Incident handler's journal

Date: 07/07/2024	**Entry:** #1
Description	A security incident occurred at a small U.S. healthcare organization. Employee workstations were infected with ransomware as part of a sophisticated cyberattack by an organized group of unethical hackers.
Tool(s) used	No tools were used.
The 5 W's	**Who**: An organized group of unethical hackers known for targeting organizations in the healthcare and transportation industries. **What:** Several employees reported being unable to access their computers for work-related files. A ransom note was displayed on their computers stating all files had been encrypted and demanding a large sum of money in exchange for the decryption key to recover the data on infected computers. Business operations came to a halt since employees could not access files and software needed to do their jobs. **When:** Early Tuesday morning and was reported @ 9:00 AM **Where:** A small U.S. healthcare clinic **Why:** Unethical hackers used phishing attacks to target employees. After an employee downloaded and opened the malware, the ransomware was activated, encrypting the company's system and critical files. The motivation behind the attack seems to be financial in nature because a note was left demanding a large sum of money in exchange for the decryption key.
Additional notes	In the event of an incident similar to this one occurs, the following precautions need to be considered

	- What should the healthcare company do to prevent this from happening again? - If a ransom is paid, what stops other groups of hackers from attempting another hack on the healthcare company? - Is a policy playbook in place for the healthcare company's recovery after a Ransomware attack?

Date: 07/10/2024	**Entry:** #2
Description	Documenting brief research into a malicious file's Sha156 file hash. An employee downloaded a suspicious file named "bfsvc.exe." The file was investigated and analyzed to capture details and find indicators of compromise (IoCs). It was then retrieved and converted into a SHA256 hash for malware analysis.
Tool(s) used	- VirusTotal - MalwareBazaar
The 5 W's	Capture the 5 W's of an incident. **Who**: A sender using email address of 76tguyhh6tgftrt7tg.su and an IP address of 114[.]114[.]114[.]114. A threat actor known as BlackTech. The group has primarily targeted organizations in East Asia. **What**: A spear phishing email with a password-protected file attachment was sent to an employee, who was given the password to open the file in the same email. The employee downloaded the file and opened it using the included password, which led to multiple

	unauthorized executable files being executed on the employee's computer. **When** The security incident occurred at 1:20 PM, an intrusion detection system (IDS) found the executable files and notified the organization's SOC team. **Where**: A Financial service company based in the United States. **Why**: BlackTech successfully tricked an employee into downloading and executing malware through a spear phishing email attempt. An IDS detected several unauthorized files from the download, and an alert was sent to the organization's SOC for investigation.
Additional notes	- Over 50 vendors have reported the file hash as malicious. Upon further investigation, this file hash is known as the malware Flagpro, commonly used by the advanced threat actor BlackTech. - The email has multiple typos. - It's strange for a resume and cover letter to be sent over a password-protected email. - The attached file clearly showed it was a '.exe' file.

Date: 07/11/2024	**Entry:** #3
Description	A security incident occurred at an organization; a malicious individual gained unauthorized access to customer PII and financial information by exploiting a vulnerability in the organization's e-commerce web application.
Tool(s) used	- Web Application Logs - Web Server Logs

	- Final Incident Report
The 5 W's	Capture the 5 W's of an incident. **Who**: A malicious actor exploited a zero-day vulnerability in the organization's e-commerce application. The individual used an external email address to contact an employee twice, claiming possession of stolen customer data and demanding payments to prevent data leakage. **What**: A malicious actor gained unauthorized access to ~50,000 customers' PII and financial information. The Threat actor sent two emails to the employee. The first email demanded the sum of $25,000 USD in cryptocurrency on Dec. 22, 2022, at 3:13 PM PT. Then, on December 28, 2022, the threat actor sent the second email, this time including a sample of the stolen customer data as proof. The payment demanded in the second email was $50,000 USD. The employee then notified the security team. The actor collected and exfiltrated customer data by modifying the order number in the URL string of a purchase confirmation page of the affected e-commerce web application. **When**: Dec. 28th, 2022, at 7:20 PM PT. **Where**: A mid-sized retail company's E-commerce website **Why**: A vulnerability in the web application allowed the malicious actor to conduct forced browsing resulting in unauthorized access to customer transaction data.
Additional notes	To prevent this from happening again, the organization should: - Constantly scan for known vulnerabilities and penetration testing. - Ensure that only authenticated users are authorized access to content. - Providing identity protection to affected customers is an excellent way to safeguard the company's integrity.

Date: 07/12/2024	**Entry:** #4
Description	A security event's analysis for a failed root SSH logins into an organization's mail server.
Tool(s) used	Splunk Cloud SIEM tool Zip file containing financial transactions, access, and authentication data logs
The 5 W's	Capture the 5 W's of an incident. **Who**: Malicious actors attempt to brute force password attacks on Buttercup Games' mail server. **What**: A large influx of attempts to root SSH login into the Buttercup Games mail server **When**: 346 events over a span of 8 days between 02/27/23 - 03/06/23 **Where**: Buttercup Games' e-commerce mail server **Why**: Failed login attempts from different IP addresses and ports
Additional notes	

Date: 07/12/2024	**Entry:** #5
Description	Investigating a potential phishing email sent to a financial service company employee.

Tool(s) used	Google's Chronicle Cloud SIEM tool
The 5 W's	Capture the 5 W's of an incident. **Who**: Malicious actor attempting to phish a financial service company's employee by pretending to be Microsoft using 'sigin.office365x24.com' **What**: An employee reposted a suspicious phishing email **When** 24 events total; First accessed on Jan. 31st, 2023 **Where** A financial services company **Why** Employees were targeted with phishing emails in hopes that one of them would click and compromise sensitive data
Additional notes	Steps: - Perform a domain search - Investigate the threat intelligence data - Investigate the addicted assets and events - Investigate resolved IPs

Date:	**Entry:** 6
Description	Provide a brief description of the journal entry.
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? **What** happened? **When** did the incident occur?

	Where did the incident happen? **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Reflections/Notes:

Were there any specific activities that were challenging for you? Why or why not?

1. Has your understanding of incident detection and response changed since taking this course?
2. Was there a specific tool or concept that you enjoyed the most? Why?