Ransomware Attack Simulation and Investigation

for Blue Teamers

2-Day Live Workshop Provided by Blue Cape Security, LLC

Instructor

Markus Schober - Founder, Blue Cape Security

Description

As a cyber security defender and investigator, understanding ransomware attacks is crucial for effective response. In this workshop, participants will learn how attackers operate, set up a C2 infrastructure with the Empire C2 framework, and execute a simulated attack, step-by-step, from initial access all the way throughout post-exploitation phases, each student in their own cloud based lab environment.

Following, we will perform a full investigation of the scenario at hand, covering log and endpoint analysis at scale as well as data collection and digital forensics concepts. For this, the tools we are going to use are Splunk, Velociraptor and several industry-established digital forensic utilities.

Upon completion of the training, participants will have a better understanding of the steps ransomware threat actors take to achieve their objectives, as well as the best practices for detecting and ultimately preventing ransomware attacks.

Copyright © Blue Cape Security LLC. All rights reserved

Requirements

- Stable internet connection and RDP client required to access the lab environment.
- Dedicated, cloud based lab environment will be provided for each student.

Audience

- Security professionals in technical roles. Beginner friendly to intermediate level.
- SOC analysts, IT administrators, System engineers, IT managers, Red Teamers, etc.

Course Agenda

The workshop spans two full days covering ransomware attack techniques and execution of a full scenario on day one and investigation and analysis of the ransomware scenario on day two.

Day 1 - Offense

Anatomy of Ransomware Attacks	- Introduction into current trends and threat landscape in cybersecurity - Examine the lifecycle of ransomware attacks - Understand the access broker model - Recognize common tactics and techniques used in ransomware attacks
Understanding Offense Is Your Best Defense	- Analyze command and control infrastructure in cyber operations - Explore commonly used frameworks for cyber-attacks and the function of beacons
Ransomware TTPs	- Utilize the MITRE ATT&CK framework for identifying attack tactics and techniques - Identify common techniques used in ransomware attacks
Attack Techniques and Fundamentals	- Understand enterprise environments and the role of active directory in cyber attacks - Explore group policy objects - Identify data sources for threat detection and analysis - Utilize logging and enhance visibility, for detection and response
Living Off the Land	- Learn about living off the land binaries (LOLBAS) in cyber attacks - Examine reconnaissance activities and explore commonly used for enumerating environments - Understand how adversaries leverage legitimate tools for malicious activities
Windows Credential Attacks	- Explore Windows authentication architecture and protocols

Copyright © Blue Cape Security LLC. All rights reserved

	- Understand the role of LSA server service in credential management - Analyze NTLM and Kerberos protocols for authentication - Understand sessions, access tokens, privileges - Perform credential dumping with Mimikatz
Lateral Movement Attacks	- Examine Windows Single Sign-On architecture - Understand lateral movement techniques such as Pass-the-Hash and Pass-the-Ticket - Analyze Windows security event logs for lateral movement
Windows Endpoint Attacks	- Identify persistence mechanisms in Windows environments - Learn about process hollowing as an evasion technique - Understand User Account Control (UAC) bypass methods
Empire C2 Framework	- Learn about the Empire C2 Framework - Understand the function of stagers, listeners, agents, and modules in the framework
Ransomware Attack Execution	Execution of ransomware simulation scenario with Empire: • Payload delivery, initial access • Persistence • Privilege escalation • Reconnaissance and discovery • Defense evasion • Credential access • Lateral movement • Data exfiltration • Ransomware staging and deployment
Ransomware and Extortion	- Learn about the aftermath of ransomware attacks - Understand extortion schemes and tactics

Day 2 - Defense

Digital Forensics and Incident Response Introduction	- Understand the incident response process - Learn about detection, triage, analysis, and containment in incident response - Explore data acquisition, live response collection, forensic analysis, and timeline analysis - Learn about different types of reporting in incident response
Scenario Investigation	- Formulate investigative questions to gather relevant information
Splunk Analysis	- Familiarize yourself with Splunk and event logs

Copyright © Blue Cape Security LLC. All rights reserved

	- Learn how identify malicious files and events such as command and control traffic, process executions, PowerShell payloads, scheduled tasks and more.
Velociraptor IR Tool Deployment	- Deploy Velociraptor server and clients for digital forensics and threat hunting
Velociraptor Analysis	- Utilize Velociraptor for rapid analysis of suspicious files, persistence mechanisms, lateral movement, and suspicious processes - Learn how to quarantine hosts using Velociraptor for effective incident response
Live Response Data Collection	- Use Kroll Artifact Parser Extractor (KAPE) for live response data collection - Implement Velociraptor for remote data collection during incident response
Forensic Analysis	- Conduct registry analysis during forensic investigations - Gather host and user information to understand system activity - Analyze application executions, scheduled tasks, and obfuscated payloads for potential threats
Rapid Event Log Analysis	- Utilize Hayabusa for quick analysis of logon events - Detect and analyze malicious PowerShell payloads in event logs
Timeline Creation and Analysis	- Construct a forensic timeline using Hayabusa and Sigma rules - Analyze suspicious detections and events within the timeline

Copyright © Blue Cape Security LLC. All rights reserved