Incident Handler's Journal Entry

Date: June 10, 2025

Entry #: 1

# Description:

This entry documents a ransomware attack on a small U.S. health care clinic that occurred on a Tuesday morning. The attack caused complete disruption of business operations and encrypted critical patient data.

# Tool(s) Used:

No tools were directly used by the incident handler at this stage; this entry records initial observations and facts.

# The 5 W's:

Who caused the incident?

* An organized group of unethical hackers known to target healthcare and transportation sectors.

What happened?

* Attackers used phishing emails to trick employees into opening malicious attachments. These attachments deployed ransomware that encrypted essential medical files, rendering them inaccessible.

When did the incident occur?

* The incident occurred on a Tuesday morning at approximately 9:00 a.m.

Where did the incident happen?

* At a small U.S. primary-care health clinic.

Why did the incident happen?

* The incident happened due to a successful phishing campaign. Employees unknowingly downloaded a malicious file, which allowed ransomware to be deployed within the network.

# Additional Notes:

This scenario highlights the critical need for phishing awareness training and a strong email filtering system. Questions to explore include: Did the clinic have endpoint protection in place? Was their data backed up and stored offline? What was their incident response plan, if any?