Malware Analysis - Egg-xecutable

Day 6

Malware Analysis - Egg-xecutable

Discover some common tooling for malware analysis within a sandbox environment.

- Malware Analysis Using Sandboxes

Malware Analysis Using Sandboxes

Overview

Room URL: https://tryhackme.com/room/malware-sandbox-aoc2025-SD1zn4fZQt

Difficulty: Medium

Category: Malware

Date Completed: 12/6/2025

Objectives

- The principles of malware analysis
- An introduction to sandboxes
- Static vs. dynamic analysis
- Tools of the trade: PeStudio, ProcMon, Regshot

Table of Contents

Introduction

Walk Through

Lessons Learned

Resources

Introduction

You discover a suspicious executable file, `HopHelper.exe`, lurking on an analyst's desktop—a potential threat that demands investigation. Rather than blindly executing it and risking system compromise, you must apply systematic malware analysis techniques to understand its true nature, capabilities, and malicious intent. By combining **static analysis** (examining the file without

execution) and **dynamic analysis** (observing its behavior in a sandboxed environment), you'll uncover exactly how this malware operates, what persistence mechanisms it employs, and how it communicates with attackers—transforming fear into knowledge and defensive strategy.

Key Concepts

- **Static Analysis**: Inspecting files for checksums, strings, imports, and resources without execution
- **Dynamic Analysis**: Observing malware behavior through registry monitoring (Regshot) and process analysis (ProcMon)
- **Golden Rule**: Never execute potentially malicious code on systems you care about—always use isolated sandboxes

---

Walk Through

1. **Static analysis:** What is the SHA256Sum of the HopHelper.exe?
    1. Launch the Windows enviroment
    2. Open `PEStudio`
    3. `CTRL + O` to open file
    4. Open `hophelper.exe`
    5. `F29C270068F865EF4A747E2683BFA07667BF64E768B38FBB9A2750A3D879CA33`
        - Malware1.png
2. **Static analysis:** Within the strings of HopHelper.exe, a flag with the format THM{XXXXX} exists. What is that flag value?
    1. In PE studio click strings on the left
    2. Scroll through the strings on the right
        - Malware2.png
3. What registry value has the HopHelper.exe modified for persistence?
    1. Launch `regshot`
    2. Changed output to `Desktop`
    3. Click shot 1
    4. After finsihed open the potential malware file
    5. Then click shot 2
    6. After finished click compare

- Malware3.png

4. **Dynamic analysis:** Filter the output of ProcMon for "TCP" operations. What network protocol is HopHelper.exe using to communicate?
    1. Open `ProcMon`
    2. Open `HopperHelper.exe`
    3. Wait for all processes to load
    4. Click the capture button
    5. `CTRL + L` for filter
    6. `Process Name` `is` `HopHelper.exe`
    7. `Operation` `contains` `tcp`
    8. `http`
        - Malware4.png

Lessons Learned

- Static analysis provides foundational threat intelligence without risking system compromise—checksums enable file tracking across networks, while string extraction reveals command infrastructure and attack vectors that inform defensive blocking strategies.
- Dynamic analysis in sandboxed environments reveals malware's true operational behavior—registry modification patterns expose persistence mechanisms, and process monitoring uncovers network communications, allowing defenders to implement targeted blocking rules, registry hardening, and behavioral detection signatures.

Resources

TryHackMe

Malware Analysis Tools