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.