**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.

***Template example of journal entry***

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

**Start of Journal by Jonathan Alphonse**

|  |  |
| --- | --- |
| **Date:** 08/01/2023  Tuesday morning, 9:00 AM. | **Entry: #1** |
| Description | An incident occurred for a small U.S. health care organization where employee workstations were infected with ransomware as part of a sophisticated cyberattack done by an organized group of unethical hackers. The incident investigation is within the Detection and Analysis and Containment, Eradication, & Recovery of the NIST Incident Response Lifecycle. |
| Tool(s) used | NA |
| The 5 W's | * **Who** caused the incident?   + An organized group of unethical hackers known for targeting organizations in healthcare and transportation industries. * **What** happened?   + Several employees reported they were not able to use their computers to access work related files. A ransom note was displayed on their computers that the group responsible had encrypted the employee’s files and demanded a large sum of money in exchange for the decryption key to recover the data on infected computers. Business operations for the health care clinic were forced to shut down and disrupted because employees were unable to access files and software needed to do their jobs. * **When** did the incident occur?   + It was occurred early Tuesday morning and was reported on 9:00AM by the organization for technical assistance to respond to the incident. * **Where** did the incident happen?   + A small U.S. health care clinic specializing in delivering primary care services * **Why** did the incident happen?   + The cause of the incident was a phishing email containing a malicious attachment crafted by the hacker organization that deployed the ransomware when downloaded and opened by targeted employees that encrypted their files and made demands for money to return the files back to normal. |
| Additional notes | How can the organization prevent an incident like this from happening again?  Should the company pay the ransom to retrieve the decryption key?  Are there any tactics or controls in place to help the organization deal with mitigating and recovering from Ransomware attacks?  References:  [NIST Releases Tips and Tactics for Dealing With Ransomware | NIST](https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware) |

|  |  |
| --- | --- |
| **Date:**  08/04/2023  1:20 PM | **Entry: #2** |
| Description | This incident investigation stage is within the Detection and Analysis phase of the NIST Incident Response lifecycle. A suspicious file downloaded on an employee’s computer is investigated and analyzed to capture details and find indicators of compromise (IoCs) within the file which is called “bfsvc.exe". The file is retrieved and converted into a SHA256 hash for malware analysis. |
| Tool(s) used | * VirusTotal investigation tool to analyze SHA256 file hash of the malicious file * MalwareBazaar from abuse.ch to check malware sample and crowdsourced information on hash file. |
| The 5 W's | * **Who** caused the incident?   + A sender with the email address of 76tguyhh6tgftrt7tg.su and an IP address of 114.114.114.114   + A threat actor with access to previously reported malware called Flagpro used by the Chinese cyber espionage APT group or state actor hackers known as BlackTech. The group has primarily targeted organizations in East Asia (e.g. Taiwan, Japan, and Hong Kong) and English-speaking countries to compromise media, construction, engineering, electronics, and financial company networks. * **What** happened?   + The threat actor sent a spear phishing email with a password protected file attachment to an employee and the password to open the file in the same email. The employee downloads and opens the file with the password, multiple unauthorized executable files are created on the employee’s computer. * **When** did the incident occur?   + The incident occurred at 1:20PM, the time an intrusion detection system found the executable files and sent out the security alert to the organization’s SOC. The timestamps details leading to the event are in the additional notes of this journal entry. * **Where** did the incident happen?   + A financial services company based in the United States. * **Why** did the incident happen?   + The threat actor was able to trick the employee into downloading and executing the malware through a spearphishing email attempt based on their target organization and the presence of several unauthorized files from the downloadwere detected by an IDS in place and an alert was sent out to the organization’s SOC for investigation. |
| Additional notes | A timeline of the events leading up to this alert:   * 1:11 p.m.: An employee receives an email containing a file attachment. * 1:13 p.m.: The employee successfully downloads and opens the file. * 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. * 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.   **Email content**: *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"*  —-----------------------------------------------  The suspicious file’s filename: bfsvc.exe  The suspicious file’s SHA256 hash value: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b  VirusTotal and MalwareBazaar both score this file with negative community scores which means the file is indeed malicious. The executable is reported to be a type of Trojan malware.  Steps to resolution:   1. Update the alert ticket status from open to investigating 2. Review the phishing Playbook and flowchart in place 3. Determine if the link(s) or attachment(s) in the email are malicious 4. A summary of the findings are written based on the type of danger the links or attachments may be capable of. 5. Escalated the status of the ticket based on danger posed by email attachment.   Links for reference  [Flagpro: The new malware used by BlackTech | NTTセキュリティテクニカルブログ (security.ntt)](https://jp.security.ntt/tech_blog/102hf3q)  [Flagpro, Software S0696 | MITRE ATT&CK®](https://attack.mitre.org/software/S0696/)  [BlackTech, Palmerworm, Group G0098 | MITRE ATT&CK®](https://attack.mitre.org/groups/G0098/)  File Analysis results  [VirusTotal - File - 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b](https://www.virustotal.com/gui/file/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/summary)  [MalwareBazaar | SHA256 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b (BlackTech) (abuse.ch)](https://bazaar.abuse.ch/sample/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/#iocs) |

