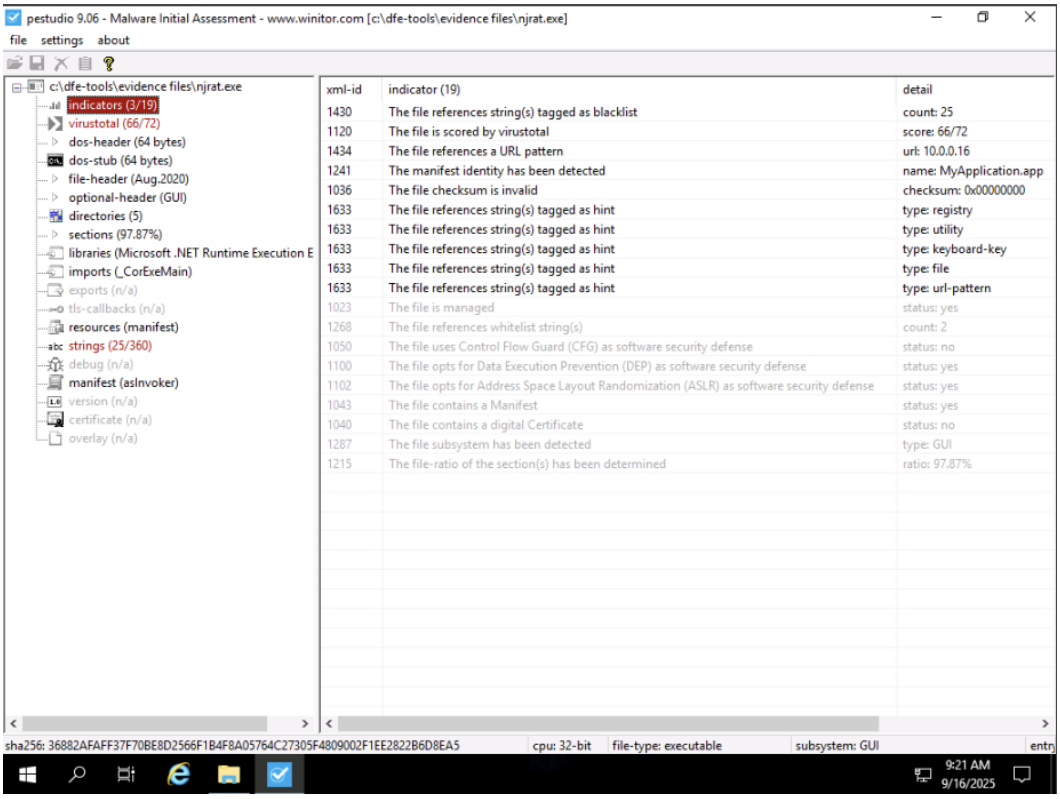
Overview of the Lab

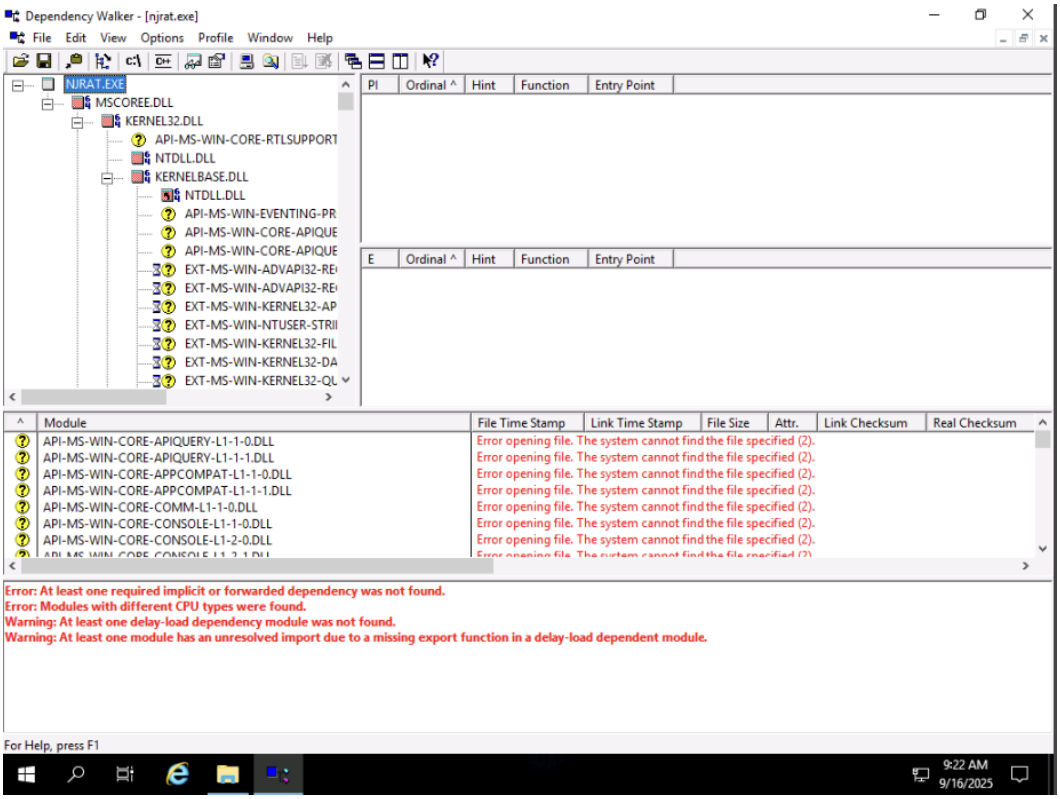
This lab familiarizes you with the process of performing static analysis on a suspicious file using tools such as **PEiD**, **Pestudio**, **Dependency Walker**.

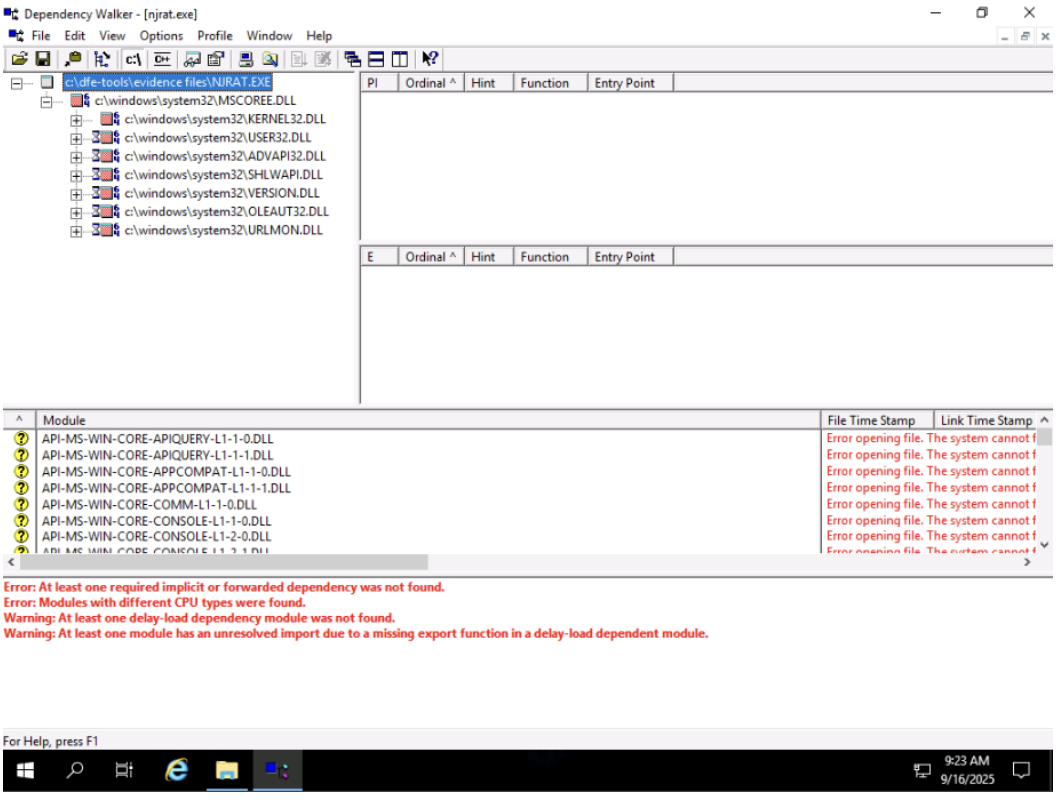
Malicious files often obfuscate their contents by using packers to evade detection. Hence, you need to check whether the suspect file contains any hidden or encrypted program or code and what kind of packer has been used to encrypt it.

