## Incident handler's journal

**Date:** 2024-08-08

**Entry:** 1

**Description:** This incident involves a ransomware attack on a healthcare clinic in the U.S., triggered by a phishing email containing a malicious attachment. The infection encrypted critical files and left a ransom note.

**The 5 W's:**

* **Who caused the incident?** An organized group of unethical hackers known for targeting organizations in the healthcare and transportation sectors.
* **What happened?** Ransomware encrypted important files at the clinic and left a ransom note demanding payment for the decryption key.
* **When did the incident occur?** The incident occurred on Tuesday at 9:00 a.m.
* **Where did the incident happen?** At a small healthcare clinic in the United States.
* **Why did the incident happen?** The attack was triggered by downloading a malicious file attached to a phishing email sent to the clinic's employees.

**Additional notes:** It is crucial to enhance security training to prevent phishing attacks and consider implementing email filtering solutions to protect against malicious attachments. Additionally, the clinic's incident response should be evaluated to improve future incident management.

**Diario del manejador de incidentes (spanish)**

**Fecha:** 2024-08-08

**Entrada:** 1

**Descripción:** El incidente documentado involucra un ataque de ransomware en una clínica de atención médica en EE. UU. El ataque fue causado por un correo electrónico de phishing que contenía un archivo adjunto malicioso. Al descargar el archivo, se desplegó el ransomware que cifró los archivos críticos de la organización y dejó una nota de rescate exigiendo un pago para la clave de descifrado.

**Herramientas utilizadas:** No se especifican herramientas de ciberseguridad utilizadas en la descripción del incidente.

**Las 5 W's:**

* **¿Quién (Who) causó el incidente?** Un grupo organizado de hackers poco éticos que se especializa en ataques al sector salud y transporte.
* **¿Qué (What) sucedió?** El ransomware cifró archivos críticos de la clínica y dejó una nota de rescate exigiendo dinero para la clave de descifrado.
* **¿Cuándo (When) ocurrió el incidente?** El martes a las 9:00 a.m.
* **¿Dónde (Where) ocurrió el incidente?** En una clínica de atención médica en Estados Unidos.
* **¿Por qué (Why) ocurrió el incidente?** El ataque ocurrió debido a la descarga de un archivo malicioso adjunto a un correo electrónico de phishing dirigido a varios empleados de la clínica.

**Notas adicionales:** El incidente resalta la importancia de tener controles adecuados contra phishing y ransomware. Se debe considerar la implementación de herramientas de filtrado de correos electrónicos y capacitación para empleados sobre la identificación de correos electrónicos sospechosos.