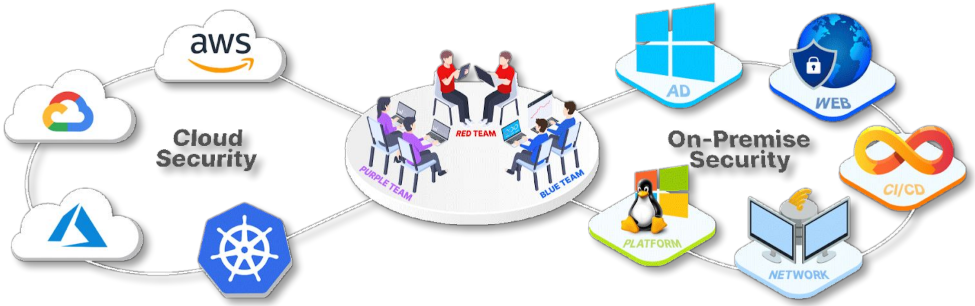
CYBERWARFARE LABS

Investigating Process Injection Threads: Essential Detection Strategies

About CyberWarFare Labs :

CW Labs is a renowned Infosec company specializing in cybersecurity practical learning. They provide on-demand educational services. The company has 3 primary divisions :

1. Learning Management System (LMS) Platform
2. CWL CyberSecurity Playground (CCSP) Platform
3. Infinity Learning Platform



INFINITE LEARNING EXPERIENCE

About Speaker :

Harisuthan S

Senior Security Engineer

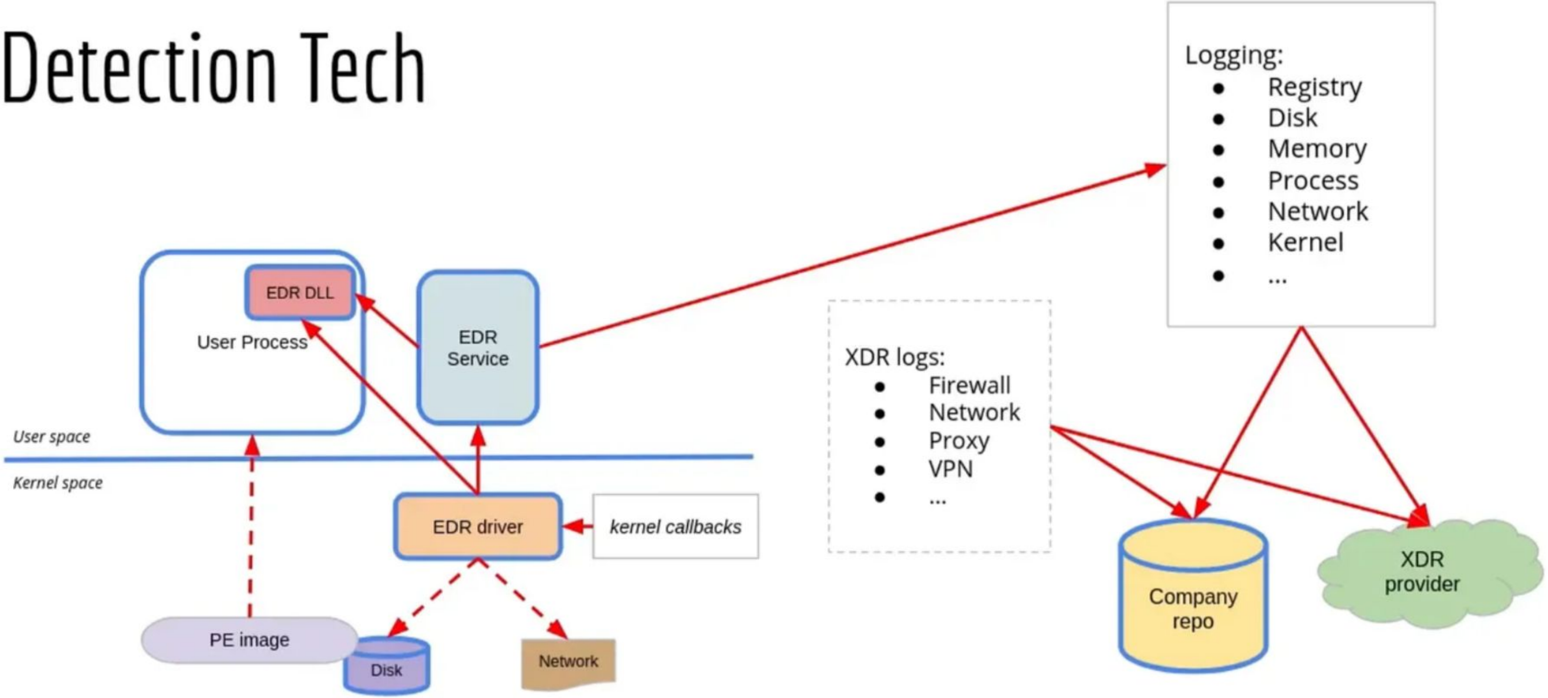
He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks.

