**Incident handler's journal**

| **Date:** Oct 17, 2024 | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident  Incident:  A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.  Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.  The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.  Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.  This incident occurred in the two phases:   1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. | | |
| Tool(s) used | None | | |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. | | |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? | | |

| **Date:** Oct 19 2024 | **Entry:** #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes |  | | |

| **Date:** Oct 20 2024 | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Capturing my first packet | | |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic. | | |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A | | |
| Additional notes |  | | |

| **Date:** Oct 20 2024 | **Entry:**  #4 | | |
| --- | --- | --- | --- |
| Description | Investigate a suspicious file hash | | |
| Tool(s) used | For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.  This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. | | |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. | | |
| Additional notes | How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? | | |