Laboratorio #3

Anderson Smith Iriarte Quintana

Paso 1: Identificar el Vector e Ataque Inicial.

Me llega un correo de uno de los empleados que presuntamente su computador muchos archivos están bloqueados y no los permite abrir, en primeras creo que seria algo de sincronización o un error del usuario, pero al decirme que dice “debes para desbloquear el equipo se debe pagar 500 BTC entonces me alerto por un presunto caso de ransomware.

Realice una búsqueda en el fw de la empresa y note que salto una alerta en un equipo y lo aisló de la red por políticas que se configurar por posible intento de hacking.

Paso 2: Análisis de Logs Del Sistema

Log #0. La alerta del Usuario al ver el daño.

Log #1. Salto una notificación de alerta el fw de aislado por posible infección al revisar el notificador de alertas denoto que había una URL que estaba marcada como Peligrosa.

Log #2. Al revisar el equipo me percato que el usuario ignoro una alerta de el programa Malwarebytes la cual decía que era no segura y se genero una **Drive – by downloading,** Siendo la fuente de infección. (en este log se usa la experiencia, herramientas como Malwarebytes y su log de alertas)

Log #3 al verificar el Windows defender se encuentra en alerta por ransomware.

Paso #3. Verificación de alcance del compromiso y sistemas afectados.

El alcance gracias a la política en el FW el único equipo comprometido es un Win 11 Pro de un empleado de bajo rango.

Paso#4: Medidas de Contención Inmediatas.

Gracias a las políticas del FW se aísla el equipo en una subred donde se encuentra el solo, al llegar al equipo vemos que el Windows Defender, por las políticas de administración de la empresa aisló correctamente el núcleo y carpetas en el Disco C:
gracias a esto el ransomware tuvo alcance a archivos no corporativos del Empleado.
Reviso en el disco C las copias de seguridad que se generan de forma autónoma todos los días a las 03:00 y verificamos con un check que está íntegra y no tiene ningún daño.

Con esto en mente procedemos con:

Plan de Recuperación.

1. **Restauración desde Copia hallada:**
   Se inicia el proceso de restauración desde la copia limpia identificada. Se reestablecen los archivos del sistema y los datos corporativos críticos, sin pérdidas aparentes. El Proceso se lleva a cabo bajo mi supervisión.

2. **Monitoreo y Validación:**
   Finalizada la restauración, se implementan herramientas de monitoreo en tiempo real para asegurar que no haya procesos residuales del ransomware activos.
   Se ejecutan escaneos completos con EDR (Endpoint Detection and Response) , malwarebytes y se revisan los logs de seguridad para validar que no hubo conexiones sospechosas ni persistencia del malware.

3. **Cambio de Credenciales:**
   Como medida adicional, se solicitó al empleado afectado cambiar sus contraseñas, especialmente las asociadas a servicios en red o acceso remoto.

4. **Actualización de Sistemas:**
   Se aprovecha el incidente para forzar la actualización de todo el software del equipo afectado, incluyendo parches de seguridad de Windows y de aplicaciones de terceros además de verificar que las políticas estén correctamente implementadas.

5. **Para finalizar.**

   El sistema es reintegrado a la red corporativa tras 48 horas de monitoreo constante sin indicios de comportamiento anómalo. Se documenta el incidente y se mejora el plan de respuesta a incidentes de la empresa, añadiendo alertas más rápidas.