

Final: Forensic Report

Examination of William L. Howard's Laptop

December 7th, 2025

Investigator: Ryan Ethier

Examination of Evidence Item

2025FALL340-440.E01:

Investigation Request

A request of investigation was issued to conduct a digital forensic examination of the computer identified to belong to William L. Howard (CEO of Kidco). The request for examination was initiated by Dewey, Cheatum, and Howe, LLP on April 18, 2024. Prior to the request for examination, it is believed that William L. Howard became concerned about company information being stolen off of their computer around November 19, 2021. The concern came from an email that William L. Howard received with an attachment that failed to open. The email was allegedly received prior to November 19, 2021, although exact dates were not provided.

The formal investigation request entailed the following:

- When did the unknown individual get access to Mr. Howard's laptop?
- How did the unknown individual get access to Mr. Howard's laptop?
- Is there evidence the unknown individual placed malware on Mr. Howard's laptop?
- Was any information potentially stolen off of Mr. Howard's laptop?
- Is there any possible indication that Mr. Howard was in on the scheme?
- Is there any evidence that the unknown individual accessed any other systems on the network?

Executive Summary

On November 17th, 2021, at 11:42:47, William L. Howard received an email from csmithjmy@protonmail.com (CJ Smith) with the subject line titled "*Important Document*". The email contained an attachment that was found to be malicious. Mr. Howard opened the attachment which then installed malware onto their laptop. The malware was able to run commands on the system and maintained activity for nearly two weeks.

Further analysis of system logs and browser artifacts revealed the malware accessed internal company resources. On November 29th, 2021, the infected system attempted to open files within Kidco's internal file server. This occurred during the same time frame that the malware was re-executed. This indicates that these actions were potentially automated and not initiated by Mr. Howard.

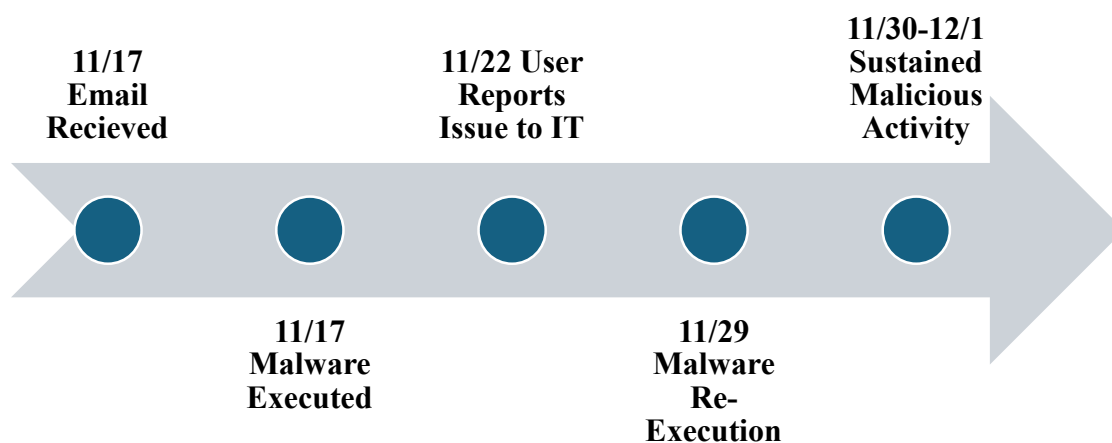
Additionally, identification of advanced malicious scripts loaded into memory were found. These scripts are associated with tools for expanding access, moving deeper into a network, and gaining control of other systems. The presence of these tools show the attacker was prepping for a larger compromise beyond Mr. Howard's laptop.

Although no direct record of files being transferred outside Kidco was found. The attacker clearly explored internal resources and possessed the capability to steal data. Considering the sophistication of the tools involved, data exposure cannot be fully ruled out.

Importantly, nothing in the evidence suggests that Mr. Howard participated or was aware of the attacker's actions. Mr. Howard's email to Kidco IT on November 22 regarding unusual behavior on his laptop supports this claim.

In conclusion, Mr. Howard's laptop was compromised through a malicious email attachment. The attacker used that access to explore company resources on the internal network and deployed advanced tools aiming to expand their control. While there is no clear evidence of data exfiltration, the advanced nature of the attack suggests sensitive information may have been staged for theft.

Timeline of Events



November 17, 2021 – Initial Compromise

11:42 – Mr. Howard receives a malicious email titled “Important Document” from csmithjmy@protonmail.com

~12:18 – The attached Report.js and Report.exe are executed, installing malware. Prefetch and logs confirm initial execution.

