# Incident handler's journal

| **Date:**<br>January 9th, 2024 | **Entry:**<br>001 |
|---|---|
| Description | Cybersecurity Documentation |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who**: An organized group of malicious hackers<br>• **What**: Ransomware<br>• **When**: Tuesday, 9th of January, at 9:00 AM<br>• **Where**: Healthcare Company<br>• **Why**: Malicious actors were able to gain access to the company's system via email using a phishing attack. Using ransomware critical files were encrypted. The inherit cause for this malicious activity is fiscal as the hackers are demanding a large sum of money. |
| Additional notes | 1. Do we have any backup files or recovery plans in place?<br>2. Are the employees trained in recognizing social engineering attempts? If not, how can we develop training solutions in the future? |

---

| **Date:**<br>January 12th, 2024 | **Entry:**<br>002 |
|---|---|

| | |
|---|---|
| Description | Understanding the Pyramid of Pain and Prevention |
| Tool(s) used | Pyramid of Pain |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who**: A threat actor known as BlackTech<br>• **What**: A malicious attachment to a password protected spreadsheet file<br>• **When**: The moment (exact time not provided in scenario) when the file was downloaded and credentials entered by the employee<br>• **Where**: A Financial Services Company<br>• **Why**: Exact reason unknown, perhaps to compromise the employee's device and account, allowing the malicious actor remote access to the system. |
| Additional notes | 1. Is the device disconnected?<br>2. Is the account deactivated? Are there recovery plans in place for employee account compromise? |

---

| | |
|---|---|
| **Date:**<br>January 15th, 2024 | **Entry:**<br>003. |
| Description | Understanding how to respond to an incident using an organization's playbook |
| Tool(s) used | Playbook |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who**: "Clyde West" (pseudonym) and "Def Communications"<br>• **What**: Suspicious file download on an employee's computer |

| | |
|---|---|
| | • **When**: When the employee downloaded the file (unknown)<br>• **Where**: Financial Services Company<br>• **Why**: Gaining persistent access to user account and device via a password protected file. |
| Additional notes | 1. I have escalated the issue to a tier 2 SOC Analyst<br>2. I have responded to the incident by thoroughly following the organization's playbook |

---

| **Date:**<br>December 28th, 2022 | **Entry:**<br>004 |
|---|---|
| Description | Reviewing A Final Report |
| Tool(s) used | Organization's Record of A Final Report |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who**: Unknown Malicious Actor<br>• **What**: Data Breach by Forced Browsing Attack<br>• **When**: Incident began at 3:13 PM, 22nd of December<br>• **Where**: Retail Company<br>• **Why**: Attackers were able to gain access to customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. The attackers threatened to release the data if the ransom remained unpaid. |

| | |
|---|---|
| Additional notes | 1. From the final report I learned about an “allowlisting” method that limits the range of acceptable URL requests.<br>2. I learned about forced browsing attacks in general and gained an awareness of possible vulnerabilities. |

---

| | |
|---|---|
| **Date:**<br>January 18th, 2024 | **Entry:**<br>005 |
| Description | Gathering intelligence on a domain name using Chronicle |
| Tool(s) used | Google Chronicle (SIEM Tool) |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who**: Unknown actor associated with a credential drop site known as `signin.office365x24.com`<br>● **What**: Credential drop site linked in a phishing email<br>● **When**: N/A<br>● **Where**: Financial Services Company<br>● **Why**: The site is used receive and transmit log information or stolen credentials |
| Additional notes | 1. I learned how to view any related intelligence on a given domain name by navigating through Google Chronicle.<br>2. I learned what a drop site is. |

Reflections/Notes: In this portfolio project I have demonstrated a persistent ability to document my work and ask necessary questions while responding to various security incidents. I have also shown my ability to learn new things and document my findings as well.