ADVANCE PROCESS INJECTION V.2 WORKSHOP

By- CyberWarFare Labs Team

About CyberWarFare Labs :

CyberWarFare Labs is an Ed-Tech Cyber Security Focused Platform which is totally engrossed in solving the problem of Cybersecurity by providing them real-time hands-on manner solutions to problems of B2C & B2B Audience. We provide Practical Labs [Simulation of critical infrastructure] like Healthcare, Nuclear Facility etc.

Partnered With :

IIT KANPUR

STARTUP INCUBATION AND INNOVATION CENTRE IIT KANPUR

C3iHub

IIT Indore

National Centre of Excellence Cybersecurity Technology And Entrepreneurship

DSCI PROMOTING DATA PROTECTION

Microsoft for Startups

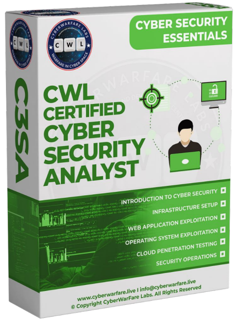
Google Cloud for Startups

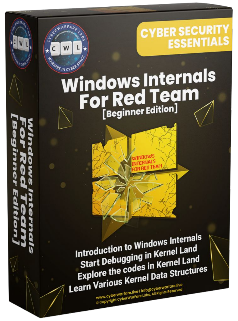
aws startup programs

#startupindia

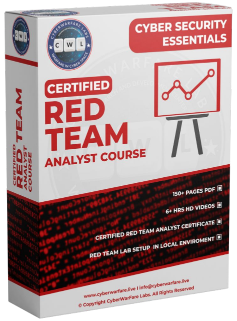
एसटीपीआई STPI

Our Offering On Courses :

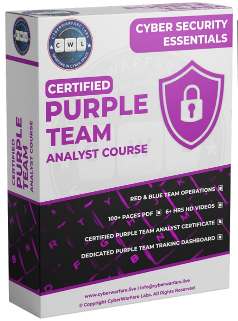

CYBER SECURITY ESSENTIALS
C3SA
CWL CERTIFIED CYBER SECURITY ANALYST
INTRODUCTION TO CYBER SECURITY
INFRASTRUCTURE SETUP
WEB APPLICATION EXPLOITATION
OPERATING SYSTEM EXPLOITATION
CLOUD PENETRATION TESTING
SECURITY OPERATIONS
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved

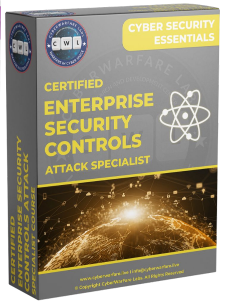

CYBER SECURITY ESSENTIALS
Windows Internals For Red Team
[Beginner Edition]
Introduction to Windows Internals
Start Debugging in Kernel Land
Explore the codes in Kernel Land
Learn Various Kernel Data Structures
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved

CYBER SECURITY ESSENTIALS
CERTIFIED RED TEAM SPECIALIST COURSE
ADVERSARY SIMULATION LAB
CERTIFIED RED TEAM SPECIALIST
MITRE ATT&CK FRAMEWORK
3 UNIQUE ATTACK PATH MANUALS
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved

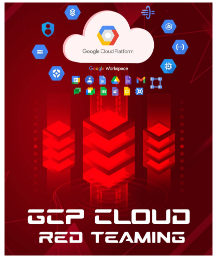

CYBER SECURITY ESSENTIALS
CERTIFIED RED TEAM ANALYST COURSE
150+ PAGES PDF
6+ HRS HD VIDEOS
CERTIFIED RED TEAM ANALYST CERTIFICATE
RED TEAM LAB SETUP IN LOCAL ENVIROMENT
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved

CYBER SECURITY ESSENTIALS
CERTIFIED AWS CLOUD RED TEAM SPECIALIST COURSE
amazon web services
150+ PAGES PDF
20+ HRS HD VIDEOS
RED TEAMING IN AWS CLOUD ENVIROMENT
CERTIFIED AWS CLOUD RED TEAM SPECIALIST [CARTS] CERTIFICATE
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved


CYBER SECURITY ESSENTIALS
CERTIFIED PURPLE TEAM ANALYST COURSE
RED & BLUE TEAM OPERATIONS
100+ PAGES PDF
6+ HRS HD VIDEOS
CERTIFIED PURPLE TEAM ANALYST CERTIFICATE
DEDICATED PURPLE TEAM TRAKING DASHBOARD
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved


CYBER SECURITY ESSENTIALS
CERTIFIED ENTERPRISE SECURITY CONTROLS ATTACK SPECIALIST
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved

Our Offering On Trainings :



About Speakers :

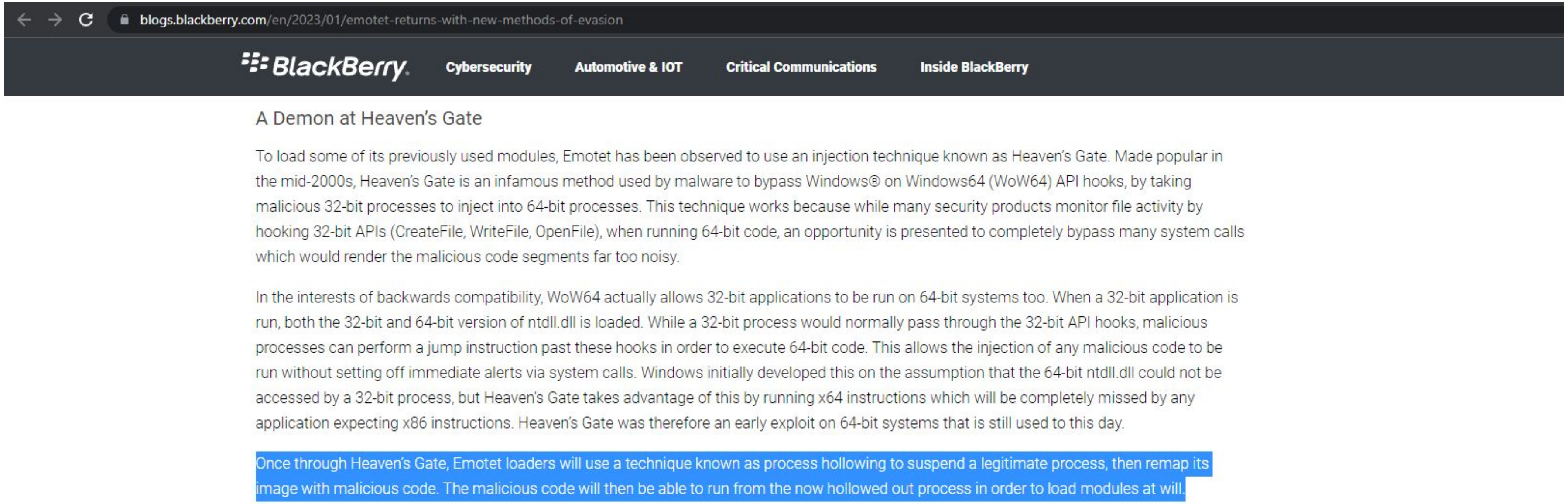
John Sherchan
(Security Researcher)

