HACKTHEBOX

Security Incident Report

HTB Trojan Sherlock - 2025-12-9-25

HTB Certified Defensive Security Analyst (HTB CDSA) Exam Report

Candidate Name: Samuel Tanner

December 9, 2025

Version: 1.0

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Contacts		
Primary Contact	**Title**	**Contact Email**
Samuel Tanner	Systems Engineer	stanner834@proton.me

3 Exam Objectives (Read Carefully)

To be awarded the HTB Certified Defensive Security Analyst (CDSA) certification, you must:

- Obtain a minimum of 80 points while investigating **Incident 1** by submitting 16 out of the 20 flags listed below **AND**
- Compose and submit a commercial-grade security incident report **for both incidents** that encompasses an **Executive Summary** and **Technical Analysis** sections **for each incident**, adhering strictly to the format and content outlined in the **Security Incident Reporting** module.
  - While the Impact Analysis and the Response and Recovery Analysis, including diagrams, can be excluded, the Technical Analysis for both incidents must be exceptionally thorough.
  - Each stage of the cyber kill chain needs to be addressed, and any activities related to process injection should be scrutinized thoroughly, considering aspects like the origin, destination, and whether a process was sacrificial.
  - Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

4 Executive Summary

sampleco engaged Samuel Tanner to investigate two (2) independent security incidents across two of sampleco' separate networks. The objective is to identify the root causes and the full extent of these incidents and to meticulously document the findings in an understandable, technically robust, and reproducible way.

Data Recovery Trojan - Malicious Software Masquerading as Recovery Tool

Incident ID: INC-2023-05-30-001

Incident Severity: High

Incident Status: **contained**

Incident Overview:

Windows 10 workstation (DESKTOP-38NVPD0) compromised through user execution of malicious software masquerading as legitimate data recovery tool. Malware downloaded from compromised website, established C2 communications, and downloaded secondary payload. Investigation conducted using memory forensics (Volatility 3), disk forensics (FTK Imager), and prefetch analysis (PECmd.exe).

Key Findings:

- User 'John' downloaded and executed Recovery_Setup.exe from suspicious domain
- Malware masqueraded as FinalRecovery v3.0.7.0325 (legitimate data recovery software)
- Confirmed C2 communications with praetorial-gears.000webhostapp.com
- Secondary payload (puk.php) downloaded from C2 infrastructure
- SHA-256 hash: c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193
- Process executed twice (PID 484) with suspicious TMP file creation
- FLSCover directory created with readme.txt (potential ransomware/info stealer indicator)
- No evidence of lateral movement or additional compromised systems

Immediate Actions:

1. Isolated DESKTOP-38NVPD0 from network to prevent lateral movement
2. Captured memory dump (memory.vmem) for forensic analysis
3. Created disk image using FTK Imager for evidence preservation
4. Extracted and analyzed prefetch files for execution timeline
5. Validated malware hash against VirusTotal (confirmed malicious)
6. Blocked IOC domains at firewall/proxy level
7. Disabled user account 'John' pending investigation completion
8. Initiated threat hunt across environment for additional compromises

Stakeholder Impact:

MEDIUM Impact - Single workstation compromised with potential data theft. User 'John' unable to access workstation during investigation and remediation. Potential exposure of data stored on local system including credentials, PII, and business documents. System requires full rebuild resulting in 1-2

days productivity loss. No evidence of data exfiltration confirmed yet (requires network traffic analysis). No impact to business operations or customer-facing systems detected.

5 Technical Analysis

Data Recovery Trojan - Malicious Software Masquerading as Recovery Tool

Affected Systems & Data

Compromised System:

- Hostname: DESKTOP-38NVPD0
- OS: Windows 10 Build 19041
- User Account: John
- IP Address: [Requires network log review]
- Status: ISOLATED - Full rebuild required

Targeted Directories:

- C:\Users\John\Downloads\Data_Recovery\ (malware staging)
- C:\Users\John\Downloads\Data_Recovery\FLSCover\ (created by malware)
- %TEMP% directory (IS-NJBAT.TMP, IS-R7RFP.TMP)

Affected User Account:

