ADVERSARY OPERATIONS & PROACTIVE HUNTING

An Offensive Approach Towards Hunting

Dark Vortex LLP

Table of Contents

Day 1

Day 2

- Proactive Endpoint Hunting
  - Sysmon
  - Detecting Initial Foothold with Macros/HTAs
  - Windows API/NT API Monitoring
  - Process Injection Detection
    - Reflective DLL
    - PowerShell CLR Injections
    - C-Sharp CLR Injections
    - Shellcode Injections
- Finding Needle in a Haystack
  - Hunting Command and Control Centers
  - Hunting DNS CnC
  - Hunting HTTP CnC
  - Hunting SMB/TCP Pivoting

Day 3

- Passive Hunting with Deception Technologies
- Gap Detection and Analytics with Adversary Simulation
    - Generating Use-cases for Open-Source Tools
        - Behavioral Detections
        - Credential Dumping Artefacts
        - Domain Discovery Artefacts
        - Domain Privilege Escalation Artefacts
- AMSI Detection and Weaknesses
- Hunting Payload Artefacts in Sysmon Logs
- LAB
    - Detecting Open Source C2 Artefacts
        - Covenant
        - Metasploit
        - Silent Trinity
    - Hunting Ransomware Artefacts

Target Audience

- Blue Teamers
- Threat Hunters
- SOC Analysts

Proactive hunting can be a difficult process to follow. Most organizations are limited to the knowledge of SOC analysts/Blue team even if they have a good security suite in place and the incidents only go off when there is an alert. But what happens if there is no alert. How do you hunt for something you don't know exist?

This training program covers the real-world attacks that help the threat hunters to enhance their detection and hunting knowledge on a lower level. The training's core focus is endpoint hunting for Windows which will include in-depth hunting for Windows API/NT API, Windows Event logs and a lot of Open-Source tools used by real-world threat actors.

Requirements

- Basic understanding of Log Analytics
- Strong will to learn and creative mindset
- Basic understanding of behavioral v/s signatured detections
- Basic programming concepts and Windows OS knowledge

What all do you get in the end

- 3 days of rigorous training program
- Course PDF and content materials

For any queries, contact paranoidninja@0xdarkvortex.dev