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 jobs.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that the clinic'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 clicked.

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: July 23, 2025	**Entry:** #001
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: In this scenario, the organization first detected the ransomware incident. In the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident.
Tool(s) used	None were provided due to the first occurence
The 5 W's	• **Who caused the incident?** An organized group of unethical hackers • **What happened?** A ransomware security incident. Employees could not access their systems. A ransom note was displayed • **Where did the incident happen?** At a health care company • **When did the incident occur?** At 9:00am on Tuesday 23rd July, 2023 • **Why did the incident happen**? The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files and disrupting business operations. The attackers' are now demanding a certain amount of money to be paid to them.
Additional notes	1. The healthcare company could prevent a recurrence of such event by having investing in staff training and awareness of phishing mails. 2. It is unadvised for the company to pay the ransom because while it guarantees data recovery, it encourages further criminal activity

---

Scenario 2

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.

On January 20, 2024, at approximately 3:13 p.m. PT, an employee received an email from an external 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 sender emailed again with a sample of the stolen data and increased the payment demand to $50,000. The employee then notified the security team, who began their investigation into the incident.

Date: July 25 2024	**Entry:** #002
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	• **Who**: A malicious actor • **What**: 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 cryptocurrency**, 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. • **Where**: At an organization • **When**: Jan 23rd, 2024 • **Why**: Forced browsing attack to modify the order number and gain access to partner 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.

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 Indicators of Compromise (IoCs) that are associated with the file.

Date: July 27 2024	**Entry:** #003
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal; an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	• **Who**: An unknown malicious actor • **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: An employee's computer at a financial services company

	• **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	• **How to prevent this from happening?** Never download 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.

Reflections/Notes:

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

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

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

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used.

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

I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it really fascinating to be able to use tools to capture network traffic and analyze it in real time. I am definitely more interested in learning more.

Date: July 27 2024	**Entry:** #003
Description	Playbook to response 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	• **Who**: A malicious actor • **What**: Investigation revealed the ticket ID A-2703 was created. An alert message was generated and flagged a positive phishing attempt • **Where**: An employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Why**: An employee downloaded and executd a malicious file attachment via e-mail.
Additional notes	• Reported to Level 2 SOC Analyst

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 has downloaded a malicious file from their mail Upon receiving and investigating the alert; • There is an inconsistency in the sender's mail address (76tguyhh6tgftrt7tg.su). There is also a mismatch with their names (Def Communications and Clyde West). • On further investigation of the message body (and subject line) of the email, it contains grammatical errors, which can be an indication of a phishing attempt. • It has been identified that the email contains malicious attachments as determined by the reputation of the file attachment through its hash values. 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.