**Incident handler's journal**

**Instructions**

|  |  |
| --- | --- |
| **Date:**  1/10/2024 | **Entry:**  Entry #1 |
| Description | This cybersecurity incident shows a classic case of a ransomware attack. The hackers have encrypted file data and are asking for money in order to give back the decryption key. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **A group of hackers**   * **What** happened?   **A ransomware attack**   * **When** did the incident occur?   Tuesday at 9:00am (year not given)   * **Where** did the incident happen?   At a health care company   * **Why** did the incident happen?   **The incident occurred because of various emails being sent to the workers of this company and unbeknown to them, when downloading such files, the hackers were able to gain access to many of the sensitive files. After gaining access, the hackers encrypted the company’s critical files, and launched their ransomware attack. The attackers seem to be acting in a financially motivating way, for they are demanding a large sum of money in exchange for the decryption key.** |
| Additional notes | The health care company needs to inform/teach their employers about safety in technologies, and about the many protocols to prevent this from happening again. |

|  |  |
| --- | --- |
| **Date:**  1/17/2024 | **Entry:**  Entry #2 |
| Description | An employee downloaded a suspicious file, which when downloaded conducted a malicious payload to be executed on their computer. |
| Tool(s) used | Hash function/ Virus Total |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **Employee** * **What** happened? * **Employee received an email with an attachment, which they downloaded.** * **When** did the incident occur? * **At 1:13 PM (no direct date has been given)** * **Where** did the incident happen? * **At our financial services company** * **Why** did the incident happen? * **Employee downloaded a trojan file, which resulted in this IoC.** |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  1/17/2024 | **Entry:**  Entry #3 |
| Description | An employee received a potential phishing email. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **Employee downloaded an email attachment.** * **What** happened? * **The attachment contained a malicious file.** * **When** did the incident occur? * **July 20, 2022 at 9:30 AM** * **Where** did the incident happen? * **At our financial services company** * **Why** did the incident happen? * **The employee didn’t notice the grammatical errors in the subject line and message body.** |
| Additional notes | Additional security measures should be taught to prevent further situations like these. |

|  |  |
| --- | --- |
| **Date:**  1/24/2024 | **Entry:**  Entry #4 |
| Description | Using Chronicle to record the names and number of assets that have accessed the domain. |
| Tool(s) used | Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **6 Assets caused an incident: Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, Roger Spence** * **What** happened? * **There are multiple “GET/POST” requests which could be considered a successful phishing attempt on these individuals.** * **When** did the incident occur? * **The first documented incident started 01/31/2023** * **Where** did the incident happen? * **Port: Unknown** * **Why** did the incident happen? * These individuals may have not paid close attention to their accounts/ what URL’s they actually were assessing. |
| Additional notes | Resolved IPS for IP address 40.100.174.34  On the timeline it is evident that there are additional “POST” requests that suggest an asset has been phished.  There are additional assets compromised: Amir David, Warren Morris  Additional Domains associated with this IP address: signin.accounts-gooqle.com, signin.office365x24.com |

Reflection Entry:

1. Were there any specific activities that were challenging for you? Why or why not?
2. Has your understanding of incident detection and response changed since taking this course?
3. Was there a specific tool or concept that you enjoyed the most? Why?

There were not many especially challenging activities, the only challenging aspect of each activity was reviewing the data and recording short, but factual information for the handler’s Journal- to be a precise and short as possible.

My understanding of incident detection and response has expanded, and I am now more knowledgeable on how to review, and document incidents.

I enjoyed using VirusTotal the most, just because it was interesting to see how a certain malicious file could affect so many other companies, and the fact you are able to gather so much information is very foreign and exciting when using its functions.