Laboratorio 3 Cursos CiberSeguridad

Jesús Rodrigo Toro Navarro

Seguridad informática

Universidad Popular del Cesar

Valledupar, Cesar

Paso 1

La información que reuniría para identificar un ataque phishing sería contenido del mensaje si usa un lenguaje alarmante, petición de información sensible (contraseñas, números de tarjeta, datos personales) o enlaces sospechosos o archivos adjuntos.

La información que se debe buscar en un ataque de phishing sería verificar si los enlaces redirigen a sitios falsificados (ej. una página que parece de tu banco, pero no lo es). Pasa el cursor sobre el enlace sin hacer clic y observa si la URL es legítima.

Paso 2

Logs del servidor de correo electrónico, un ejemplo sería un usuario informa que recibió un correo extraño del "Departamento de TI". Al revisar los logs del servidor de correo: Se detecta que el mensaje llegó desde una IP desconocida fuera del país. El dominio del remitente es muy parecido al de la empresa (ej. @empresa-soporte.com en vez de @empresa.com).

Logs de envío/recepción, un ejemplo sería

Logs de filtros antispam/antivirus, un ejemplo sería el correo con un archivo adjunto .doc fue marcado como "probablemente spam" pero entregado al buzón. El filtro antispam le asignó un puntaje bajo porque el mensaje no tenía malas palabras ni enlaces sospechosos.

Logs del Gateway de correo, un ejemplo sería En el portal del gateway (como Proofpoint, Mimecast, etc.): Se observa que el mismo correo fue enviado a 15 empleados. Algunos clicaron el enlace, y el sistema registró que fueron redirigidos a una página falsa de inicio de sesión de Microsoft 365. El gateway lo marcó como sospechoso después de que varios usuarios ya lo habían abierto. Conclusión: Es una campaña masiva de phishing que superó los filtros iniciales.

Logs de Seguridad General, un ejemplo sería Un equipo del área contable muestra una alerta del antivirus: Se detectó que un archivo descargado del correo ejecutó un proceso inusual. El archivo intentó conectarse a un servidor en Rusia para descargar más malware.

Logs de Autenticación, un ejemplo sería el usuario que recibió el correo ingresó sus credenciales en una página falsa. Luego: Se registra un inicio de sesión con sus credenciales desde una IP extranjera (Rusia, China, etc.). El inicio de sesión ocurrió fuera del horario habitual, y desde un sistema operativo diferente (por ejemplo, Linux en vez de Windows)

Qué buscar:

- Errores frecuentes: Busca mensajes de error repetitivos, como 500 Internal Server Error, 403 Forbidden, 404 Not Found o errores de base de datos. Si hay un aumento en la frecuencia de estos errores, puede indicar un mal funcionamiento del sistema o un ataque.
- Fallos en la autenticación: Un número elevado de fallos de inicio de sesión (Failed login) puede ser un indicio de un intento de ataque de fuerza bruta.
- Errores en la configuración: Registros que indiquen cambios inesperados en la configuración del sistema o aplicaciones.

1. Herramientas manuales y básicas

- Excel o Google Sheets
  Ideal para comenzar, filtrar por columnas, identificar repeticiones o eventos raros (IPs, usuarios, horas).
- Notepad++ / VS Code
  Útiles para revisar logs en texto plano, buscar palabras clave o patrones con expresiones regulares.

2. Herramientas de línea de comandos

- grep, awk, sed (Linux/Unix)
  Para buscar eventos por fecha, usuario, IP, etc.
- PowerShell (Windows)
  Para filtrar eventos de seguridad o del visor de eventos.

PASO 3

Lo que se debe hacer cuando se identifica los sistemas comprometidos es aislar y Contener el Sistema Comprometido para así evitar que el atacante siga accediendo y que el ataque se propague a otros sistemas, también revisar los Sistemas Interconectados para asegurarse de que el ataque no se ha extendido a otros sistemas de la red y evaluar los posibles puntos de entrada del atacante.

Evalúa el impacto en la infraestructura crítica

Debes analizar si el ataque afectó a sistemas clave para la operación del negocio. Esto incluye sistemas financieros, productivos, de control de accesos o cualquier sistema que soporte operaciones críticas.

¿Qué considerar como infraestructura crítica?

Servidores de autenticación (ej. Active Directory), sistemas ERP, CRM o de facturación, servidores de archivos compartidos, bases de datos centrales, sistemas de correo y comunicación interna, plataformas de servicios al cliente (call centers, portales web)

¿Qué evaluar?

¿Hubo interrupciones del servicio?

