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: 19-10-2023	**Entry:** 1
Description	A small health care clinic had a security incident where a phishing email containing a malicious attachment was downloaded and opened. Once opened, ransomware encrypted the organization's computer files and demanded payment to decrypt them.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** A group of unethical hackers who target organizations in healthcare and transportation both sent the malware and created it. ● **What:** A ransomware security incident ● **When:** Tuesday at 9:00 am. ● **Where:** The incident happened at a small U.S health care clinic specializing in delivering primary care services. ● **Why:** An employee clicked on a phishing email attachment that installed malware on the employee's computer. After gaining access the attackers launched ransomware onto the company's systems and encrypted critical files. The attackers want money to decrypt the files.
Additional notes	Employees should be trained not to click on phishing emails. It can be hard to

	spot good phishing attempts but training should be done to minimize it. Is it a good idea to pay the attackers?

Date: 22-10-2023	**Entry:** 2
Description	A phishing alert was received based on a suspicious file being downloaded to an employee's computer. The file was confirmed malicious and
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An employee downloaded a suspicious file. ● **What**: Phishing incident ● **When:** Wednesday, July 20, 2022 09:30:14 AM ● **Where**: The employee's PC. ● **Why**: A malicious actor sent a fake application email containing a malicious file attachment as their "resume". The employee downloaded and opened the file.
Additional notes	Employees need to be taught to avoid phishing attempts. Perhaps the computer should block a download like that?

Date: 24-10-2023	**Entry:** 3

Description	Examining a suspicious domain signin.office365x24.com which has been used to dump stolen logs or credentials. Six different computers at our organization have accessed the site.
Tool(s) used	Used Google’s Chronicle to sift through log information through the site.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: **ashton-davidson 3 POST**, bruce-monroe, coral-alvarez, **emil-palmer 3 POST**, jude-reyes,roger-spence, **warren-morris POST,** amir-david were all the host PCs that accessed the site. ● **What**: A phishing incident ● **When** Between January 31, 2023 and July 09, 2023 ● **Where**: 40.100.174.34, signin.accounts-gooqle.com, signin.office365x24.com were the phishing sites ● **Why**: A phishing website caught three employees and they shared personal data such as login credentials.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 24-10-2323	**Entry:** 4
Description	Using virustotal to inspect a suspicious file.
Tool(s) used	VirusTotal
The 5 W's	N/A
Additional notes	Domain names: org.misecure.com is reported as a malicious contacted domain under the Relations tab in the VirusTotal report. IP address: 207.148.109.242 is listed as one of many IP addresses under the Relations tab in the VirusTotal report. This IP address is also associated with the org.misecure.com domain as listed in the DNS Resolutions section under the Behavior tab from the Zenbox sandbox report. Hash value: 287d612e29b71c90aa54947313810a25 is a MD5 hash listed under the Details tab in the VirusTotal report. Tools: Input capture is listed in the Collection section under the Behavior tab from the Zenbox sandbox report. Malicious actors use input capture to steal user input such as passwords, credit card numbers, and other sensitive information. TTPs: Command and control is listed as a tactic under the Behavior tab from the Zenbox sandbox report. Malicious actors use command and control to establish communication channels between an infected system and their own system.

Date: 24-10-2023	**Entry:** 5
Description	Reviewing a final report
Tool(s) used	Cybersecurity final report
The 5 W's	Capture the 5 W's of an incident. ● **Who**: The web development team who left a vulnerability in the e-commerce web application. ● **What**: A forced browsing attack to access customer transaction data. ● **When**: December 22, 2022 ● **Where**: The company's e-commerce website. ● **Why**: The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	Are there potentially more vulnerabilities in the e-commerce application? Injection attacks like this should be stopped via proper code practices, this in on the software engineers.

Reflections/Notes:

- I really enjoyed working with Google chronicle, I found it to be extremely intuitive and I was impressed by the depth of information it could give me.
- I now understand the complexity of finding and stopping cybersecurity incidents. I believe I am better suited to handling cybersecurity response given the tools taught in this course.