Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Static Malware Analysis

DFIR-12-L1
Malware Investigation

Lab Objective

Understand how analysis reports can help reveal how malware works.

Lab Mission

Learn how malware analysis is based, among other things, on written descriptions of suspicious files, and determine if the descriptions are enough to verify that such files can compromise a system.

Lab Duration

15–20 minutes

Requirements

- Basic working knowledge of Google search

Resources

- Environment & Tools
  - Browser
- Extra Lab Files
  - ***w32_stuxnet_dossier.pdf***
  - ***Investigation-WannaCry-cyber-attack-and-the-NHS.pdf***

Textbook References

- Chapter 12: Threat Hunting
  - Section 2: Malware Investigation

Lab Task: Locate and Study Malware Reports

In this task, you will locate malware investigation reports and study them.

1. Read the ***w32_stuxnet_dossier*** PDF file and answer the following questions to understand how the malware impacted the infected devices.
    a. What systems were impacted by Stuxnet?
    b. What types of systems were affected by the malware?
    c. What type of malware is Stuxnet?
    d. What country was targeted?
    e. What operating systems did Stuxnet run on?
2. Read the ***Investigation-WannaCry-cyber-attack-and-the-NHS*** PDF file and explain how the malware impacted the OS.
    a. What country was mostly affected by WannaCry?
    b. What type of Malware was WannaCry considered?
    c. How many devices were affected by WannaCry?