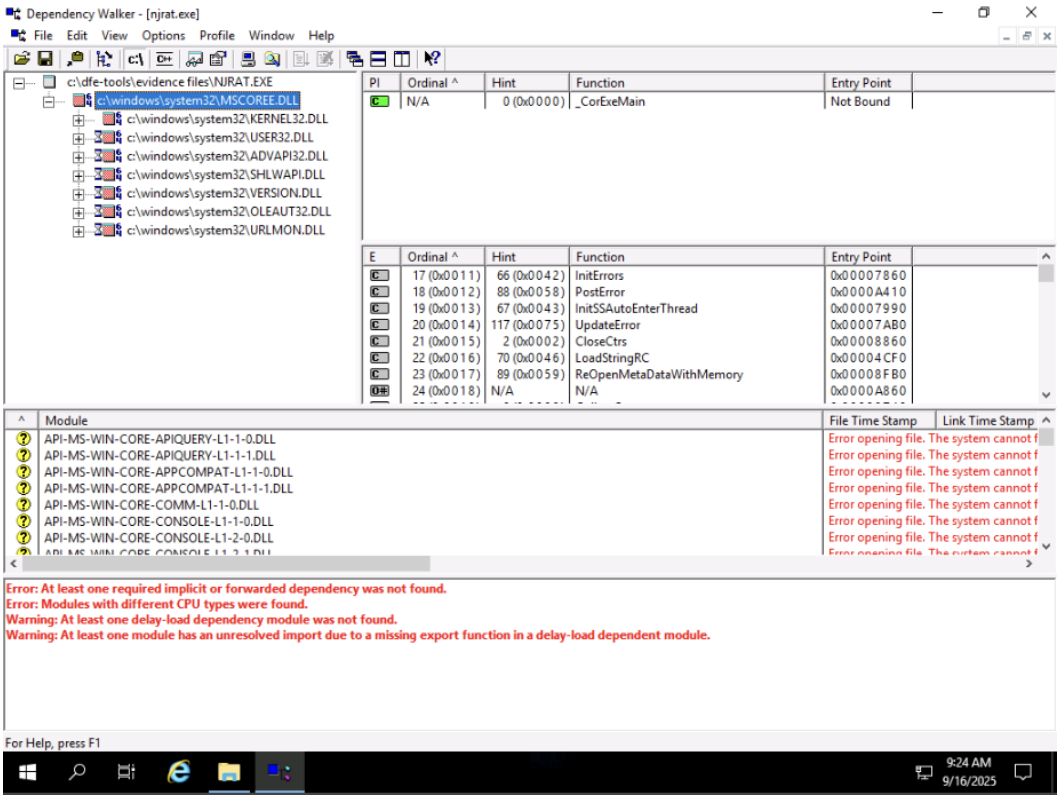


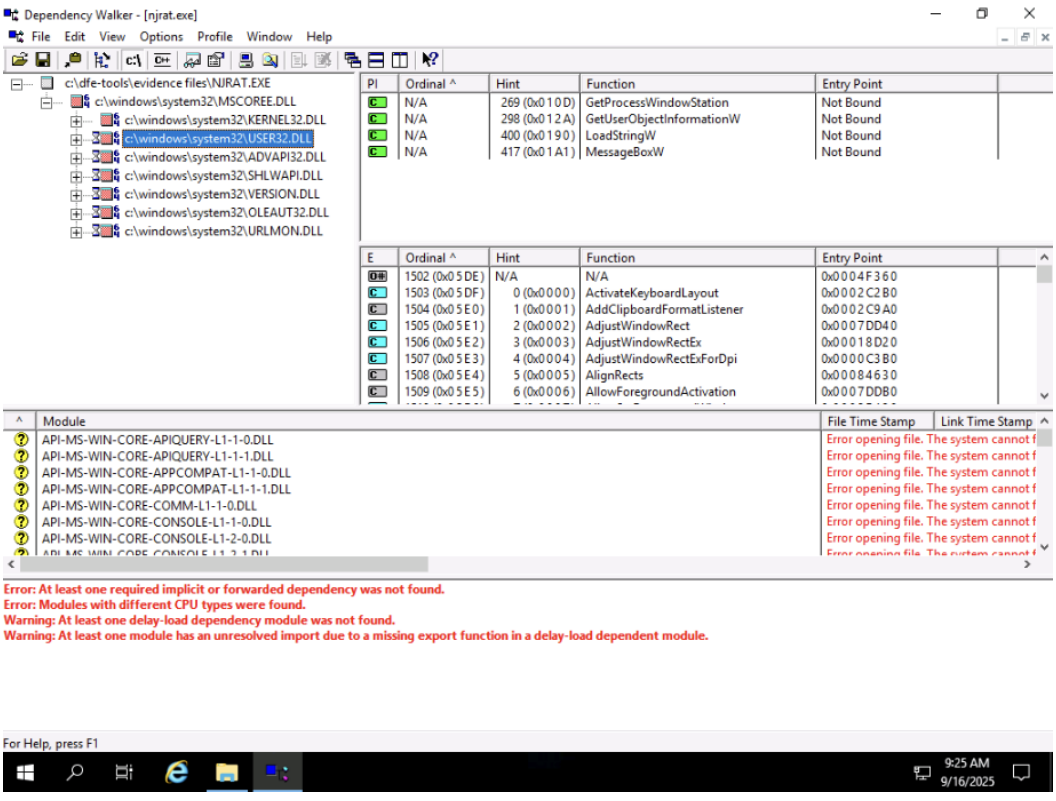

pestudio 9.06 - Malware Initial Assessment - www.winitor.com [c:\dfe-tools\evidence files\njrat.exe]
file settings about
c:\dfe-tools\evidence files\njrat.exe
indicators (3/19)
virustotal (66/72)
dos-header (64 bytes)
dos-stub (64 bytes)
file-header (Aug.2020)
optional-header (GUI)
directories (5)
sections (97.87%)
libraries (Microsoft .NET Runtime Execution E
imports (_CorExeMain)
exports (n/a)
tls-callbacks (n/a)
resources (manifest)
strings (25/360)
debug (n/a)
manifest (asInvoker)
version (n/a)
certificate (n/a)
overlay (n/a)
property value
md5 8A71E8EBF8C24D8F7B48A29FC023815E
sha1 3C279527D5F1DBA32466FBD19B7D073DF291E596
sha256 36882AFAFF37F70BE8D2566F1B4F8A05764C27305F4809002F1EE2822B6D8EA5
md5-without-overlay n/a
sha1-without-overlay n/a
sha256-without-overlay n/a
first-bytes-hex 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text M Z @
file-size 24064 (bytes)
size-without-overlay n/a
entropy 5.523
imphash F34D5F2D4577ED6D9CEEC516C1F5A744
signature Microsoft Visual C# v7.0 / Basic .NET
entry-point FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
file-version n/a
description n/a
file-type executable
cpu 32-bit
subsystem GUI
compiler-stamp 0x5F3CC6FF (Tue Aug 18 23:30:23 2020 - UTC)
debugger-stamp n/a
resources-stamp empty
exports-stamp n/a
version-stamp n/a
certificate-stamp n/a
sha256: 36882AFAFF37F70BE8D2566F1B4F8A05764C27305F4809002F1EE2822B6D8EA5
cpu: 32-bit
file-type: executable
subsystem: GUI
9:20 AM
9/16/2025

