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.

Date:

2023-05-24

Entry:

0001

Description

The journal entry describes a security incident that occurred at a small U.S. healthcare clinic specializing in primary care services. The incident resulted in a significant disruption to the clinic's business operations due to the encryption of their computer files by ransomware deployed through a phishing email. The clinic received a ransom note demanding a large sum of money in exchange for the decryption key.

Tool(s) used

The specific cybersecurity tools used in this scenario are not mentioned. However, to prevent and mitigate such incidents, organizations typically employ a range of cybersecurity tools and measures. These may include antivirus software, firewalls, intrusion detection systems (IDS), email security filters, endpoint protection, and security awareness training for employees.

The 5 W's

1. Perpetrators: The incident was caused by an organized group of unethical hackers. The scenario mentions that these hackers are known to target organizations in healthcare and transportation industries. The specific identity or motive of the hackers is not provided.

2. Incident Details: The incident involved the deployment of ransomware on the clinic's computer systems, encrypting critical files. Employees were unable to access their computers, leading to a shutdown of business operations. The clinic received a ransom note that confirmed the encryption and demanded a large sum of money for the decryption key.

3. Time of Incident: The incident occurred on a Tuesday morning at approximately 9:00 a.m.

4. Location of Incident: The incident occurred within the network and computer systems of the healthcare clinic.

5. Cause of Incident: The incident was caused by targeted phishing emails that were sent to several employees of the clinic. These phishing emails contained a malicious attachment, which, when downloaded, installed malware on the employee's computer. The attackers gained access to the clinic's network through this malware and proceeded to deploy the ransomware, encrypting the company's files.

Additional notes

It is crucial for organizations to have robust cybersecurity measures in place to mitigate the risks associated with phishing attacks and ransomware. Employee education and awareness regarding phishing emails can help prevent such incidents. Regular backups of critical files are also important to ensure that data can be recovered in case of a ransomware attack.

Date:

2023-05-25

Entry:

0002

Description

An employee's computer was infected with malware after opening a password-protected spreadsheet file that was attached to an email. The file, when opened, executed a malicious payload on the user's computer.

Tool(s) used

Cybersecurity tools used include network traffic analysis tools, file hash generators (for SHA256 and MD5), sandbox environment for file behaviour analysis, and MITRE ATT&CK® framework for TTPs identification.

The 5 W's

1. Who caused the incident? The incident was caused by an unknown threat actor who sent the malicious email to the employee.

2. What happened? The employee downloaded and opened a malicious file attached to an email, leading to the execution of malware on their system.

3. When did the incident occur? The specific time of the incident would be mentioned here. As it isn't mentioned in your scenario, let's assume it occurred at 10:15 AM on 2023-05-25.

4. Where did the incident happen? The incident occurred on an employee's computer within our company's network.

5. Why did the incident happen? The incident happened because of successful spear-phishing: the attacker sent a seemingly harmless spreadsheet, which contained a hidden malicious payload, and the employee opened it.

Additional notes

The incident suggests a lack of awareness regarding email security and safe internet usage among employees. It is recommended to conduct an employee cybersecurity training program emphasizing the dangers of downloading and opening unexpected email attachments, even if they appear to come from known senders. Further, endpoint security solutions should be evaluated for their effectiveness in detecting such malicious activities. The specifics of the malware (hash values, IP, domain, etc.) have been documented for future reference and are being used to update our security controls and to aid in the investigation.

Date:

2023-05-25

Entry:

0003

Description

A phishing alert was received indicating that a malicious file (bfsvc.exe) was downloaded onto an employee's computer via an email from a suspicious source. The file's hash value has been confirmed as malicious.

Tool(s) used

Email security gateway, Endpoint detection and response (EDR) solution, hash analysis tools, and SIEM for alert correlation and event logs.

The 5 W's

1. Who caused the incident? The incident was initiated by an unknown threat actor operating under the alias "Clyde West" and the email address 76tguyhh6tgftrt7tg.su.

2. What happened? The employee received a phishing email and downloaded the attachment named "bfsvc.exe", which has been confirmed as a malicious file.

3. When did the incident occur? The incident occurred on Wednesday, July 20, 2022, at 09:30:14 AM, when the phishing email was received and the malicious attachment was presumably downloaded.

4. Where did the incident happen? The incident happened on an employee's computer within the company's network, with the email sent to hr@inergy.com.

5. Why did the incident happen? The incident happened due to successful spear-phishing: the attacker sent a seemingly harmless email under the guise of a job application, which contained a malicious file. The file was downloaded and likely executed by the employee.

Additional notes

The identified file hash will be used to search across other systems to see if any other endpoints have been compromised with the same file. The email headers will be examined to glean more information about the origin of the attack. It's recommended to isolate the affected machine from the network for a more detailed forensic analysis, and to avoid potential lateral movement of the malware. Security awareness training should be reiterated, with a focus on the risks of downloading and opening unsolicited email attachments. The incident will be escalated to level-two analysts for deeper investigation and remediation.

Date: 2023-05-25

Entry: 0004

Description

Review of a major security incident that occurred on December 28, 2022, involving a data breach of the company's e-commerce web application. Unauthorized access was gained to customer PII and financial information due to a vulnerability in the web application.

Tool(s) used

Web application vulnerability scanner, web server logs, penetration testing tools, email security tools, and security information and event management (SIEM) system.

The 5 W's

1 Who caused the incident? The incident was initiated by an unknown external threat actor.

2 What happened? A vulnerability in the e-commerce web application was exploited, enabling the attacker to access and exfiltrate customer PII and financial information.

3 When did the incident occur? The security incident occurred on December 28, 2022, at 7:20 p.m., PT.

4 Where did the incident happen? The incident happened on the company's e-commerce web application.

5 Why did the incident happen? The incident happened due to a vulnerability in the web application that allowed the attacker to perform a forced browsing attack.

Additional notes

After confirming the vulnerability, the company informed the affected customers and offered free identity protection services. As a future course of action, the company is implementing routine vulnerability scans and penetration testing, and enhancing access control mechanisms to prevent unauthorized access to content. The incident underscores the importance of regular and thorough vulnerability assessments of all public-facing applications to mitigate the risk of similar breaches in the future. Additionally, this incident also underlines the need for training employees to recognize and report suspicious emails promptly.

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.

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.

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.

Q: Were there any specific activities that were challenging for you? Why or why not?

A: The initial activity was the most challenging - if only because it involved reformatting the events of the incident into a new format.

Q: Has your understanding of incident detection and response changed since taking this course?

A: Yes, I have gained a better understanding of the systematic way in which incidents are detected, triaged, and and addressed by security teams.

Q: Was there a specific tool or concept that you enjoyed the most? Why?

A: I found the technical tools the most interesting (Suricata, Splunk, and Chronicle), they offer a depth of information and analysis that is incredibly helpful.