John Sherchan, Red Team Security Researcher at CyberwarFare Labs. He has been working in reverse engineering, malware development and analysis, and source
code review. He has very good knowledge of Windows Internals (Both User & Kernel Mode). He has reversed several AV and EDRs to comprehend their architecture. He is currently engaged in AV/EDR evasion projects at his place of employment.

Agenda Of Workshop :

In order to better prepare intermediate and advanced information security professionals, CyberWarFare Labs is hosting a hands-on workshop on the subject of "Advanced Process Injection techniques V.2"

- A thorough examination of Process Injection V.2 techniques
- Introduction to C for Offensive Operations
- Obtain materials + interact with the instructor
- Earn a certificate of attendance



A Demon at Heaven's Gate

To load some of its previously used modules, Emotet has been observed to use an injection technique known as Heaven's Gate. Made popular in the mid-2000s, Heaven's Gate is an infamous method used by malware to bypass Windows® on Windows64 (WoW64) API hooks, by taking malicious 32-bit processes to inject into 64-bit processes. This technique works because while many security products monitor file activity by hooking 32-bit APIs (CreateFile, WriteFile, OpenFile), when running 64-bit code, an opportunity is presented to completely bypass many system calls which would render the malicious code segments far too noisy.

In the interests of backwards compatibility, WoW64 actually allows 32-bit applications to be run on 64-bit systems too. When a 32-bit application is run, both the 32-bit and 64-bit version of ntdll.dll is loaded. While a 32-bit process would normally pass through the 32-bit API hooks, malicious processes can perform a jump instruction past these hooks in order to execute 64-bit code. This allows the injection of any malicious code to be run without setting off immediate alerts via system calls. Windows initially developed this on the assumption that the 64-bit ntdll.dll could not be accessed by a 32-bit process, but Heaven's Gate takes advantage of this by running x64 instructions which will be completely missed by any application expecting x86 instructions. Heaven's Gate was therefore an early exploit on 64-bit systems that is still used to this day.

Once through Heaven's Gate, Emotet loaders will use a technique known as process hollowing to suspend a legitimate process, then remap its image with malicious code. The malicious code will then be able to run from the now hollowed out process in order to load modules at will.

Table of contents

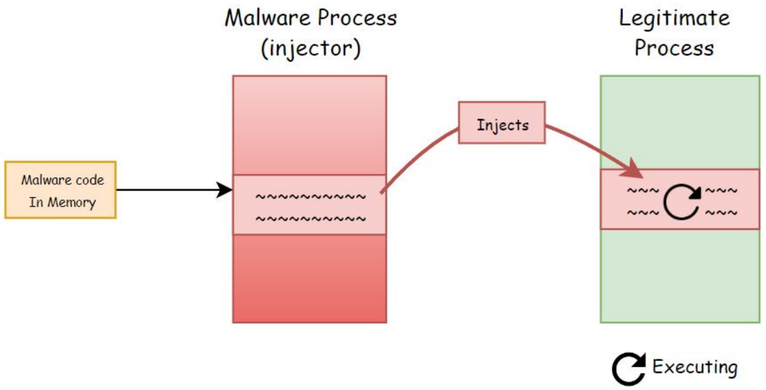
1. Pre-Requisites
2. Process Injection Mindset
3. Classic Process Injection
4. APC Code Injection
5. Section Mapping
6. CWL New Offerings - Mini Courses

PRE-REQUISITES

- Vmware/VirtualBox
- Windows 10 x64
  - Lab version: Windows 10 version 22H2 (x64bit)
- Any IDE or Editor (Visual studio 2022 is preferred)
- System Informer
- Programming Language:
  - *C/C++*
- Lab codes:
  - https://drive.google.com/file/d/1m9RqiOz5lQyT6VeTAde_gAEEY8cy1KFj/view?usp=share_link

Basic Mindset for Process Injection (remote)

- Injecting PE/DLL/shellcode (malicious) into another process' address space
    - To hide from the AV products
    - To hide from the naked eye of the analyst
    - Sometimes, to access the resources (network, memory, files etc.) owned by another process
- When performing process injection, we need to have the following queries in our mind
    - How can we access the remote process?
    - How can we send our malicious code to the remote process?
    - How can we execute our malicious code which is inside the remote process?



Process Injection - Access Remote Process

- Getting Access to Remote Process
  - Obtain a handle to the remote process
    - Handle is value given to the user-mode processes when they try to access some object (process, thread, file, etc) from user-land
- Obtaining the handle
  - Opening a executing process
    - Win32 API: **OpenProcess**
    - NT API: **NtOpenProcess**
  - Creating a new legitimate process
    - Win32 API: **CreateProcessA**
    - NT API: **NtCreateProcessEx, NtCreateUserProcess**
  - Duplicating existing process handle from another process
    - Win32 API: **DuplicateHandle**
    - NT API: **NtDuplicateObject**

Process Injection - Sending Malicious Code

- ➔ Many ways to send malicious code to remote process, but few queries to have in our mind
  - ◆ Do we have enough privilege to write code into the remote process?
    - PROCSS_VM_OPERATION, PROCESS_VM_WRITE
  - ◆ Can we locate the address of the malicious code in the remote process that we just sent?
  - ◆ Is the memory region in remote process has enough memory access rights to write & execute code in that memory region?
    - Commonly we look for writable (W) & executable (X) memory region
      - ○ But in modern OS because of security reason memory region is usually either writable or executable (W^X).