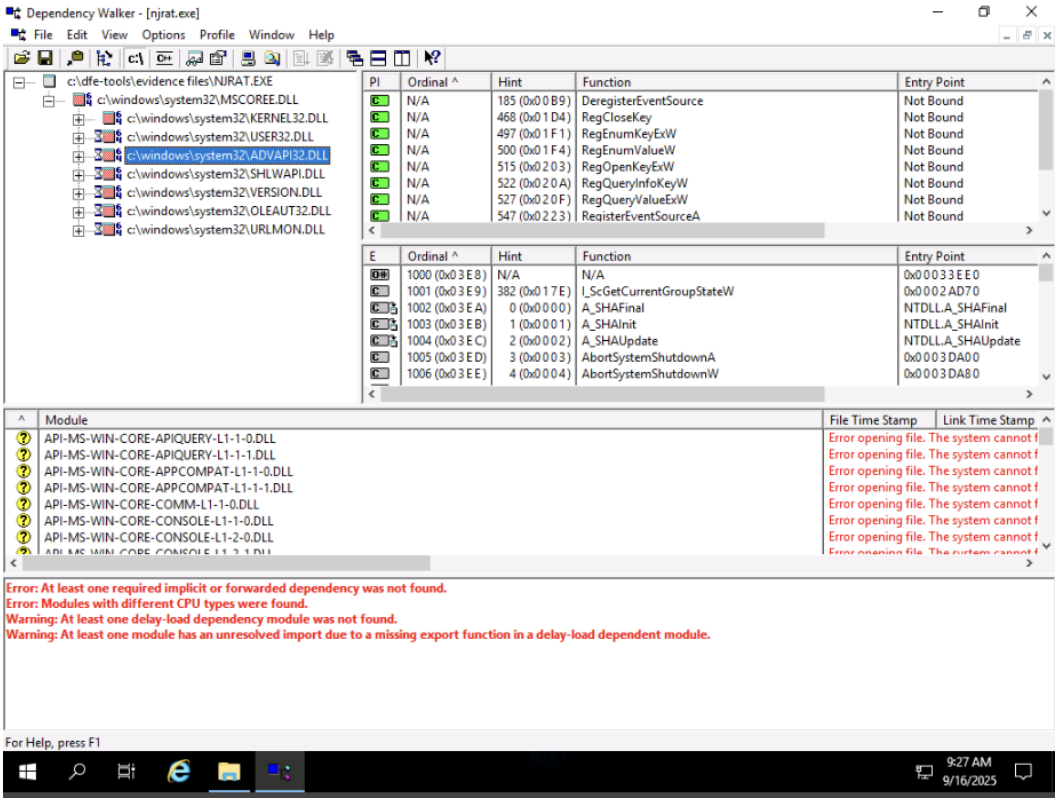

pestudio 9.06 - Malware Initial Assessment - www.winitor.com [c:\dfe-tools\evidence files\njrat.exe]
file settings about
c:\dfe-tools\evidence files\njrat.exe
indicators (3/19)
virustotal (66/72)
dos-header (64 bytes)
dos-stub (64 bytes)
file-header (Aug.2020)
optional-header (GUI)
directories (5)
sections (97.87%)
libraries (Microsoft .NET Runtime Execution E
imports (_CorExeMain)
exports (n/a)
tls-callbacks (n/a)
resources (manifest)
strings (25/360)
debug (n/a)
manifest (asInvoker)
version (n/a)
certificate (n/a)
overlay (n/a)
xml-id indicator (19) detail
1430 The file references string(s) tagged as blacklist count: 25
1120 The file is scored by virustotal score: 66/72
1434 The file references a URL pattern url: 10.0.0.16
1241 The manifest identity has been detected name: MyApplication.app
1036 The file checksum is invalid checksum: 0x00000000
1633 The file references string(s) tagged as hint type: registry
1633 The file references string(s) tagged as hint type: utility
1633 The file references string(s) tagged as hint type: keyboard-key
1633 The file references string(s) tagged as hint type: file
1633 The file references string(s) tagged as hint type: url-pattern
1023 The file is managed status: yes
1268 The file references whitelist string(s) count: 2
1050 The file uses Control Flow Guard (CFG) as software security defense status: no
1100 The file opts for Data Execution Prevention (DEP) as software security defense status: yes
1102 The file opts for Address Space Layout Randomization (ASLR) as software security defense status: yes
1043 The file contains a Manifest status: yes
1040 The file contains a digital Certificate status: no
1287 The file subsystem has been detected type: GUI
1215 The file-ratio of the section(s) has been determined ratio: 97.87%
sha256: 36882AFAFF37F70BE8D2566F1B4F8A05764C27305F4809002F1EE2822B6D8EA5
cpu: 32-bit
file-type: executable
subsystem: GUI
9:21 AM
9/16/2025

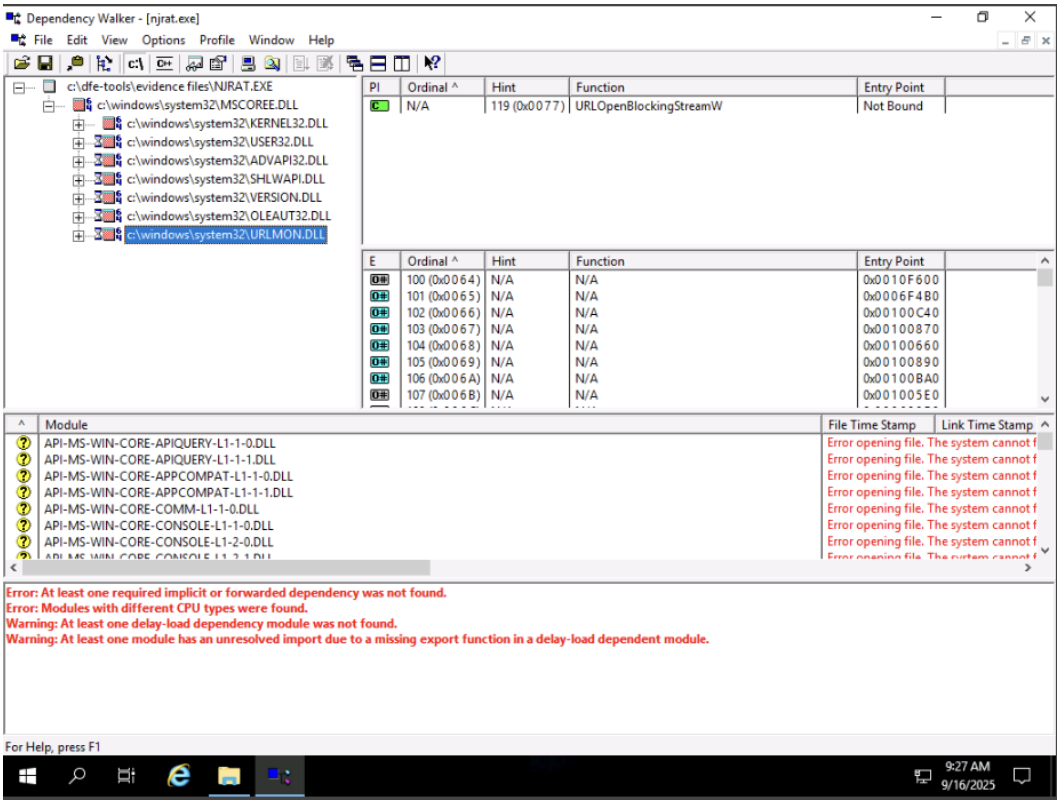

Dependency Walker - [njrat.exe]
File Edit View Options Profile Window Help
NJRAT.EXE
MSCOREE.DLL
KERNEL32.DLL
API-MS-WIN-CORE-RTLSUPPORT
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVENTING-PR
API-MS-WIN-CORE-APIQUE
API-MS-WIN-CORE-APIQUE
EXT-MS-WIN-ADVAPI32-RE
EXT-MS-WIN-ADVAPI32-RE
EXT-MS-WIN-KERNEL32-AP
EXT-MS-WIN-NTUSER-STRI
EXT-MS-WIN-KERNEL32-FIL
EXT-MS-WIN-KERNEL32-DA
EXT-MS-WIN-KERNEL32-QU
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
Error opening file. The system cannot find the file specified (2).
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
9:22 AM
9/16/2025


Dependency Walker - [njrat.exe]
File Edit View Options Profile Window Help
c:\dfe-tools\evidence files\NJRAT.EXE
c:\windows\system32\MSCOREE.DLL
c:\windows\system32\KERNEL32.DLL
c:\windows\system32\USER32.DLL
c:\windows\system32\ADVAPI32.DLL
c:\windows\system32\SHLWAPI.DLL
c:\windows\system32\VERSION.DLL
c:\windows\system32\OLEAUT32.DLL
c:\windows\system32\URLMON.DLL
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
Error opening file. The system cannot f
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
9:23 AM
9/16/2025


Dependency Walker - [njrat.exe]
File Edit View Options Profile Window Help
c:\dfe-tools\evidence files\NJRAT.EXE
c:\windows\system32\MSCOREE.DLL
c:\windows\system32\KERNEL32.DLL
c:\windows\system32\USER32.DLL
c:\windows\system32\ADVAPI32.DLL
c:\windows\system32\SHLWAPI.DLL
c:\windows\system32\VERSION.DLL
c:\windows\system32\OLEAUT32.DLL
c:\windows\system32\URLMON.DLL
PI Ordinal ^ Hint Function Entry Point
N/A 0 (0x0000) _CorExeMain Not Bound
E Ordinal ^ Hint Function Entry Point
17 (0x0011) 66 (0x0042) InitErrors 0x00007860
18 (0x0012) 88 (0x0058) PostError 0x0000A410
19 (0x0013) 67 (0x0043) InitSSAutoEnterThread 0x00007990
20 (0x0014) 117 (0x0075) UpdateError 0x00007AB0
21 (0x0015) 2 (0x0002) CloseCtrs 0x00008860
22 (0x0016) 70 (0x0046) LoadStringRC 0x00004CF0
23 (0x0017) 89 (0x0059) ReOpenMetaDataWithMemory 0x00008FB0
24 (0x0018) N/A N/A 0x0000A860
Module File Time Stamp Link Time Stamp
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
Error opening file. The system cannot f
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
9:24 AM
9/16/2025


