# Diario del Gestor de Incidentes - Entrada 1

|  |  |
| --- | --- |
| Fecha | 14/07/2025 |
| Entrada | 1 |
| Descripción | Incidente de ransomware que afectó gravemente la operativa de una pequeña clínica sanitaria en EE. UU., tras una campaña de phishing dirigida. Los sistemas fueron cifrados y los atacantes dejaron una nota de rescate solicitando un pago por la clave de descifrado. Se activó el protocolo de respuesta a incidentes. |
| Herramienta(s) utilizada(s) | - Correo electrónico corporativo (fuente del incidente) - Antivirus/EDR (detección de malware en estaciones de trabajo) - Herramientas forenses (en análisis inicial) - Sistema de gestión de incidentes (registro del presente informe) |
| ¿Quién causó el incidente? | Un grupo organizado de ciberdelincuentes conocido por atacar los sectores sanitario y de transporte. |
| ¿Qué ha ocurrido? | Los atacantes accedieron a la red interna mediante correos electrónicos de phishing. Al abrir un archivo adjunto malicioso, se instaló un ransomware que cifró los archivos críticos. Se mostró una nota de rescate en los sistemas afectados. |
| ¿Cuándo se produjo el incidente? | Martes por la mañana, aproximadamente a las 9:00 a.m. |
| ¿Dónde ocurrió el incidente? | En la red informática interna de una pequeña clínica sanitaria en Estados Unidos. |
| ¿Por qué ocurrió el incidente? | Debido a la apertura de correos electrónicos de phishing con archivos adjuntos maliciosos por parte de empleados. Esto permitió a los atacantes desplegar ransomware y cifrar archivos esenciales para el funcionamiento de la clínica. |
| Notas adicionales | - Se recomienda analizar los correos maliciosos para identificar patrones y mejorar los filtros de correo. - ¿Se realizaron copias de seguridad recientemente? - ¿Los sistemas estaban completamente parcheados y protegidos por EDR? - Coordinarse con el equipo legal y de cumplimiento para evaluar implicaciones regulatorias (ej. HIPAA). - Determinar si hubo exfiltración de datos además del cifrado. |