- Username: John
- Account Type: Standard user (no admin privileges observed)
- Status: DISABLED pending credential reset

Scope Verification:

- No additional compromised systems detected
- No lateral movement indicators found
- No suspicious authentication events from John's account

Evidence Sources & Analysis

Memory Forensics (Volatility 3):

```
vol3 -f memory.vmem windows.info
# 19041 OS Build

vol -f memory.vmem windows.envars | findstr /i "computername"
#DESKTOP-38NVPD0 desktop hostname

$env:PYTHONIOENCODING = 'utf-8'
vol -f memory.vmem filescan | findstr /i ".zip"
# Data_Recovery.zip

vol -f "C:\HTB\memory capture\memory.vmem" -o "C:\HTB\memory capture\dump_output"
windows.dumpfiles
findstr /s /i "Data_Recovery.zip" *.*
#praetorial-gears.000webhostapp.com is where the malicious Data_Recovery file was downloaded
```

```
vol3 -f memory.vmem windows.pstree
# PID 484: Recovery_Setup.exe (Parent PID: 60)
```

Disk Forensics (FTK Imager):

- Extracted Recovery_Setup.exe from disk image
- File path: C:\Users\John\Downloads\Data_Recovery\Recovery_Setup.exe
- Preserved file metadata and timestamps

Prefetch Analysis (PECmd.exe):

```
PECmd.exe -f RECOVERY_SETUP.EXE-A808CDAB.pf
```

Results:

- First execution: 2023-05-30 02:06:29 UTC
- Execution count: 2
- Referenced TMP files: IS-NJBAT.TMP, IS-R7RFP.TMP
- Referenced directories: FLSCover\

Browser Cache Analysis:

- Download URL recovered from SharedCacheMap log
- Source: http://praetorial-gears.000webhostapp.com/wp-content/uploads/2023/05/Data_Recovery.zip

VirusTotal Analysis:

- Hash: c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193
- Detection: Multiple AV vendors flagged as malicious
- Relations tab: Multiple malicious URLs associated with sample

File System Artifacts:

- Data_Recovery.zip (downloaded archive)
- Recovery_Setup.exe (primary malware)
- IS-NJBAT.TMP, IS-R7RFP.TMP (installer artifacts)
- FLSCover\readme.txt (malware-created file)
- puk.php (downloaded secondary payload)

Indicators of Compromise (IoCs)

File Hashes (SHA-256):

- c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193 (Recovery_Setup.exe)

Network Indicators:

- Domain: praetorial-gears.000webhostapp.com
- URL: http://praetorial-gears.000webhostapp.com/wp-content/uploads/2023/05/Data_Recovery.zip
- Downloaded payload: puk.php
- Protocol: HTTP (unencrypted C2 communications)

File System Indicators:

- C:\Users*\Downloads\Data_Recovery\Recovery_Setup.exe
- C:\Users*\Downloads\Data_Recovery.zip
- IS-NJBAT.TMP (installer artifact pattern)
- IS-R7RFP.TMP (installer artifact pattern)
- FLSCover\ directory creation
- FLSCover\readme.txt

Process Indicators:

- Process Name: Recovery_Setup.exe
- PID: 484
- Parent PID: 60
- Claimed Identity: FinalRecovery v3.0.7.0325
- Execution from Downloads folder

Behavioral Indicators:

- Multiple TMP file creation with IS-*.TMP pattern
- Outbound HTTP connections to 000webhostapp.com domain
- Secondary payload download (puk.php)
- Creation of non-standard directory (FLSCover)
- Execution of unsigned executable from Downloads folder

YARA Rule for Detection:

```
rule Data_Recovery_Malware {
    meta:
        description = "Detects Recovery_Setup.exe malware"
        hash = "c34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193"
        severity = "high"
    strings:
        $s1 = "FinalRecovery" ascii
        $s2 = "IS-NJBAT.TMP" ascii
        $s3 = "FLSCover" ascii
        $tmp = /IS-[A-Z0-9]{5,}\.TMP/ ascii
    condition:
        uint16(0) == 0x5A4D and
        (2 of ($s*) or $tmp)
}
```