|  |  |
| --- | --- |
| **Date:**  December 28, 2022, at 7:20 p.m., PT, | **Entry: #3** |
| Description | An organization experienced a security incident in which an individual was able to gain unauthorized access to customer PII and financial information by using forced browsing to exploit a vulnerability in the organization’s e-commerce web application. The incident investigation is within the Containment, eradication, and recovery, and Post-incident phases of the NIST Incident Response Lifecycle. |
| Tool(s) used | * Web application and web server access logs associated to the incident for investigation. * Incident final report for reference |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An individual used an external email address to contact an employee two times claiming they have customer data and made demands for payments to ensure the customer data is leaked on public forums. This individual had knowledge of a zero day vulnerability on the organization’s ecommerce application that allowed the theft of customer PII and financial information. * **What** happened?   + An individual using an external email address sent two emails to an employee claiming they have possession of stolen customer data. The first time they demanded ransom of 25,000 USD cryptocurrency payment on at 3:13 p.m., PT, on December 22, 2022. a couple days later on December 28, 2022, the individual included a sample of the stolen customer data and an increased payment demand of 50,000 USD which prompted the employee to notify the security team * **When** did the incident occur? On December 28, 2022, at 7:20 p.m., PT, * **Where** did the incident happen? a mid-sized retail company. * **Why** did the incident happen? A 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 in the affected e-commerce web application. The attacker was able to access customer purchase confirmation pages that exposed customer data which the attacker then collected and exfiltrated. |
| Additional notes | **Response and remediation** The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.  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. **Recommendations** To prevent future recurrences, we are taking the following actions:   * Perform routine vulnerability scans and penetration testing. * Implement the following 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:**  3/6/23  6:24:02.000 PM | **Entry:** #4 |
| Description | The possiblilty of security issues with an organization’s mail server are investigated and am analysis is conducted for any failed SSH logins for the root account on the mail server. The incident investigation occurred within the Detection and Analysis phase of the NIST Incident Response Lifecycle. |
| Tool(s) used | * Splunk Cloud SIEM tool * ZIP file containing relevant information in the time range and relevant to the incident: financial transactions, access, and authentication data logs |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Possible password brute force attacks on several system user’s accounts from various * **What** happened? A large volume of failed SSH login attempts on the root account of the mail server and an investigation is conducted for any possible security issues * **When** did the incident occur? 8 days straight Between 2/27/23-3/6/23 and at the same time of 1:39:51.000 AM * **Where** did the incident happen? At the e-commerce store Buttercup Games * **Why** did the incident happen? Failed logins from many different IP addresses and port numbers for the past couple days occurring around the same time and out of the normal business hour time |
| Additional notes | **Network hosts from which each event originated**   * **mailsv** - Buttercup Games' mail server. Examine events generated from this host. * **www1** - One of Buttercup Games' web applications. * **www2** - One of Buttercup Games' web applications. * **www3** - One of Buttercup Games' web applications. * **vendor\_sales** - Information about Buttercup Games' retail sales.   **Source file where the events originate from**  **tutorialdata.zip:./mailsv/secure.log**  Steps   1. Narrow the search results for events from the mail server, **mailsv**    1. Under SELECTED FIELDS, click or enter host and mailsv. The complete search term added to the search bar is now: **index=main host=mailsv** . The search results have narrowed to over 9000 events that are generated by the mail server. 2. Search for a failed login for root    1. Enter **index=main host=mailsv fail\* root** into the search bar. This search expands on the search from the previous task and searches for the keyword **fail\***. The wildcard tells Splunk to expand the search term to find other terms that contain the word *fail* such as *failure*, *failed*, etc. Lastly, the keyword **root** searches for any event that contains the term root. The search results show about 346 failed loggin attempt events for the root account on the mail server 3. Look for any anomalous behavior   Around the same times, sessions for the root account are being opened using the sudo su command by the following users: nsharpe, djohnson, and myuan to switch to the root user. The owners of these accounts will need to be reached asap for the actions found with in the logs for the following that shows sudo commands being invoked to determine if account compromise from a malicious hacker, unintentional reasons, or foulplay.  Thu Mar 06 2023 01:39:51 mailsv1 sudo: djohnson ; TTY=pts/0 ; PWD=/home/djohnson ; USER=root ; COMMAND=/bin/su  References: [Follow-along guide for Splunk sign-up | Coursera](https://www.coursera.org/learn/detection-and-response/supplement/Wg478/follow-along-guide-for-splunk-sign-up) |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

|  |
| --- |
| Reflections/Notes: Record additional notes.  Were there any specific activities that were challenging for you? Why or why not?  The most challenging activities for me was in incident entry #4 with getting access to my Splunk Cloud instance so I can set up the test environment. I also had some difficulties with providing too much information at times for all my incident journal entries and making sure I kept my log entries short but informative and with resource insights.  Has your understanding of incident detection and response changed since taking this course?  It has grown to be much more greater understanding with getting to do the hands-on challenges provided within the course to test what I have learned. It made me challenge myself and got me out of my comfort zone in a good way to show the work a cybersecurity professional does and get experience  Was there a specific tool or concept that you enjoyed the most? Why?  I really loved and enjoyed using the VirusTotal and MalwareBazaar to investigate a suspicious email attachment to determine if it was malicious or not. It really sparked alot of interest in me as I found threat hunting to be just like being a cyber detective looking for clues within a case and to leave no stone unturned in making a final decision of if there is a possible threat. It felt to me like a treasure hunt but with the twist of keeping organization systems as well myself safe from malicious attempts to attack or disrupt computer systems and networks. I was always fascinated with malware analysis in general and learning how malware can be used to attack and compromise systems and to find ways to stop them. |