Agenda

- Introduction to Process Injection Techniques
- Understanding Classic Process Injection and Process Hollowing
- Investigating Process Injection Threats
- Conclusion

Why traditional monitoring fails

Detection Tech



Logging:
- Registry
- Disk
- Memory
- Process
- Network
- Kernel
- ...

XDR logs:
- Firewall
- Network
- Proxy
- VPN
- ...

Ref: https://medium.com/@s12deff/understanding-edr-from-a-red-teamers-perspective-f4fe32b5608a

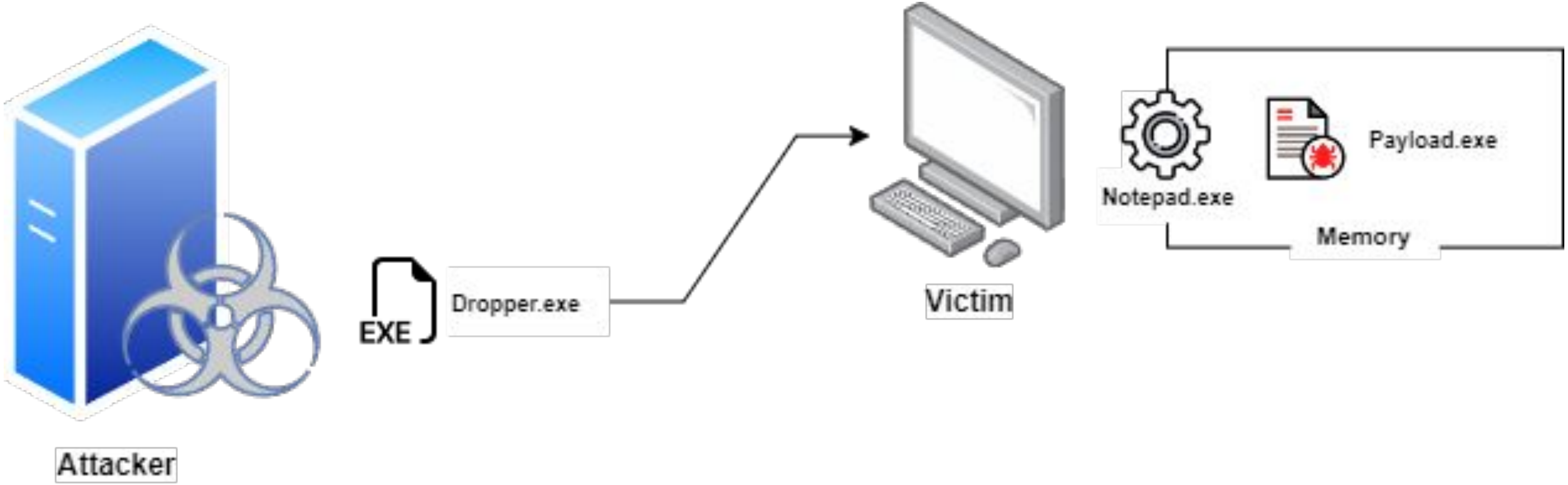
Introduction to
Process Injection Techniques

Process Injection Techniques

Attackers often seek ways to maintain persistence while evading defense solutions. One commonly used technique is process injection.