Root Cause Analysis

Primary Vulnerability:

- User education gap: User downloaded and executed unsigned executable from untrusted source
- Lack of application whitelisting/control allowing arbitrary executable execution
- No web filtering blocking known malicious file hosting services (000webhostapp.com)
- Insufficient endpoint protection: AV/EDR did not prevent execution

Contributing Factors:

1. **Social Engineering Success:**
   - Malware masqueraded as legitimate FinalRecovery software
   - Used data recovery theme to appear benign and necessary
   - Hosted on semi-legitimate looking domain name
2. **Technical Control Gaps:**
   - No execution restrictions on Downloads folder
   - No browser warnings for suspicious downloads
   - No DNS filtering blocking free hosting services
   - Endpoint protection signature-based only (behavioral detection not enabled)
3. **Administrative Controls:**
   - No policy restricting software installation
   - Insufficient user security awareness training
   - No mandatory security review before software installation
4. **Detection Gaps:**
   - No real-time monitoring of process execution from Downloads folder
   - No SIEM alerting on unsigned executable execution
   - No network monitoring for suspicious download activity
   - User report was primary detection method (not automated)

Attack Success Factors:

- Unsophisticated attack exploited basic security gaps
- Relied entirely on user execution (no exploitation required)
- Used HTTP for C2 (should have been easily detected)
- Success indicates multiple layers of defense were bypassed or absent

Technical Timeline

Initial Compromise Phase:

- 2023-05-30 01:25:08 GMT - Data_Recovery.zip created on attacker server (file timestamp)
- 2023-05-30 [Time Unknown] - User 'John' visited malicious website and downloaded Data_Recovery.zip
- URL: http://praetorial-gears.000webhostapp.com/wp-content/uploads/2023/05/Data_Recovery.zip
- Download Location: C:\Users\John\Downloads\Data_Recovery.zip
- Evidence: Browser SharedCacheMap log

Extraction and Preparation:

- 2023-05-30 [Time Unknown] - User extracted Data_Recovery.zip
- Extraction location: C:\Users\John\Downloads\Data_Recovery\
- Contents: Recovery_Setup.exe (primary malware executable)

First Execution:

- 2023-05-30 02:06:29 UTC - First execution of Recovery_Setup.exe
- Process ID: 484
- Parent Process: PID 60

- Evidence: Prefetch file RECOVERY_SETUP.EXE-A808CDAB.pf
- Execution method: User double-click (manual execution)

Malware Operational Phase:

- 2023-05-30 02:06:29 - 02:07:59 UTC - Malware active execution
- Created installer temporary files:
  - IS-NJBAT.TMP
  - IS-R7RFP.TMP
- Created malicious directory: FLSCover\
- Dropped file: FLSCover\readme.txt
- Masqueraded as: FinalRecovery v3.0.7.0325

Command & Control Communication:

- 2023-05-30 02:07:59 UTC - Process active in memory (windows.pstree evidence)
- Established C2 connection to praetorial-gears.000webhostapp.com
- Downloaded secondary payload: puk.php
- Protocol: HTTP (unencrypted)
- Multiple malicious URLs accessed (VirusTotal relations)

Second Execution:

- 2023-05-30 [Time Unknown] - Second execution of Recovery_Setup.exe
- Evidence: Prefetch execution count = 2
- Purpose: Unknown (may be user retry or automated re-execution)

Memory Capture:

- 2023-05-30 02:09:03 UTC - Memory snapshot captured
- Source: windows.info SystemTime
- Format: VMware memory dump (memory.vmem)
- Process still active in memory at time of capture

Detection and Response:

- 2023-05-30 [Post-Incident] - Suspicious activity reported
- System isolated from network
- Forensic investigation initiated
- Memory and disk images acquired
- IOC extraction and analysis completed

Active Investigation Timeline:

- Volatility 3 analysis completed
- FTK Imager disk forensics completed
- PECmd.exe prefetch analysis completed
- VirusTotal hash validation completed
- Threat hunting initiated (ongoing)

Total Dwell Time:

- Minimum: 3 minutes 34 seconds (02:06:29 to 02:09:03 UTC)
- Maximum: Unknown (detection time not specified)
- Time to Detection: Not automated, user-reported

