Incident handler's journal

Date: 02/25/2024	**Entry:** 1
Description	On Tuesday morning at approximately 9:00am several employees were unable to access their computers. They reported a ransom note from an organized group of hackers who demanded payment in return for restoration of and access to encrypted data on the network.
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by an organized group of unethical hackers. • **What** happened? The attackers gained access to the network through a series of targeted phishing emails sent to several company employees. The company was unable to access critical data and was forced to shut down their computer systems. • **When** did the incident occur? The incident occurred at approximately 9:00 am 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 at least one or more employees unknowingly granted the hackers access to the system by entering authorization information through a company email.
Additional notes	Although it is unlikely the company will regain access to their company data without paying the ransom, future attacks can be avoided by using hardware or

	software based multi-factor authentication. In the event that the user's email or password were compromised it still requires a second form of authentication to access company files which the attackers would not be able to obtain. Employee training in avoiding future phishing emails is also recommended.

Date: 02/25/24	**Entry:** 2
Description	A security alert was received indicating that a suspicious file was downloaded on an employee's computer. The employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Tool(s) used	VirusTotal was used to identify the malicious software using its SHA256 hash. 58 vendors identified the software as malicious. Several IP addresses were identified. 7 MITRE ATT&CK Tactics and Techniques were identified.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A company employee. • **What** happened? • 1:11 p.m.: An employee receives an email containing a file attachment. • 1:13 p.m.: The employee successfully downloads and opens the file. • 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.

	• 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC. • **When** did the incident occur? The incident occurred at approximately 1:15 p.m. • **Where** did the incident happen? The incident occurred on the employee's computer in the office. • **Why** did the incident happen? The incident happened because the employee downloaded a malicious file onto their computer.
Additional notes	See alert: A-2703. Several IoC's were identified on VirusTotal. Recommendations: Employee training in identifying phishing emails and other types of social engineering attacks. It is also worth considering adjustment of company policy to only allow downloads of software from certain sites or with appropriate authorization.

Date: 02/25/24	**Entry:** 3
Description	An individual gained unauthorized access to customer PII and SPII. Approximately 50,000 customer records were affected leading to an estimated $100,000 in costs to the company.
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by an unknown attacker. • **What** happened?

	The attacker exploited a vulnerability in the e-commerce web application that allowed a forced browsing attack which granted access to customer transaction data. • **When** did the incident occur? The incident occurred on December 28, 2022. • **Where** did the incident happen? The incident happened on-site at the company. • **Why** did the incident happen? The incident occurred because of a web application vulnerability.
Additional notes	See Final Report. Recommendations: • Perform routine vulnerability scans and penetration testing. • Implement the following access control mechanisms: • Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. • Ensure that only authenticated users are authorized access to content.

Date: 02/26/24	**Entry:** 4
Description	An alert was received that an employee received a phishing email in their inbox. A suspicious domain name contained in the email body was investigated using Chronicle and determined to be malicious.
Tool(s) used	Chronicle was used to identify a suspicious domain name as malicious and to search for further evidence of employees having received similar phishing

	emails containing this domain.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A company employee alerted the security department of a suspicious email. • **What** happened? The employee alerted the security team to the email but did not click the link. Upon further investigation using Chronicle login information was submitted to the domain by 3 other employees within the company. • **When** did the incident occur? The indication of compromise via email is approximately 8 months ago. • **Where** did the incident happen? The incident occurred at the company. • **Why** did the incident happen? The incident happened because a previous employee accessed the link in an email.
Additional notes	After investigation, it was determined that the suspicious domain has been involved in phishing campaigns. Multiple assets may have been impacted by the phishing campaign as logs showed that login information was submitted to the suspicious domain via **`POST`** requests. Two additional domains were identified as malicious:**`signin.accounts-gooqle.com`**, **`login.office365x24.com.`** An additional domain was linked to a second IP address:**`40.100.174.34.`**

Reflections/Notes:

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

   Some of the activities took time to complete. Although they were not particularly challenging they were nonetheless valuable tools and skills to develop.

2. Has your understanding of incident detection and response changed since taking this course?

   Some of the mystery around incident detection and response I had at the beginning of the course has been removed.

3. Was there a specific tool or concept that you enjoyed the most? Why?

   I really enjoyed using Wireshark and Chronicle the most. Of all the tools they seemed to be the most powerful and easy to navigate.