TryHackMe Advent of Cyber 2025 Day 16 Challenge Report

Windows Registry Forensics Investigation

1. Executive Summary

This report documents the completion of Day 16 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on Windows Registry forensics investigation of the compromised dispatch-srv01 system. Successfully analyzed Registry Hives using Registry Explorer, investigated malicious software installation, identified persistence mechanisms, and reconstructed the attack timeline starting October 21, 2025.

2. Windows Registry Fundamentals

2.1 What is the Windows Registry?

The Windows Registry is the operating system's 'brain' - a centralized database storing all configuration settings Windows needs to function. Unlike a human brain in one location, the Registry is stored across multiple separate files called Hives, each containing different configuration data.

2.2 Registry Hives

Registry Hives are individual files containing binary data organized by configuration type:

Hive Name	Configuration Type	Location
SYSTEM	System settings, drivers, services	C:\Windows\System32\config
SOFTWARE	Installed applications, settings	C:\Windows\System32\config
SECURITY	Security policies, permissions	C:\Windows\System32\config
SAM	User accounts, passwords	C:\Windows\System32\config
NTUSER.DAT	User-specific settings	C:\Users\[Username]
USRCLASS.DAT	User shell settings	C:\Users\[Username]\AppData\Local\Microsoft\Windows

Important: Registry Hives contain binary data and cannot be opened directly by double-clicking.

2.3 Registry Root Keys

Windows organizes Registry Hives into structured Root Keys viewable through Registry Editor:

- **HKEY_LOCAL_MACHINE (HKLM):** Contains SYSTEM, SOFTWARE, SECURITY, SAM
- **HKEY_CURRENT_USER (HKCU):** Contains NTUSER.DAT
- **HKEY_USERS (HKU):** Contains NTUSER.DAT, USRCLASS.DAT
- **HKEY_CLASSES_ROOT (HKCR) & HKEY_CURRENT_CONFIG (HKCC):** Dynamically populated, no separate hive files

3. Registry Forensics

3.1 Forensic Importance

Registry forensics extracts and analyzes evidence from the Registry. Investigators analyze:

- Registry data
- Event logs
- File system data
- Memory data

3.2 Key Forensic Registry Locations

- **USB Devices:** HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
- **Recently Run Programs:** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- **Installed Software:** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- **Startup Programs:** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- **Recent Files:** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

3.3 Registry Explorer Tool

Built-in Registry Editor cannot:

- Open offline hives (collected from other systems)
- Parse binary data into readable format

Registry Explorer Solution: Open-source forensic tool that parses binary data, allows offline analysis, prevents modification

4. Investigation Procedure

4.1 Step 1: Launch Registry Explorer

Clicked Registry Explorer icon on taskbar to launch forensic tool

4.2 Step 2: Load Registry Hives

1. File → Load hive
2. Navigate to C:\Users\Administrator\Desktop\Registry Hives
3. Select hive file (SYSTEM, SOFTWARE, NTUSER.DAT)

4.3 Step 3: Handle Dirty Hives

Critical Technique: Hold SHIFT while clicking Open to load transaction log files

Purpose: Ensures clean hive state with complete transactions from live systems

Received confirmation message: "Successfully replayed transaction logs"

4.4 Step 4: Navigate Registry Keys

Navigation Methods:

4. Manual: Browse folder structure
5. Search: Type key name in search bar
6. Bookmarks: Use Available Bookmarks tab

5. Forensic Investigation Results

Timeline: Abnormal activity started October 21, 2025

5.1 Question 1: Installed Application

Question: What application was installed on dispatch-srv01 before abnormal activity started?

Investigation Path:

7. Loaded SOFTWARE hive
8. Navigated to: ROOT\Microsoft\Windows\CurrentVersion\Uninstall
9. Filtered installations by date (before October 21, 2025)
10. Identified suspicious application

Answer: DroneManager Updater

5.2 Question 2: Application Launch Path

Question: What is the full path where the user launched the application from?

Investigation Path:

11. Loaded NTUSER.DAT hive
12. Navigated to: ROOT\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store
13. Searched for DroneManager-related entries
14. Located full execution path

Answer: C:\Users\dispatch.admin\Downloads\DroneManager_Setup.exe

5.3 Question 3: Persistence Mechanism

Question: Which value was added by the application to maintain persistence on startup?

Investigation Path:

15. Returned to SOFTWARE hive
16. Navigated to: ROOT\Microsoft\Windows\CurrentVersion\Run
17. Identified DroneManager-related startup entry
18. Located persistence value with background execution flag

Answer: "C:\Program Files\DroneManager\dronehelper.exe" –background

6. Attack Chain Analysis

6.1 Initial Compromise

19. User dispatch.admin downloaded DroneManager_Setup.exe to Downloads folder
20. Setup disguised as legitimate drone management updater
21. Installation occurred before October 21, 2025

6.2 Persistence Establishment

22. Installed to C:\Program Files\DroneManager\
23. Created dronehelper.exe component
24. Added Run key for automatic startup
25. Used --background flag for stealth execution

6.3 Post-Installation

26. Abnormal activity began October 21, 2025
27. Malware executed on every system startup
28. Maintained persistent access to dispatch-srv01

7. Key Skills Developed

- Windows Registry architecture understanding
- Registry Hives identification and location
- Registry Root Keys mapping
- Registry Explorer forensic tool usage
- Dirty hive handling with transaction logs
- Forensic artifact location knowledge
- Persistence mechanism identification
- Timeline reconstruction from registry data

8. Conclusion

Day 16 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in Windows Registry forensics. Successfully investigated the compromised dispatch-srv01 system using Registry Explorer to analyze offline hives, identify malicious software installation, track execution paths, and uncover persistence mechanisms.

The investigation revealed DroneManager Updater malware installed via social engineering (disguised as legitimate software), establishing persistence through Run key registry modification for automatic startup execution. Registry forensics proved essential for reconstructing attack timelines and identifying compromise indicators that traditional log analysis might miss. Understanding Registry structure and forensic techniques is fundamental for Windows incident response.

Challenge Status: **COMPLETED ✓**