Incident Handler's Journal

Date: April 17, 2023	**Entry:** #1
Description	Today, I encountered a cybersecurity incident involving a health care company. The incident was a ransomware attack carried out by an organized group of unethical hackers. The attackers gained access to the company's systems using a phishing attack, and once inside, they launched their ransomware, encrypting critical files. The motive behind this incident appears to be financial, as the attackers left a ransom note demanding a substantial sum of money in exchange for the decryption key.
Tool(s) used	None.
The 5 W's	**Who:** An organized group of unethical hackers. **What:** A ransomware security incident. **Where:** At a health care company. **When:** The incident occurred on Tuesday at 9:00 a.m. **Why:** The incident happened because unethical hackers were able to access th company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	To prevent a similar incident from occurring again, the health care company should consider implementing the following measures: 1. Employee training and awareness: Conduct regular cybersecurity training sessions to educate employees about phishing attacks and other common social engineering techniques. This will help employees recognize and report suspicious emails or activities.

	2. Strong email security measures: Implement email filters and spam detection systems to prevent phishing emails from reaching employees' inboxes. Additionally, use email authentication protocols like DMARC, SPF, and DKIM to verify the authenticity of incoming emails. 3. Multi-factor authentication (MFA): Enable MFA for all user accounts to add an extra layer of security. This will make it more difficult for attackers to gain unauthorized access even if they have stolen or guessed passwords. 4. Regular system patching and updates: Keep all software and systems up to date with the latest security patches and updates. This helps address known vulnerabilities that attackers could exploit. 5. Data backup and recovery: Regularly back up critical data and ensure the backups are stored securely and offline. This will allow the organization to recover the encrypted files without paying the ransom. Regarding whether the company should pay the ransom to retrieve the decryption key, it is generally not recommended. Paying the ransom does not guarantee that the attackers will provide the decryption key or that they won't launch further attacks. Additionally, it encourages criminal behavior and funds illegal activities. Instead, the company should focus on restoring systems from backups and working with incident response professionals to investigate the incident, mitigate the damage, and enhance the security measures to prevent future incidents.

Incident Handler's Journal

Date: May 13, 2023	**Entry:** #2
Description	As a member of the Buttercup Games e-commerce store, my current assignment involves evaluating potential security vulnerabilities associated with our mail server. Specifically, I have been tasked with investigating any instances of failed SSH logins for the root account. By thoroughly analyzing these failed login attempts, I aim to identify and address any potential security concerns within our mail server infrastructure.
Tool(s) used	Splunk
The 5 W's	**Who:** Employee/Malicious Actors spoofing as an Employee **What:** A ransomware security incident. **Where:** Butter Cup Games Servers **When:** N/A **Why:** Routine audit of security protocol to ensure maximum security
Additional notes	By leveraging the company-provided data, we conducted thorough SQL searches to detect any failed logins that might indicate the presence of a malicious actor. Regrettably, our analysis did not reveal any findings that could be deemed suspicious or indicative of malicious intent. To enhance our investigation, we will refine our search criteria, incorporate anomaly detection techniques, cross-reference data from multiple sources, and leverage threat intelligence feeds. Additionally, implementing real-time monitoring and collaborating with security experts will further bolster our ability to identify and mitigate potential threats.

Date: March 16, 2023	**Entry:** #3
Description	As an employee at a financial services company, I recently received an alert regarding a phishing email that was discovered in an employee's inbox. Upon reviewing the alert, I promptly identified a suspicious domain name within the body of the email: **signin.office365x24.com.** To ensure the safety and security of our organization, I embarked on an investigation to determine whether other employees have also received phishing emails containing this particular domain and if any of them have inadvertently visited the domain. This proactive approach will allow us to promptly address any potential threats and mitigate the risk of a successful phishing attack.
Tool(s) used	Chronicle
The 5 W's	**Who:** Employee email, Unknown Malicious Actor based in India **What:** Phishing email campaign **Where:** Headquarters Network **When:** May 4, 2023 - 9:02AM **Why:** The company possesses valuable intellectual property (IP) that may attrac the attention of foreign industry competitors.
Additional notes	After a comprehensive examination of the resolved IP, ET intelligence rep list, assets, and timeline pertaining to the security alert, our investigation confirms the presence of multiple compromised devices on the network. By closely analyzing the POST request, I successfully identified the machines that may have fallen victim to the phishing campaign. Subsequently, this discovery led me to uncover the IP address of the communicating server, which, upon further scrutiny, revealed additional suspicious domains associated with it. As a precautionary measure, the affected devices have been quarantined, while the IDS/IPS systems have been updated. Furthermore, we are actively developing new training programs to enhance

	employee awareness and resilience against sophisticated phishing campaigns.

Date: January 21, 2023	**Entry:** #4
Description	I am a level-one Security Operations Center (SOC) analyst at a financial services company. Recently, I received a phishing alert concerning a potentially harmful file that was downloaded onto an employee's computer. Taking immediate action, I conducted an investigation into the hash of the email attachment, and it was confirmed to be malicious. Now, armed with this crucial information, I am tasked with following my organization's established process to thoroughly investigate the incident and effectively resolve the alert in accordance with our organization's security policies and procedures.
Tool(s) used	None
The 5 W's	**Who:** Malicious Actor Impersonating a Job Seeker **What:** Medium Severity Phishing Alert **Where:** Email Infrastructure / Potential Impact on Main Network **When:** Wednesday, July 20, 2022 09:30:14 AM **Why:** Motivated by Disgruntled Employees, Competitors, or Potential Disruption by Nation States
Additional notes	Upon careful examination of the ticket, it has been unequivocally established that the sender is a malicious actor attempting to lure employees into opening a malicious file. Numerous inconsistencies have been identified, such as the email originating from a .su domain, grammatical errors evident in the body of the text, and, notably, the presence of a known and documented malicious file hash.

Reflection:

None of the activities were particularly challenging for me as the instructions provided, coupled with my technical experience, helped me successfully complete all the labs. However, my understanding of incident detection and response has evolved during the course. I now recognize the significance of properly configuring the parameters of the Intrusion Detection System (IDS) and Security Information and Event Management (SIEM). Without appropriate setup, one would find themselves constantly firefighting instead of proactively preventing incidents.

Among the tools and concepts explored, I found Splunk to be the most enjoyable. Its user-friendly graphical user interface (GUI) made it easy to navigate, and it efficiently parsed and correlated all the necessary information for making swift decisions. The convenience and comprehensiveness offered by Splunk's interface greatly enhanced my experience in incident detection and response.