Dependency Walker - [njrat.exe]
File Edit View Options Profile Window Help
c:\dfe-tools\evidence files\NJRAT.EXE
c:\windows\system32\MSCOREE.DLL
c:\windows\system32\KERNEL32.DLL
c:\windows\system32\USER32.DLL
c:\windows\system32\ADVAPI32.DLL
c:\windows\system32\SHLWAPI.DLL
c:\windows\system32\VERSION.DLL
c:\windows\system32\OLEAUT32.DLL
c:\windows\system32\URLMON.DLL
PI Ordinal ^ Hint Function Entry Point
N/A 269 (0x010D) GetProcessWindowStation Not Bound
N/A 298 (0x012A) GetUserObjectInformationW Not Bound
N/A 400 (0x0190) LoadStringW Not Bound
N/A 417 (0x01A1) MessageBoxW Not Bound
E Ordinal ^ Hint Function Entry Point
1502 (0x05DE) N/A N/A 0x0004F360
1503 (0x05DF) 0 (0x0000) ActivateKeyboardLayout 0x0002C2B0
1504 (0x05E0) 1 (0x0001) AddClipboardFormatListener 0x0002C9A0
1505 (0x05E1) 2 (0x0002) AdjustWindowRect 0x0007DD40
1506 (0x05E2) 3 (0x0003) AdjustWindowRectEx 0x00018D20
1507 (0x05E3) 4 (0x0004) AdjustWindowRectExForDpi 0x0000C3B0
1508 (0x05E4) 5 (0x0005) AlignRects 0x00084630
1509 (0x05E5) 6 (0x0006) AllowForegroundActivation 0x0007DDB0
Module File Time Stamp Link Time Stamp
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
Error opening file. The system cannot f
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
9:25 AM
9/16/2025





Lab 2: Performing System Behaviour Analysis

Lab Scenario

Since its discovery in 2014, Emotet has been one of the most destructive malware to affect government, public, and private entities alike by stealing sensitive information such as users' banking credentials, locally stored IDs and passwords, etc. Emotet is a kind of banking Trojan that spreads via emails containing malicious attachments or links. When the main Emotet module is unloaded on the target system, it downloads binary files that contain the actual payload, or distribute other malware such as Zeus Panda, TrickBot, and IcedID. It also collects sensitive information and stealthily connects to its Command and Control (C2) server to either receive further instructions or export the stolen data.

By constantly changing its identifiable features, Emotet can easily evade detection by traditional anti-virus engines. The main Emotet module is heavily obfuscated which is resolved dynamically during runtime. As an investigator, you need to examine the infection lifecycle of Emotet malware in real-time -how it unloads itself into a system and spread the infection by using both system and network properties.

Lab Objectives

Emotet is originally known to belong to a malware family of banking Trojans that mostly spread via the distribution of spam/phishing emails with malicious hyperlinks or attachments. Once it gains access to any system, it downloads additional modules of payloads with malicious functions.

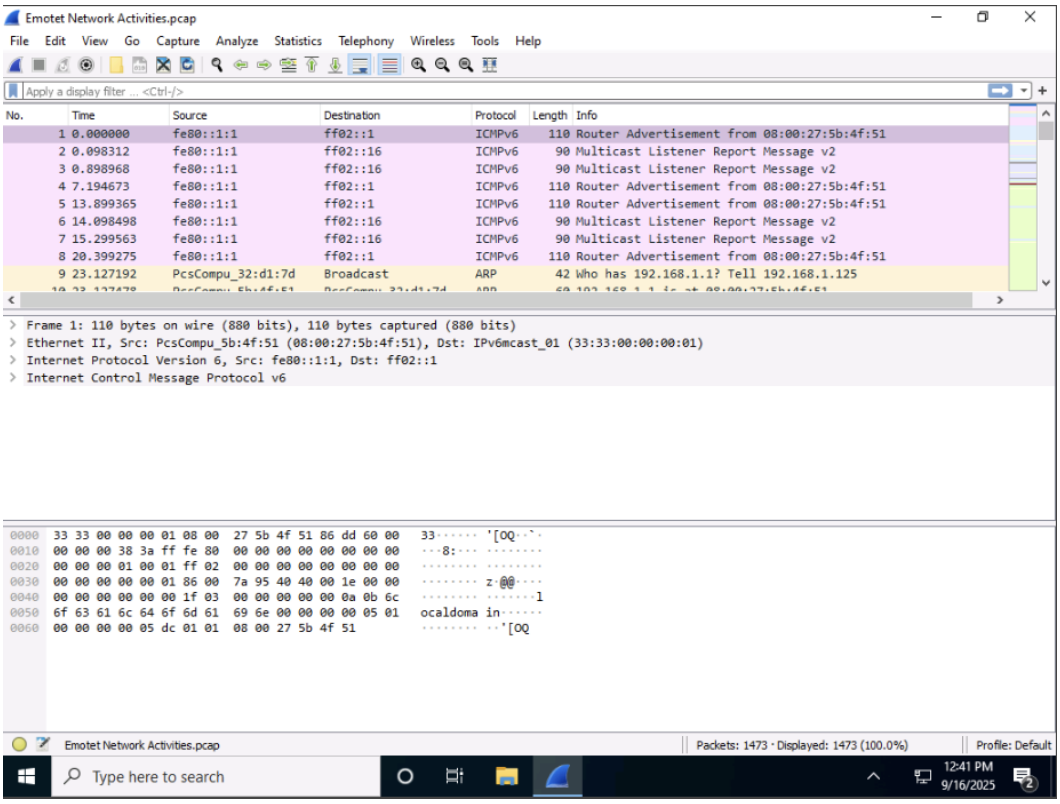
The objective of this lab is to provide you with a hands-on experience of how the Emotet malware variants operate when they are executed on the system in real-time.