- Time to Containment: Unknown (isolation time not recorded)

Nature of the Attack

Attack Classification: Trojan Downloader / Information Stealer / Potential Ransomware

MITRE ATT&CK Mapping:

Initial Access (TA0001):

- T1566.002 - Phishing: Spearphishing Link
  - User directed to malicious download via compromised/malicious website
  - Social engineering leveraging fake data recovery software
  - Hosted on free web hosting service (000webhostapp.com)

Execution (TA0002):

- T1204.002 - User Execution: Malicious File
  - User manually executed Recovery_Setup.exe
  - No exploitation required, relied on user interaction
  - Double execution recorded in prefetch (user may have run twice)
- T1129 - Shared Modules
  - Installer framework detected (IS-*.TMP files suggest Inno Setup)
  - Leveraged legitimate installer technology for malicious purposes

Defense Evasion (TA0005):

- T1036.005 - Masquerading: Match Legitimate Name or Location
  - Masqueraded as FinalRecovery v3.0.7.0325 (legitimate data recovery tool)
  - Used data recovery theme to appear benign and necessary
  - Executed from common legitimate location (Downloads folder)
- T1027 - Obfuscated Files or Information
  - ZIP archive used to evade email/web gateway inspection
  - Secondary payload disguised as PHP file (puk.php)
  - May contain packed/encrypted code (requires further analysis)

Command and Control (TA0011):

- T1071.001 - Application Layer Protocol: Web Protocols
  - HTTP communications to C2 infrastructure
  - Domain: praetorial-gears.000webhostapp.com
  - Unencrypted traffic (easier detection but attacker didn't use HTTPS)
- T1105 - Ingress Tool Transfer
  - Downloaded secondary payload: puk.php
  - Multi-stage malware deployment
  - Additional tools likely downloaded (requires network log analysis)

Discovery (TA0007):

- T1082 - System Information Discovery (Suspected)
  - Standard malware behavior to profile victim system
  - Required for tailored payload delivery
  - Evidence: Multiple executions suggest environment assessment

Collection (TA0009):

- T1005 - Data from Local System (Suspected)
  - FLSCover directory creation suggests data staging
  - readme.txt may contain instructions or ransom note
  - Potential information stealer based on behavioral indicators

Exfiltration (TA0010):

- T1041 - Exfiltration Over C2 Channel (Potential)
  - C2 communications confirmed
  - Data exfiltration not confirmed (requires network traffic analysis)
  - HTTP protocol would facilitate data upload

Attack Characteristics:

- Sophistication Level: LOW to MEDIUM
- Social engineering effective but technical execution basic
- Used unencrypted HTTP (poor OPSEC)
- Multiple TTP indicators easily detectable
- Likely automated/commodity malware (not targeted APT)

Threat Actor Assessment:

- Likely opportunistic cybercriminal
- Mass distribution campaign targeting general users
- Financial motivation (data theft or ransomware)
- Low sophistication indicates script kiddie or crimeware-as-a-service
- No indicators of nation-state or advanced persistent threat

Malware Behavior Summary:

1. Initial dropper/installer stage (Recovery_Setup.exe)
2. Creates persistence mechanisms (not yet identified)
3. Establishes C2 communications
4. Downloads additional payloads (puk.php)
5. Creates data collection infrastructure (FLSCover directory)
6. Potential ransomware or data exfiltration final stage

Indicators of Ransomware Potential:

- readme.txt file (common ransom note file)
- FLSCover directory (could be 'Files Cover' or data staging)
- Masquerading as recovery software (ironic if ransomware)

Indicators of Information Stealer:

- C2 communications for data exfiltration

- Directory creation for data staging
- Multiple execution attempts
- Secondary payload download

A Appendix

A.1 Technical Timeline

Time	Activity
12:00	Volatility Memory Forensics
13:00	FTK Imager Disk Forensics
13:30	Virus Total Analysis
13:55	PEcmd.exe Prefetch File Analysis
14:30	Dynamic Analysis and Log Review of Malware

End of Report

This report was rendered
by SysReptor with
♥