Incident handler's journal

Date: 01-08-2024	**Entry:** 1
Description	At approximately 9:00 AM on a Tuesday morning, a small U.S. health care clinic specializing in primary care services had to shut down business operations because employees were unable to access the files and software needed to do their job. The cause of the incident were phishing emails containing a malicious attachment that installed malware on several employees' computers, enabling the attackers to deploy ransomware that encrypted critical files. The attackers demanded payment of a large sum in exchange for a decryption key to restore access to the patient data that had been encrypted by their ransomware. The health care clinic had to shut down its computer systems and contact multiple organizations to report and resolve the incident. This activity occurred in the Post-Incident Activity phase of the NIST Incident Response Lifecycle because I documented and reviewed an incident to determine what preventative actions should be taken moving forward.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • Who caused the incident? A group of unethical hackers who target organizations in the healthcare and transportation industries caused the incident. • What happened? The hackers sent phishing emails containing a malicious attachment to several employees. When employees downloaded the attachment, it installed malware that gave the hackers access to the network and enabled them to deploy ransomware that

	encrypted critical files. The hackers then demanded payment in exchange for a decryption key to restore access to the files. • When did the incident occur? The incident occurred at approximately 9:00 AM on a Tuesday morning. • Where did the incident happen? The incident happened at a small U.S. health care clinic. • Why did the incident happen? The incident happened because the attackers exploited the employees' lack of awareness of signs of phishing, weak email filtering protocols, and the lack of robust anti-virus software to gain access to the system and encrypt critical files.
Additional notes	The company could respond to the incident by reconfiguring its firewall to exclude external email addresses, implementing additional email filters to flag and/or scan messages with attachments, and conducting targeted anti-phishing training with employees.

Date: 01-09-2024	**Entry:** 2
Description	In this entry I describe using VirusTotal to investigate the file hash of a potentially malicious file attached to a suspected phishing attempt. This activity occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle because I analyzed the file hash of the attachment to determine whether it was malicious.
Tool(s) used	VirusTotal is a website that offers the free ability to analyze suspicious files, domains, URLs, and IP addresses for malicious content. VirusTotal also offers additional services and tools for enterprises.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker who sent a phishing email with a malicious attachment caused the incident. • **What** happened? An employee opened the email and downloaded the attached file, which generated a security alert. • **When** did the incident occur? The incident occurred on 01-09-2024. • **Where** did the incident happen? The incident happened at a financial service company. • **Why** did the incident happen? The incident happened because the employee downloaded a malicious file and entered the password contained in the email to open the file, which executed a malicious payload on their computer.
Additional notes	VirusTotal indicated that the file hash had been reported as malicious by over 50 vendors. The file has a high vendor score of 55/69, a negative community score of -71, and more malware detections than non-detections under security vendors' analysis in the details tab.

Date: 01-10-2024	**Entry:** 3
Description	In this entry, I describe how I used a playbook to respond to a phishing alert. This activity occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle because I analyzed the alert and escalated it for further handling.
Tool(s) used	I used VirusTotal, a service that uses crowdsourcing to analyze suspicious files,

	domains, URLs, and IP addresses for malicious content, to confirm the file hash of the email attachment was malicious.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker who sent a phishing email containing a malicious file caused the incident. • **What** happened? An employee downloaded a suspicious file from an external email onto their computer. This download prompted a security alert, and the file attachment was deemed malicious upon further investigation of its file hash. • **When** did the incident occur? The incident occurred on 01-10-2024. • **Where** did the incident happen? The incident occurred at a financial services company. • **Why** did the incident happen? The incident happened because existing security controls failed to filter out a phishing attempt, and an employee failed to report the suspicious message rather than downloading the attachment from an external sender.
Additional notes	Grammatical errors in the email body and subject line and inconsistency between the sender's email address and the name used in the email body were signs that this email was potentially a phishing attempt. Additionally, the email contained a password protected file with the password itself included in the email body, which was also suspicious. The file hash of the attached file was confirmed to be malicious using VirusTotal, and the alert severity was medium. Based on these findings and the playbook steps outlined by my organization, I chose to escalate this alert.