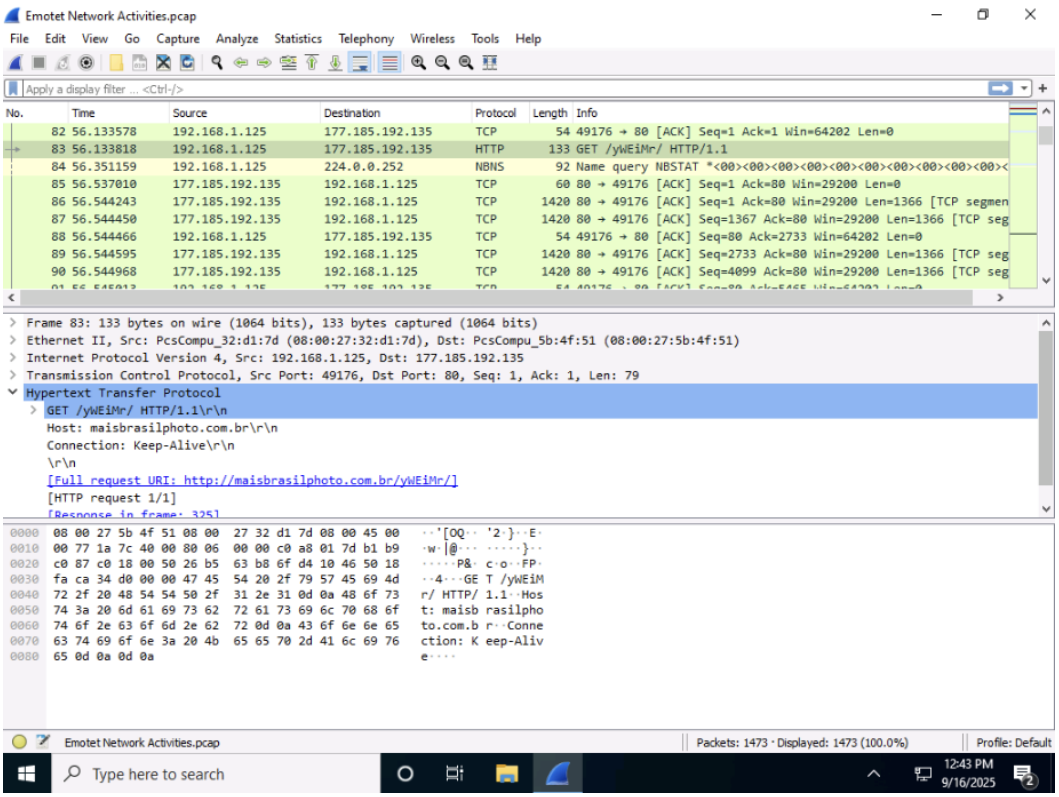
Overview of the Lab

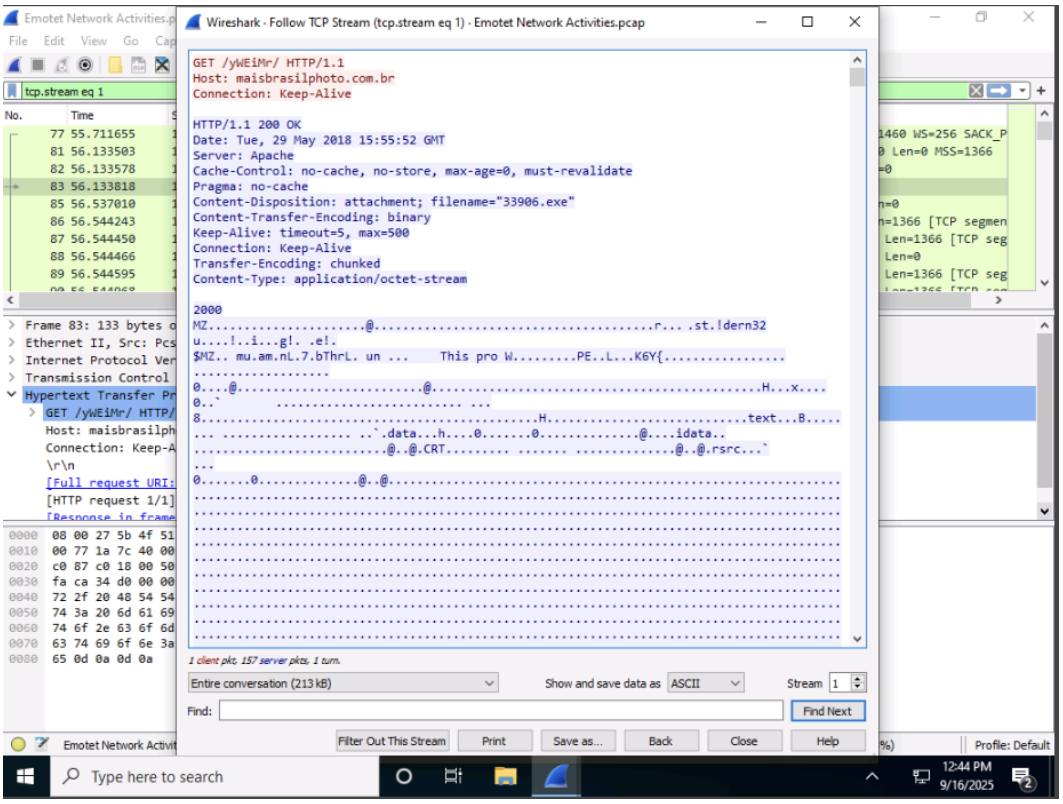
This lab familiarizes you with the process of examining how a variant of Emotet malware interacts with the target system and its network properties in real-time using tools such as Process Monitor and Wireshark.

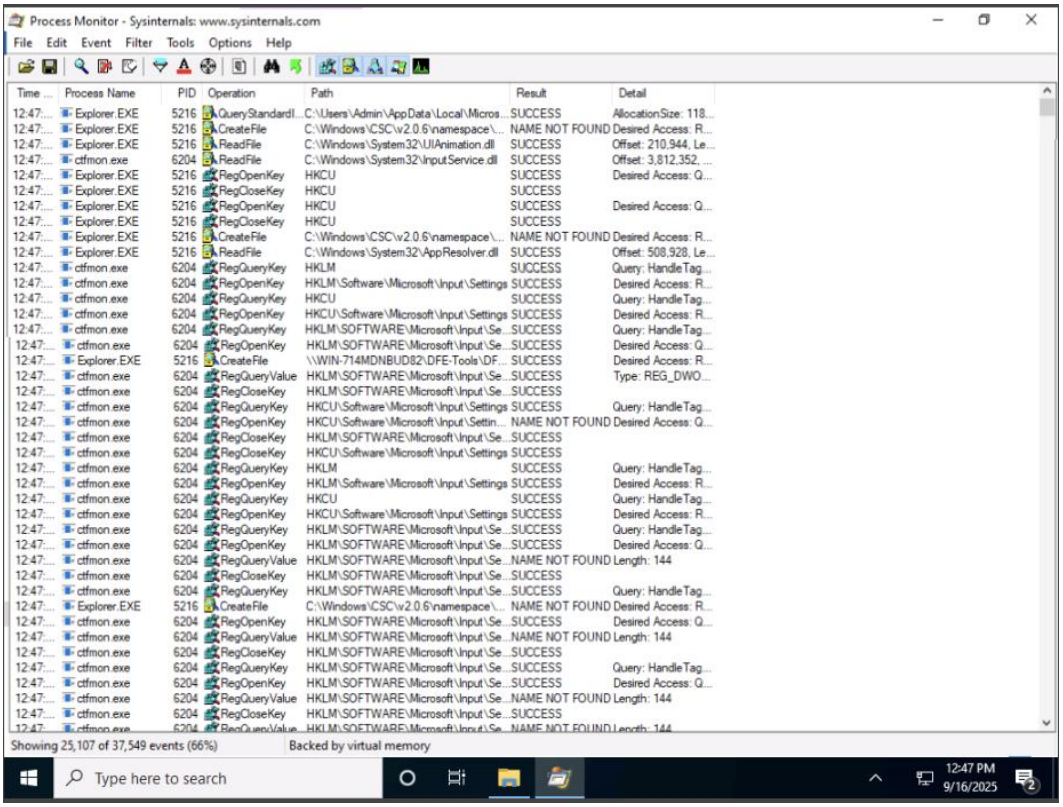
It is generally recommended to take a **snapshot** of the **forensic workstation** before running any malware specimen so that it can be reverted to its original state if it starts malfunctioning. However, you are **not required** to take any **snapshot** of the **Windows Server 2019** virtual machine before starting this lab as we will not be dealing with any active variant of **Emotet malware** here. As a result, its execution will not pose any harm on the system's performance.

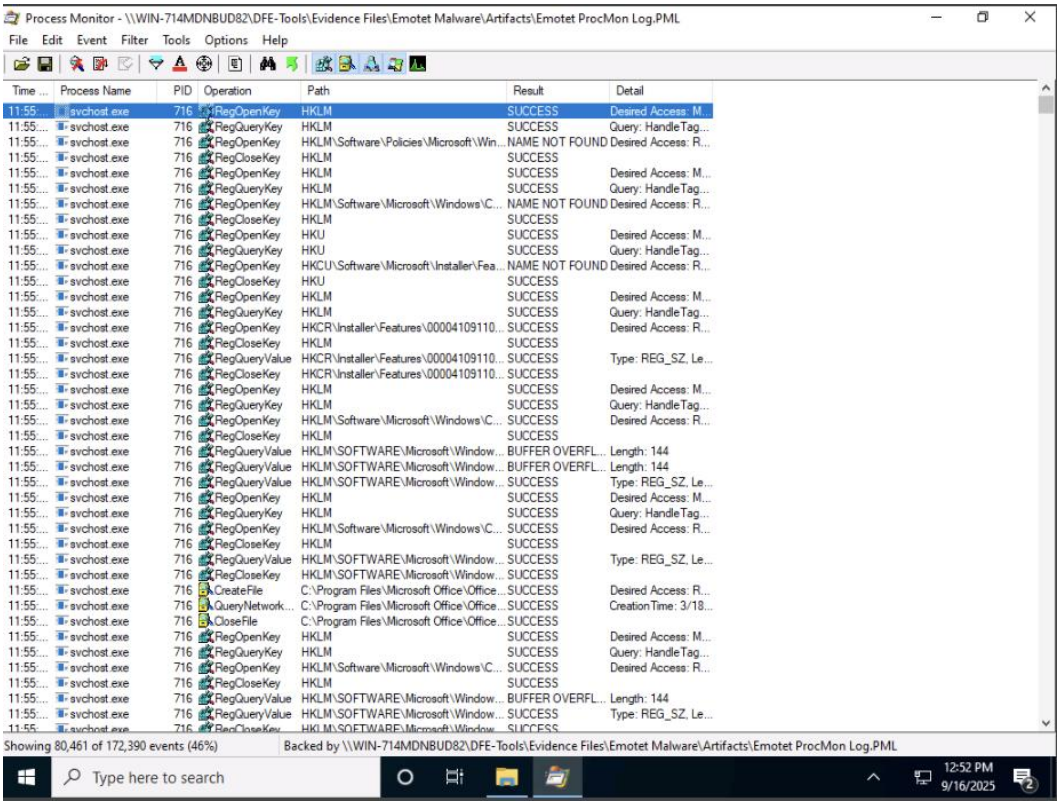
Due to lab requirements, I was unable to fully complete the Emotet system behavior analysis portion of review a Word document, as it required signing in with a personal Microsoft account, which I could not provide.