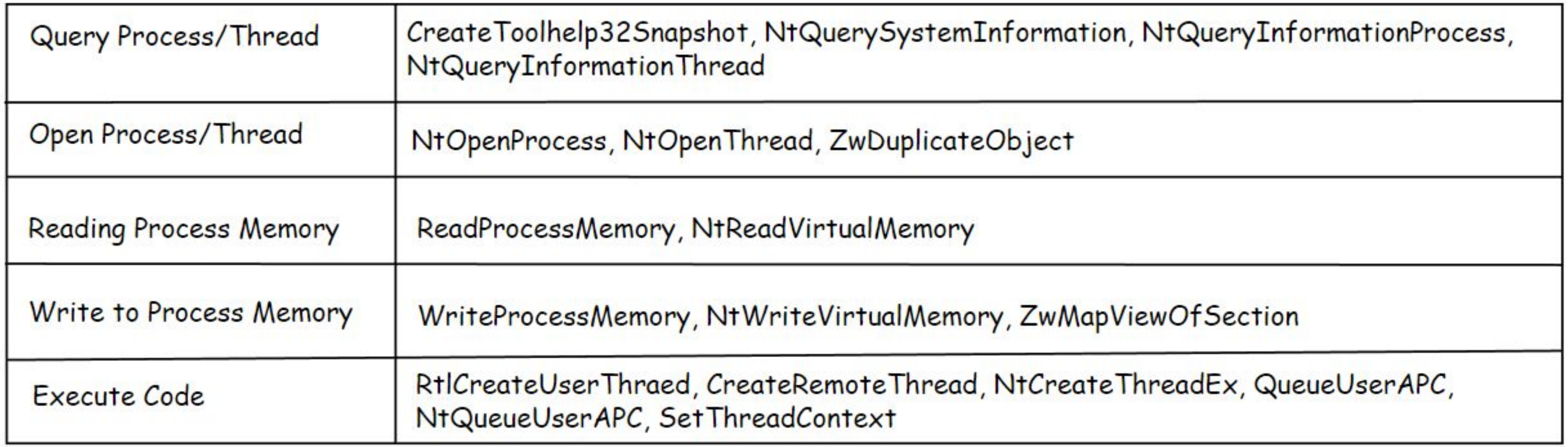
Process Injection - Sending Malicious Code

- Usually sending/injecting malicious code in remote process involves
  - Allocating new memory region with READ, WRITE & Execute access in remote process
    - Win32 API: **VirtualAllocEx**
    - NT API: **NtAllocateVirtualMemory**
    - Access Rights: PAGE_READWRITE, (PAGE_READWRITE | PAGE_EXECUTE)
  - Writing payload into the memory
    - Win32 API: **WriteProcessMemory**
    - NT API: **NtWriteVirtualMemory**
- Additionally, changing memory protection also involves in this stage
  - Usually, memory protection PAGE_READWRITE is changed to PAGE_EXECUTE_READ and vice versa.
    - Win32 API: **VirtualProtectEx**
    - NtAPI: **NtProtectVirtualMemory**

Process Injection - Execute the Malicious code

- Common ways to perform execution
  - Create a new thread in target process
    - Win32 API: **CreateRemoteThread**
    - NT API: **NtCreateThreadEx**, **RtlCreateUserThread**
  - Queuing APC in alertable thread
    - Win32 API: **QueueUserAPC**
    - NT API: **NtQueueUserAPC**
  - Hijacking the executing thread
    - Win32 API: **SetThreadContext**
    - NT API: **NtSetContextThread**
- Last phase of the injection
  - Some APIs that are used in this stage are heavily monitored by the AV/EDR products

Process Injection - Common APIs

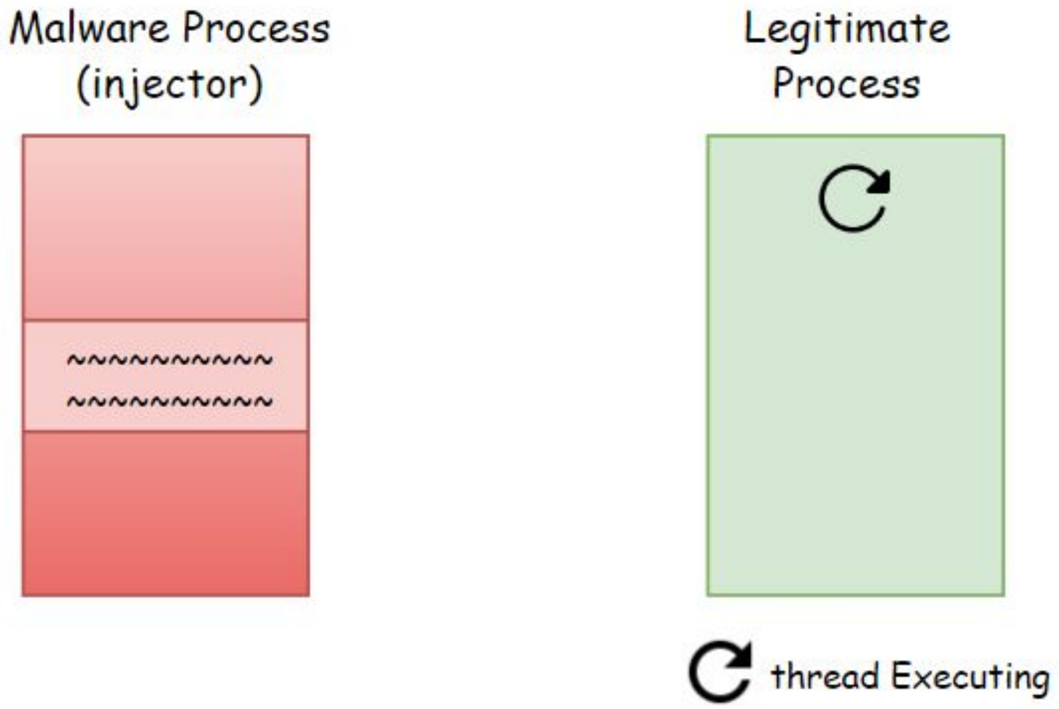


Query Process/Thread	CreateToolhelp32Snapshot, NtQuerySystemInformation, NtQueryInformationProcess, NtQueryInformationThread
Open Process/Thread	NtOpenProcess, NtOpenThread, ZwDuplicateObject
Reading Process Memory	ReadProcessMemory, NtReadVirtualMemory
Write to Process Memory	WriteProcessMemory, NtWriteVirtualMemory, ZwMapViewOfSection
Execute Code	RtlCreateUserThraed, CreateRemoteThread, NtCreateThreadEx, QueueUserAPC, NtQueueUserAPC, SetThreadContext

