**Incident handler's journal**

|  |  |
| --- | --- |
| Date:  10/13/2023 | Entry:  #001 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | * Who: Organized group of unethical hackers * What: A ransomware security incident * When: Tuesday 9:00 AM * Where: U.S. health care clinic specializing in delivering primary-care services * Why: An organized group of unethical hackers gained 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. they deployed their ransomware, which encrypted critical files. The also displayed Ransome note stating that all the company’s files were encrypted and in exchange for restoring access to the encrypted files, a large sum of money was demanded in exchange for the decryption key. |
| Additional notes | The group targeted Healthcare and transportation industries. |

|  |  |
| --- | --- |
| Date:  July 20, 2022 | Entry:  #002 (Ticket ID A-2703) |
| Description | Documenting a suspicious file hash |
| Tool(s) used | Virustotal, Phishing incident response playbook  For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more.  It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in  the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.  This incident occurred in the Detection and Analysis phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| 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 * When: Wednesday, July 20, 2022, 09:30:14 AM * Where: An employee's computer at a financial services company * Why: The Employee received an email from Def Communications <76tguyhh6tgftrt7tg.su> and the Ip is <114.114.114.114>. The subject line of the malicious email is Re: Infrastructure Engineer role. The attackers have attached the file and request the receiver to open it with the password. The file was downloaded on an employee’s computer. After investigation the file has been identified as malicious An employee was able to download and execute a malicious file attachment via e-mail. |
| Additional notes | This file was analyzed on Virustotal and 55 security vendors and 2 sandboxes flagged this file as malicious. The community score for this file is 55/72. The popular threat label for this file is trojan.flagpro/fragtor and the threat category as trojan.  The Case has been escalated. |

|  |  |
| --- | --- |
| Date:  December 28, 2022, at 7:20 PM | Entry:  #003 |
| Description | Documenting a data theft security incident |
| Tool(s) used | None |
| The 5 W's | * Who: vulnerability in the e-commerce web application. * What: The company experienced a major security incident involving a data breach of over one million users * When: At approximately 3:13 p.m., PT, on December 22, 2022, * Where: Mid-size retail company with physical store locations who conducts in e-commerce which account for 80% of its sales. * Why: A vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer 2 purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders. |
| Additional notes | To prevent future recurrences, we are taking the following actions:   * Perform routine vulnerability scans and penetration testing. * Implement the following access control mechanisms: * Implement allow listing to allow access to a specified set of URLs and automatically block all requests outside of this URL range. * Ensure that only authenticated users are authorized access to content. |

|  |  |
| --- | --- |
| Date:  March 6, 2023, at 1:38 AM | Entry:  #004 |
| Description | Documenting an unauthorized failed SSH logins for the root account |
| Tool(s) used | Splunk |
| The 5 W's | * Who: 194.8.74.23 port 3768. * What: A failed login attempts for the "root" user over SSH from IP address 194.8.74.23 on port 3768 for the mail server. * When: March 6, 2023, at 1:39:51 AM * Where: Mail server of Buttercup Games * Why: Multiple failed SSH logins for the root account.  rom IP address 194.8.74.23 on port 3768. The event occurred on a machine named "mailsv," and the log entry is sourced from a file named secure.log with the sourcetype labeled as "secure-2." |
| Additional notes | Multiple failed login attempts were made. Around 346 failed login attempts were found using Splunk. |

|  |  |
| --- | --- |
| Date:  Jan 31st, 2023 (UTC) 14:40:40 | Entry:  #005 |
| Description | Documenting a phishing incident |
| Tool(s) used | Google Chronicle |
| The 5 W's | * Who: Organization Kamtron Systems Pvt. Ltd. Domain Name: OFFICE365X24.COM * What: Employee received a phishing email in their inbox. * When: Jan 31st, 2023 (UTC) 14:40:40 * Where: Financial services company * Why: Received an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: signin.office365x24.com. Investigated the incident and found it Malicious. The score for the domain was 2/89 and 2 security vendors flagged this domain as malicious. |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| Date:  July 25 2024 | Entry:  #006 |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. |
| The 5 W's | * Who: N/A * What: N/A * Where: N/A * When: N/A * Why: N/A |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. |

|  |  |
| --- | --- |
| Date:  July 25 2024 | Entry:  #007 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Like Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic. |
| The 5 W's | * Who: N/A * What: N/A * Where: N/A * When: N/A * Why: N/A |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. |

|  |
| --- |
| Reflections/Notes:     1. Were there any specific activities that were challenging for you? Why or why not?   I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.     1. Has your understanding of incident detection and response changed after taking this course?   After taking this course, my understanding of incident detection and response has evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.     1. Was there a specific tool or concept that you enjoyed the most? Why?   I really enjoyed learning about network traffic analysis and applying what I learned through network protocol analyzer tools. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it really fascinating to be able to use tools to capture network traffic and analyze it in real time. I am more interested in learning more about this topic, and I hope to one day become more proficient in using network protocol analyzer tools. |