Incident handler's journal

Date: 4/19/2024	**Entry:** #1
Description	On Tuesday, at 9:00 am, a U.S healthcare clinic network fell victim to a sophisticated phishing attack orchestrated by unethical hackers. The attack commenced with the reception of a phishing email containing a malicious attachment, which, upon opening, surreptitiously installed malware on an unsuspecting employee's computer. Subsequently, the malware propagated throughout the company's network, encrypting critical files and rendering them inaccessible. The perpetrators then issued a ransom demand, seeking a substantial sum of money in exchange for the decryption key.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who**? organization group of unethicall hackers. ● **What**? The incident involved a phishing email carrying a malicious attachment that facilitated the installation of malware on an employee's computer, leading to the encryption of vital company files. This incident constitutes a ransomware attack. ● **When**? The attack occurred on Tuesday at 9:00 am. ● **Where**? The incident transpired within the confines of a healthcare company's network infrastructure. ● **Why**? The attack was committed via a phishing email, exploiting human vulnerabilities to gain unauthorized access to the company's network and encrypt sensitive files for ransom.
Additional notes	Employee education and awareness regarding potential cyber threats, particularly phishing emails, are essential to strengthening the company's defenses against future attacks.

	Implementing robust email filtering systems and conducting regular phishing simulation exercises can enhance employees' ability to identify and report suspicious emails promptly. Strengthening cybersecurity measures by implementing multi-layered defenses, including advanced threat detection mechanisms and endpoint protection solutions.

Date: 4/28/2024	**Entry: #2**
Description	On April 28, 2024, at 1:11 PM, an employee at a financial services company received an email containing an attached password-protected spreadsheet file. The employee, unaware of the malicious intent, proceeded to open the file using the provided password. Subsequently, a malicious payload embedded within the file was executed on the employee's computer, leading to the creation of multiple unauthorized executable files at 1:15 PM. At 1:20 PM, the intrusion detection system (IDS) flagged the presence of the executable files, triggering an alert to the Security Operations Center (SOC). As a SOC analyst, I promptly responded to the alert by creating the SHA256 hash of the file to uncover additional indicators of compromise (IoCs) associated with the malicious payload.
Tool(s) used	VirusTotal, a comprehensive tool known for its ability to provide detailed insights into the malicious nature of files, was utilized to analyze the SHA256 hash and collect valuable information about the nature and behavior of the malicious payload.

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was precipitated by an employee who unwittingly opened a malicious file sent by a hacker via email. ● **What** happened? Upon opening the file, a malicious payload was executed on the employee's computer, resulting in the creation of unauthorized executable files. ● **When** did the incident occur? ○ 1:11 PM: The employee received the malicious email. ○ 1:13 PM: The employee downloaded and opened the password-protected file. ○ 1:15 PM: Multiple unauthorized executable files were generated on the employee's computer. ○ 1:20 PM: The IDS detected the presence of the executable files, triggering an alert to the SOC. ● **Where** did the incident happen? The incident happened on the employee's work computer within the premises of the financial services company. ● **Why** did the incident happen? The incident occurred due to the employee's inadvertent action of downloading and opening the malicious file attached to the email.
Additional notes	1. Implement robust email security protocols, including email filtering and scanning mechanisms, to detect and block malicious attachments before they reach end-users' inboxes. 2. Employ endpoint protection solutions, such as antivirus software and advanced threat detection mechanisms, to proactively identify and mitigate the risks posed by malicious files and payloads. 3. Promptly remove any remnants of the malicious file from affected devices to prevent further exploitation or persistence of the threat

	within the network infrastructure.

Date: 4/28/2024	**Entry: #3**
Description	As a level-one Security Operations Center (SOC) analyst at a financial services company, I undertook the task of investigating and resolving an alert concerning a suspicious file that an employee had opened, as detailed in the previous journal entry.
Tool(s) used	The Phishing Playbook was employed to assist level-one SOC analysts in delivering an appropriate and timely response to phishing incidents.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was initiated by an employee, who opened a malicious file sent by a hacker via email. ● **What** happened? An attacker employed a phishing tactic by sending a deceptive email to the company's HR department. The email, purportedly from "Def Communications" with the sender's name as "Clyde West," contained numerous indicators of deception, including discrepancies between the sender's email address (76tguyhh6tgftrt7tg.su) and the name in the email body. Moreover, grammatical errors were evident in both the email's body and subject line. The email contained a password-protected attachment named "bfsvc.exe," which, when downloaded and opened by the recipient, led to the execution of a known malicious file. ● **When** did the incident occur?

	The incident occurred on July 20, 2022, at 9:30 AM. ● **Where** did the incident happen? The incident transpired at the employee's work computer, and the subsequent investigation was conducted at the SOC analyst's workstation. ● **Why** did the incident happen? The incident occurred due to the employee's unwitting action of downloading and opening the malicious file attached to the phishing email.
Additional notes	The company should prioritize providing comprehensive training programs for its employees to enhance their ability to discern and differentiate between legitimate emails and suspicious ones, thereby reducing the likelihood of falling victim to phishing attacks in the future.

Date: 4/29/2024	**Entry:#4**
Description	Upon receiving an alert, it was noted that an employee had received a phishing email in their inbox. The email contained a suspicious domain name, signin.office365x24.com. As a security analyst, my objective is to investigate whether other employees have also received phishing emails containing this domain or if any employee has visited the domain.
Tool(s) used	I utilized Chronicle, a Security Information and Event Management (SIEM) tool. Chronicle provides a comprehensive platform for collecting, analyzing, and reporting on data from various sources, making it a valuable asset for analysts in investigating security incidents.

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was instigated by a hacker who sent the phishing email. ● **What** happened? A suspicious domain name, signin.office365x24.com, was identified in the email body. ● **When** did the incident occur? N/A ● **Where** did the incident happen? The incident occurred within the email body. ● **Why** did the incident happen? The incident transpired as a result of a hacker's action in sending a phishing email.
Additional notes	To mitigate the risk of similar incidents in the future, it is imperative to educate employees on how to recognize and differentiate phishing emails from legitimate ones. Providing comprehensive training on cybersecurity awareness will empower employees to identify and report phishing attempts promptly, thereby reducing the likelihood of falling victim to such attacks.