This technique involves injecting malicious payloads into the memory of legitimate processes, allowing attackers to bypass defenses and complicate security investigations. Based on their characteristics and behavior, process injection techniques are categorized into various types

Basic Working of Process Injection



Commonly used Process Injection Techniques

- Classic Process Injection
- APC Code Injection
- Section Mapping
- Module Stomping
- Process Hollowing
- Process Doppelganging
- Transacted Hollowing
- Process Herpaderping
- Process Ghosting

Commonly used Process Injection Techniques

- Classic Process Injection
- APC Code Injection
- Section Mapping
- Module Stomping
- Process Hollowing
- Process Doppelganging
- Transacted Hollowing
- Process Herpaderping
- Process Ghosting

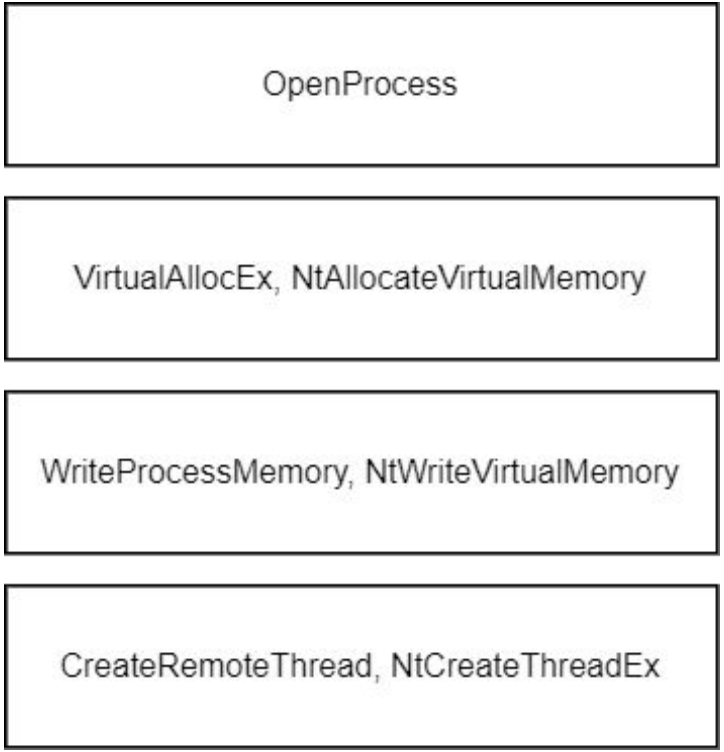
Query Process/Thread	NtQuerySystemInformation, NtQueryInformationProcess, NtQueryInformation Thread
Open Process/Thread	NtOpenProcess, NtOpenThread
Read Process/Thread	ReadProcessMemory, NtReadVirtualMemory
Write Process/Thread	WriteProcessMemory, NtWriteVirtualMemory
Execution	CreateRemote Thread, NtCreate ThreadEx, QueueUserAPC, NtQueueUserAPC, Set ThreadContext

Understanding Classic Process Injection and Process Hollowing

Classic Process Injection

Classic process injection is a technique used by attackers to inject malicious code into legitimate processes, allowing the code to execute within the context of a trusted process.

This method is often used to evade detection by security tools, since the malicious code runs under the umbrella of a legitimate process, making it harder to identify as a threat.



OpenProcess

VirtualAllocEx, NtAllocateVirtualMemory

WriteProcessMemory, NtWriteVirtualMemory

CreateRemoteThread, NtCreateThreadEx

Process Injection : Investigation

Identifying and investigating process injection can be complex, as it involves correlating data from logs, events, and process memory to detect suspicious and malicious activities.

Sysmon

Event Logs

Step: 01 : Identifying and prioritizing suspicious processes

The first step in an investigation is to review the activity associated with process creation. In the context of process injection techniques, it's commonly observed that process creation plays a crucial role in this process.

The most effective correlation starts by filtering events related to Event ID 4688, which indicates "A new process has been created" in Windows security logs.

```
event.code: "4688" and (not process.executable: "C:\\Windows\\System32\\wbem\\WmiPrvSE.exe" AND not
process.executable: "C:\Windows\\System32\\conhost.exe" AND not process.executable:
"C:\\Windows\\System32\\svchost.exe")
```

- Unusual programs that typically shouldn't be involved in process creation—such as **Notepad**, **winlogon**.exe, **rundll32**.exe, and **taskmgr**.exe—are often red flags. These uncommon applications usually do not engage in process creation activities.

