**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  10/02/2023. | **Entry:**  1 |
| Description | U.S. Healthcare clinic was attacked by ransomware via a phishing email attachment, using NIST Detection and Analysis guidelines. |
| Tool(s) used | No cybersecurity tools were used in this scenario. |
| The 5 W's | * A group of unethical hackers known to target organizations in the healthcare and transportation industries are responsible for this incident. * A ransomware attack encrypted critical files via a phishing email attachment. * The incident occured on a Tuesday morning at 9:00 A.M. * The incident occured at a small U.S. health care clinic specializing in primary-care services. * The incident happened for financial gain. |
| Additional notes | SPII may be compromised.  How could this incident be prevented in the future? |

|  |  |
| --- | --- |
| **Date:**  10/06/2023 | **Entry:**  2 |
| Description | Alert recieved about a suspicious file being downloaded on an employee's computer. Using NIST Detection and Analysis guidelines. |
| Tool(s) used | VirusTotal- An analyzer for suspicious files, domains, IPs and URLs to detect malware and other breaches. |
| The 5 W's | * An unknown malicious actor caused this incident. * A malicious file was sent to an employee, who opened it. * 10/06/2023 at 1:11 P.M. * The incident happened at where the employee worked. * The incident happened to exfiltrate data. |
| Additional notes | Retrieved the malicious file and created a SHA256 hash of the file. Used VirusTotal to verify malware, which is known as Flagpro |

|  |  |
| --- | --- |
| **Date:**  10/07/2023 | **Entry:**  3 |
| Description | HR member downloads malware from a phishing email. Using NIST Detection and Analysis guidelines. |
| Tool(s) used | VirusTotal- An analyzer for suspicious files, domains, IPs and URLs to detect malware and other breaches. |
| The 5 W's | * The incident was caused by the operator of the email address 76tguyhh6tgftrt7tg.su. The malware, Flagpro, was created by BlackTech APT group. * A .exe file was sent as an attachment to our HR department pretending to be a resume. * Incident happened on Wednesday, July 20th, 2022 at 9:30:14 AM * The incident happened in the HR office. * The reason the attack happened was to exfiltrate data. |
| Additional notes | Sender IP address: 114.114.114.114 Sender email address: 76tguyhh6tgftrt7tg.su, spoofed to Def Communications  Receiver's IP address: 176.157.125.93  Receiver's email address: hr@inergy.com  Message Body: contains "I am writing for to express..." and "There is attached my resume..." which are grammatical errors pointing to a phishing attempt.  Attachment: The attachment is an executable, which is not the format of a resume and cover letter.  As a level-one SOC analyst, The ticket has been updated and escalated to a level-two SOC analyst. |

|  |  |
| --- | --- |
| **Date:**  10/10/2023 | **Entry:**  4 |
| Description | As a level-one SOC analyst for a mid-sized retail company, I am tasked with reviewing the final report of a major incident using NIST Post-Incident Activity guidelines. |
| Tool(s) used | N/A |
| The 5 W's | * An unknown attacker caused the incident. * The attacker exploited 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 vulnerabiity allowed the attacker to access and exfiltrate PII. The attacker then contacted an employee and demanded payment in exchange for not posting the sensitive information online. * The incident occured on December 28, 2022 at 7:20 PM, PT * The incident happened somewhere in the company, not specified. * The incident happened for monetary gain. |
| Additional notes | The organization offered free identity protection services to the affected customers. |

|  |  |
| --- | --- |
| **Date:**  10/12/2023 | **Entry:**  5 |
| Description | Received a Chronicle alert about a phishing email. Using NIST Detection and Analysis guidelines. |
| Tool(s) used | SIEM tool Chronicle. |
| The 5 W's |  |
| Additional notes | Assets: ashton-davidson-pc  bruce-monroe-pc  coral-alvarez-pc  emil-palmer-pc  jude-reyes-pc  roger-spence-pc There are 6 POSTs to the /login.php page, suggesting a possible successful phish. In IP address 40.100.174.34, there is an additional asset, warren-morris-pc, and 3 POSTs  Result: office365x24.com is malicious. |

|  |
| --- |
| Reflections/Notes: Record additional notes.  Were there any specific activities that were challenging for you? Why or why not?  The activities were not challenging for me. Everything made sense as I was doing it. The way these activities are structured makes it so you are not out of your element when completing them.  Has your understanding of incident detection and response changed since taking this course?  I did not really understand what goes in to incident detection and response. I now know how in depth it really is.  Was there a specific tool or concept that you enjoyed the most? Why?  Ever since the beginning of the certification, I was being told about SIEM tools, and the general concepts relating to them. I was really excited to learn about splunk. At first glance, I thought that I would like to try to learn more about splunk than Chronicle, however, I really enjoy the GUI of Chronicle more than splunk. |