12:23 – Mr. Howard replies to the sender stating he cannot open the attachment, unaware it was malicious.

November 17 – 22, 2021 – Early Malware Activity

- Malware launches hidden PowerShell commands and repeatedly attempts outbound communication to 13.90.131.107 (443)
- No user interaction associated with this traffic.
- No successful lateral movement detected during this period

November 22, 2021 – User Notices Issues

22:18 – Mr. Howard emails IT reporting a “...black window with red letters...”, consistent with visible malware execution.

November 28-29, 2021 – Renewed Execution, Privilege Escalation Attempts, Internal Probing

- New Prefetch artifacts show the malware re-executed through Powershell.
- PowerShell Operational Logs show advanced attack tools, including:
 - o Invoke-SMBExec
 - o MD4 hash generation code
 - o Service-based command execution logic
 - o Privilege escalation via fodhelper registry hijack (UAC bypass)
- Browser/WebCache artifacts show attempts to access internal Kidco file share, such as:
 - o <file:///kidco-dc1/IT/website-galore-contract.doc>
- The access times align with renewed malware execution.

November 30 – December 1, 2021 – Sustained Malicious Traffic

- Security and Sysmon logs record continuous outbound PowerShell traffic to 13.90.131.107 (443)
- Activity suggests ongoing reconnaissance or preparation for data exfiltration.

After December 1, 2021

- No further malicious activity appears in logs.
- Likely explanations include:
 - o Malware failed to escalate privileges

- Attacker abandoned session
- System reboot

Tools and Methodology

A wide variety of industry-standard digital forensic tools were used throughout the course of this investigation. Each tool served a specific purpose in validating artifacts, correlating activity, and rebuilding the sequence of events on Mr. Howard's laptop.

Autopsy / Sleuth Kit

Purpose: Primary forensic platform

Use Cases:

- Examined file system artifacts, including Prefetch, browser cache, WebCacheV01.dat, and user directories
- Extracted PowerShell logs, and malicious files
- Performed keyword searches (email addresses, filenames, IP addresses)

Windows Event Viewer (Parsed Logs)

Purpose: System behavior verification

Use Cases:

- Reviewed Security, System, PowerShell Operational, TerminalServices, and Sysmon logs
- Identified malware related execution activity
- Confirmed outbound PowerShell network traffic and RDP activity

Timeline Explorer

Purpose: Chronological correlation

Use Cases:

- Organized exported logs and CSV artifacts into a unified timeline
- Correlated Prefetch executions, file modifications, PowerShell activity, and network events

Registry Explorer (Eric Zimmermans's Tool)

Purpose: Inspection of registry hives

Use Cases:

- Identified evidence of program execution
- Validated whether the malware attempted privilege escalation

PEStudio

Purpose: Static malware analysis

Use Cases:

- Examined suspicious files (Report.exe and Report.js) without execution
- Identified malicious indicators, embedded URLs, and execution flags

Evidence

Provided Evidence

The following is a list of digital evidence provided. The Disk Image **2025FALL340-440.E01** was provided by third party forensic firm **Grouppunch**

| Item | Description | Type |
|------|-------------------------|------------|
| 1 | 2025FALL340-440.E01 | Disk Image |
| 2 | 2025FALL340-440.E02 | Disk Image |
| 3 | 2025FALL340-440.E03 | Disk Image |
| 4 | 2025FALL340-440.E01.txt | Text File |

Discovered Evidence

The following is a list of digital evidence found during the investigation.

| Item | Description | Type |
|------|--|------------------------|
| 1 | Outlook.pst | Personal Storage Table |
| 2 | Microsoft-Windows-PowerShell%4Operational.evtx | Event Log File |
| 3 | Microsoft-Windows-Sysmon%4Operational | Event Log File |
| 4 | Security.evtx | Event Log File |
| 5 | Report.exe | Executable File |
| 6 | Psss.ps1 | PowerShell Script |
| 7 | v.txt | Text File |
| 8 | System.evtx | Event Log File |

Findings

MBR DATA

Disk Signature: 8C 3A FB F9

Partition Type: NTFS

Starting Sector: 2048

Partition Size: ~85.9 GB (85,897,248,768 bytes)

Machine Information

Computer Name: WIN-T7LSMB0Q80T

Time Zone of Computer: Central Standard Time

Last Shutdown Time: November 29, 2021, at 00:35:14 (12:35:14 AM CST)

Finding 1 – Malicious Email and Initial Compromise

1. Microsoft Outlook – outlook.pst Email Records

The outlook.pst file was extracted and reviewed to validate Mr. Howard's claim regarding the suspicious email. Analysis confirmed that on November 17, 2021, Mr. Howard received an email titled "Important Report" from sender csmithjmy@proton.mail displayed as "C.J Smith."

