Incident Handler's journal

Date: 3/13/2024	**Entry:** 1
Description	Initial incident journal entry for the security incident at the U.S. healthcare clinic.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? **-** An organized group of unethical hackers targeted the health care clinic. • **What** happened? - The clinic's computer systems were infected with ransomware, encrypting critical files and disrupting business operations. • **When** did the incident occur? - The incident occurred on a Tuesday at 9:00 a.m. • **Where** did the incident happen? - The incident happened at a small U.S. healthcare clinic specializing in primary-care services. • **Why** did the incident happen? - The incident occurred due to employees downloading a malicious attachment from phishing emails sent by the hackers.
Additional notes	1. Did the clinic have a response plan in place for such incidents, and if so, how was it executed? 2. How could the healthcare company prevent an incident like this from occurring again? 3. Should the company pay the ransom to retrieve the decryption key? 4. What steps can be taken to improve employee awareness and training regarding phishing attacks? 5. Are there legal and regulatory implications for the clinic regarding patient data privacy and ransomware payments?

Date: 3/16/2024	**Entry: 2**
Description	Tracking security incidents, including the investigation and analysis of a suspicious file download leading to malware, using SHA256 hashing and VirusTotal for IoC discovery.
Tool(s) used	**VirusTotal website**
The 5 W's	Capture the 5 W's of an incident. • **Who caused the incident?** An employee received a suspicious email attachment. • **What happened?** The employee downloaded a password-protected spreadsheet and executed a malicious payload. • **When did the incident occur?** Timeline: 1:11 p.m. - Email received, 1:13 p.m. - File downloaded, 1:15 p.m. - Malicious program executed. • **Where did the incident happen?** On the employee's computer at the Financial service company. • **Why did the incident happen?** Due to the employee opening a malicious attachment from an email.
Additional notes	• The file hash has been reported as malicious by over 50 security vendors. • The file hash corresponds to the malware Flagpro. This is commonly used by the group BlackTech. • 57 out of 71 security vendors and 3 sandboxes flagged the file as malicious. • Threat labels include trojan.flagpro/fragtor, indicating a trojan malware family.

Date: 3/18/2024	**Entry: 3**
Description	Investigating potential phishing incident involving a suspicious email attachment.
Tool(s) used	Security incident tracking system, and threat intelligence tools.
The 5 W's	Capture the 5 W's of an incident. • **Who**: An employee who opened a phishing email and downloaded a malicious attachment. From Unknown sender (Def Communications). • **What**?: The employee opened a password-protected attachment named "bfsvc.exe" from an email impersonating "Def Communications." • **When**?: Wednesday, July 20, 2022, at 09:30:14 AM. • **Where**?: Email sent to hr@inergy.com. At the employee's computer within the organization's network. • **Why**?: The incident occurred due to the employee falling victim to a phishing email containing a known malicious file. Attempted phishing attack to deliver malware via email attachment.
Additional notes	1. Identified known malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. 2. Email sender details indicate potential impersonation (Def Communications). 3. Attachment is password-protected, indicating potential malicious intent. 4. Reviewed alert details, and identified inconsistencies in the sender information, and grammatical errors in the email. 5. Confirmed the malicious nature of the attachment through file hash analysis. 6. Escalated the incident to level-two SOC analyst for further investigation and response.

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.