









Incident handler's journal

 Date: July 4th, 2025	 Entry#: 001
 Description	<p>At approximately 9:00 a.m. on Tuesday, a small American healthcare clinic specializing in primary care services experienced a significant cybersecurity incident that severely disrupted its business operations. Multiple employees reported being unable to access essential files, such as medical records, due to system inaccessibility.</p> <p>Shortly after, ransom notes appeared on affected systems, indicating that all organizational files had been encrypted. The note was attributed to a known organized cybercriminal group that frequently targets entities in the healthcare and transportation sectors. The attackers demanded a substantial ransom payment in exchange for the decryption key.</p> <p>Initial investigation revealed the attack was initiated through a targeted phishing campaign. Several employees received emails with malicious attachments. Upon downloading these attachments, malware was installed on their machines, allowing the attackers to infiltrate the clinic's network. Ransomware was then deployed to encrypt critical data across systems.</p> <p>The incident forced the clinic to shut down its IT infrastructure temporarily and contact external cybersecurity partners and law enforcement for support.</p>
 Tools Used During the Incident	<p>The specific cybersecurity tools active during the incident were not disclosed. However, based on the attack vector and the impact, it is evident that several critical defense mechanisms were either absent or ineffective.</p>

 The 5 W's of the Incident	<ul style="list-style-type: none"> Who caused the incident? A known organized group of unethical hackers that frequently targets the healthcare and transportation sectors. What happened? A phishing email containing a malicious attachment was sent to multiple employees. Once opened, the attachment installed malware, granting attackers access to the clinic's network. Ransomware was deployed, encrypting sensitive files and disrupting operations. When did the incident occur? On a Tuesday morning at approximately 9:00 a.m. Where did the incident occur? In a small U.S.-based healthcare clinic specializing in primary care services. Why did the incident happen? The attackers exploited human error through phishing, taking advantage of weak email security controls and insufficient employee training. The downloaded malware provided access to internal systems, enabling the deployment of ransomware.
 Additional Notes & Recommendations	<p>Security Tools That Should Have Been in Place:</p> <ul style="list-style-type: none"> Endpoint Detection and Response (EDR)/Antivirus: To detect and block malware once downloaded. Email Security Filters (Anti-Phishing): To prevent malicious emails from reaching users' inboxes.

	<ul style="list-style-type: none">● Firewall and IDS/IPS (Intrusion Detection/Prevention Systems): To monitor and flag suspicious network activity.● Backup Solutions (Cloud or Offline): To ensure data recovery in the event of encryption or destruction.● SIEM (Security Information and Event Management): For real-time threat detection and response through centralized logging and analysis.● Security Awareness Training: To educate staff on identifying and handling suspicious emails or attachments.
--	---