- Suspicious execution of Windows architecture programs can raise concerns, especially when an executable in one architecture format (such as x64) is behaving unexpectedly, particularly if we observe any executable related to the x32 architecture. This discrepancy is uncommon and warrants further investigation.

- Process creation activity from suspicious file locations, such as Temp or Download directories, is generally considered a red flag. If any processes are initiated from these locations, it raises concerns. Furthermore, if an attacker gains higher privileges, they may execute processes from legitimate file paths, such as C:\Windows\System32, making detection even more challenging.

- If a process is assigned the privileged PAGE_EXECUTE_READWRITE, it is considered over-privileged. Attackers often exploit this to create or obtain processes with elevated privileges through process creation.

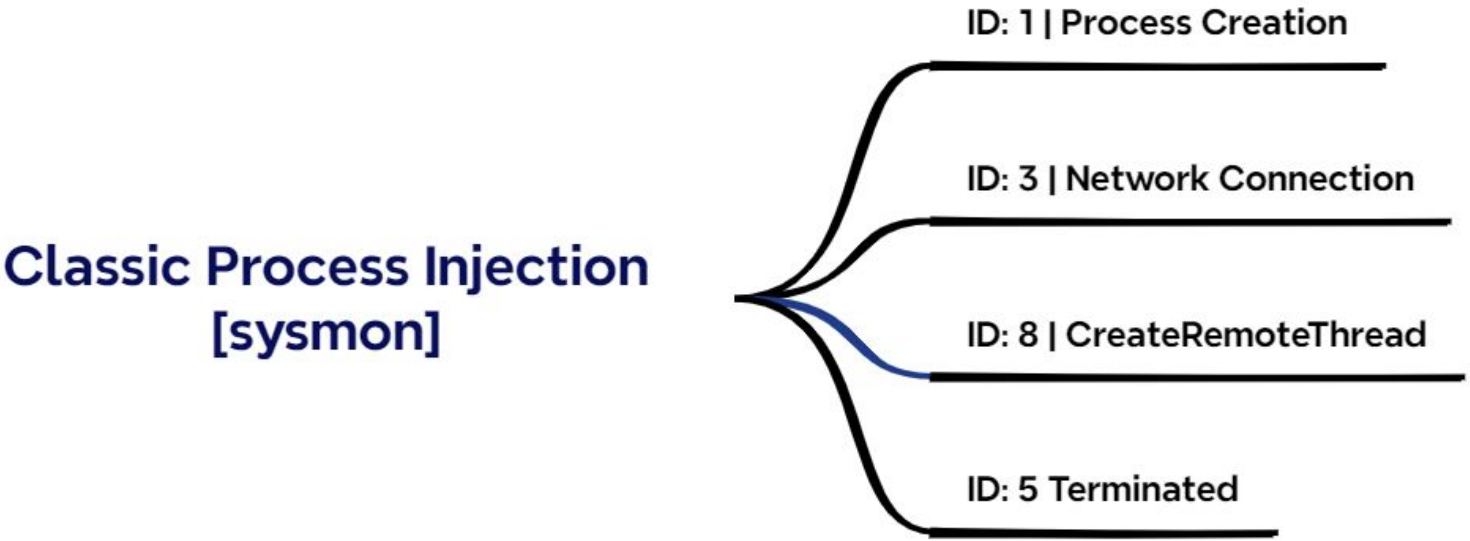
Step: 02 : Retrieving the Process ID linked to the suspicious process

Based on the previous step, we identified both ProcessHollowing.exe and notepad.exe as suspicious.

