**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  06/16/2023 | **Entry:**  01 |
| Description | A U.S. health care clinic experienced a ransomware attack on Tuesday at 9:00 a.m. The next steps are to determine a response and a recovery. |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An organized group of unethical hackers. * **What:** 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. * **When:** Tuesday at 9:00 a.m. * **Where:** A small U.S. health care clinic. * **Why:** An organized group of unethical hackers wanted money. |
| Additional notes | * Demanded money in exchange for the decryption key. * Severely disrupted their business operations. * The company was forced to shut down their computer systems. * Employees were unable to access the files and software needed to do their job. * Should a ransom be paid? * Is there a way to recover without paying? * What should be done in the future to prevent this from happening again? |

|  |  |
| --- | --- |
| **Date:**  06/23/2023 | **Entry:**  02 |
| Description | A user may have opened a malicious email and opened attachments or clicked links. This may have been a possible phishing attempt, will investigate further to determine if this is the case. |
| Tool(s) used | Phishing Playbook ver. 1.0 |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114 **to** hr@inergy.com> <176.157.125.93 * **What:** Email with malicious links or attachments. 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. bfsvc.exe * **When**: July 20, 2022, 09:30:14 AM * **Where**: at a financial services company. * **Why:** to steal sensitive information or download malicious software or code on the recipient's device. |
| Additional notes | Email contains links or attachments; attachment has already been verified malicious. |

|  |  |
| --- | --- |
| **Date:**  06/23/2023 | **Entry:**  03 |
| Description | An individual was able to gain unauthorized access to customer personal identifiable.  information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Unknown threat actor via email. * **What**: The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it.   On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000.   * **When**: December 28, 2022, at 7:20 p.m., PT * **Where**: At a mid-sized retail company. * **Why**: Vulnerability in the e-commerce web application allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. |
| Additional notes | 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.  To prevent future recurrences, we are taking the following actions:   * Perform routine vulnerability scans and penetration testing. * Implement access control mechanisms: * Implement allowlisting 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:**  06/28/2023 | **Entry:**  04 |
| Description | Identifying any possible security issues with the mail server. Explore any failed SSH logins for the root account. Determining if the server has been compromised and or any vulnerabilities exist. |
| Tool(s) used | Splunk |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** “mailsv” or mail server device * **What:** Failed login attempt * **When:** 02/27/2023-03/06/2023 every day at 1:39:51 AM * **Where:** Multiple IPs on a variety of ports including 87.194.216.51, 187.231.45.62, 211.166.11.101, 67.133.102.54, 86.212.199.60, 193.33.170.23, 217.15.20.146, 233.77.49.94, 107.3.146.207, 128.241.220.82. * **Why**: Incorrect login info. |
| Additional notes | May be a possible brute force attack. Multiple failed login attempts from a large host of IPs on many ports for several days all at the same time down to the second. At the vary least these logins seem to be tool assisted as they are too fast to be a human typing. |

|  |  |
| --- | --- |
| **Date:**  06/28/2023 | **Entry:**  05 |
| Description | Received an alert that an employee received a phishing email in their inbox. Will investigate further to determine both the severity of the threat and if any machines have been compromised. |
| Tool(s) used | Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Six different host including ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc * **What:** ashton-davidson-pc and emil-palmer-pc seem to have been successfully phished. * **When:** 01/31/2023 at 14:41:10 * **Where:** signin.office365x24.com * **Why:** To steal user credentials. |
| Additional notes | signin.office365x24.com is a malicious domain specifically a drop site for logs or stolen credentials. |

|  |
| --- |
| Reflections/Notes: Record additional notes.   1. **Were there any specific activities that were challenging for you? Why or why not?**   The 4th journal entry caught me off guard. I didn’t immediately pick up on the odd nature of the failed login attempts. The timing and repetitive nature stood out to me after I had moved on from the activity causing me to go back and rewrite multiple sections. The instruction material didn’t outright say there was a problem which in hindsight I found quite enjoyable.   1. **Has your understanding of incident detection and response changed since taking this course?**   My understanding of detection and response has been greatly expanded upon. Before I assumed something along the lines of detection via logs, firewalls, and a response but nothing to specific beyond that. Learning about the frameworks has been a great help but, I must admit that they still feel very unfamiliar, and I use them in a sort of self-perceived clumsy way. I look forward to increasing my skills with in-depth practice in the future.   1. **Has your understanding of incident detection and response changed since taking this course?**   So far, I have enjoyed network structure and design the most followed by SQL(which I was looking forward to learning the most), Suricata, Wireshark, tcpdump, Splunk, Chronicle, Linux commands, and the threat actor mindset. as I have some experience and or familiarity with most of these and find them genuinely interesting, but I’d have to say I enjoyed Linux commands and SQL the most, as they seem both very practical with a wide range of uses even outside of the practice of cybersecurity. |