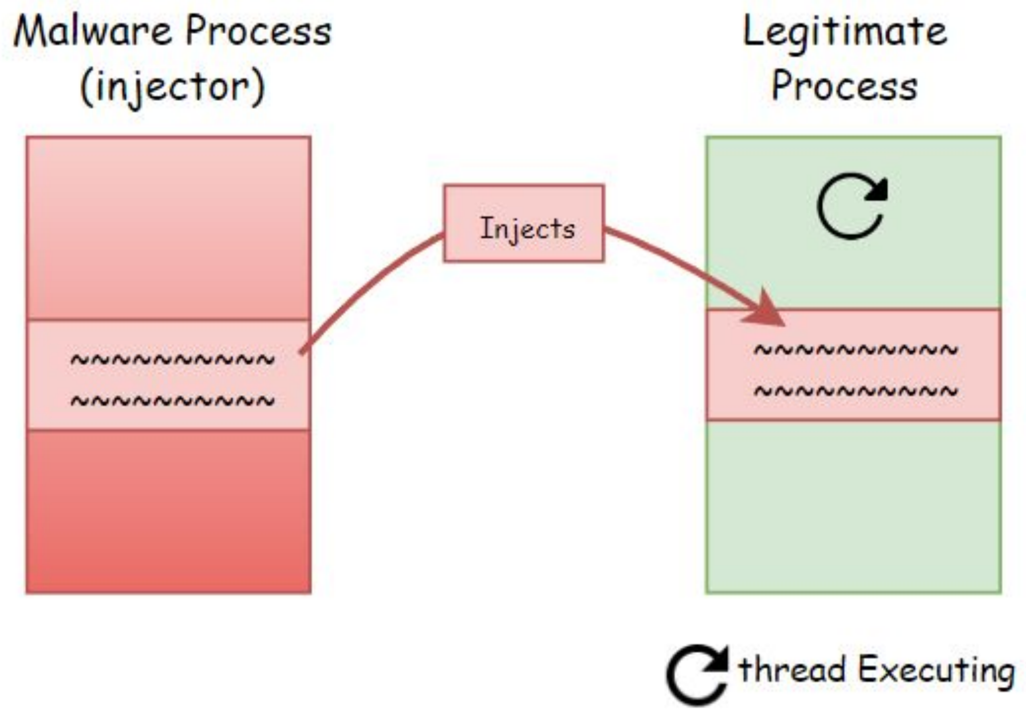
Classic Process Injection - steps

- Obtain Handle to a target process
  - *CreateToolHelp32Snapshot, OpenProcess, NtQuerySystemInformation*
- Allocate new memory region at target process
  - *VirtualAllocEx, NtAllocateVirtualMemory*
- Write payload into newly allocated memory
  - *WriteProcessMemory, NtWriteVirtualMemory*
- Create new remote thread
  - *CreateRemoteThread, NtCreateThreadEx*

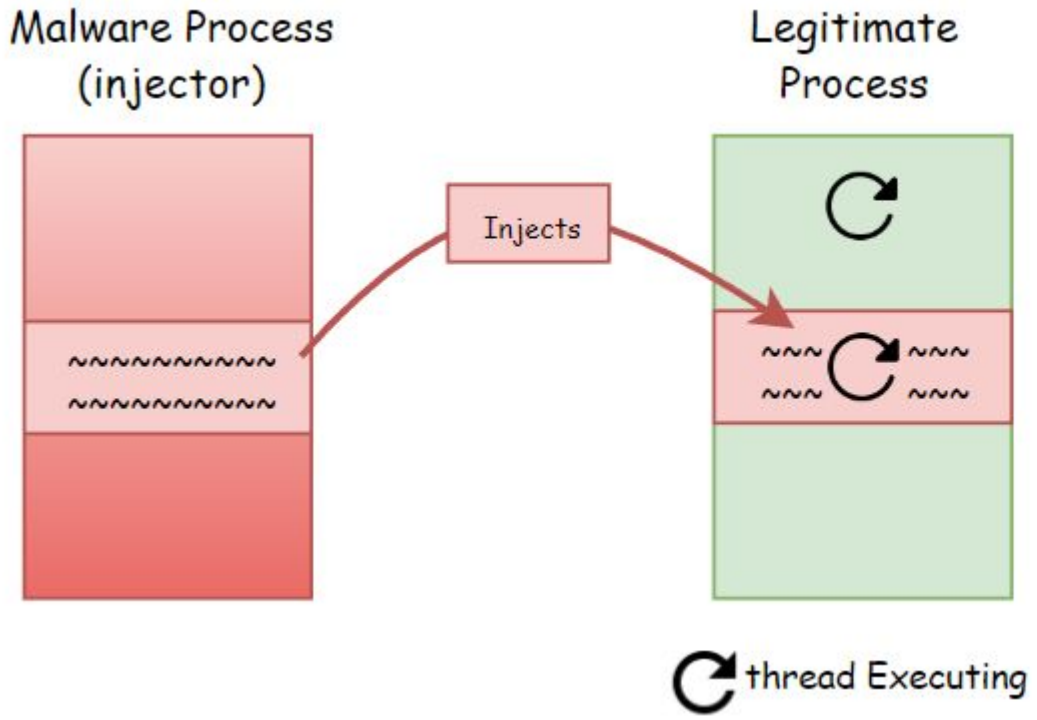
Classic Process Injection


Malware Process (injector)
~~~~~~~~~~~
~~~~~~~~~~~
Legitimate Process
thread Executing

Classic Process Injection


Malware Process (injector)
Legitimate Process
Injects
~~~~~~~~~~
~~~~~~~~~~
~~~~~~~~~~
~~~~~~~~~~
thread Executing

Classic Process Injection



Classic Process Injection - API calls

- ➔ Kernel32.dll :
  - *CreateToolHelp32Snapshot, Process32First, Process32Next, Thread32First, Thread32Next, OpenProcess, WriteProcessMemory, VirtualProtectEx, OpenThread*
- ➔ Ntdll.dll:
  - *NtQuerySystemInformation,NtAllocateVirtualMemory, NtWriteVirtualMemory*