By executing the command below, we can specifically filter events associated with both processes.

```
event.code: "4688" and *classicprocessinjection.exe*
```

Step: 04 : Sysmon Correlation



Classic Process Injection [sysmon]

ID: 1 | Process Creation

ID: 3 | Network Connection

ID: 8 | CreateRemoteThread

ID: 5 Terminated

Step: 05 : Sysmon Correlation

Process Creation

```
event.dataset: "windows.sysmon_operational" and event.code: "1" and *classicprocessinjection.exe*
```

Network Connection

```
event.dataset: "windows.sysmon_operational" and event.code: "3" and *classicprocessinjection.exe* or
*notepad.exe*
```

Step: 05 : Sysmon Correlation

CreateRemoteThread

```
event.dataset: "windows.sysmon_operational" and event.code: "8"  and *classicprocessinjection.exe* or
*notepad.exe*
```

Process Tampered

```
event.dataset: "windows.sysmon_operational" and event.code: "25"  and *classicprocessinjection.exe* or
*notepad.exe*
```

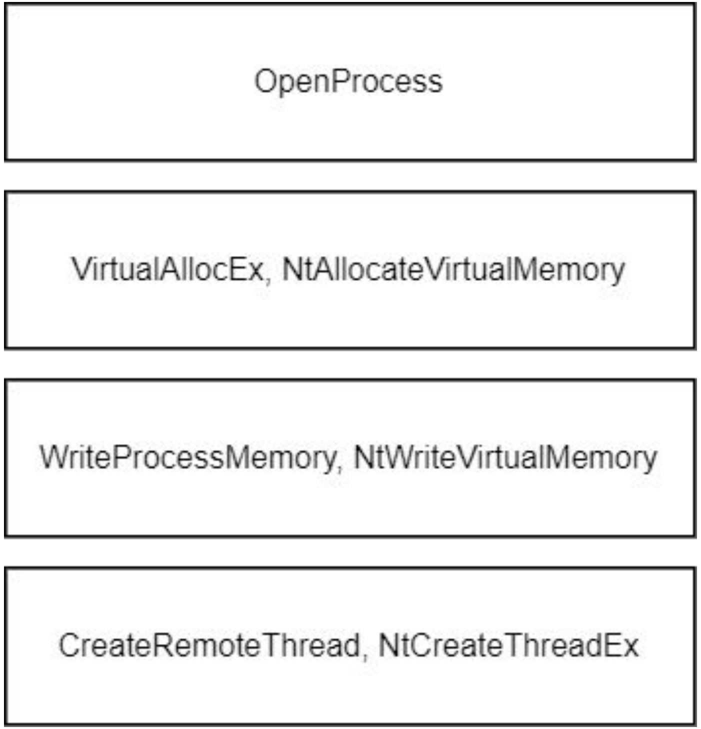
Process Hollowing

Create Suspended Process

Unmap Executable Sections

Inject Malicious Code

Resume Process Execution



OpenProcess

VirtualAllocEx, NtAllocateVirtualMemory

WriteProcessMemory, NtWriteVirtualMemory

CreateRemoteThread, NtCreateThreadEx

Process Hollowing : Investigation

Identifying and investigating process hollowing can be complex, as it involves correlating data from logs, events, and process memory to detect suspicious and malicious activities.

Sysmon

Event Logs

OSQuery

Step: 01 : Identifying and prioritizing suspicious processes

The first step in an investigation is to review the activity associated with process creation. In the context of process injection techniques, it's commonly observed that process creation plays a crucial role in this process.

The most effective correlation starts by filtering events related to Event ID 4688, which indicates "A new process has been created" in Windows security logs.

```
event.code: "4688" and (not process.executable: "C:\\Windows\\System32\\wbem\\WmiPrvSE.exe" AND not
process.executable: "C:\Windows\\System32\\conhost.exe" AND not process.executable:
"C:\\Windows\\System32\\svchost.exe")
```

Step: 02 : Retrieving the Process ID linked to the suspicious process

Based on the previous step, we identified both ProcessHollowing.exe and notepad.exe as suspicious.

By executing the command below, we can specifically filter events associated with both processes.

