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: 7-29-2025	**Entry:** 001 - Documenting a Cybersecurity Incident
Description	A small US health care clinic experienced a security event on Tuesday at approximately 9:00AM; employees were unable to access files such as medical records. This scenario outlines how the organization first detected the ransomware incident. For analysis, the organization contacted several others for technical assistance. For containment, the organization shut down their computer systems.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. • **An organized group of unethical hackers caused this incident** • **Attackers were able to gain access to the medical system by using targeted phishing emails that included a malware attachment; once the attachment was downloaded and the attacker had access, ransomware was deployed, which encrypted the sensitive files and software in exchange for a decryption key**

	• **This event occurred on Tuesday at approximately 9:00AM** • **This incident happened at a small US healthcare clinic** • **The unethical hackers target organizations in the healthcare and transportation industries**
Additional notes	This event could have been avoided with increasing training on social engineering awareness, and the importance of verifying the sender of an email before downloading any attachments.

Date: 8-10-2025	**Entry:** 002
Description	A suspicious file containing malware has been downloaded by an employee.
Tool(s) used	VirusTotal, Pyramid of Pain
The 5 W's	Capture the 5 W's of an incident. • **Cyber espionage group BlackTech is behind this attack** • **Employee received email and downloaded attachment containing malware** • **The incident occurred today at around 1:11pm. The attachment was downloaded at 1:13pm.** • **The incident happened at a financial services company** • **This incident occurred due to social engineering and employees being susceptible to phishing attempts.**
Additional notes	The file is malicious. 59/72 security vendors flagging the file as malicious. This file has mostly been associated with the trojan flagpro, which has been used by cyber espionage group, BlackTech, since about 2020. Once the group gained access, they were able to install tools that would allow them to access even

	more systems.

Date: 8-12-2025.	**Entry:** 003
Description	An email with an attachment containing trojan flagpro was discovered.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Someone named Clyde West from Def Communications caused the incident to occur** • **An email with an attachment containing trojan flagpro was discovered** • **The email containing the attachment was sent at 9:30am** • **This happened at Inergy, a financial services company** • **The user saw that Inergy was hiring for an Infrastructure Engineer, and took the opportunity to send an inquiry email to HR, hoping to infect their systems**
Additional notes	The email received by the employee contained many misspellings and improper grammar, which is usually indicative of a phishing attempt. The sender did not even spell the company name correctly. Additionally, the email address and IP provided appear to be suspicious as well. The attached filename appeared on VirusTotal as suspicious.

Date: 8-19-2025	**Entry:** 004
Description	A single attacker accessed PII and financial information of over 50,000 customers, and asked for $50,000 in exchange for not posting the records publicly.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **This was caused by a single attacker.** • **An individual was able to access PII and financial information of over 50,000 customers. The individual then asked for $50,000 in exchange for not posting the records publicly.** • **The security incident occurred on December 28, 2022 at 7:20pm** • **This happened at a mid-sized retail company.** • **The incident occurred because there was a vulnerability in the e-commerce web app that allowed the attacker to perform a forced browsing attack and accessed the customer data.**
Additional notes	Routine vulnerability scans may have prevented this? Is paying the ransom easier than dealing with the fallout of this going public? This case especially shows the importance of having a business continuity plan in place. The executives will need to decide which mitigation tactic is best in this case, while also taking into account their reputation and legal issues.