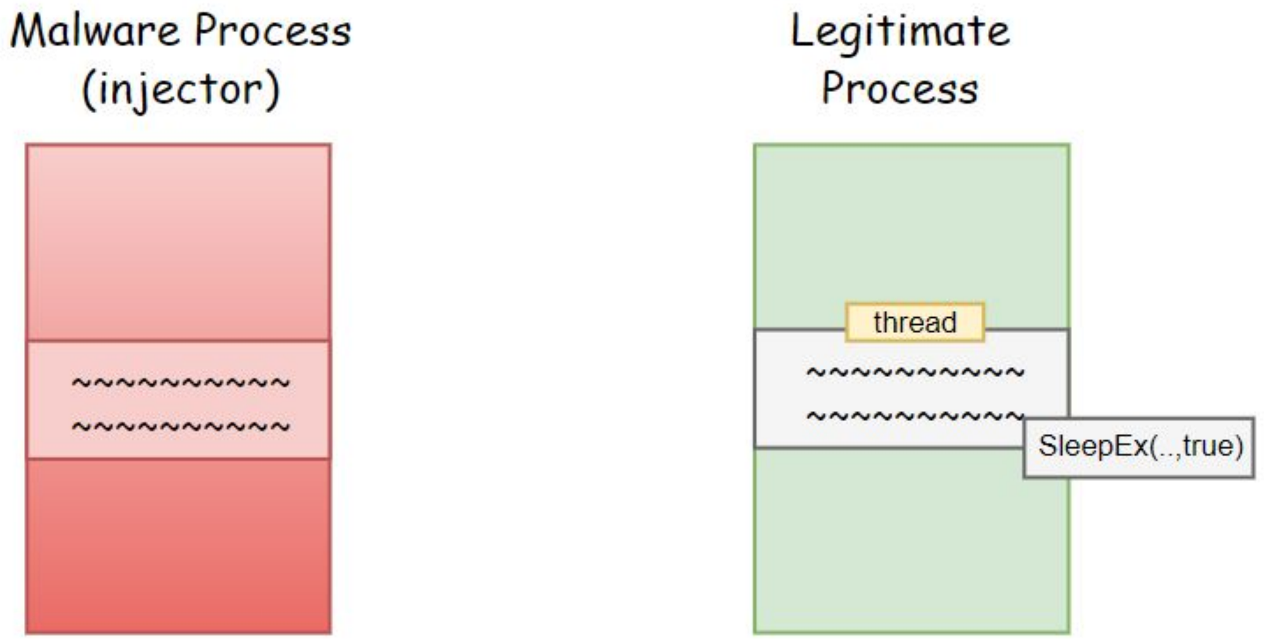
APC Code Injection

- ➔ APC stands for Asynchronous Procedure Call
- ➔ APC functions execute asynchronously in context of a particular thread
- ➔ In this techniques our shellcode is placed in APC Queue of the thread.
- ➔ The payload will get executed when the thread goes to alertable state
- ➔ Wait routines puts thread in alertable state, such as:
  - *SleepEx()*
  - *WaitForSingleObjectEx()*
  - *WaitForMultipleObjectEx()*

APC Code Injection - Steps

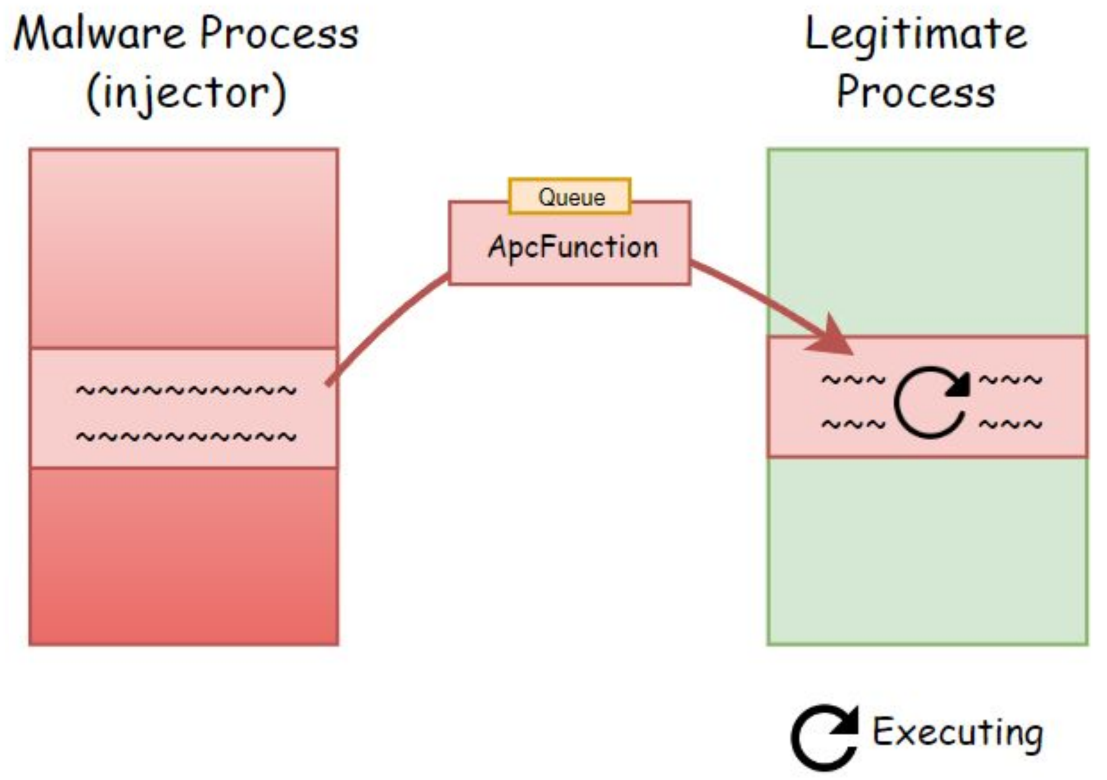
- Find the process to inject our payload
  - *CreateToolHelp32Snapshot*, *NtQuerySystemInformation*
- Find all the threads in that process
  - *Thread32First*, *Thread32Next*
- Allocate memory in that process
  - *VirtualAllocEx*, *NtAllocateVirtualMemory*
- Write the payload into that allocated memory
  - *WriteProcessMemory*, *NtWriteVirtualMemory*
- Put the APC function in the queue for all threads
  - *QueueUserAPC*, *NtQueueUserAPC*
- APC function here points to our shellcode

APC Code Injection



Malware Process (injector)
~~~~~~~~~~~
~~~~~~~~~~~
Legitimate Process
thread
~~~~~~~~~~~
~~~~~~~~~~~
SleepEx(..,true)

APC Code Injection



APC Code Injection - API calls

- Kernel32.dll :
  - *CreateToolHelp32Snapshot, Process32First, Process32Next, Thread32First, Thread32Next, OpenProcess, WriteProcessMemory, VirtualProtectEx, OpenThread, QueueUserAPC*
- Ntdll.dll:
  - *NtQuerySystemInformation,NtAllocateVirtualMemory, NtWriteVirtualMemory*

