PARA: Equipo Ejecutivo de Orion Health Services
DE: Alex Andrés Mellado Gamboa, Analista de Ciberseguridad
FECHA: 12/11/2025
ASUNTO: Informe de Estado Crítico - Incidente de Ransomware (Orion-Lock)
PARA: Equipo Directivo de Orion Health Services
DE: Alex Andrés Mellado Gamboa, Analista de Ciberseguridad
FECHA: 12/11/2025
ASUNTO: Informe de Situación Crítica: Incidente de *Ransomware* (Orion-Lock)

1. Resumen ejecutivo

El lunes por la mañana, Orion Health Services fue víctima de un ataque de ransomware, logrando acceder a nuestra red interna, bloqueando sistemas, y cifrando archivos confidenciales de suma importancia, exigiendo un rescate por los archivos. Hemos logrado identificar el punto de entrada del atacante malicioso y contener los sistemas infectados. Dado que los registros comprometidos son la nómina de empleados, horarios de citas de pacientes, y credenciales internas del sistemas se ha clasificado este incidente como Criticidad Alta.

2. Análisis del incidente

La intensiva investigación dio como resultado el vector de ataque utilizado por los ciberdelincuentes.

- El **vector de ataque** inicial fue ocasionado por un correo de phishing enviado a un miembro del equipo de finanzas.
- El **mecanismo** fue ocasionado por la descarga de un archivo malicioso Excel. Lo que provocó que los atacantes lograrán ejecutar código malicioso en el equipo.
- La **propagación** del ataque se realizó a través de una herramienta conocida como **Mimikatz,** lo cual permitió la recolección de credenciales y moverse lateralmente por la red de la empresa, lo que permitió como objetivo final comprometer los servidores principales.
- **Indicadores técnicos,** se detectó tráfico inusual desde uno de los servidores internos hacía una IP extranjera, y los archivos quedaron cifrados con extensión .orionlock.

3. Evaluación del impacto

El ataque ha comprometido la confidencialidad, disponibilidad e integridad de los siguientes activos:

- **Datos sensibles**: La nómina de empleados, registros de citas de pacientes como **datos críticos**
- **Sistema comprometido:** Las credenciales del sistema han sido comprometidas, por lo cual, el servidor de archivos está paralizado.
- **Operatividad:** El sistema actualmente está paralizado (sistema de recursos humanos y finanzas) lo cual compromete la operación del negocio.
- **Servidor respaldo:** Actualmente se encuentra cifrado la mitad de los datos para realizar respaldo de seguridad, por lo cual, tendrá complicaciones para su posterior recuperación.

4. Acciones inmediatas

Como acciones críticas se tomó las siguientes operaciones:

- **Bloqueo:** Se ha bloqueado la ip maliciosa del sistema.
- **Aislamiento**: Se ha aislado los sistemas comprometidos de los otros sistemas, para su posterior análisis, contención y erradicación del ransomware en los equipos afectados.
- **Restauración de cuentas:** Se ha forzado el restablecimiento de cuentas a los usuarios de Orion Health Services de finanzas y de recursos humanos.

5. Recomendaciones

Como recomendaciones a seguir se considera lo siguiente:

- **No pago del rescate:** Se instruye a la administración, gerencia el no pago del rescate, ya que esos archivos no se recuperarán.
- **Restauración:** Se debe restaurar el sistema a través de las copias de seguridad, en este caso se debe restaurar desde los datos que no fueron cifrados.

- **Notificación Legal**: Como los datos del sistema fueron modificados, con posibilidad de filtración de datos, se debe evaluar los aspectos legales a la notificación de las partes afectadas. En este caso con la autoridad de protección de datos de Australia.
- **Implementar 2FA**: Implementación de autenticación de dos factores para dificultar el acceso a las cuentas de la compañía.
- **Reforzar mejoras en copias de seguridad:** Como el respaldo/copia de seguridad fue afectado de forma parcial, es posible considerar la implementación de la regla “3-2-1”, es decir, tres copias de seguridad en soportes distintos, una copia fuera de la compañía.