Incident handler's journal

Scenario 1

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: January 16th, 2024	**Entry: #1**
Description	The Cybersecurity incident occurred in the Detection and Analysis phase and Containment, Eradication, and Recovery phase.
Tool(s) used	None were provided due to the first occurrence.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Organized group of hackers • **What** happened? Ransomware. Employees being unable to use computers to access files like medical records, business operations shut down, ransom notes. • **When** did the incident occur? Tuesday Morning, January 16th 2024. • **Where** did the incident happen? Health care company. • **Why** did the incident happen? The incident took place as the attackers gained access into the company's network with phishing emails. Those phishing emails contained malicious attachments and were downloaded by the employees. Soon after they were downloaded, the ransomware would be deployed (encrypted critical files) and cause major disruptions in the business operation by encrypting the files. They are now demanding a certain amount of money to be paid to them.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? More training and awareness of phishing emails. 2. Should the company pay the ransom to retrieve the decryption key? No. It may not guarantee data recovery and may encourage further criminal activity.

Reflections/Notes for scenario 1:

- How many entries are there so far? 1 entry.
- The type of security incident the organization was affected by ransomware via phishing.
- The root cause of the incident is the phishing emails. The attacker used the malicious attachments via email as an attack vector. Once the attachment is clicked by the recipient of the email address, the ransomware would be deployed.
- Providing more training and education may solve the problems. Secure backup data from being encrypted by the ransomware. Isolate the infected systems from the network to prevent the spread of ransomware. Sometimes, cybersecurity firms may offer decryption tools for specific ransomware. Communicate to the relevant stakeholders. If possible, report to the authorities.

Scenario 2 (Continuous)

The organization experienced a security incident on January 22, 2024, at 7:20 p.m, PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted. At approximately 3:13 p.m., PT, on January 20, 2024, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. On January 22, 2024, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000. On the same day, the employee notified the security team, who began their investigation into the incident.

Date: January 22th, 2024	**Entry: #1**
Description	An individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. The incident occurred in the Detection and Analysis phase and Containment, Eradication, and Recovery phase.
Tool(s) used	• Playbook
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Cyber criminal (malicious actor) • **What** happened? The email was sent from the external email address to the employee. It claimed to have successfully stolen customer data. The

	sender requested $25,000 in crypto currency, to which was ignored by the employee on January 22nd 2024. • **When** did the incident occur? 7:20 pm. • **Where** did the incident happen? Organization. • **Why** did the incident happen? Individuals gained access to customer personal information and financial information.
Additional notes	• How to prevent this from happening? • Should we increase the training section to raise more awareness of cyber attacks? • Reporting to Level 2 SOC analyst. • Conduct investigation using a playbook.

Date: January 23rd , 2024	**Entry: #2**
Description	An individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information due to the vulnerability in the e-commerce web application. The attacker forced browsing attacks and access customer transaction data by modifying the order number (URL string of the purchase confirmation page). The incident occurred in the Containment, Eradication, and Recovery phase.
Tool(s) used	• Vulnerability scans • Penetration testing • Access Control mechanism
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Cyber criminal (malicious actor)

	• **What** happened? The email was sent from the external email address to the employee. It claimed to have successfully stolen customer data. The sender requested $25,000 in crypto currency, to which was ignored by the employee on January 22nd 2024. However, on January 23rd, 2024, the same employee received the email again but this time the sender requested $50,000. Roughly, 50,000 customer records were affected. • **When** did the incident occur? On January 23rd, 2024. • **Where** did the incident happen? Organization. • **Why** did the incident happen? Forced browsing attack to modify the order number and gain access to customer information.
Additional notes	• How to prevent this from happening? Routine scans and penetration systems. Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL Range. • Conduct more training. • Reported to Level 2 SOC Analyst. • Conduct investigation using a playbook. • Remind the users to report any incident activity.

Reflections/Notes for scenario 2:

- How many entries are there so far? Two entries.
- The type of security incident the organization was unauthorized access and blackmailing.
- The attacker used the forced browsing attack to modify the order number and gain access to customer information.
- Providing more training and education may solve the problems. Routine scans and penetration systems. Implement allowlisting to allow access to a specified set of URLs.

Scenario 3 (Continuous)

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.
You investigate this alert and discover that 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.
Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.
Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Date: January 17th, 2024	**Entry: #1**
Description	This incident occurred in the Detection and Analysis phase. The scenario allows me to investigate a suspicious file hash. I analyzed and determine if the alert signified a real threat. SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Tool(s) used	VirusTotal : Investigative tools to analyze files and URLs for malicious content such as viruses, worms, trojans, and more.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Cyber criminal (malicious actor) • **What** happened? The email contains malicious file (The file hast is written in the description box)

	• **When** did the incident occur? 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC. • **Where** did the incident happen? Financial Service Company. • **Why** did the incident happen? Upon receiving the malicious content on the email, the employee downloaded and executed the malicious file.
Additional notes	• How to prevent this from happening? Never ever downloaded suspicious files from emails. • Should we increase the training section to raise more awareness of cyber attacks? Yes, we should • Should I report this to Level 2 SOC Analyst? Yes. Depending on the playbook the organization uses, it might be different in handling the incident like this.

Date: January, 18th 2024	**Entry: #2**
Description	Playbook to respond to phishing incidents. Playbook is created during the Preparation phase. However, it can be used during Detection & Analysis, Containment Eradication and Recovery, and Post Incident Activity.
Tool(s) used	• Playbook • Alerting ticket status (JIRA, etc.)
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Cyber criminal (malicious actor) • **What** happened? Upon investigating, the ticket ID was created (A-AD3CO). The alert message has been generated and flagged as a positive phishing attempt. The severity of the damage is medium. The

	user opened a malicious email and opened attachments. The status is escalated. • **When** did the incident occur? January, 17th 2024 (1:20 pm) • **Where** did the incident happen? Financial Service Company. • **Why** did the incident happen? This happened as a result of an employee opening a malicious file and clicking a link from an unknown sender.
Additional notes	• Reported to Level 2 SOC Analyst.

Ticketing:

Ticket ID	Alert Message	Severity	Details	Ticket status
A-AD3CO	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket comments
The alert detected that an employee downloaded and opened a malicious file from a phishing email. The sender's name is too good to be true. The name is "Security IT team" and the email address is "kdfjlsfjdk@gmail.com". The email body and subject line contained grammatical errors. The email's body also contained a password-protected attachment, "bfsvc.exe," which was downloaded and opened on the affected machine. The alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.

Reflections/Notes for scenario 3:

- How many entries are there so far? Two entries.
- The type of security incident the organization was affected by is Phishing.
- The attacker used the email address as an attack vector to carry out the attack.
- Providing more training and education may solve the problems.