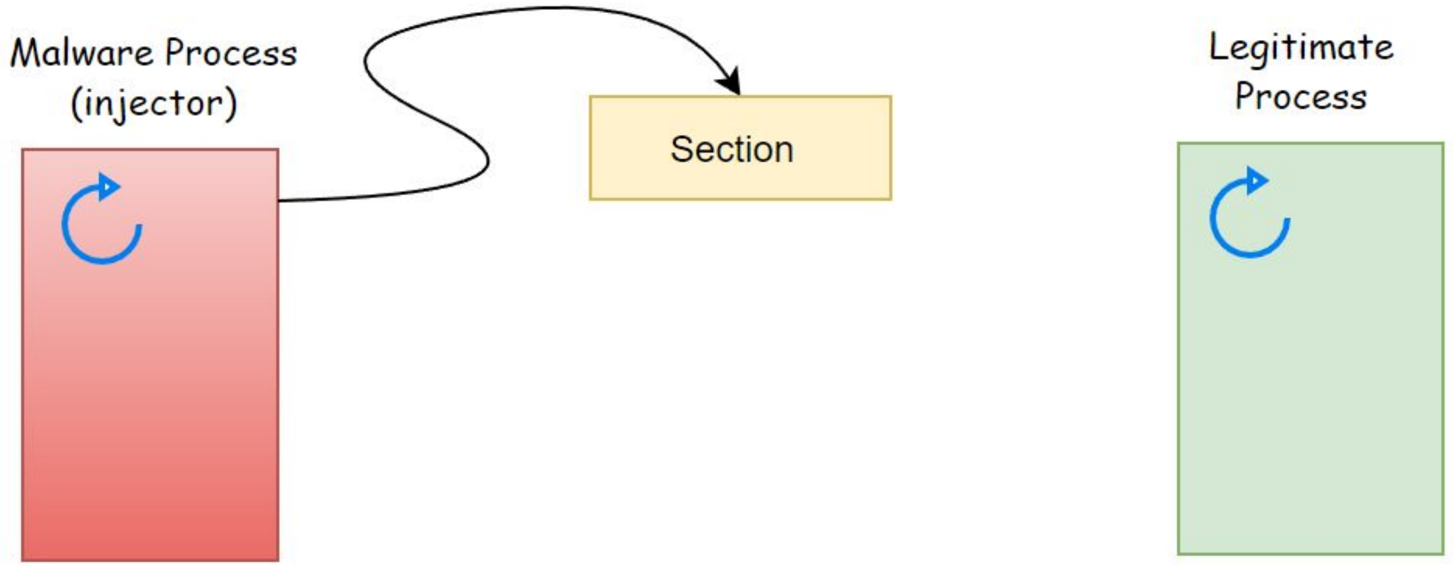
Section Mapping

- Block of memory that can be shared between multiple processes [1]
- In memory, each section has corresponding views, which are parts of the section that are visible to processes.
  - Act of creating a view for a section is known as mapping a view of the section [1]
- In this technique a section is created and view of section is mapped to both local & target process with different page protection

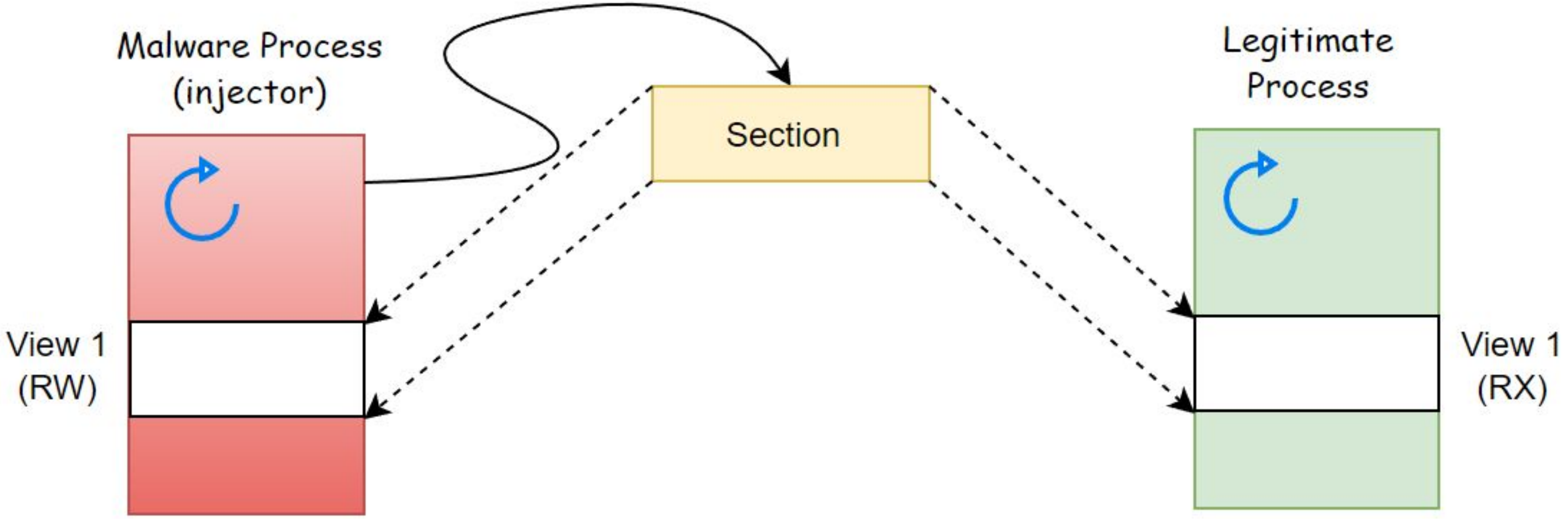
Section Mapping - Steps

- Create a new section with full RWX page protection
  - *NtCreateSection*
- Map a view of section to local process (injector) with RW page protection
  - *NtMapViewOfSection*
- Map a view of section to target process with RX page protection
  - *NtMapViewOfSection*
- Write a payload to a view mapped to a local process
  - *memcpy*
- Create a remote thread with a base address of view mapped to remote process
  - *CreateRemoteThread*, *NtCreateThreadEx*, *RtlCreateUserThread*

