**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  15/08/2025 | **Entry:**  1 |
| Description | Documenting a cybersecurity incident. |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organised group of unethical hackers. * **What**: A ransomware attack * **When**; on Tuesday, approximately at 9 am * **Where:** At a U.S. health care clinic specializing in delivering primary-care services * **Why**: The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. A ransom note was displayed on their computers which stated that all the company's files were encrypted and in exchange for restoring access to the encrypted files, a large sum of money was demanded for the decryption key. |
| Additional notes | * How can the company prevent such security incidents from happening in the future? * How will they resolve the issue that has happened now? |

|  |  |
| --- | --- |
| **Date:**  17/08/2025 | **Entry:**  2 |
| Description | Documenting a malware attack |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: a malicious actor * **What**: send an email that contained a malicious attachment to one of the employees computer * **When** : not specified * **Where**: the financial service where I work as an L1 SOC * **Why**: I received an alert about a suspicious file being downloaded on an employee's computer. It was discovered that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. |
| Additional notes | * Retrieved the malicious file and created a SHA256 hash of the file. * Used VirusTotal to uncover additional IoCs that are associated with the file. |

|  |  |
| --- | --- |
| **Date:**  17/08/2025 | **Entry:**  3 |
| Description | Documentation on investigating the malware attack. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: an email from ‘Def Communications’ in the name of Clyde West caused this incident. * **What**: a phishing email was send which contained a malicious attachment. * **When**: The email was sent at July 20, 2022 at 09:30:14 AM * **Where**: the incident occurred in one of the employee’s computer working at a financial service company * **Why**: The incident happened because the employee downloaded the attachment file named "bfsvc.exe" and then entered the password which resulted in a malware to enter into the computer. |
| Additional notes | * The sender email seemed to be impersonating a legitimate email, and was not matching with name given at the end. * The body of the message had a lot of grammatical errors. * The email also contained an attachment file which is a usual sign of phishing emails. |

|  |  |
| --- | --- |
| **Date:**  17/08/2025 | **Entry:**  4 |
| Description | Reviewing the final report of Post-incident Activity phase of the NIST Incident Response Lifecycle. |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: a malicious actor unknown to the company * **What**: An employee received an external email which 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 first email was ignored thinking it was a spam mail. But then 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. * **When**: First email was sent on December 22, 2022 approximately at 3:13 p.m. The second email was sent on December 28, 2022 to the same employee. * **Where**: The incident happened at a at a mid-sized retail company where I joined as a level-one security operation center (SOC) analyst. * **Why**: The incident happened due to vulnerability in the e-commerce web application which 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 allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. |
| Additional notes | * There was a single log source showing an exceptionally high volume of sequentially listed customer orders, which was found after analyzing the web server logs. * Perform routine vulnerability scans and penetration testing. (recommendation) * Implement routine vulnerability scan and access control mechanisms |

|  |
| --- |
| Reflections/Notes: Record additional notes.   * While writing this journal, I got to see what handling real cyber incidents feels like. There were different cases like ransomware and phishing, and reading about them made me realize how easy it is for attackers to fool people or get into systems. The way each incident was written using the “who, what, when, where, why” style really helped me understand what actually went wrong and what should’ve been done. * Some actions taken were simple—like checking the bad file in VirusTotal or looking closely at what happened in logs—and they actually helped to find out the root of the problem. Often, these problems started because someone clicked on a bad email or there was a weak spot in the web application. This journal made me realize that if we train people better and keep checking for weak spots, a lot of these problems can be stopped before they become very serious. * As a beginner, I found some parts of the instructions really hard to understand. There were times I felt confused or worried if I was doing things right because so many terms and steps were new for me. I realized I still need to learn a lot more, and I hope with practice and help, things will get easier over time. |