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: May 17, 2025	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Organized hacking group ● **What**: Ransomware attack ● **When**: Tuesday, 9:00am ● **Where**: Health care clinic ● **Why**: Attackers gained access through phishing emails containing malicious attachments that installed ransomware.
Additional notes	1. The phishing vector indicates a need for enhanced employee training and stricter email filtering. 2. How could the health care company prevent an incident like this from occurring again? 3. Should the company pay the ransom to retrieve the decryption key?

Reflections/Notes:

- This incident had immediate business impact and potential long-term legal/reputational consequences due to the healthcare nature and PII involvement.
- Urgent focus is on containment, eradication, and potential recovery strategies.
- Emphasis on identifying the exact ransomware variant and checking for publicly available decryption tools before considering ransom payment.
- Phishing remains a highly effective initial access vector, highlighting the need for robust email security and continuous employee training.

Scenario #2

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.

You retrieve the malicious file and create a SHA256 hash of the file. 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: May 20 2025	**Entry:** #1
Description	Investigate a suspicious file hash
Tool(s) used	I investigated a suspicious file hash using VirusTotal, a tool that scans files and URLs for malware. This analysis, conducted in the Detection and Analysis phase, confirmed the file was malicious.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown attacker • **What**: Malicious file attachment that contains the SHA256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **When**: It happened at 1.20pm, an alert was sent to the organization's SOC analyst after the IDS detected the file. • **Where**: an employee's computer at a financial services company.

	• **Why**: An employee has downloaded and executed a malicious file attachment via e-mail.
Additional notes	• The incident indicates a need for enhanced employee training and stricter email filtering. • How can this incident be prevented in the future?

Reflections/Notes:

- This incident highlights a potential gap in current email security controls for password-protected attachments or a need for stricter user training around opening such files from unknown sources.
- The quick execution by the user after downloading indicates good social engineering by the attacker.
- The priority now is to determine the scope of the compromise using VirusTotal and other forensic methods, and then proceed to containment and eradication.

Date: May 21 2025	**Entry:** #2
Description	A phishing email with sender inconsistencies, poor grammar, and a password-protected **bfsvc.exe** executable led to an alert. The employee downloaded and executed the file, which hash analysis confirmed as malicious. The incident has been escalated to a Level 2 SOC Analyst for further investigation and containment.
Tool(s) used	Use alert ticket
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown attacker • **What**: The employee downloaded and executed a malicious file (bfsvc.exe) from a phishing email. • **When**: It happened on May 20, 2025, 1.20pm. • **Where**: The event occurred on an employee's computer at a financial services company.

	• **Why**: The employee was deceived by a phishing email containing social engineering cues. The lack of user awareness and the ability to execute password-protected attachments led to successful execution of the malicious file.
Additional notes	• The sender's domain ("76tguy6hh6tgftrt7tg.su") is clearly suspicious and inconsistent with both the displayed name ("Def Communications") and the referenced contact ("Clyde West") • The subject line and body contained noticeable grammar errors - indication of phishing.

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	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. There is an inconsistency between the sender's email address "76tguy6hh6tgftrt7tg.su"" the name used in the email body "Clyde West," and the sender's name, "Def Communications." 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. Having previously investigated the file hash, it is confirmed to be a known malicious file. Furthermore, 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:

- This case highlights the ongoing challenge of user behavior as a security risk.
- We may need to review endpoint policies to restrict execution of **.exe** files from downloads and apply stricter scanning of password-protected attachments.
- A refresher phishing awareness campaign may be warranted, particularly for high-risk departments.

Scenario #3

The organization experienced a security incident on May 23, 2025, 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 May 23, 2025, 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 May 25, 2025, 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. Between May 25 and May 30, 2025, the security team concentrated on determining how the data was stolen and the extent of the theft.

Date: May 23 2025	**Entry:** #1
Description	Final analysis and closure of a data breach incident on May 23, 2025 involving unauthorized access to approximately 50,000 customer PII and financial records. Investigation and containment were executed via phishing incident response playbook.
Tool(s) used	phishing incident response playbook
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown external threat actor • **What**: Unauthorized access to internal data systems allowed the theft of approximately 50,000 customer records, including PII and financial information.

	• **When**: The breach is believed to have occurred between May 25 and May 30, 2025. The first extortion attempt was made on May 23, but the breach wasn't reported until the second email on May 25. • **Where**: The incident occurred within the organization's internal data repositories. • **Why**: The incident was likely a result of credential compromise, phishing, or exploitation of a misconfigured system. Lack of timely reporting and awareness by the employee contributed to delayed response.
Additional notes	• Further forensic investigation confirmed the unauthorized data access and full scope of affected records. • The initial extortion email on May 23 was deleted by the employee and not reported, missing an early opportunity to investigate. • Roughly $100,000 in damages, including direct costs and estimated loss of customer trust/revenue.

Reflections/Notes:

- The delayed reporting significantly impacted the organization's ability to contain the breach early.
- Employee training and internal incident reporting protocols need review and reinforcement.
- Endpoint and access monitoring should be improved, particularly for repositories containing sensitive customer data.
- This case highlights the importance of responding to even suspicious or vague threats with due diligence.
- Playbook will be updated to include specific workflow triggers for handling extortion-based breaches, as well as earlier employee phishing interaction analysis.
- The Playbook was useful in managing cross-functional coordination and ensuring no containment steps were missed.