TryHackMe Advent of Cyber 2025

Day 6 Challenge Report

Malware Analysis Fundamentals

1. Executive Summary

This report documents the completion of Day 6 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on malware analysis fundamentals, examining the HopHelper.exe sample using both static and dynamic analysis techniques. Through tools including PeStudio, Regshot, and Process Monitor, successfully identified persistence mechanisms, network communications, and command-and-control infrastructure.

2. Challenge Overview

Objective: Analyze a suspicious executable (HopHelper.exe) using static and dynamic analysis methodologies to understand its functionality, persistence mechanisms, and network behavior.

Tools Used: PeStudio, Regshot, Process Monitor (ProcMon)

3. Malware Analysis Principles

Malware analysis examines malicious files to understand functionality, operation, and defense methods. By analyzing samples, we determine how malware operates and develop prevention strategies.

Key Benefits:

- Identify attacker infrastructure (C2 servers) for blocking
- Discover artifacts for compromise detection
- Translate technical findings into defensive measures
- Understand attacker tactics, techniques, and procedures

3.1 Sandboxes

Sandboxes are isolated environments for executing potentially dangerous code safely, functioning as disposable digital playgrounds that protect sensitive data and systems.

Virtual Machine Benefits:

- Complete system control
- Snapshotting for state restoration
- Network isolation capabilities
- Safe execution of malicious samples

3.2 Analysis Types

Static Analysis:
Examining files without execution. Includes reviewing checksums, strings, imports, and resources.

Dynamic Analysis:
Executing samples to observe behavior, system interactions, and network activity.

4. Static Analysis with PeStudio

PeStudio enables static analysis of Windows executables without execution, revealing critical information about malware characteristics.

Component	Description & Analysis Value
Checksums	Unique identifiers (SHA256) for tracking files. Searchable for prior identification.
Strings	Readable character sequences revealing IPs, URLs, commands, or passwords.
Imports	Libraries and functions the application depends on (e.g., CreateFileW).
Resources	Icons and embedded data. Malware may disguise itself or hide within resources.

4.1 HopHelper.exe Analysis

SHA256 Checksum:

`F29C270068F865EF4A747E2683BFA07667BF64E768B38FBB9A2750A3D879CA33`

This SHA256 hash serves as threat intelligence, enabling tracking across systems and correlation with known malware databases.

Strings Analysis:
Examined strings within HopHelper.exe to identify embedded commands, URLs, and configuration data.

Flag Discovered: THM{STRINGS_FOUND}

5. Dynamic Analysis - Registry Monitoring

5.1 Regshot Methodology

Regshot captures registry snapshots before and after malware execution, identifying persistence mechanisms through comparison.

Analysis Process:

1. Configured output path to Desktop
2. Created first snapshot (1st Shot → Shot)
3. Executed HopHelper.exe
4. Created second snapshot (2nd Shot → Shot)
5. Generated comparison report (Compare button)

6. Searched report using Ctrl+F for 'hophelper'

Persistence Mechanism Identified:

HopHelper.exe established persistence by modifying the Windows Run registry key, ensuring execution on system startup.

Modified Registry Key: HKU\S-1-5-21-1966530601-3185510712-10604624-1008\Software\Microsoft\Windows\CurrentVersion\Run\HopHelper

6. Dynamic Analysis - Process Monitoring

6.1 Process Monitor (ProcMon)

Process Monitor from Sysinternals monitors process interactions with Windows, revealing registry operations, file access, and network connections.

Monitoring Procedure:

7. Launched Process Monitor
8. Started event capture
9. Executed HopHelper.exe
10. Allowed one minute for full execution
11. Stopped capture (Play button)

Applied Filters:

Filter 1 - Process Name:

- Process Name → is → HopHelper.exe

Isolated events specific to HopHelper.exe, removing noise from other processes.

Filter 2 - TCP Operations:

- Operation → contains → TCP

Revealed network communication attempts.

Key Operations Monitored:

- RegOpenKey - Registry access
- CreateFile - File system operations
- TCP Connect - Network connections
- TCP Receive - Incoming network data

Network Protocol Identified:

Expanded TCP Connect path entries to reveal protocol details.

Protocol: HTTP

6.2 Command & Control Infrastructure

Extracted IP address and protocol from Process Monitor TCP operations to identify C2 server.

Discovery Method:

1. Copied IP address from TCP Connect operation
2. Combined with identified HTTP protocol
3. Constructed full URL and accessed via browser

C2 Web Panel: http://breachblocker-sandbox

7. Key Skills Developed

- Static analysis with PeStudio
- Dynamic analysis with Regshot and Process Monitor
- Registry persistence mechanism identification
- Network traffic analysis and C2 detection
- Checksum generation for threat intelligence
- String extraction and analysis
- Safe sandbox environment usage

8. Conclusion

Day 6 of the TryHackMe Advent of Cyber 2025 provided comprehensive malware analysis training. Through combined static and dynamic analysis of HopHelper.exe, successfully identified persistence mechanisms, network communications, and command-and-control infrastructure.

The challenge demonstrated how proper malware analysis translates technical findings into actionable defenses, enabling organizations to block attacker infrastructure, detect compromised systems, and understand adversary tactics.

Challenge Status: **COMPLETED ✓**