(Mock) Incident Handler’s Journal

A person touching a screen with a finger

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/31/24

**Table of Contents:**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Incident Handler’s Journal (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2-4**

**Scenario** - E1: Ransomware Attack

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

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. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

**Incident Handler’s Journal Entries**

|  |  |
| --- | --- |
| **Date & Time**: 01/30/24 @ 09:00:00 MST | **Entry Title**:  E1: Ransomware Attack |
| **Description** | Documenting an incident |
| **Tool(s) Used** | None |
| **The 5 W’s** | * **Who?**   Organized Group of Unethical Hackers   * **What?**   Phishing/Ransomware Attack   * **When?**   Tuesday morning at 9am MST   * **Where?**   Small US Healthcare Clinic – Company Database   * **Why?**   The threat actor group deployed ransomware on the company database hosting customer data, via a phishing campaign carried out on company employees, to extort the company for monetary gain in return for the decryption key |
| **Reflection Notes** | Poor email security awareness left the company vulnerable to phishing attacks and improper network segmentation allowed the threat actors to access other systems and install ransomware before being detected. |

|  |  |
| --- | --- |
| **Date & Time**: 1/30/24 @ 13:20:00 MST | **Entry Title**:  E2: IDS Alert |
| **Description** | Documenting an incident |
| **Tool(s) Used** | VirusTotal |
| **The 5 W’s** | * **Who?**   Unknown   * **What?**   Trojan Horse Attack   * **When?**   Tuesday afternoon at 1:11pm MST   * **Where?**   Financial Services Company – Employee Device   * **Why?**   Threat actor injected malicious code into an employee’s device to gain access to the device and likely the company network |
| **Reflection Notes** | Poor email security awareness left the company vulnerable to the trojan horse attack and improper training led to the employee accidentally delivering the payload by opening & unlocking the document. When the malware was hashed and scanned with VirusTotal it was identified as a known malicious code. |

|  |  |
| --- | --- |
| **Date & Time**: 1/30/24 @ 15:00:00 MST | **Entry Title**:  E3: NIDS Alert |
| **Description** | Documenting an event |
| **Tool(s) Used** | Wireshark |
| **The 5 W’s** | * **Who?**   IP Source 172.21.224.2   * **What?**   Suspicious Web-traffic   * **When?**   Tuesday afternoon at 3:00pm MST   * **Where?**   IP Destination 35.235.244.34, Destination Port 22   * **Why?**   Unknown IP had suspicious Web-traffic, so an alert was triggered |
| **Reflection Notes** | Through further analysis of the packets captured and analyzed using Wireshark, it appears the alert was a false-positive as the inspected packets didn’t show any signs of being malicious. Possibly look at adjusting signatures to account for this event and decrease false positives. |

|  |  |
| --- | --- |
| **Date & Time**: 1/30/24 @ 16:00:00 MST | **Entry Title**:  E4: NIDS Alert |
| **Description** | Documenting an event |
| **Tool(s) Used** | TCPDump |
| **The 5 W’s** | * **Who?**   IP Source 172.17.0.2, Source Port 46498   * **What?**   Suspicious Web-traffic   * **When?**   Tuesday morning at 4:00pm MST   * **Where?**   IP Destination 146.75.38.132, Destination Port 80   * **Why?**   Unknown IP had suspicious Web-traffic, so an alert was triggered |
| **Reflection Notes** | After an NIDS alert was triggered, TCPDump was used to capture live packets for analysis. After analysis, it appears the alert was a false-positive as the inspected packet traffic didn’t show any signs of being malicious. Possibly look at adjusting signatures to account for this event and decrease false positives. |