Orion Health Services es un proveedor de tecnología sanitaria de tamaño mediano con 250 empleados. Gestionan datos confidenciales de pacientes y proporcionan software basado en la nube a clínicas de Australia y Nueva Zelanda.

El lunes por la mañana, el equipo de TI notó un tráfico saliente inusual desde uno de sus servidores internos. Al mediodía, varios empleados informaron que habían quedado excluidos de los sistemas y apareció una nota de rescate en la unidad compartida.

Eres un Graduado en Analista de Ciberseguridad en el equipo de seguridad interna. Se le ha pedido que ayude a investigar el incidente y preparar un informe para el equipo ejecutivo.

Tipo de incidente: Ataque de ransomware

Punto de entrada inicial: Un correo electrónico de phishing enviado a un miembro del equipo financiero, que contiene un archivo adjunto malicioso de Excel

Datos comprometidos:

- Registros de nómina de empleados
- Horarios de citas de pacientes
- Credenciales internas del sistema

Sistemas afectados:

- Servidor de archivos
- Sistemas de recursos humanos y finanzas
- Servidor de respaldo (parcialmente cifrado)

Indicadores de compromiso (IOC):

- Inicio de sesión sospechoso desde una IP extranjera
- Uso de Mimikatz para la recolección de credenciales
- Archivos cifrados con extensión .orionlock