¿Se accedieron o modificaron datos críticos?

¿Se instalaron herramientas de acceso remoto (RATs) o malware persistente?

¿Hubo exfiltración de datos confidenciales (clientes, finanzas, RRHH)?

¿Qué tan rápido se puede aislar y restaurar el sistema comprometido?

¿Qué se debe tener en cuenta para evaluar el impacto en la disponibilidad, integridad y confidencialidad de los datos?

Disponibilidad: Evaluar si los datos y los sistemas que los gestionan siguen siendo accesibles y operativos, o si el incidente ha interrumpido su disponibilidad.

Integridad: Evaluar si los datos han sido modificados, alterados o corrompidos durante el incidente, lo que podría afectar su exactitud y confiabilidad.

Confidencialidad: Evaluar si los datos sensibles han sido expuestos, filtrados o robados, lo que podría afectar la privacidad y seguridad de los datos.

PASO 4

4.1 Medidas de Contención Inmediatas:

¿Qué medidas se pueden implementar para detener el ataque y prevenir una mayor propagación?

- Desconectar sistemas comprometidas: Lo que se debe hacer es aislar inmediatamente los sistemas infectados de la red (LAN/Wi-Fi), sin apagarlos si se realizará un análisis forense, bloquear puertos o direcciones IP sospechosas en el firewall, eliminar acceso remoto o cerrar sesiones activas del usuario comprometido.

- Actualización de Sistemas: Lo que se debe hacer es aplicar parches de seguridad críticos al sistema operativo y a las aplicaciones vulnerables, actualizar el antivirus, firewall, y EDR en todos los endpoints y verificar configuraciones de seguridad (por ejemplo, deshabilitar macros por defecto en Office, limitar ejecución de scripts, etc.).

- Cambio de Credenciales: Lo que se debe hacer es reestablecer inmediatamente las contraseñas de todos los usuarios afectados y aquellos con privilegios elevados, forzar cierre de sesión en todos los dispositivos y revocar tokens de acceso activos (en plataformas como Microsoft 365, Google Workspace, VPN, etc.) y auditar accesos posteriores al ataque para detectar uso indebido de credenciales.

4.2 Plan de Recuperación:

Desarrollar un plan para restaurar los sistemas afectados y volver a la operación normal.

- Restauración desde Copias de Seguridad:

Pasos a seguir:

1. **Verificar la integridad de las copias de seguridad**:

   Asegúrate de que las copias de seguridad más recientes no estén comprometidas. Realiza una **comprobación exhaustiva** de las copias antes de restaurarlas.

   Verifica que los archivos y bases de datos sean consistentes y completos.

2. **Restaurar sistemas críticos**:

Restauración de servidores principales (como Active Directory, bases de datos clave, servidores de correo).

Restauración de servicios internos como archivos compartidos, ERP, CRM, etc.

Recuperación de dispositivos de usuarios afectados (si es posible, restaurar desde una imagen conocida limpia).

3. **Restaurar aplicaciones y configuraciones**:

   Asegúrate de restaurar las **aplicaciones** a la versión que era segura antes del ataque.

   Si el atacante modificó configuraciones, **verifica todas las configuraciones de seguridad**, como contraseñas de administración, reglas de firewall, y permisos.

4. **Revisar las políticas de seguridad**:

   Asegúrate de que las **políticas de contraseñas, acceso remoto y autenticación de usuarios** estén correctamente implementadas y sean seguras.

5. **Aislar el sistema de la red** hasta que la restauración esté completada y verificada.

Monitoreo y Validación:

Pasos a seguir:

1. **Monitoreo constante post-restauración**:

   Activar monitoreo en tiempo real para todos los sistemas restaurados, observando especialmente:

   - Logs de seguridad.
   - Tráfico de red y conexiones sospechosas.
   - Comportamientos anómalos de los usuarios o servicios.

   Asegúrate de que las **herramientas de detección de intrusos (IDS/IPS)** estén funcionando correctamente.

2. **Verificar la integridad de los datos**:

Revisar los archivos restaurados para asegurarte de que no estén alterados ni contengan malware.

Realiza **escaneos completos con antivirus y antimalware**.

3. **Validación de acceso de usuarios**:

   Verifica que los **usuarios solo tengan los accesos necesarios** y que **no haya cuentas de usuario** o privilegios adicionales asignados por el atacante.

   Autenticación multifactor (MFA): Habilita MFA si no estaba activado anteriormente.

4. **Restauración de servicios internos**:

   Asegúrate de que los **servicios de correo electrónico, intranet y demás aplicaciones críticas** estén operativos.

