Incident handler's journal

Date: 12/20/24	**Entry 1:** U.S. Health Care Clinic Incident
Description	U.S health care clinic fell victim to a phishing attack that resulted in ransomware being downloaded, and now disruption of business operations.
Tool(s) used	No tools were used
The 5 W's	● **Who**: A malicious threat group of unethical hackers ● **What**: The email opened was a phishing email which had a downloadable file containing malware. After this was downloaded, the organization's files were encrypted and demanding money so they may continue operations ● **When**: This incident occurred on Tuesday at 9:00 a.m. ● **Where**: Incident occurred in the U.S health care clinic ● **Why**: Malicious phishing email was opened containing ransomware. Since this was a ransomware attack, it would seem their goal was for financial gain.
Additional notes	I would like to review the email to look for signs that this had malicious intent. After review, there can be some additional training with the organization on how to spot these inconsistencies and prevent this from happening in the future.

Date: 12/23/2024	**Entry: 2** **Malicious Payload Executed**
Description	Employee downloaded malicious payload from email attachment

Tool(s) used	VirusTotal, MalwareBazaar
The 5 W's	● **Who:** The APT is known as BlackTech. The source IP from the email came from 114.114.114.114. ● **What**: Once the malicious payload was downloaded, multiple executable files were created on the employee's computer. The malware's file hash is known as 'Flagpro'. ● **When:** First successful download occurred at 1:13 p.m ● **Where:** The financial service company from employee's computer ● **Why:** This malicious executable file was identified as a trojan horse malware. The employee may have perceived this as a normal email. There are also many grammatical errors within the email sent, which are common signs of a phishing attempt.
Additional notes	SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

---

Date: 12/24/24	**Entry: 3** Review of Incident Final report
Description	Data exfiltration by web based-exploit attack.
Tool(s) used	N/A

The 5 W's	● **Who**: Malicious threat actor (no name or organization stated) ● **What**: Through a vulnerability in the web server by cross-site scripting, an adversary was able to access customer transaction data, which was then collected and exfiltrated by the threat actor. ● **When:** Initial email received from the threat actor occurred on Dec, 22, 2022 at 3:13 p.m. Second email received was on Dec, 28, 2022 at 7:20 p.m. ● **Where**: Employee from retail company ● **Why**: Vulnerabilities within the web servers coding is why this incident was able to occur. The flaw in the coding was exploited, which led to the data breach and data exfiltration.
Additional notes	One way this incident could have been prevented was implementing prepared statements within the web servers coding. This would have stopped the threat actor from gaining access to customer data within the URL. Since this was overlooked upon development, it was a key vulnerability within the application. The team has taken the necessary steps to prevent future occurrences of this, like: ● Performing routing vulnerability scans and penetration testing ● Implementing additional control mechanisms ● AAA (Authentication, Authorization, and Accounting)

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

There wasn’t anything that felt incredibly challenging for me, but the one that did engage my thinking process the most was Entry 2. This is because I had to find multiple OSNIT resources to get a detailed idea of what was occurring within the incident.

2. **Has your understanding of incident detection and response changed since taking this course?**
   It has drastically changed. With the amount of notes I have been taking and rewatching videos, it has given me much more understanding of what to expect, and the process of incident detection & response.
3. **Was there a specific tool or concept that you enjoyed the most? Why?**
   The coding aspect is what I enjoy the most. Also, the searching or finding of patterns concepts also excites me. Finding patterns, solving puzzles, and problem solving keeps my brain moving which is very fun to me. And the coding aspect is enjoyable to me because I am actively learning languages and it can be used as a form of architecture since you have the ability to build something with code.