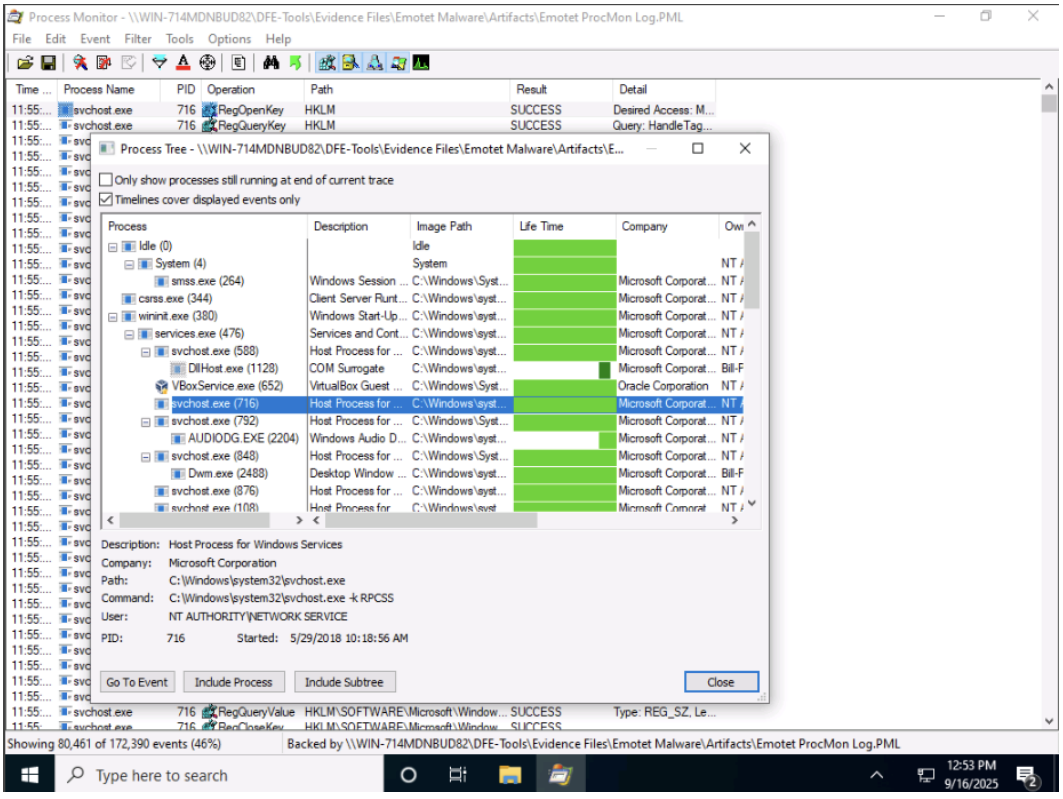

Emotet Network Activities.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 08:00:27:5b:4f:51
2 0.098312 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
3 0.898968 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
4 7.194673 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 08:00:27:5b:4f:51
5 13.899365 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 08:00:27:5b:4f:51
6 14.098498 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
7 15.299563 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 20.399275 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 08:00:27:5b:4f:51
9 23.127192 PcsCompu_32:d1:7d Broadcast ARP 42 Who has 192.168.1.1? Tell 192.168.1.125
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: PcsCompu_5b:4f:51 (08:00:27:5b:4f:51), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
Internet Control Message Protocol v6
0000 33 33 00 00 00 01 08 00 27 5b 4f 51 86 dd 60 00 33 ..... '[OQ..`.
0010 00 00 00 38 3a ff fe 80 00 00 00 00 00 00 00 00 ...8:... ....
0020 00 00 00 01 00 01 ff 02 00 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 01 86 00 7a 95 40 40 00 1e 00 00 .... z.@@....
0040 00 00 00 00 00 00 1f 03 00 00 00 00 00 0a 0b 6c l
0050 6f 63 61 6c 64 6f 6d 61 69 6e 00 00 00 00 05 01 ocaldoma in......
0060 00 00 00 00 05 dc 01 01 08 00 27 5b 4f 51 ....'[OQ
Emotet Network Activities.pcap
Packets: 1473 · Displayed: 1473 (100.0%)
Profile: Default
Type here to search
12:41 PM
9/16/2025

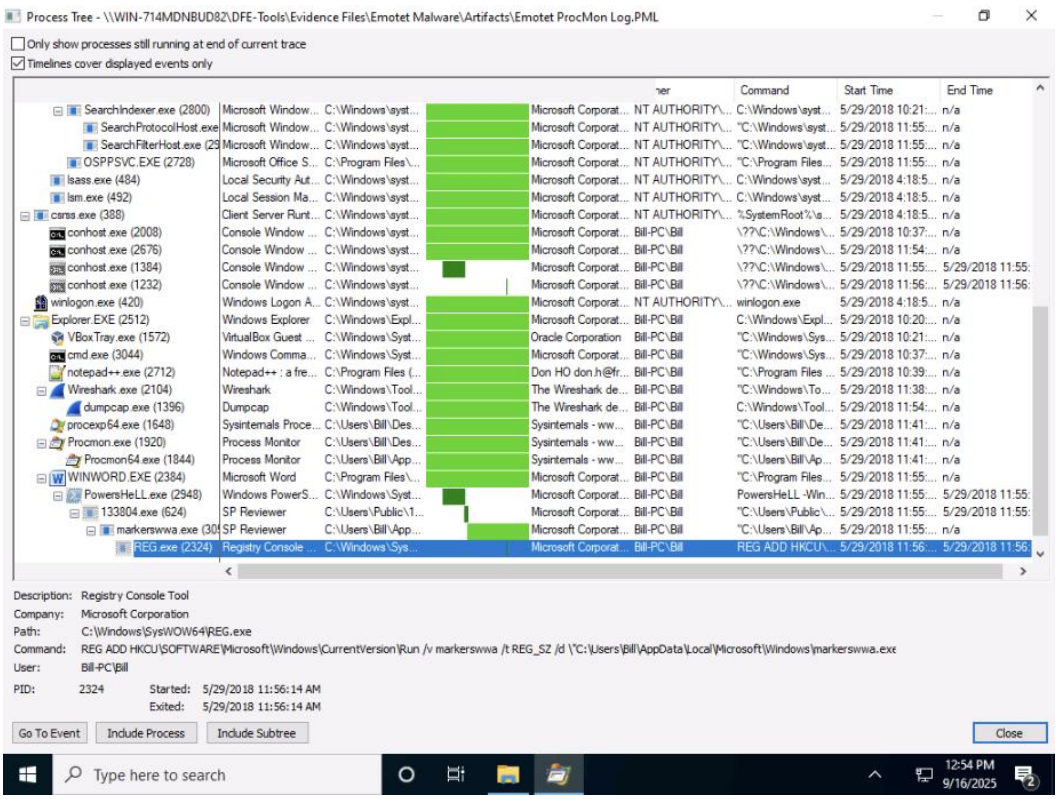

Emotet Network Activities.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
82 56.133578 192.168.1.125 177.185.192.135 TCP 54 49176 → 80 [ACK] Seq=1 Ack=1 Win=64202 Len=0
83 56.133818 192.168.1.125 177.185.192.135 HTTP 133 GET /yWEiMr/ HTTP/1.1
84 56.351159 192.168.1.125 224.0.0.252 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><
85 56.537010 177.185.192.135 192.168.1.125 TCP 60 80 → 49176 [ACK] Seq=1 Ack=80 Win=29200 Len=0
86 56.544243 177.185.192.135 192.168.1.125 TCP 1420 80 → 49176 [ACK] Seq=1 Ack=80 Win=29200 Len=1366 [TCP segmen
87 56.544450 177.185.192.135 192.168.1.125 TCP 1420 80 → 49176 [ACK] Seq=1367 Ack=80 Win=29200 Len=1366 [TCP seg
88 56.544466 192.168.1.125 177.185.192.135 TCP 54 49176 → 80 [ACK] Seq=80 Ack=2733 Win=64202 Len=0
89 56.544595 177.185.192.135 192.168.1.125 TCP 1420 80 → 49176 [ACK] Seq=2733 Ack=80 Win=29200 Len=1366 [TCP seg
90 56.544968 177.185.192.135 192.168.1.125 TCP 1420 80 → 49176 [ACK] Seq=4099 Ack=80 Win=29200 Len=1366 [TCP seg
Frame 83: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
Ethernet II, Src: PcsCompu_32:d1:7d (08:00:27:32:d1:7d), Dst: PcsCompu_5b:4f:51 (08:00:27:5b:4f:51)
Internet Protocol Version 4, Src: 192.168.1.125, Dst: 177.185.192.135
Transmission Control Protocol, Src Port: 49176, Dst Port: 80, Seq: 1, Ack: 1, Len: 79
Hypertext Transfer Protocol
GET /yWEiMr/ HTTP/1.1\r\n
Host: maisbrasilphoto.com.br\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://maisbrasilphoto.com.br/yWEiMr/]
[HTTP request 1/1]
[Response in frame: 325]
0000 08 00 27 5b 4f 51 08 00 27 32 d1 7d 08 00 45 00 ..'[OQ.. '2.}..E.
0010 00 77 1a 7c 40 00 80 06 00 00 c0 a8 01 7d b1 b9 .w.|@... .....}..
0020 c0 87 c0 18 00 50 26 b5 63 b8 6f d4 10 46 50 18 .....P&. c.o..FP.
0030 fa ca 34 d0 00 00 47 45 54 20 2f 79 57 45 69 4d ..4...GE T /yWEiM
0040 72 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 r/ HTTP/ 1.1..Hos
0050 74 3a 20 6d 61 69 73 62 72 61 73 69 6c 70 68 6f t: maisb rasilpho
0060 74 6f 2e 63 6f 6d 2e 62 72 0d 0a 43 6f 6e 6e 65 to.com.b r..Conne
0070 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 ction: K eep-Aliv
0080 65 0d 0a 0d 0a e....
Emotet Network Activities.pcap
Packets: 1473 · Displayed: 1473 (100.0%)
Profile: Default
Type here to search
12:43 PM
9/16/2025