   Verificar las conexiones a las bases de datos para asegurar que los datos sean accesibles y coherentes.

5. **Revisar logs**:

   Revisa los logs de todas las plataformas para detectar cualquier **actividad sospechosa posterior** a la restauración.

Evaluación Post-Incidente:

Pasos a seguir:

1. **Revisión del impacto**:

   Evalúa el impacto sobre la **disponibilidad, integridad y confidencialidad** de los datos.

   ¿Se perdió alguna información crítica? ¿Hubo exfiltración de datos confidenciales?

   ¿Cuánto tiempo estuvo fuera de servicio la infraestructura crítica?

2. **Lecciones aprendidas**:

   ¿Qué controles fallaron? ¿Por qué el ataque de phishing fue exitoso?

   ¿Hubo un retraso en la detección del ataque? ¿Cuánto tiempo tardó en contenerse?

Revisa el **proceso de respuesta a incidentes** y ajusta la **comunicación interna**.

3. **Análisis forense completo**:

   Realiza un análisis forense **para entender el alcance completo del ataque**, incluyendo los vectores de entrada y cualquier otro sistema afectado.

   Recopila evidencia para la posible implicación de las autoridades o para informes legales.

4. **Actualizar procedimientos y políticas de seguridad**:

   Revisar y reforzar las políticas de seguridad (actualización de contraseñas, MFA, segmentación de red, etc.).

   Asegúrate de que los usuarios estén entrenados para detectar ataques de **phishing** y que el **software de seguridad** esté actualizado.

5. **Informe post-incidente**:

   Elabora un **informe detallado** con los hallazgos, los daños evaluados y las acciones tomadas.

   Comparte este informe con los **stakeholders** (gerencia, clientes, autoridades, etc.).

4.3 Comunicación:

Alta Dirección / Gerencia Ejecutiva

- **¿Qué informar?**

  Resumen del incidente: ¿Qué ocurrió? ¿Cómo se detectó?

  Impacto estimado en la disponibilidad, integridad y confidencialidad de los sistemas y datos.

  Medidas que se han tomado hasta ahora para contener el ataque.

  Acciones futuras para restaurar los sistemas y mitigar la propagación.

  Lecciones aprendidas y cambios en los protocolos de seguridad a implementar.

Clientes / Proveedores (si aplica)

- **¿Qué informar?**

  Si el incidente afectó sus datos o servicios, se debe **notificar la brecha de seguridad** de acuerdo con las regulaciones aplicables (como GDPR, CCPA, etc.).

  Asegurarse de que se toman las **medidas adecuadas para mitigar riesgos**.

  Informar sobre las **acciones que se están tomando** para remediar el incidente y restaurar la confianza.

Usuarios Afectados

- **¿Qué informar?**

  Avisar sobre el compromiso (si afecta a sus cuentas o dispositivos).

  Acciones que deben tomar: cambiar contraseñas, usar autenticación multifactor (MFA), no abrir correos sospechosos, y estar alerta ante actividades inusuales.

  Instrucciones claras para reportar actividades sospechosas y cómo colaborar en la mitigación (por ejemplo, identificar correos sospechosos).

CISCO

2.1.1 Tipos de malware

Los ciberdelincuentes utilizan muchos tipos diferentes de software malicioso, o malware, para llevar a cabo sus actividades. El malware es cualquier código que se puede utilizar para robar datos, eludir los controles de acceso o causar daño o comprometer un sistema. Saber cuáles son los diferentes tipos y cómo se propagan es clave para contenerlos y eliminarlos.

Seleccione los encabezados para obtener más información sobre algunos de los programas maliciosos más comunes.

- Spyware
- Adware
- Puerta trasera
- Ransomware
- Scareware
- Rootkit

2.1.2 Síntomas del malware

Así que ahora conoce los diferentes tipos de malware. Pero, ¿cuáles cree que podrían ser sus síntomas?

Haga una pausa y vea lo que se le ocurre y, cuando esté listo, seleccione la imagen para revelar algunas respuestas posibles.

Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes de malware. Entre ellos se encuentran:

- un aumento en el uso de la unidad de procesamiento central (CPU), lo que ralentiza el dispositivo
- el equipo se congela o se bloquea con frecuencia
- una disminución en la velocidad de navegación web
- problemas inexplicables con las conexiones de red
- archivos modificados o eliminados
- una presencia de archivos, programas o iconos de escritorio desconocidos.
- se ejecutan procesos o servicios desconocidos
- los programas se cierran o reconfiguran solos
- se envían correos electrónicos sin el conocimiento o el consentimiento del usuario.