Incident handler's journal

Date: 05/29/24	**Entry:** Entry #1
Description	A small U.S healthcare clinic experienced a ransomware attack by a group of unethical hackers through a phishing email.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A group of unethical hackers known to target the healthcare and transportation industry. ● **What** happened? All of the critical files and software needed to do business were encrypted so the clinic had to shut down. ● **When** did the incident occur? It occurred on Tuesday at 9:00 am. ● **Where** did the incident happen? The incident happened at a small U.S healthcare clinic. ● **Why** did the incident happen? The attackers were able to gain access to the internal system through a phishing email that they sent to employees. The email contained an attachment that contained malware and once they were able to get into the system, they encrypted all of the files. Their motivation seems to be financial because they demanded a large sum of money for the decryption key.
Additional notes	In the future, the company needs to perform daily backups of their most critical data so that they will always be able to retrieve it and continue operations in any future ransomware attack.

Date: 05/30/24	**Entry:** Entry #2
Description	Investigating malware on an employee’s computer.
Tool(s) used	Virus Total.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The email was sent by a Clyde West from Def Communications using this IP address: <114.114.114.114> ● **What** happened? The attacker sent an email containing a password protected file to an employee’s computer, the password was provided in the email. Once the employee opened the file, several unauthorized executable files were created on the computer. ● **When** did the incident occur? The employee received an email at 1:11 pm, at 1:15 the executables were created and the IDS sent an alert at 1:20 pm. ● **Where** did the incident happen? This incident happened at a financial services company. ● **Why** did the incident happen? The attackers were able to get access to the system through a phishing email to an employee. Once the attachment from the email was open, unauthorized executable files were created and ran on the computer. The files were malicious so it compromised the employee’s computer.
Additional notes	The file hash has been detected as the known malware flagpro. The file is known malware that has been detected by multiple other sources. Maybe it can be added to the IDS/IPS system.

Date: 05/30/24	**Entry:** Record the journal entry number. Entry #3
Description	Investigating a Data breach.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An unknown attacker. ● **What** happened? An employee received an email from an unknown sender claiming that he had stolen personal information and demanded payment in cryptocurrency. The employee believed the email to be spam and deleted it. Later that day, the employee received an email from the same sender with a sample of the data and still asking for money. The employee then notified the security team. The attacker obtained the PII of over 50,000 customers and obtained financial information that caused $ 100,000 in direct costs and lost revenue. ● **When** did the incident occur? The incident happened on December 28 2022 at 7:20 pm PT. ● **Where** did the incident happen? At a mid-size retail company. ● **Why** did the incident happen? The attacker was able to access the system through a web app vulnerability in the e-commerce website. The attacker was able to perform a forced browsing attack and obtain customer's payment information by changing the order number in the URL string of a confirmation page. The attacker then accessed thousands of confirmation pages and exfiltrated sensitive customer data.
Additional notes	