**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

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.

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry.  04/30/2024 | **Entry:**  Record the journal entry number.  1 |
| Description | Provide a brief description about the journal entry.  A small U.S. health care clinic experienced a security incident involving an organized group of unethical hackers that encrypted the company's files demanding a large sum of money in exchange for the decryption key. |
| Tool(s) used | List any cybersecurity tools that were used.  None yet |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   organized group of unethical hackers   * **What** happened?   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.   * **When** did the incident occur?   Tuesday morning 9:00 a.m   * **Where** did the incident happen?   Company’s network   * **Why** did the incident happen?   Employee downloaded and installed the malware that was in the email that was sent to him |
| Additional notes | Include any additional thoughts, questions, or findings.  A firewall should have been setup to filter suspicious emails |

You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.

Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert.

In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.

Ticket ID: A-2703 Alert Message: SERVER-MAIL Phishing attempt possible download of malware Severity: Medium Details: The user may have opened a malicious email and opened attachments or clicked links. Ticket status: Escalated

Ticket comments

Server-mail phishing attempt possible download of malware. A human resource employee from a financial services company downloaded an email attachment which was an executable that populated many others on the device. There is grammatical errors and misspellings including the company name. The attachment file is and executable whereas resumes are usually sent as pdf’s.

Additional information

Known malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:

From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 09:30:14 AM

To: <hr@inergy.com> <176.157.125.93>

Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West

Attachment: filename="bfsvc.exe"

|  |  |
| --- | --- |
| **Date:**  07/20/2022 | **Entry:**  #2 |
| Description | An employee from a financial services company downloaded an email attachment, put in the provided passkey, and executed a malicious payload that included harmful executables. |
| Tool(s) used | Intrusion detection system and file hashing SHA256 |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Human resource employee * **What** happened? Opened a suspicious email and downloaded the attachment, input the provided passkey, and harmful executables populated their computer. * **When** did the incident occur? 1:15 PM * **Where** did the incident happen? Inergy * **Why** did the incident happen? Employee was unknowledgeable with phishing when it comes to emails. Employee assumed it was a resume for a job position. |
| Additional notes | Employee needs training  There is grammatical errors and misspellings including the company name. The attachment file is and executable whereas resumes are usually sent as pdf’s. |

|  |  |
| --- | --- |
| **Date:**  12/22/2022 | **Entry:**  #3 |
| Description | An attacker was able to modify the URL string of a purchase confirmation page, access customer personal identifiable information and financial information, and used it as ransom against the company |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Vulnerability within e-commerce web application * **What** happened? By modifying the order number in a URL string of a purchase confirmation page, the attacker was able to preform a forced browsing attack and access customer transaction data * **When** did the incident occur? 3:13 PM * **Where** did the incident happen? Email * **Why** did the incident happen? Vulnerable application |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  03/06/2023 | **Entry:**  #4 |
| Description | Failed attempts at root account login |
| Tool(s) used | Splunk |
| The 5 W's | Capture the 5 W's of an incident.   * Numerous internet protocol addresses * Incorrect passwords * 1:39:51 am * Mail server * Someone trying to gain access to root account |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  06/17/2024 | **Entry:**  #5 |
| Description | Employee at a financial company received a phishing email |
| Tool(s) used | Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * Employees * Email contained suspicious domain signin.office365x24.com * February 01, 2023 * Email * Trying to steal credentials |
| Additional notes | Assets Timeline  Ashton-davidson-pc committed post  bruce-monroe-pc  coral-alvarez-pc  emil-palmer-pc committed post  jude-reyes-pc  roger-spence-pc  amir-david-pc  ashton-davidson-pc committed post  bruce-monroe-pc  coral-alvarez-pc  emil-palmer-pc committed post  jude-reyes-pc  roger-spence-pc  warren-morris-pc committed post  signin.accounts-gooqle.com  signin.office365x24.com |

|  |
| --- |
| Reflections/Notes: Record additional notes.  Were there any specific activities that were challenging for you? Why or why not?  No, everything was pretty much straight forward.  Has your understanding of incident detection and response changed since taking this course?  Yes, I have got to know more about the tools that are available like virus total, splunk, and chronicle.  Was there a specific tool or concept that you enjoyed the most? Why?  Both splunk and chronicle, how they were able to show verbose descriptions on issues. |