Incident Handler's Journal Entry

Date: July 28, 2024

Entry: 1

# Description

A healthcare clinic experienced a ransomware attack that encrypted critical files and disrupted business operations.

# Tool(s) used

Antivirus software, ransomware detection tools, phishing analysis tools.

# The 5 W's

* Who caused the incident?  
  An organized group of unethical hackers targeting healthcare and transportation industries.
* What happened?  
  The clinic's files were encrypted by ransomware after a phishing attack.
* When did the incident occur?  
  Tuesday morning at approximately 9:00 a.m.
* Where did the incident happen?  
  A small U.S. healthcare clinic.
* Why did the incident happen?  
  The attackers exploited phishing emails that contained a malicious attachment to deploy ransomware.

# Additional notes

- The ransom note demanded money in exchange for the decryption key.  
- The phishing attack led to business disruptions, as employees couldn’t access critical files and systems.  
- The company reported the incident to external organizations for technical support.