The attached Report.zip carried the malicious JavaScript file (report.js). This script executed a dropper (Report.exe) that installed malware on the system at approximately 12:18 CST. Both Prefetch artifacts and PowerShell logs confirm execution.

Mr. Howard replied to the sender at 12:23 CST stating he could not open the attachment, which demonstrates no awareness of the malicious activity. On November 22, 2021, Mr. Howard emails IT reporting unusual behavior ("black screen with red letters"), which supports they were uninvolved in the scheme.

Finding 2 – Security Event Logs and PowerShell Activity

1. Windows Security Logs – Security.evtx

Security logs were examined for unauthorized logins or lateral movement originating from outside the laptop. No external logon attempts were identified. All access occurred through Mr.

Howard's local user profile. This indicates the attacker operated within his session after the malware executed.

Numerous Windows Filtering Platform events (Event ID 5156) showed outbound connections from Powershell.exe to **13.90.131.107:443**.

2. Windows PowerShell Event Logs – Powershell.evtx

PowerShell logs revealed repeated execution of hidden commands as such:

powershell -exec bypass -Noninteractive -windowstyle hidden -e

These parameters enable execution of malicious scripts without user visibility and bypass policy restrictions. This behavior is inconsistent with a normal computer user and indicates advanced attacker behavior.

Finding 3 – Advanced Tools and Lateral Movement

1. PowerShell Operational Logs – PowerShell%4Operational.evtx

This log provided the most significant evidence regarding the attacker's intent. The following were identified:

- **Invoke-SMBExec**, a tool used for remote command execution and lateral movement
- **MD4 hashing routines**, used for "Pass-the-hash" authentication
- **Privilege escalation code** via registry hijacking and FodHelper.exe UAC bypass, confirming an attempt to elevate access to Administrator.
- **Base64-encoded payloads** designed to download additional modules from the attacker's server.

2. v.txt – Privilege Escalation Scanner Results

A recovered text file within Uses/Public contained results from a Windows privilege escalation vulnerability scanner. This demonstrates the attacker tested the system for exploitable CVEs (Common Vulnerabilities and Exposures) confirming systematic attempts to gain SYSTEM-level control.

3. Internal Resource Probing

WebCache and browser artifacts show attempted automated access to **file:///kidco-dc1/IT/website-galore-contract.doc**. This indicates some internal reconnaissance and attempted access to corporate resources.

Finding 4 – Evidence of User Negligence

A file named passwords.xlsx was recovered from Mr. Howard's desktop file location. This file contained multiple personal and corporate credentials stored in plaintext. The presence of this file demonstrates poor security hygiene and a lack of technical sophistication.

However, this artifact strongly supports the fact that:

- Mr. Howard was not acting maliciously and lacked the skills to cooperate in the attack.
- His behavior is consistent of a non-technical user prioritizing convenience over security.
- The easily accessible password file indicates Mr. Howard did not attempt to hide information.

Conclusion

The forensic examination confirms that Mr. Howard's laptop was compromised on November 17, 2021, when they opened a malicious email attachment sent from a ProtonMail account. The attachment executed malware that ran hidden PowerShell commands, attempted privilege escalation, and probed internal Kidco resources. The attacker deployed advanced post-exploitation tools commonly used for lateral movement.

While no conclusive evidence of completed data exfiltration was found, the attacker clearly attempted to access internal file shares and maintained persistence on the system. The tools and techniques observed demonstrated both the capability and intent to expand access within the network.

Nothing in the evidence suggests that Mr. Howard participated in the attack. Their actions are consistent with a non-technical user who was simply targeted and exploited.

Based on these findings, the incident is best classified as a phishing-driven malware compromise followed by attempted internal reconnaissance and privilege escalation.

The investigation revealed several areas where Kidco should strengthen its security posture. Most importantly, all employees should receive updated phishing awareness training and instruction on proper password handling.



Recoverable Signature

X

Ryan Ethier
Investigator

Signed by: 2c60997a-2ddd-4c41-a292-2f6fba9b3bea