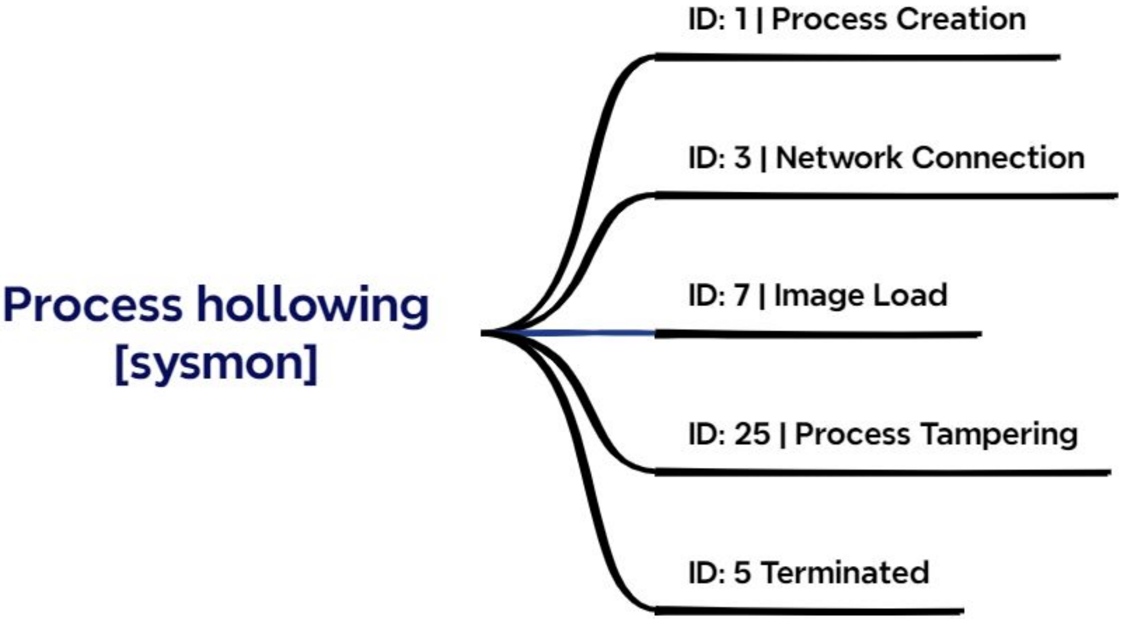
```
event.code: "4688" and (process.executable: "C:\\Users\\Administrator\\Downloads\\ProcessHollowing.exe" OR
process.executable: "C:\Windows\\SysWOW64\\notepad.exe")
```

Step: 03 : Identifying the memory protection permission | Optional

Additionally, to verify the maliciousness, it is recommended to review the privileged PAGE_EXECUTE_READWRITE, as it indicates over-privileged processes. Attackers often exploit this to create or obtain processes with elevated privileges.

```
select * from process_memory_map where pid=<PID>;
```

Step: 04 : Sysmon Correlation



Process hollowing [sysmon]

ID: 1 | Process Creation

ID: 3 | Network Connection

ID: 7 | Image Load

ID: 25 | Process Tampering

ID: 5 Terminated

Step: 05 : Sysmon Correlation

Process Creation

```
event.dataset: "windows.sysmon_operational" and event.code: "1" and (process.executable:
"C:\\Users\\Administrator\\Downloads\\ProcessHollowing.exe" OR process.executable:
"C:\Windows\\SysWOW64\\notepad.exe")
```

Network Connection

```
event.dataset: "windows.sysmon_operational" and event.code: "3"  and (process.executable:
"C:\\Users\\Administrator\\Downloads\\ProcessHollowing.exe" OR process.executable:
"C:\Windows\\SysWOW64\\notepad.exe")
```

Step: 05 : Sysmon Correlation

Image Load

```
event.dataset: "windows.sysmon_operational" and event.code: "7"  and process.executable: process.executable:
"C:\Windows\\SysWOW64\\notepad.exe"
```

Process Tampered

```
event.dataset: "windows.sysmon_operational" and event.code: "25"  and (process.executable:
"C:\\Users\\Administrator\\Downloads\\ProcessHollowing.exe" OR process.executable:
"C:\Windows\\SysWOW64\\notepad.exe")
```

CWL
CyberWarFare Labs

GIVEAWAY ALERT

GET **50%** OFF

Blue Team Fundamentals (BTF) Course

To Win BTF 50% OFF, Participate to this link

https://www.linkedin.com/events/investigatingprocessinjectionth7251616807457837059/

Thank You

**For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings**, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live