Cyber Sky
منصة تعليمية للأمن السيبراني

المسار التعليمي

Cyber Sky Malware Developer

APT attacks and adversary simulation

XPP **CSMD 1** **CSMD 2** **CSMD 3**

Cyber Sky
منصة تعليمية للأمن السيبراني

First course (XPP) is Preparation for malware development, discussing C/C++ programming

- Chapter 1: (Files Management)
  - Important DataTypes.
  - CreateFile
  - WriteFile
  - ReadFile
  - HardLink
  - SymLink
  - CopyFile
  - DeleteFile
  - MoveFile
  - CreateDirectory
  - RemoveDirectory
  - File Searching.

- Chapter 2 : (Registry Win32Api) :-
  - Registry winapi32
  - RegCreateKey
  - RegistrySetValue
  - RegOpenKey
  - RegCloseKey

- Chapter 3 : (Process/IPC win32api) :-
  - CreateThread
  - CreateProcess
  - WaitForSingleObject
  - CreateMutex
  - CreateToolhelp32Snapshot
  - Process32First
  - Process32Next

Cyber Sky
منصة تعليمية للأمن السيبراني

CSMD 1

Chapter 1:

- The common terms.
- Introduction to PE files.
- Visiting our environment.
- PE files in practice.
- EXE & DLL.
- Revision of the theories.

Chapter 2 :

- Payload concept.
- What are droppers?
- Payload storing places.
- Executing payload in different sections.
- Revision of the theories.

Chapter 3 :

- Encoding & Encryption.
- Base64 Encoding.
- Encrypting using XOR.
- Encrypting using AES.
- AV & Function WinApi call detection.
- How to hide WinApi calls from AV.
- Revision of the theories.

Cyber Sky
منصة تعليمية للأمن السيبراني

- Chapter 4:
  - Backdoor concept.
  - Theory behind backdooring PE.
  - Transform legitimate application to trojan.
  - Fix the execution of shellcode.
  - Revision of the theories.

- Chapter 5 :
  - What is code injection?
  - Where to inject and why (integrity levels) ?
  - Injecting a stored shellcode into remote process.
  - Dll injection technique.
  - Implementing injector with a dll.
  - Revision of the theories.

Cyber Sky
منصة تعليمية للأمن السيبراني

CSMD 2

Chapter 1:

- Introduction CSMD 2 .
- Malware lifecycle.
- First Stage.
- Second Stage.
- Third Stage.

Chapter 2 :

- Introduction to malware persistence
- Startup Folder technique.
- Run/RunOnce Registry technique.
- WinLogon technique.
- Shortcut infection.
- Persistence automation

Chapter 3:

- Code injection review
- Alternative classical injection.
- Thread Hijacking
- MapView injection
- APC injection.
- Advanced APC injection

Cyber Sky
منصة تعليمية للأمن السيبراني

- Chapter 4:
  - Introduction to malware self-protection.
  - Introduction to Anti debugging techniques.
  - VM artifacts.
  - Identification via Processes.
  - Libs enumeration and detection.
  - Computer username identification
  - Parent process detection.
- Chapter 5 Bonus:
  - PE-In-depth

Cyber Sky
منصة تعليمية للأمن السيبراني

CSMD 3 Advanced

- Chapter 1:Persistence techniques
  - COM hijacking
  - IFEO exploitation
  - WMI subscriptions
  - and more

- Chapter 2 : Privilege escalation techniques
  - Dll hijacking
  - Task hijacking
  - leaked handles exploitation in depth
  - token hijacking
  - name pipes exploitation .

- Chapter 3 : Persistence techniques
  - Scheduled tasks manipulation
  - service hijacking
  - WMI subscriptions.

- Chapter 4 : Advanced code injection techniques
  - Thread hijacking
  - detour hooking
  - inline-patching

- Chapter 5 : Stealth techniques
  - PPID spoofing
  - self debugging
  - advanced data obfuscation.