**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

|  |  |
| --- | --- |
| **Date:** 6/18/2023 | **Entry: #1** |
| Description | Health care clinic ransomware attack |
| Tool(s) used | **Logs, Intrusion Detection System** |
| The 5 W's | Capture the 5 W's of an incident.  **Who:** The incident was caused by group of organized unethical hackers  **What:** The hackers sent a phishing email that downloaded ransomware to the organization’s computers, encrypting the files.  **When** did the incident occur? The incident happened on 9:00 AM Tuesday morning.  **Where** did the incident happen? The incident happened at the Health Care Clinic via the email servers.  **Why** did the incident happen? The organization left a ransom note that demands payment in exchange for the encryption key. It is likely this is a financially motivated attack. |
| Additional notes | Not recommended to pay ransom as there is not a guarantee that the business’s files will be unencrypted. Business operations were disrupted severely. Future plans to train employees on social engineering recommended. |

|  |  |
| --- | --- |
| **Date:** 6/18/23 | **Entry#2** |
| Description | Checking suspected malware’s SHA256 hash |
| Tool(s) used | **Virustotal** |
| The 5 W's | **Who:** Blacktech, suspected chinese cyberespionage group  **What:** Employee received an email containing a malicious attachment, which executed when opened. The hash value has been analyzed and found to be related to Flagpro, a known trojan/backdoor.  **When:** 1:11 PM is when the file was received. 1:13 PM was when the file was initially opened. At 1:15 PM the file began downloading the malicious files, likely because it was using pauses to try to decrease detectability.  **Where:** Employee’s computer, email attachment  **Why:** Backdoor; trojan malware, likely for use of stealing company secrets |
| Additional notes | Recommend changing naming rules of temporary files that Flagpro creates such as %TEMP%\~MY[0-9A-F].tmp, etc. We can also insert the investigation commands used by Flagpro can be flagged in the IDS/IPS. |

|  |  |
| --- | --- |
| **Date:** 6/19/23 | **Entry#3** |
| Description | Using Chronicle to scan a domain |
| Tool(s) used | Google Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: * **What**: Phishing scam using fake website portal * **When**: 01-31-2023 at 14:40:45 and 14:44:50 * **Where**: Domain signin.office365x24.com, signin.accounts-gooqle.com * **Why**: Phishing scam, gain unauthorized access to systems |
| Additional notes | POST requests to the login.php from ashton-davidson-pc, emil-palmer-pc, and warren-morris-pc indicate a successful phishing scam as POST requests usually mean information is sent from an endpoint to an external source. |