Incident handler's journal

Date: 26/07/2023	**Entry: 1**
Description	An incident regarding ransomware took place on Tuesday morning, at approximately 9:00 a.m. at a small U.S. health care clinic. 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.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** - An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries ● **What** - Ransomware security incident ● **When** - Tuesday morning, at 9:00 a.m ● **Where** - A healthcare company ● **Why** - 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. A ransom note was left, which stated that all the company's files were encrypted. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key
Additional notes	● How could the health care company prevent an incident like this from happening again? ● Should the company pay the ransom to retrieve the decryption key?

Date: 27/07/2023	**Entry: 2**
Description	Analyzing a packet capture file
Tool(s) used	Wireshark, a network protocol analyzer which is used to analyze a packet capture file
The 5 W's	Capture the 5 W's of an incident. ● **Who** - N/A ● **What** - N/A ● **When** - N/A ● **Where** - N/A ● **Why** - N/A
Additional notes	A powerful graphical user interface for understanding network traffic, which seemed quite straightforward in use

---

Date: 02/09/2023	**Entry: 3**
Description	Investigating a suspicious file hash
Tool(s) used	Virus Total, which analyzes files and URLs for malicious content such as viruses, worms, trojans etc.
The 5 W's	Capture the 5 W's of an incident. ● **Who** - Threat actor by the name of BlackTech ● **What** - A phishing email sent to an employee which created a malware attack via a trojan ● **When** - Email recieved at 1:11pm. Detection at 1:20pm ● **Where** - Financial services company

	● **Why** - An employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. A known threat actor who has malicious intent. Motive is unknown
Additional notes	● How to educate employees on how to avoid being vulnerable to phishing attacks? ● Subject header had grammatical errors which indicated that it was a phishing email ● Email address from sender did not match the name ● File attachment sent was malicious

---

Date: 04/09/2023	**Entry: 4**
Description	Review a final report
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** - Unknown threat actor ● **What** - Ransomware attack after a data breach ● **When** - December 28, 2022, at 7:20 p.m. ● **Where** - Mid-sized retail company ● **Why** - At approximately 3:13 p.m., PT, on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen 50,000 customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000

	cryptocurrency payment. The employee assumed the email was spam and deleted it. On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000. On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft. Eventually the incident was closed and a thorough investigation had been conducted. The financial impact of the incident was estimated to be $100,000 in direct costs and potential loss of revenue.
Additional notes	• How to educate employees on how to avoid being vulnerable to phishing attacks? • Perform routine vulnerability scans and penetration testing. • Implement the following access control mechanisms: ➢ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. ➢ Ensure that only authenticated users are authorized access to content.