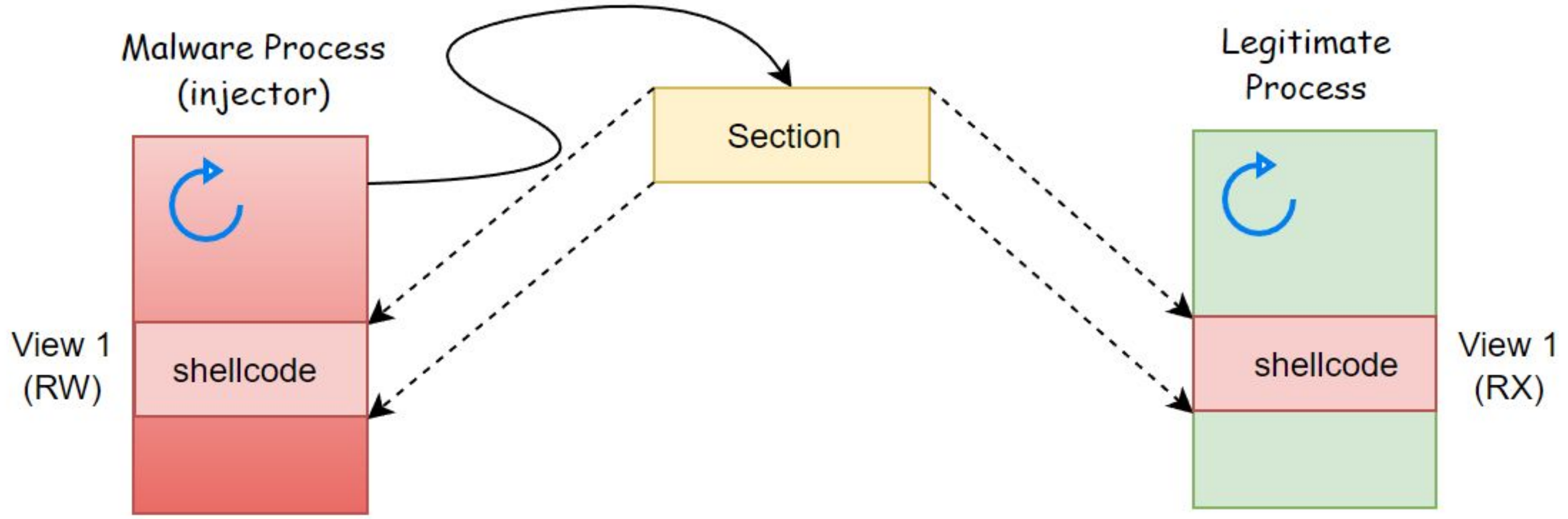
Section Mapping



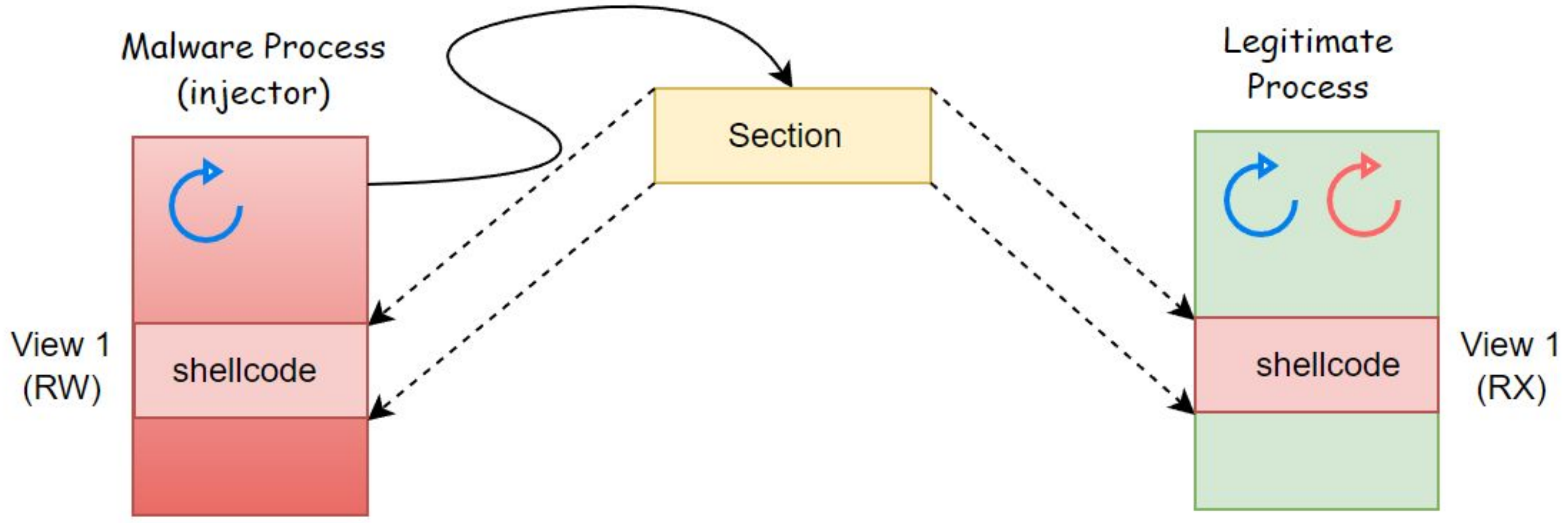
Section Mapping



Section Mapping



Section Mapping



Section Mapping - API calls

- Kernel32.dll :
  - *OpenProcess, CreateRemoteThread*
- Ntdll.dll:
  - *NtCreateSection, NtMapViewOfSection, NtCreateThreadEx*

