**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:**  Record the date of the journal entry.  3/11/2024 | **Entry:**  Record the journal entry number.  1 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  A small U.S health care clinic had a security incident on Tuesday at 9:00 am that severely messed with their business operations due to a phishing email which contained a malicious attachment. When downloaded, the ransomware was released to encrypt the organization’s computer files. The unethical hackers also left a ransom note which states that the company’s files were encrypted and demanded money in exchange for the decryption key. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An organized group of unethical hackers * **What** happened? Several employees were not able to use their computers to access files like medical records. As a result of that, business operations had to shut down since the employees needed to access the files and software to do their job. * **When** did the incident occur? Tuesday morning, at approximately 9:00 am * **Where** did the incident happen? In a small U.S. health care clinic * **Why** did the incident happen? The ransom note was displayed on the employee’s computers by the organized group of unethical hackers and the note demanded a large sum of money in exchange for the decryption key since they also stated that they already encrypted all the company’s files. The attackers do it by sending the phishing emails to the employees of the company which contained a malicious attachment that installed malware on the employee’s computer once it was downloaded. Once there, they unleash their ransomware which encrypted critical files that make the company not be able to access critical patient data. It led to major disruptions in their business operations which forced the company to shut down their computer systems and contact several organizations to report the incident and receive technical assistance. | | |
| Additional notes | Include any additional thoughts, questions, or findings.  How are we going to prevent ransomware attacks from happening again so that the business does not lose their operations? | | |

| **Date:**  Record the date of the journal entry.  3/20/2024 | **Entry:**  Record the journal entry number.  2 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  There was an alert about a suspicious file being downloaded on an employee’s computer, which was an email containing an attachment that the employee received. The attachment was a password-protected spreadsheet and the spreadsheet’s password was provided in the email itself. The employee downloaded the file, and then entered the password to open the file. As soon as the employee opened the file, a malicious payload was executed into their computer. | | |
| Tool(s) used | List any cybersecurity tools that were used.  VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An advanced threat actor, BlackTech, used a file hash, known as the malware Flagpro, which caused the incident.   * **What** happened?   An employee received an email containing a file attachment, which the employee successfully downloaded and opened the file. Once there, multiple unauthorized executable files were created on the employee’s computer.   * **When** did the incident occur?   The incident occurred at 1:20 pm.   * **Where** did the incident happen?   The incident happens in a financial services company on an employee’s computer.   * **Why** did the incident happen?   The threat actor probably wanted to steal some money or some other important information from the employee’s computer because he chose to target a financial services company. | | |
| Additional notes | Include any additional thoughts, questions, or findings.  What can we do effectively and efficiently just to prevent another malicious attack from happening again? | | |

| **Date:**  Record the date of the journal entry.  3/20/2024 | **Entry:**  Record the journal entry number.  3 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  In response to the phishing attack of an employee’s computer being affected by a malicious actor with a downloadable attachment, we need to use the playbook in order to follow the organization’s process to complete the investigation and resolve the alert. The organization’s security policies and procedures describe how to respond to specific alerts, including what to do when receiving a phishing alert. | | |
| Tool(s) used | List any cybersecurity tools that were used.  Playbook | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   The sender’s name, “Def Communications”, has caused the incident.   * **What** happened?   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.  The incident occurred on July 20, 2022 at 09:30:14 AM.   * **Where** did the incident happen?   The incident happens in the Inergy Financial Services Company on an employee's computer.   * **Why** did the incident happen?   The threat actor probably wanted to steal some money or some other important information from the employee’s computer because he chose to target a financial services company. | | |
| Additional notes | Include any additional thoughts, questions, or findings.  It is good to use the playbook as a way to properly deal with the attack more effectively and efficiently so that we don’t make the attack escalate much worse than before. The malicious actors are extremely clever of how they really tricked users so we need to be more careful and calculative of how we truly deal with malicious attacks like this one. | | |

| **Date:**  Record the date of the journal entry.  3/20/2024 | **Entry:**  Record the journal entry number.  4 | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry.  At approximately 3:13 p.m., PT, on December 22, 2022, 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 December 28, 2022, 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 December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft. | | |
| Tool(s) used | List any cybersecurity tools that were used.  Web application access logs | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. * **What** happened?   The organization experienced a security incident on December 28, 2022, 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.   * **When** did the incident occur?   The incident occurred on December 28, 2022, at 7:20 p.m., PT.   * **Where** did the incident happen?   The incident happened at a mid-sized retail company on an e-commerce web application.   * **Why** did the incident happen?   The attacker wanted to get hold on customer personal identifiable information (PII) and financial information. | | |
| Additional notes | Include any additional thoughts, questions, or findings.  What kinds of vulnerability scans and penetration testing will be performed? | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

| Reflections/Notes: Record additional notes.  What surprised you the most about all the information about the incidents happening that were collected so far?  What surprised me is how the malicious actor was able to be smart and clever of how to truly deceive users from the downloadable attachment to the modification of a URL string to tamper with the customer’s order transaction.  Why can we not just prevent the attack from happening next time without having to follow the rules, policies, and procedures?  It does not work that way because malicious attackers are really clever and cunning so they will always come up with some ways to deceive the users. We need to follow rules, policies, and procedures just to effectively and efficiently prevent future cyber attacks from happening. |
| --- |