SESION 3 EL INCIDENTE CRITICO

Laboratorio: el incidente crítico

Duración: 1 hora

Objetivos:

1. Identifique el vector de ataque inicial.

2. Examine los archivos de registro para descubrir signos de comportamiento dañino.

3. Identificar el alcance de la obligación y los sistemas impactados.

4. Proponer medidas de contención y recuperación.

Paso 1: identificar el vector de ataque inicial

1.1 Revisión de indicadores iniciales

En un chequeo estándar en el negocio, se encuentran algunos indicadores impares

• Se recibieron varios correos electrónicos cuestionables en el departamento de recursos humanos. Algunos incluían archivos con títulos como "Leaf_de_vida_updated.exe".

• Los trabajadores anotan el sistema informático que se ejecuta lentamente, particularmente cuando usan el sistema de organización de archivos.

• Los intentos inesperados de inicio de sesión se detectan en tiempos impares de las direcciones IP en el extranjero.

Estos son signos obvios de posibles acciones dañinas.

1.2 Evaluación de evidencia

Después de una inspección más detallada:

• Se reconoce que los correos electrónicos dudosos se originan en una dirección falsa que se asemeja a un sitio web de trabajo genuino.

1. El correo electrónico incluye un archivo que parece ser un PDF, pero en realidad es un archivo ejecutable (.exe), que indica un intento de phishing con un archivo adjunto dañino.

• Los nuevos enlaces a servidores desconocidos se monitorean poco después de que algunos usuarios ejecutan ese archivo.

🔍 Vector de ataque identificado:

1. Correo electrónico con un archivo adjunto dañino. El documento, cuando se ejecuta, permitió un enlace lejano por un hacker.

Paso 2: Examine los registros del sistema para descubrir signos de acciones dañinas.

2.1 Colección de registros

Se analizaron los siguientes registros:

• Registros de servidor de correo electrónico:

Se detectaron múltiples correos electrónicos con el mismo archivo adjunto enviado a diferentes usuarios internos. Muchos trabajadores accedieron y dirigieron los documentos.

• Registros del sistema de bases de datos:

Se encontraron reuniones inusuales fuera de las horas normales en una cuenta especial que generalmente no usa ese tiempo.

• Registros de seguridad (SIEM):

Se observaron varios intentos de acceder de forma remota desde direcciones IP no identificadas, inmediatamente después de la ejecución de un archivo dañino. Además, se observan modificaciones en la configuración interna del firewall.

2.2 Análisis de actividad maliciosa

Con la aplicación de Splunk y Wireshark, se descubren los patrones posteriores

• Splunk:

Imagine varios intentos de inicio de sesión fallidos seguidos de un inicio de sesión exitoso en una cuenta de usuario de alto nivel.

Posteriormente, se detecta un flujo de datos masivo a una IP externa.

• Wireshark:

Identifica una actividad de red inusual en el puerto 4444, a menudo utilizada por programas de control remoto dañinos (como Enterpreter).

📌 Conclusión:

El intruso logró crear una conexión distante con al menos un grupo, desde el cual comenzó la investigación de la red y se dio el consentimiento para acceder a los archivos de datos críticos.

Mi visitante eventual de Windows 11

Paso 3: Calcule el alcance de la dedicación y los sistemas impactados.

3.1 Identificación de sistemas comprometidos

Desde el análisis de registro y el tráfico:

• Se reconocen tres áreas de trabajo dedicadas. Todos forman parte del departamento de personal.

• Un equipo con detalles de inicio de sesión expuestos en un archivo de texto simple en una computadora habilitó el intruso para comunicarse con el servidor de la base de datos.

• Se infringe el servidor de la base de datos de registros de empleados y se toman detalles privados del personal.

Además:

- Verifique si el servidor web también se ha violado. No se descubre ninguna prueba, sin embargo, se recomienda una vigilancia regular.

3.2 Evaluación de impacto

Disponibilidad:

• El sistema de base de datos experimentó una breve pausa porque el atacante cambió su configuración.

Integridad:

• Algunos documentos fueron alterados para ocultar signos de la violación, lo que arroja dudas sobre la confiabilidad de algunos registros.

Confidencialidad:

• Se verifica la divulgación de información privada como nombres, residencias y números de identificación del personal.

🛑 Impacto general:

Medio alto. Se violó la privacidad y se encontraron cambios en la información y algunas interrupciones.

Paso 4: Proponer medidas de contención y recuperación

4.1 Medidas de contención inmediatas

1. Desconectar sistemas comprometidos:

El engranaje dañado se separó del sistema para evitar la propagación.

2. Cambio de credencial:

Todas las contraseñas de los usuarios se restablecieron, otorgando la entrada a los sistemas que habían sido bloqueados, particularmente aquellos con una autoridad significativa.

3. Actualización de sistemas y parches:

Las actualizaciones finales de seguridad se instalaron en cada computadora y software.

4. Direcciones IP maliciosas:

El tráfico malicioso vinculado a IPS fue detenido por el firewall.

4.2 Plan de recuperación

1. Restauración desde copias de seguridad:

o el servidor de la base de datos se restableció utilizando el último soporte (12 horas antes del ataque).

o las computadoras impactadas se limpiaron y se configuraron de nuevo.

2. Monitoreo posterior:

Durante tres días, se realizó un examen exhaustivo de la actividad de la red y los puntos de entrada, con la ayuda de herramientas de información de seguridad y gestión de eventos (SIEM).

3. Evaluación posterior a la incidente:

O un documento de la empresa que enumera los problemas encontrados (contraseñas reveladas, no se creó una gestión de acceso adecuada a pesar de MFA).

o un esquema para que el personal reconozca el phishing comenzó.

4.3 Comunicación

• El grupo de liderazgo recibió un resumen y estrategia iniciales.

• Se les dijo a los trabajadores de TI que tomaran medidas de seguridad adicionales.

• Las personas impactadas fueron informadas directamente y se realizó una solicitud urgente de nuevas contraseñas.

• Se pensó que los funcionarios calificados estaban informados por la divulgación de información privada, siguiendo las reglas de las regulaciones de privacidad locales.

MI VISOR DE EVENTUALIDADES DE WINDOWS 11