**Incident handler's journal- Natalie Sanchez**

|  |  |
| --- | --- |
| **Date:**  August 26, 2024 | **Entry:**  #1 |
| Description | A small U.S. health care clinic experienced a ransomware security incident on Tuesday at 9:00 AM which severely disrupted their business operations. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** - An organized group of unethical hackers caused the incident * **What**? A ransomware incident. * **When**? Tuesday at 9:00 AM * **Where**? At a small U.S. health care clinic * **Why**? The incident happened because a phishing email that contained a malicious attachment was downloaded, and ransomware was deployed encrypting the organization's computer files. The attackers left a ransom note demanding a large sum of money in exchange for the decryption key. |
| Additional notes | What are ways for the healthcare company to prevent an incident like this from occurring again.  Should the company pay the ransom to retrieve the key? |

|  |  |
| --- | --- |
| **Date:**  August 26, 2024 | **Entry:**  #2 |
| Description | An alert was received indicating that a suspicious file was being downloaded on an employee’s computer. The employee had received an email containing a password-protected spreadsheet file as an attachment. The password for the spreadsheet was provided in the email. The employee downloaded the file and entered the password to open it. Upon opening the file, a malicious payload was executed on their computer. |
| Tool(s) used | Virus Total Analysis |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The threat actor who sent the malicious email. * **What** happened? Multiple unauthorized executable files were created on the employee’s computer. * **When**? 1:13 PM * **Where**? Occurred on the employee’s computer within the financial services company’s network. * **Why**? To compromise the employee’s computer and potentially gain unauthorized access to sensitive information or disrupt operations. |
| Additional notes | The malicious file was identified and a SHA256 hash was created for further analysis.  Virus Total was used to uncover additional Indicators of Compromise (IoCs) associated with the file.  Has the employee’s computer been isolated from the network to prevent further spread of the malware?  Are there any other employees who received similar emails?  It might be beneficial to conduct a company-wide phishing awareness training to prevent similar incidents in the future. |

|  |  |
| --- | --- |
| **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. |

|  |  |
| --- | --- |
| **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. |