INFORME TÉCNICO DE INCIDENTE DE SEGURIDAD INFORMÁTICA

Ataque de Ransomware a Servidor SIOS
Dirigido a: Gerencia General y Oficina de Control Interno
Entidad: E.S.E. HOSPITAL SAN JOSÉ DE MAICAO
Fecha del incidente: 25 de abril de 2025, 2:00 a.m.
Tiempo de recuperación: 28 horas continuas

---

1. Descripción del Incidente
El día 25 de abril de 2025, a las 2:00 a.m., se identificó una grave afectación a los sistemas informáticos del hospital, producto de un ataque tipo **ransomware**. El incidente comprometió la totalidad del servidor principal donde se alojan los sistemas de información SIOS y sus módulos críticos:

- Admisiones
- Citas
- Contratación
- Módulo Gerencial
- Historia Clínica
- SysNetServices
- Plataforma Web de Producción
- Contabilidad
- Presupuesto
- Enfermeria
- Inventario
- Gestión Farmacéutica
- Auditoria
- Cartera
- Activos Fijos

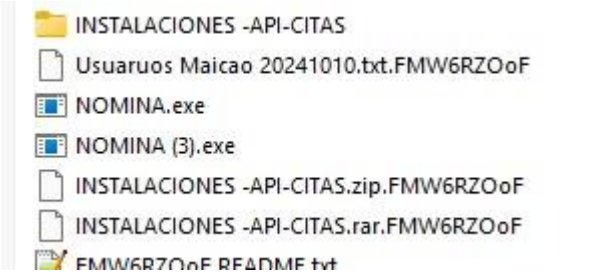
El ataque alteró las extensiones de todos los archivos, incluyendo ejecutables, configuraciones, respaldos, documentos, y especialmente las **bases de datos SQL**, dejándolos inoperables. Se evidenció el uso de la extensión .FMW6RZOoF, asociada a una variante moderna de ransomware, como se observa en la imagen adjunta.

---

2. Evidencia del Ataque
En el análisis forense preliminar se identificaron los siguientes patrones:

- Archivos renombrados masivamente con extensión .FMW6RZOoF.
- Inaccesibilidad de los archivos originales.
- Interrupción total de los servicios relacionados con los módulos administrativos y asistenciales.
- Aparición de archivos tipo "README" con exigencias de pago para recuperar los datos cifrados.

Imagen de muestra del cambio de extensiones:



(Ver Imagen con captura de pantalla que evidencia la alteración masiva de archivos)

---

3. Medidas de Respuesta y Recuperación
La restauración comenzó inmediatamente después de detectar el ataque, y se desplegó el protocolo de contingencia:

- Se procedió a aislar el servidor afectado de la red interna.
- Se activó el proceso de recuperación mediante copias de seguridad externas.
- La recuperación total del sistema tomó **28 horas ininterrumpidas**, dadas las dimensiones de los datos y configuraciones afectadas.
- Durante los días siguientes, se continuó con la restauración manual y validación de **registros clínicos y contables** que no estaban incluidos en el último respaldo.

---

4. Análisis Técnico del Ataque
Este ransomware corresponde a variantes de **criptomalware** que encriptan archivos y sistemas operativos, exigiendo un rescate económico para su liberación. Se caracterizan por:

- **Alta evasividad**, utilizando técnicas de cifrado moderno.
- **Entrada por vulnerabilidades de día cero**, archivos adjuntos en correos o conexiones RDP abiertas.
- Afectación a sistemas Windows y servicios SQL.

A pesar de contar con **barrera perimetral mediante Fortinet** y un sistema de protección endpoint como **Kaspersky**, el ataque evidencia la **sofisticación de nuevas variantes** de ransomware capaces de evadir controles tradicionales.
Ejemplos de ransomware similares:

- **WannaCry (2017):** afectó hospitales en Reino Unido y empresas globales, explotando vulnerabilidades SMB.
- **Ryuk y Conti:** enfocados en entidades de salud por su alta dependencia operativa de la información digital.
- **LockBit y BlackCat:** actuales amenazas activas con variantes que combinan cifrado y robo de datos.

---

5. Reflexión Institucional y Recomendaciones

Este incidente deja en evidencia que **ningún sistema es infalible**, incluso con herramientas de seguridad reconocidas. Se requiere:

- Reforzar auditorías y simulacros de ciberseguridad.
- Establecer backups offline (cold backups).
- Desplegar políticas estrictas de acceso remoto.
- Ampliar la capacitación del personal sobre ingeniería social y ciberamenazas.
- Evaluar soluciones EDR y segmentación de red para mayor contención.

---

6. Conclusión

El ataque fue contenido gracias al trabajo conjunto del equipo técnico y las medidas de respaldo existentes, aunque con una alta carga operativa posterior para la restauración de información crítica. Este evento debe motivar una **actualización integral de nuestra estrategia de ciberseguridad**, con foco en prevención avanzada, detección temprana y protocolos de recuperación más robustos.

Elaborado por:
ING. John Berdugo Escobar
Área de Sistemas
E.S.E. HOSPITAL SAN JOSÉ DE MAICAO
Fecha: 2 de mayo de 2025