Dynamic Malware Analysis BY P3NGU1N

Which tools and software do we need?

🎯 Which of the following tools is different from the others in terms of its function?

- Ollydbg
- Procmon
- Radare
- IDA

ANSWER: Procmon

🎯 What activities cannot be viewed with Procmon?

- Network
- File
- Registry
- Process
- Syscalls

ANSWER: Syscalls

🎯 Which of the following tools does not provide hash information of files?

- Powershell
- Certutil
- Procmon
- HashMyFile

ANSWER: Procmon

Creating Virtual Machine

🎯 What is the Network configuration that provides Internet access through the network interface of the host operating system?

- NAT
- Bridge
- Host-Only
- Private

ANSWER: NAT

🎯 What name should a registry key be created to disable the ASLR feature?

ANSWER: MoveImages

What Should We Pay Attention to when we conduct a Dynamic Analysis?

🎯 Which tool should be used to detect network activities?

- Regshot
- HashMyFiles
- Fiddler
- Process Hacker

ANSWER: fiddler

🎯 What command should be typed in the "Run" application to switch to the “temp folder”.

ANSWER: %temp%

Dynamic Malware Analysis Example #1

🎯 **Note:** You can use the clipboard to paste data to the lab machine or copy data from the lab machine.

(Desktop/Malware Samples/law.exe)

Question:

What is the domain name that the malware connects to for data hijacking?

ANSWER: us2.smtp.mailhostbox.com

🎯 (Desktop/Malware Samples/law.exe) Connect Virtual Machine via 'Connect' Button. On which port does the malware communicate over?

ANSWER: 587

🎯 (Desktop/Malware Samples/law.exe) Connect Virtual Machine via 'Connect' Button. What is the name of the executable file that the malicious application writes to the AppData directory?

ANSWER: AheGmkp.exe

🎯 (Desktop/Malware Samples/law.exe) Connect Virtual Machine via 'Connect' Button. Which Registry Key does the malware use to ensure persistence?

ANSWER: HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

Dynamic Malware Analysis Example #2

🎯 (Desktop/Malware Samples/payment advice.exe)(Password:infected) Connect Virtual Machine via 'Connect' Button. What is the domain name of the web application that the malware is requesting to learn its IP address?

ANSWER: checkip.dyndns.org

🎯 (Desktop/Malware Samples/payment advice.exe) What is the domain name that the malware connects to for data hijacking?

ANSWER: mail.stilltech.ro

🎯 What port does the malware communicate over?

ANSWER: 587

🎯 What is the username used by the malware to authenticate to the mail server it connects for data hijacking?

ANSWER: office@stilltech.ro

🎯 What is the password that the malware uses to authenticate to the mail server it connects for data hijacking?

ANSWER: eurobit555ro

QUIZ:

🎯 **Which of the following products is not used for virtualization?**

ANSWER: IDA Pro

🎯 **What filter should be created to list file creation events in Procmon?**

ANSWER: Operation is CreateFile

🎯 **Which filter should be created to list process creation events in Procmon?**

ANSWER: **Operation is Process Start**

🎯 **Which tool would be more appropriate to use to analyze network activities?**

ANSWER: **Wireshark**

🎯 **What types of activities are not displayed in Procmon?**

ANSWER: syscalls

🎯 **What protocol does the Fiddler tool monitor?**

ANSWER: http

🎯 **Which command should be entered in the "Run" application to access the directory where the applications that will start automatically when the operating system is started are stored?**

ANSWER: **shell:startup**

🎯 **What filter should be entered to list the activities with destination port 443 on Wireshark?**

ANSWER: **tcp.dstport == 443**

🎯 **Which of the following is an advantage of dynamic malware analysis?**

ANSWER: Speed

🎯 **Which of the following is not a method used by malware to ensure persistence?**

ANSWER: **Renaming itself**