Wireshark · Follow TCP Stream (tcp.stream eq 1) · Emotet Network Activities.pcap
GET /yWEiMr/ HTTP/1.1
Host: maisbrasilphoto.com.br
Connection: Keep-Alive
HTTP/1.1 200 OK
Date: Tue, 29 May 2018 15:55:52 GMT
Server: Apache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="33906.exe"
Content-Transfer-Encoding: binary
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/octet-stream
2000
1 client pkt, 157 server pkts, 1 turn.
Entire conversation (213 kB)
Show and save data as
ASCII
Stream
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Type here to search
12:44 PM
9/16/2025


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Showing 25,107 of 37,549 events (66%)
Backed by virtual memory
Type here to search
12:47 PM
9/16/2025


Process Monitor - \\WIN-714MDNBUD82\DFE-Tools\Evidence Files\Emotet Malware\Artifacts\Emotet ProcMon Log.PML
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 80,461 of 172,390 events (46%)
Backed by \\WIN-714MDNBUD82\DFE-Tools\Evidence Files\Emotet Malware\Artifacts\Emotet ProcMon Log.PML
Type here to search
12:52 PM
9/16/2025


Process Monitor - \\WIN-714MDNBUD82\DFE-Tools\Evidence Files\Emotet Malware\Artifacts\Emotet ProcMon Log.PML
Process Tree - \\WIN-714MDNBUD82\DFE-Tools\Evidence Files\Emotet Malware\Artifacts\E...
Only show processes still running at end of current trace
Timelines cover displayed events only
Process Description Image Path Life Time Company
Description: Host Process for Windows Services
Company: Microsoft Corporation
Path: C:\Windows\system32\svchost.exe
Command: C:\Windows\system32\svchost.exe -k RPCSS
User: NT AUTHORITY\NETWORK SERVICE
PID: 716 Started: 5/29/2018 10:18:56 AM
Go To Event
Include Process
Include Subtree
Close
Showing 80,461 of 172,390 events (46%)
Backed by \\WIN-714MDNBUD82\DFE-Tools\Evidence Files\Emotet Malware\Artifacts\Emotet ProcMon Log.PML
Type here to search
12:53 PM
9/16/2025



Lab 3: Forensic Examination of a Suspicious Microsoft Office Document

Lab Scenario

Richard, an employee from the finance team of an Austrian company, got an email from their vendor regarding the payment of invoice. The email had the invoice attached in form of a Microsoft Word document. As it was already the end of the month, Richard downloaded and opened the Word document to process the invoice. After some time, his system started malfunctioning. Suspecting something to be wrong, Richard informed the cyber-security team of his company to probe into the matter.

Jason from the cyber forensic wing was assigned to the case. As a part of the investigation, Jason monitored the Richard's compromised machine, disconnected it from the network, and collected the suspicious Word document. He now needs to parse the suspicious Word document code via forensic tools and see whether the document contains any malicious strings or code.

Lab Objectives

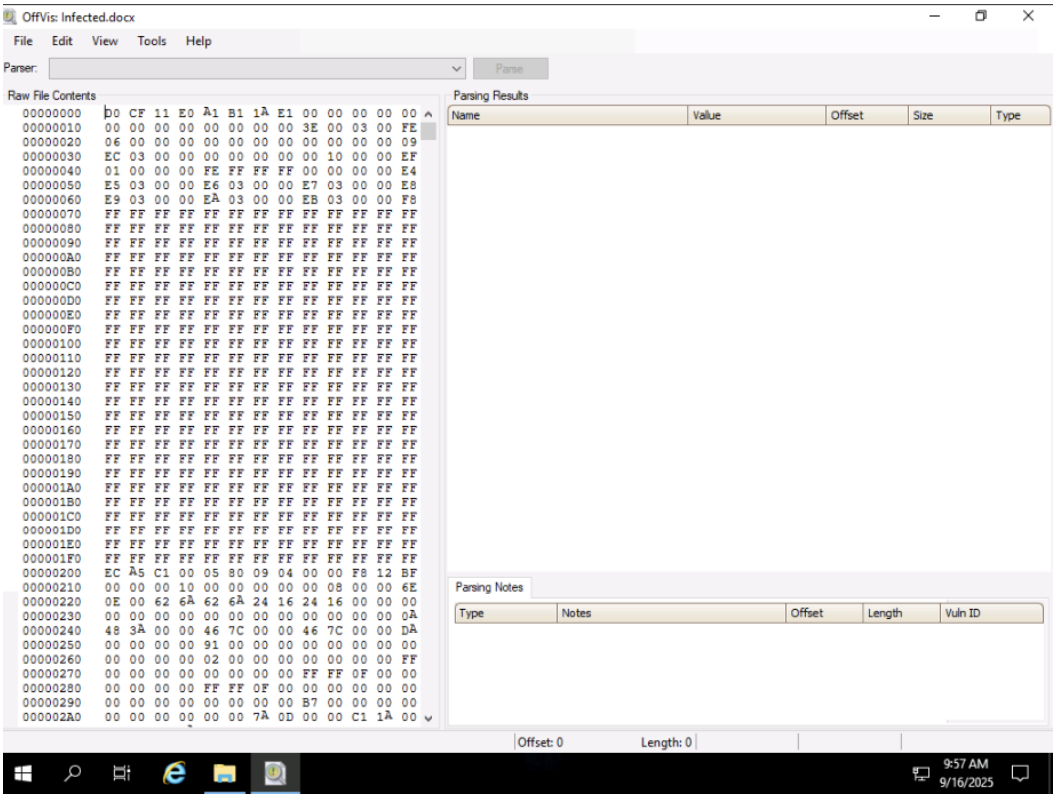
MS Office files such as Word documents and Excel sheets often act as carriers in spam campaigns since attackers try to transmit a packed executable masqueraded as a

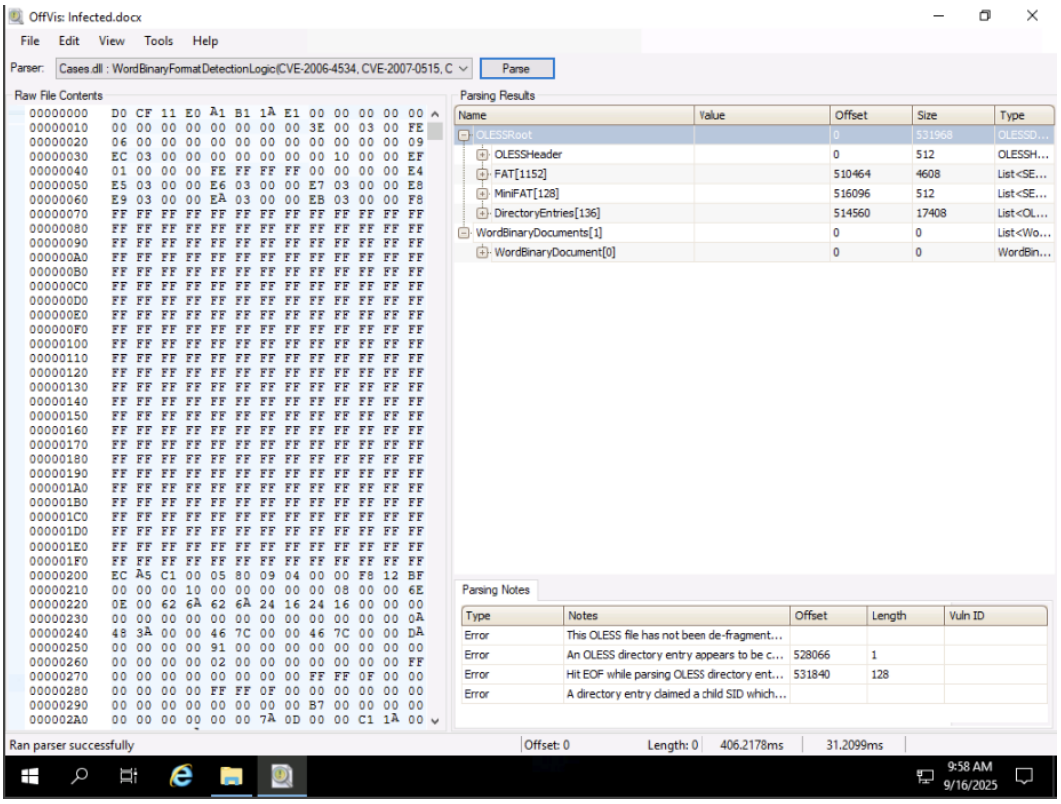
document. Investigators, therefore, need to know how to analyze a suspicious MS Office document and find malicious code or strings without executing the file on the system.

