Blue Team Level 1 Certification (Standard)

○ PA7) Report Writing
● 7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge
● 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
● 7 Topics

○ TI2) Threat Actors & APTs
● 6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
● 7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
● 7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
● 5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
● 6 Topics | 1 Quiz

○ Section Introduction, Global Campaigns

○ Types of Malware Used by Threat Actors

○ Global Campaign: Trickbot

○ Global Campaign: Sodinokibi

○ Global Campaign: Magecart

○ Global Campaign: Emotet

Activity) End of Section Review, Global Campaigns

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
● 5 Topics

○ DF2) Forensics Fundamentals
● 10 Topics | 5 Quizzes

Section Introduction, Global Campaigns

Blue Team Level 1 Certification (Standard) > TI6) Malware and Global Campaigns > Section Intr... IN PROGRESS

This section is designed to provide a deeper dive into the malware used by malicious actors, and cover some of the most prolific malware campaigns that operate today on a global scale, as well as the actors behind them. We will cover Emotet, Sodinokibi Ransomware, Trickbot, and MageCart.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand what malware and tools are commonly used by malicious actors.
- Understand the details behind four global malware campaigns, the motivations behind the activity, and technical details regarding the malware.

< Previous Lesson

Mark Complete ✓

Next Topic >

Back to Lesson

Privacy & Cookies Policy

Privacy - Terms