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: Tuesday 09:00	**Entry:** No. 001
Description	A GPs office in the US lost access to their systems and data to ransomware. An unethical hacking group claimed responsibility and demanded a large sum of money. The access to the systems and data was gained through phishing emails with a malicious attachment.
Tool(s) used	None.
The 5 W's	**Who**: An organised group of unethical hackers **What**: A ransomware incident **When**: Tuesday 09:00 **Where**: A primary care physician company in the US **Why**: The phishing attack ended up successful by giving the group access to critical files and systems for encryption. The motivation seems to be financial.
Additional notes	The health care company is highly recommended to contact the authorities for assistance seeing as the information the group gained access to violates HIPAA.

Date: July 20, 2022 09:30:14 AM	**Entry:** No. 002
Description	The SOC analysts received a phishing alert and an alert about a suspicious file being downloaded to an employee's computer. The origin of the file in question was an email. It bore signs of being a phishing email such as having an abundance of spelling errors, an email address not matching the name of the sender. The file is a trojan. The ticket was updated and escalated.
Tool(s) used	Virustotal
The 5 W's	**Who**: A threat actor claiming to be someone called "Clyde West" **What**: A phishing incident **When**: July 20, 2022 09:30:14 AM **Where**: Financial services company **Why**: Unknown exact motivation behind threat actor with intention of infecting the financial services company with a trojan, possibly to gain access to SPII and PII.
Additional notes	

Date: December 28, 2022, at 7:20 p.m.	**Entry:** No. 003
Description	An employee received an email from a threat actor claiming to have stolen customer data and was requesting a payment of $25,000 in cryptocurrency, which later increased to $50,000. A sample of the data was sent to prove that the threat actor had indeed gained access to customer PII. The data was stolen using a forced browsing attack, taking advantage of a vulnerability. The incident

	was disclosed to customers with an offer for free identity protection services.
Tool(s) used	None
The 5 W's	**Who**: unknown threat actor **What**: forced browsing attack to access customer transaction data **When**: December 22, 2022 **Where**: retail company **Why**: gain leverage with financial motivation
Additional notes	

Date: October 4th, 2023	**Entry:** No. 004
Description	Using Wireshark to analyse a packet capture file
Tool(s) used	Wireshark is a network packet sniffer with a GUI. It allows for an overview of network activity and its analysis. This exercise had me investigating the traffic to a website, which allowed me to use filters to locate specific packets. I was able to examine single packets for protocol and data layers.
The 5 W's	**Who**: N/A **What**: N/A **When**: N/A **Where**: N/A **Why**: N/A
Additional notes	This exercise prompted me to look into getting more practice and experience with Wireshark both as part of a training course and my own self study projects.