# Incident handler's journal

## Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| | |
|---|---|
| **Date:** September 20, 2023 | **Entry:**<br>**#1** |
| Description | This incident unfolded in two distinct phases:<br>1. **Detection and Analysis**: The narrative highlights the organization's initial detection of the ransomware incident. In the analysis phase, the organization sought technical assistance by reaching out to other organizations.<br>2. **Containment, Eradication, and Recovery**: The scenario outlines specific measures taken by the organization in order to contain the incident, such as shutting down the company’s computer systems. Recognizing the need for external expertise in the efforts to eradicate and recover, the company sought assistance from other organizations. |
| Tool(s) used | None |
| The 5 W's | ● **Who**: Unethical hackers working as an organized group<br>● **What**: A security breach involving ransomware<br>● **When**: At a healthcare company |

| | |
|---|---|
| | - **Where**: Tuesday at 9:00 a.m.<br>- **Why**: The incident transpired as a result of an unethical hacker group gaining access to the company's systems through a phishing attack. Subsequently, the attackers deployed their ransomware on the company's systems, thereby encrypting crucial files. Since the hackers left behind a ransom note that demanded a substantial sum of money in exchange for the decryption key, the motivation behind the attack appears to be financial. |
| Additional notes | After reviewing this scenario, I am left asking the following questions:<br>1. What proactive measures can the healthcare company take to avoid a recurrence of such an incident?<br>2. Should the company fulfill the ransom demand in order to obtain the decryption key? |

---

| | |
|---|---|
| **Date:** October 4, 2023 | **Entry:**<br>**#2** |
| Description | Analyzing a packet capture file |
| Tool(s) used | To conduct the analysis, I needed to examine the packet capture file. To do this, I employed Wireshark because it serves as a network protocol analyzer that features a graphical user interface. Its significance in cybersecurity lies in its capability to facilitate security analysis in capturing network traffic. As a result, Wireshark aids in the detection and investigation of potential malicious activities. |

| | |
|---|---|
| The 5 W's | - **Who:** N/A<br>- **What:** N/A<br>- **When:** N/A<br>- **Where:** N/A<br>- **Why**: N/A |
| Additional notes | This event warrants escalation because the email’s attached file has a known malicious hash, which I uncovered by using VirusTotal. |

---

| | |
|---|---|
| **Date:** October 14, 2023 | **Entry:**<br>**#3** |
| Description | Capturing a packet |
| Tool(s) used | In this analysis, I employed tcpdump to capture and scrutinize network traffic. Tcpdump, a network protocol analyzer, is accessed through the command-line interface. |
| The 5 W's | - **Who:** N/A<br>- **What:** N/A<br>- **When:** N/A<br>- **Where:** N/A<br>- **Why**: N/A |
| Additional notes | The resulting output should provide some intriguing insights. |

---

| | |
|---|---|
| **Date:** October 14, 2023 | **Entry:**<br>**#4** |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this analysis, I utilized VirusTotal, an investigative tool, to examine the file hash that has been reported as malicious.<br>This incident transpired during the Detection and Analysis phase, thereby necessitating a more in-depth examination in order to ascertain the validity of the alert. |
| The 5 W's | ● **Who**: A malicious actor that remains unidentified<br>● **What**: An email containing a malicious file attachment with the SHA-256 file hash was sent to an employee: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b<br>● **When**: Following the detection of the file by the intrusion detection system, an alert was forwarded at 1:20 p.m. to the organization's SOC.<br>● **Where**: An employee's computer at a financial service company<br>● **Why**: An employee successfully downloaded and opened the email's malicious file. |
| Additional notes | To prevent future incidents, it may be beneficial to implement screening measures beforehand. Additionally, it would be helpful to enhance security awareness training for employees so that they exercise more caution when clicking on links. |