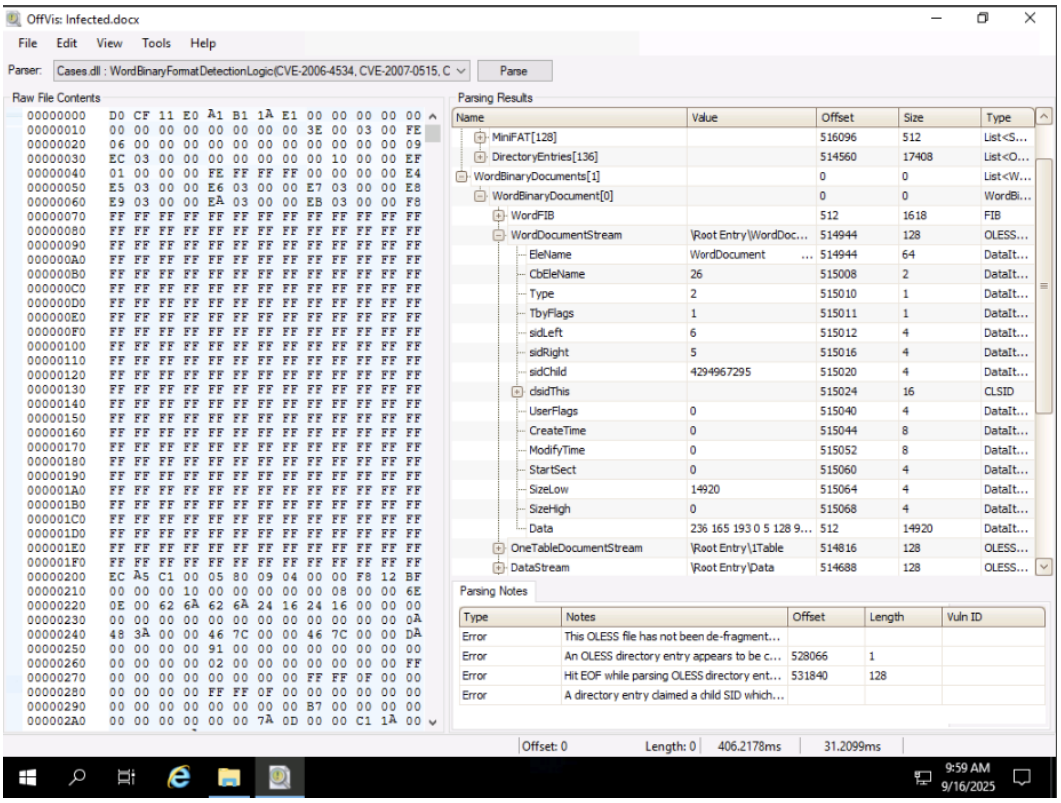
The objective of this lab is to help you understand how to perform static analysis on any suspicious MS Office document and see whether it contains any malicious elements or code.

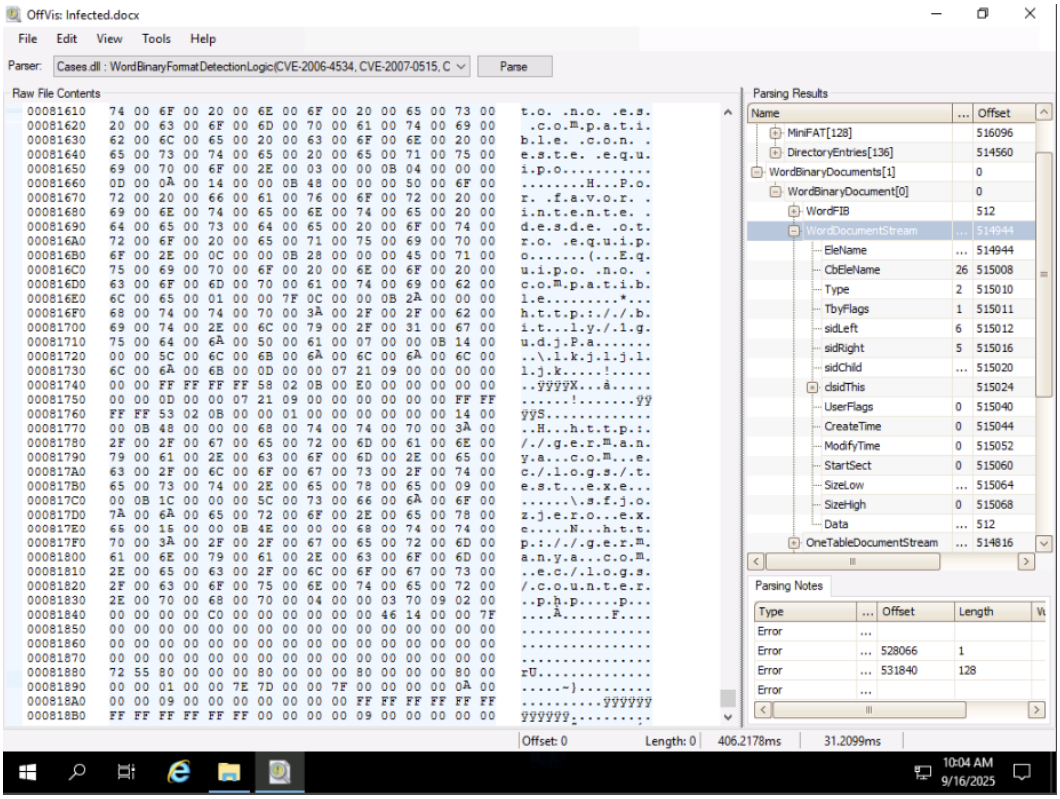
Overview of the Lab

In this lab, we will parse and examine the Word document using OffVis tool to know more about its impact on the system and the network.




OffVis: Infected.docx
File Edit View Tools Help
Parser: Cases.dll : WordBinaryFormatDetectionLogic(CVE-2006-4534, CVE-2007-0515, C
Parse
Raw File Contents
Parsing Results
Name Value Offset Size Type
OLESSRoot 0 531968 OLESSD...
OLESSHeader 0 512 OLESSH...
FAT[1152] 510464 4608 List<SE...
MiniFAT[128] 516096 512 List<SE...
DirectoryEntries[136] 514560 17408 List<OL...
WordBinaryDocuments[1] 0 0 List<Wo...
WordBinaryDocument[0] 0 0 WordBin...
Parsing Notes
Type Notes Offset Length Vuln ID
Error This OLESS file has not been de-fragment...
Error An OLESS directory entry appears to be c... 528066 1
Error Hit EOF while parsing OLESS directory ent... 531840 128
Error A directory entry claimed a child SID which...
Ran parser successfully
Offset: 0 Length: 0 406.2178ms 31.2099ms
9:58 AM
9/16/2025


OffVis: Infected.docx
File Edit View Tools Help
Parser: Cases.dll : WordBinaryFormatDetectionLogic(CVE-2006-4534, CVE-2007-0515, C
Parse
Raw File Contents
Parsing Results
Name Value Offset Size Type
MiniFAT[128] 516096 512 List<S...
DirectoryEntries[136] 514560 17408 List<O...
WordBinaryDocuments[1] 0 0 List<W...
WordBinaryDocument[0] 0 0 WordBi...
WordFIB 512 1618 FIB
WordDocumentStream \Root Entry\WordDoc... 514944 128 OLESS...
EleName WordDocument 514944 64 DataIt...
CbEleName 26 515008 2 DataIt...
Type 2 515010 1 DataIt...
TbyFlags 1 515011 1 DataIt...
sidLeft 6 515012 4 DataIt...
sidRight 5 515016 4 DataIt...
sidChild 4294967295 515020 4 DataIt...
clsidThis 515024 16 CLSID
UserFlags 0 515040 4 DataIt...
CreateTime 0 515044 8 DataIt...
ModifyTime 0 515052 8 DataIt...
StartSect 0 515060 4 DataIt...
SizeLow 14920 515064 4 DataIt...
SizeHigh 0 515068 4 DataIt...
Data 236 165 193 0 5 128 9... 512 14920 DataIt...
OneTableDocumentStream \Root Entry\1Table 514816 128 OLESS...
DataStream \Root Entry\Data 514688 128 OLESS...
Parsing Notes
Type Notes Offset Length Vuln ID
Error This OLESS file has not been de-fragment...
Error An OLESS directory entry appears to be c... 528066 1
Error Hit EOF while parsing OLESS directory ent... 531840 128
Error A directory entry claimed a child SID which...
Offset: 0 Length: 0 406.2178ms 31.2099ms
9:59 AM
9/16/2025



Module 12: Malware Forensics – Summary

This module focused on analyzing and understanding malware through both static and dynamic forensic techniques. In Lab 1, we performed static analysis on a suspicious executable file to identify hidden or encrypted code, PE headers, libraries, and malicious strings using tools such as PEiD, Pestudio, and Dependency Walker. Lab 2 explored the behavior of an Emotet variant, examining how it interacts with the system and network properties in real-time using Process Monitor and Wireshark. Due to lab requirements, I was unable to fully complete the Emotet analysis portion, as it required signing in with a personal Microsoft account. Lab 3 involved performing forensic examination of a suspicious Microsoft Word document to detect any embedded malicious code or strings using the OffVis tool. The labs collectively provided hands-on experience in identifying malware functionality, infection vectors, and potential system impact.