Date: 01-11-24	**Entry:** 4
Description	In this entry I describe my findings from reviewing a final report documenting a data breach of over one million users of a mid-sized retail companies e-commerce platform. This activity occurred in the Post-Incident Activity phase of the NIST Incident Response Lifecycle because I was reviewing documentation associated with the incident to identify recommendations and preventative actions for the future.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker seeking to ransom customer data in exchange for payment caused the incident. • **What** happened? The attacker exploited a vulnerability in the e-commerce web application to perform a forced browsing attack and access customer data by modifying the order number in the URL string of the confirmation page. The attacker collected and exfiltrated customer information, then emailed an employee requesting payment in exchange for not releasing the data publicly. • **When** did the incident occur? The incident occurred in December 2022. The exact date of initial compromise is unknown, but the first ransom email was sent at 3:13 PM on 12-22-22. A second email demanding increased payment was sent 12-28-22, at which time the security team was notified and conducted its investigation through 12-31-22. • **Where** did the incident happen? The incident happened at a mid-retail company. • **Why** did the incident happen? The incident happened because an attacker was able to exploit a web application vulnerability through a forced browsing attack.

Additional notes	To prevent similar incidents in the future, the security team recommended performing routine vulnerability scans and penetration testing, implementing allowlisting to automatically block all requests outside of a specified set of URLs, and ensuring only authenticated users are authorized access to content.

Date: 01-12-2024	**Entry:** 5
Description	This entry describes my use of Splunk to explore failed SSH logins for the root account of the mail server for an e-commerce store called Buttercup Games. This investigation occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle because I was attempting to identify potential issues with the mail server by analyzing failed logins.
Tool(s) used	I used Splunk, which is a cybersecurity tool used to collect, search, and monitor log data.
The 5 W's	N/A
Additional notes	My initial search query index=main produces over 100,000 results. Modifying my search to index=main host=mailsv fail* root narrowed the results to only events generated by the mail server that contain the term root and versions of the term fail, such as failed or failure. Using the asterisk as a wildcard after the term fail ensured that results containing terms like failure or failed would not be excluded. This modified search reduced the results to under 350 events, which

	is a more manageable starting point for further investigating potential security issues with the mail server.

Date: 01-13-2024	**Entry:** 6
Description	This entry describes an investigation of a suspicious domain using Chronicle.
Tool(s) used	I used Chronicle, which is a cloud-native cybersecurity tool designed to retain, analyze, and search data. This investigation occurred in the Detection and Analysis phase of the NIST Incident Response Lifecycle because I was gathering and analyzing data related to the incident.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker who sent a phishing email caused the incident. • **What** happened? An alert was generated by an employee who received a phishing email in their inbox. I reviewed the alert and used Chronicle to investigate the domain name contained in the email. • **When** did the incident occur? The incident occurred on 01-13-2024. • **Where** did the incident happen? The incident occurred within a financial services company's email application. • **Why** did the incident happen? The incident happened because the existing security features failed to identify the phishing attempt and filter it out before it could be opened by employees.
Additional notes	Using Chronicle, I identified that the domain signin.office365x24.com is categorized as a drop site for logs or stolen credentials. I discovered that at

	least six assets have accessed this domain, which resolves to the IP address 40.100.174.34. I identified additional domains related to the initial suspicious domain by resolving its IP address. I determined that login information was submitted to the suspicious domain via Post requests.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes:
Were there any specific activities that were challenging for you? Why or why not? I found it challenging to use Chronicle because the instructions and graphics in the activity did not match the latest version of Chronicle. I intend to explore other activities using Chronicle to familiarize myself with the latest version of the platform. The activity still provided a helpful introduction to using this tool.

Has your understanding of incident detection and response changed since taking this course? My understanding of incident detection and response has changed since taking this course because I find many of the tools used in the course relatively straightforward to use. I initially felt overwhelmed by the prospect of using tools like Chronicle, Splunk, Suricata, VirusTotal, and more. However, having the opportunity to complete activities with practice data made me feel more confident in my ability to use these tools. Additionally, this course provides links to several user guides and online resources that I can use to deepen my understanding of different cybersecurity tools.

Was there a specific tool or concept that you enjoyed the most? Why? The tool that I enjoyed using the most was VirusTotal because I found the interface easy to use. I appreciate that the tool is free to use and operates using crowdsourced data. I hope to complete more practice investigations using VirusTotal to help myself become accustomed to the tool.