Incident handler's journal

CyberCrab™ – Advanced Threat Defense

Security Analyst Name: Sunay Sabriev

Date: August 16, 2025	Entry: #1
Description	This journal entry documents a ransomware attack on a small U.S. health care clinic, which disrupted business operations by encrypting critical files, including medical records, following a phishing email campaign.
Tool(s) used	None specified in the scenario. Potential tools for investigation (e.g., antivirus software, network monitoring tools) were not mentioned.
The 5 W's	Capture the 5 W's of an incident. • Who caused the incident? An organized group of unethical hackers targeting healthcare and transportation industries. • What happened? A ransomware attack encrypted the clinic's files, rendering them inaccessible, and a ransom note demanded payment for a decryption key. • When did the incident occur? Tuesday morning at approximately 9:00 a.m. • Where did the incident happen? At a small U.S. health care clinic specializing in primary-care services. • Why did the incident happen? The attackers gained access through phishing emails with malicious attachments that installed malware when downloaded by employees.
Additional notes	The clinic's lack of robust email filtering or employee training on phishing may have contributed to the incident. Further investigation is needed to determine the specific ransomware variant and the extent of data compromise.

Date: September 14, 2025	**Entry:** #2
Description	This journal entry documents the investigation of a phishing alert received regarding a suspicious email with a malicious attachment. The investigation follows the organization's Phishing Playbook to evaluate the alert, confirm the malicious nature of the attachment, and escalate the ticket appropriately.
Tool(s) used	• VirusTotal (for file hash analysis) • Email analysis tools (to evaluate sender, receiver, and message details)
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The sender, claiming to be "Clyde West" from "Def Communications," using the email address and IP address 114.114.114.114. • **What** happened? A phishing email was sent to hr@inergy.com with a malicious attachment (bfsvc.exe) that was verified as malicious based on its file hash. • **When** did the incident occur? The email was sent on Monday, Stepmber 15, 2025, at 09:30:14 AM. • **Where** did the incident happen? The incident occurred on the recipient’s email system at hr@inergy.com, associated with IP address 176.157.125.93. • **Why** did the incident happen? The incident likely occurred to deliver malicious software via the attachment, potentially to steal sensitive information or gain unauthorized access to the recipient’s system.

Additional notes	The email contains several red flags indicating a phishing attempt: 1. The sender's email address (<76tguyhh6tgftrt7tg.su>) is suspicious and does not match the claimed identity ("Def Communications"). 2. The message body contains a grammatical error ("for to express"), which is common in phishing emails. 3. The attachment (bfsvc.exe) is an executable file, which is unusual for a job application and was confirmed malicious via its hash. Further investigation by a level-two SOC analyst is recommended due to the confirmed malicious nature of the attachment.