**Incident handler's journal**

| **Date:**  Sunday June 8th | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | We are going to analyze the following event:  A small U.S. healthcare clinic suffered a security incident on Tuesday at 9:00 a.m. that severely disrupted its business operations.  The cause of the security incident was a phishing email containing a malicious attachment. Once downloaded, ransomware was deployed, encrypting the organization's computer files.  An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanding money in exchange for the decryption key. | | |
| Tool(s) used | Using NIST Framework, to apply standards and prepare a response for the event, SIEM Tools, Wireshark to analyze network packets, Forensics tool to prevent encryption. Backup and recovery systems. | | |
| The 5 W's | * **Who** caused the incident?   The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.   * **What** happened?   An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key.   * **When** did the incident occur?   Tuesday morning at 9:00 AM.   * **Where** did the incident happen?   Small U.S health care clinic.   * **Why** did the incident happen?   A phishing email served as the initial point of entry into the clinic's systems.  A successful **social engineering attack (phishing)** led to the deployment of **ransomware**. | | |
| Additional notes | 1. How could the health care company prevent an incident like this from  occurring again?  2. Should the company pay the ransom to retrieve the decryption key?  3. ¿Any phishing training for the employers?  4. ¿Principle of least privilege on users?  5. ¿Backup strategy? | | |

| **Date:**  Thursday June 12th | **Entry:**  #2 | | |
| --- | --- | --- | --- |
| Description | Analyzing my first network packet with Wireshark and applying filters for specific searching.  In this activity, I was able to analyze network packets using Wireshark and learn what each section shown in the captured packet means. In this case, I was able to identify the following data:   * **No.**: The index number of the packet in this capture file * **Time**: The packet's timestamp * **Source**: The source IP address * **Destination**: The destination IP address * **Protocol**: The protocol contained in the packet * **Length**: The total length of the packet * **Info**: Some information about the packet data (the payload) as interpreted by Wireshark | | |
| Tool(s) used | Wireshark packet analyzer | | |
| The 5 W's | N/A | | |
| Additional notes | Filtering by transport protocol or by source and destination IP will provide us with more specific results and save us a lot of time when identifying suspicious activity. | | |

| **Date:**  Sunday June 15th | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Analyzing a hash that belongs to a Trojan named "trojan.flagpro/fragtor." In many systems where it's been detected, it appears as a "backdoor." It has been observed in companies such as McAfee, Malware Bytes, Google, Fortinet, and others.  It's a Win.exe executable, meaning it's a Windows executable. It runs on Windows systems, opening a backdoor in the system by making connections to external shells with other devices on the network. | | |
| Tool(s) used | In this analysis work, I have worked with VirusTotal. VirusTotal is a free online service that analyzes files and URLs for viruses, malware, and other threats using multiple antivirus engines. | | |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file * **Why**: An employee was able to download and execute a malicious file attachment via e-mail. | | |
| Additional notes | Security training for the employers? | | |

| **Date:**  Saturday June 21st | **Entry:**  #4 | | |
| --- | --- | --- | --- |
| Description | Use of Suricata to create signatures and alert rules for system intrusion detection. | | |
| Tool(s) used | Suricata, an open-source intrusion detection and prevention system (IDPS) that analyzes network traffic in real time using rules and signatures.  Thanks to Suricata, we have created alerts for packets from our network and external IPs that meet the established criteria. In this case, we were able to configure the following alert:  **alert http SHOME\_NET any -> SEXTERNAL\_NET**  **any (msg: "GET on wire";**  **flow: established, to\_server; content: "GET";**  **http\_method; sid:12345; rev:3;)**  It detects and generates an alert when a device on the internal network ($HOME\_NET) makes an HTTP request using the GET method to an external address ($EXTERNAL\_NET), as long as the connection is established and directed to a server. | | |
| The 5 W's | * N/A | | |
| Additional notes | Knowing how to use the eve.json and fast.log files is important for filtering data and obtaining relevant information. | | |

| Reflexion/notes | "**Were there any specific activities that challenged you? Why or why not?**"  For the moment, and based on our prior experience, we believe we're maintaining a good pace within the course, and we're completing the lessons without complications.  "**Has your understanding of incident detection and response changed since taking this course?**  I've improved my incident response capabilities; I've never had this much knowledge before about applying standards and preparing reports for real security issues.  "**Were there any specific tools or concepts that you liked best? Why?**"  In my opinion, Suricata is excellent for real-time threat detection on the network, while Splunk is superb for centralized data analysis and long-term security intelligence. |
| --- | --- |