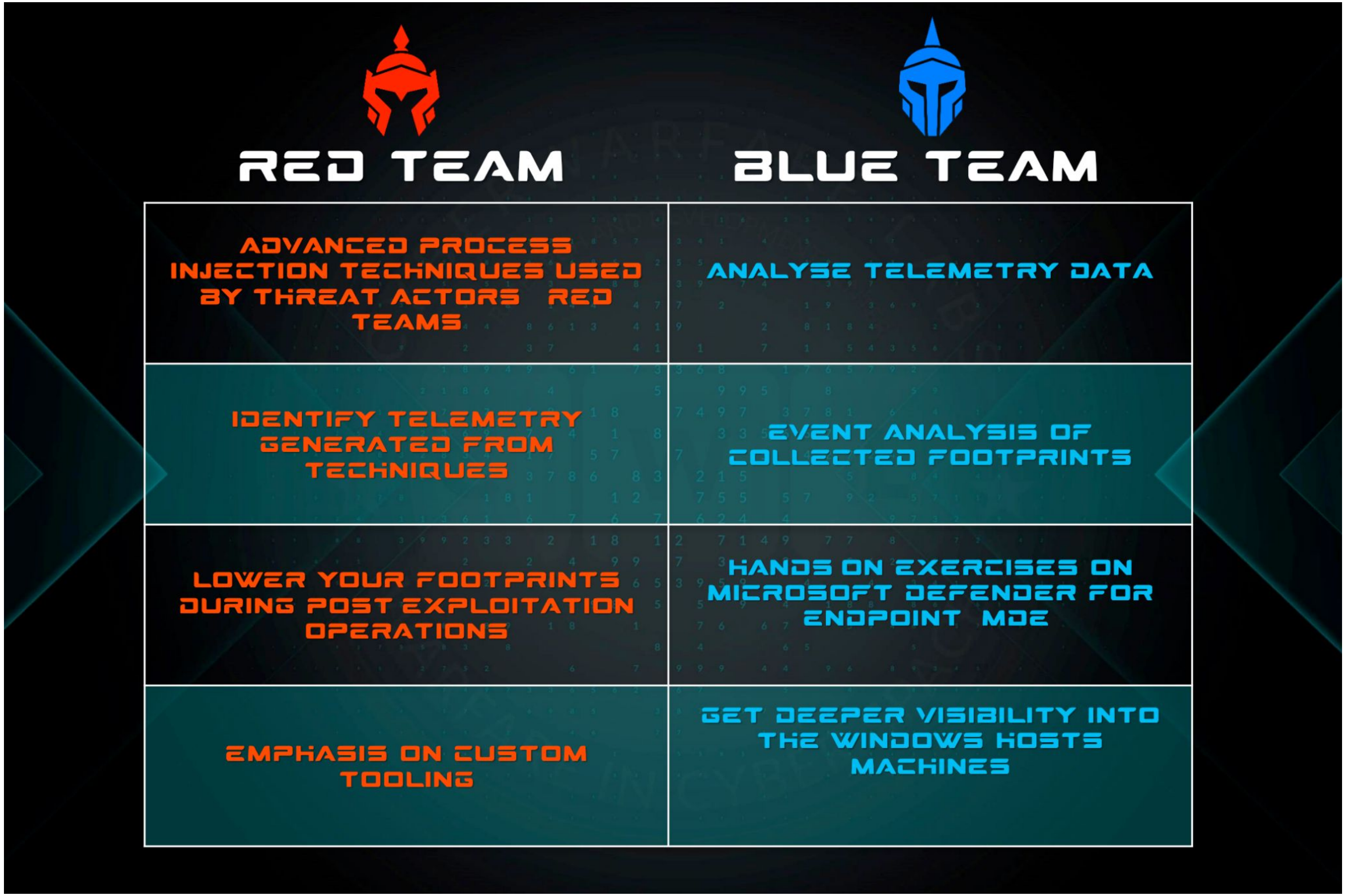
References

- https://blogs.blackberry.com/en/2023/01/emotet-returns-with-new-methods-of-evasion
- https://attack.mitre.org/techniques/T1055/

Presenting our New Offering:

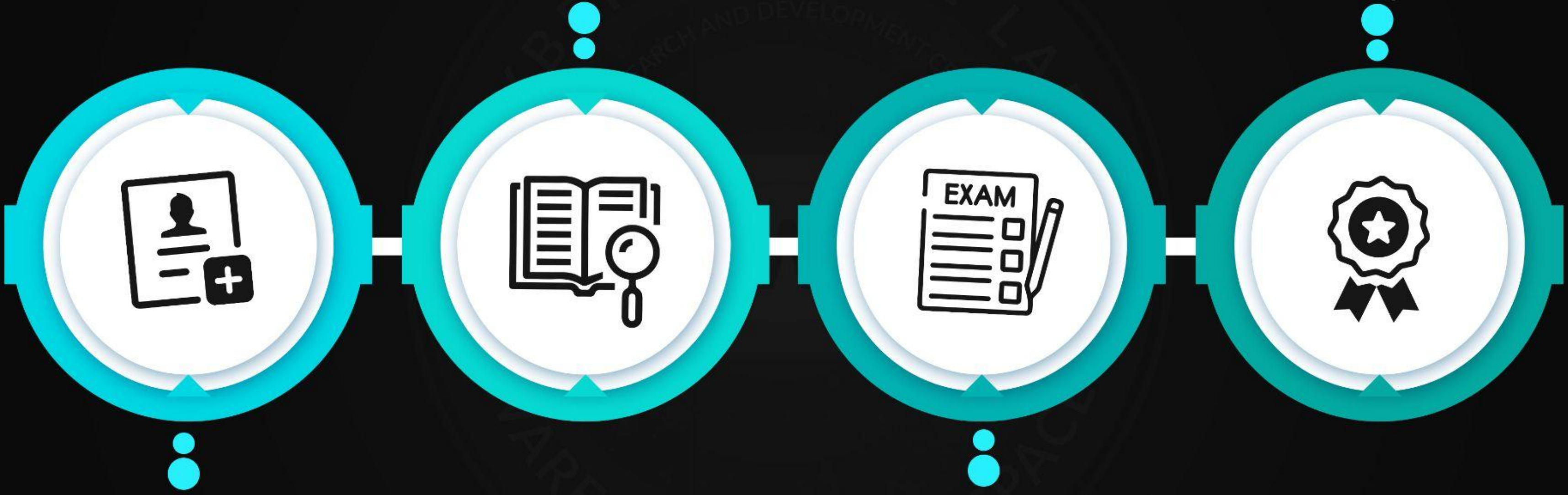
- Mini-Courses
- Easy to grasp & focus on specific techniques
- Affordable & Smooth practical learning + Exam Procedure

CYBERWARFARE LABS
CWL
WARFARE IN CYBER SPACE
ATTACK & DETECT ADVANCE PROCESS INJECTION TECHNIQUES
MINI-COURSE
www.cyberwarfare.live I info@cyberwarfare.live
© Copyright CyberWarFare Labs. All Rights Reserved
ADVANCE PROCESS INJECTION V.2
MINI-COURSE



RED TEAM	BLUE TEAM
ADVANCED PROCESS INJECTION TECHNIQUES USED BY THREAT ACTORS RED TEAMS	ANALYSE TELEMETRY DATA
IDENTIFY TELEMETRY GENERATED FROM TECHNIQUES	EVENT ANALYSIS OF COLLECTED FOOTPRINTS
LOWER YOUR FOOTPRINTS DURING POST EXPLOITATION OPERATIONS	HANDS ON EXERCISES ON MICROSOFT DEFENDER FOR ENDPOINT MDE
EMPHASIS ON CUSTOM TOOLING	GET DEEPER VISIBILITY INTO THE WINDOWS HOSTS MACHINES

ATTACK & DETECT ADVANCE PROCESS INJECTION TECHNIQUES CERTIFICATION PROCEDURE :



Enroll in "Attack & Detect Advance Process Injection Techniques"Mini-Course

Study the materials & Practise the Labs

Attempt MCQ Examination & achieve the 80% passing criteria

Earn Digital Badge

Thank You !

For any queries
Mail : info@cyberwarfare.live

Know more visit at www.cyberwarfare.live

Follow us on :