**Incident handler's journal**

| **Date:**  10/9/24 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | This entry covers an incident with a small U.S. health care clinic that experienced a security incident involving ransomware on their critical files. | | |
| Tool(s) used |  | | |
| The 5 W's | * Who: Employees downloading malicious files * What: Ransomware encrypted critical files * When: Tuesday, 09:00 * Where: Organization network/devices * Why: Malicious attachments downloaded by employees | | |
| Additional notes | Lack of employee readiness seems to be the cause of this incident. Without them downloading the ransomware, there would be no security incident. | | |

| **Date:**  10/14/24 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | This entry covers an incident where a financial services company experienced a security incident involving phishing emails that downloaded executable files on an employees device | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | * Who: Employee downloaded malicious email attachment * What: Trojan email attachment * When: 1:11 pm - 1:20 pm * Where: Employee device * Why: File downloaded and password used on file | | |
| Additional notes | The VirusTotal Vendor Ratio found 60/73. The Community Score gave the hash value a -216. These two scores very likely indicate this file as malware. | | |

| **Date:**  10/14/24 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | This entry covers an incident involving a retail store that does 80% of their sales online. A malicious actor held customer data ransom. This data was collected through a website vulnerability by modifying an order number included in the URL text of a purchase confirmation page. | | |
| Tool(s) used | SIEM tools for log analysis | | |
| The 5 W's | * Who: Employee received ransom email * What: Website vulnerability * When: 12/22/22, 7:20 pm * Where: Website database * Why: Website vulnerability allowed forced browsing attack | | |
| Additional notes | The final report gives recommendations to secure the website vulnerability:   1. Perform vulnerability scans 2. Implement allowlisting to allow access to a specified set of URLs 3. Validate authentication of users to specific content | | |

| **Date:**  10/14/24 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Multiple login attempts failed for the mail server on an e-commerce store ‘Buttercup Games’. | | |
| Tool(s) used | Splunk | | |
| The 5 W's | * Who: No person in particular * What: Failed login attempts * When: 3/6/23, 1:39:51.000 am * Where: mailsv (Mail server) * Why: Login attempts failed outside of normal business hours | | |
| Additional notes | Events that occur outside of normal business hours can be an indicator of malicious activity. | | |

| Reflections/Notes:   * I found that the examples provided were very informative in using SIEM tools and analyzing logs to find security events. Entering in event information to record the specifics is an important skill and this exercise helped hone the ability to sufficiently document events. |
| --- |