Laboratorio # 3

PASO 1

Simulación de Ataque Phishing: El Vector de Ataque Inicial

Escenario:

Un usuario recibe un correo electrónico aparentemente legítimo de su "banco" notificándole de una actividad sospechosa en su cuenta. El mensaje incluye un enlace para confirmar su identidad y un archivo adjunto que aparentemente contiene detalles de la transacción que debe revisar. Sin embargo, el correo es un ataque de phishing destinado a robar las credenciales del usuario.

Detalles del Correo Electrónico:

De:

servicio@bancomex.com (falso, parece legítimo pero es un dominio de un atacante)

Asunto:

"Alerta de actividad sospechosa en tu cuenta"

Cuerpo del mensaje:

Estimado usuario,
Hemos detectado actividad sospechosa en su cuenta de Bancomex. Para garantizar la seguridad de sus fondos, le solicitamos que verifique su identidad inmediatamente.

Haga clic en el siguiente enlace para confirmar su cuenta y evitar bloqueos:
Confirmar cuenta

Además, adjuntamos un archivo con detalles de la transacción sospechosa. Por favor, revise el archivo adjunto y siga las instrucciones para completar la verificación.

¡Actúe ahora! Si no lo hace, su cuenta podría ser bloqueada temporalmente por razones de seguridad.

Archivo adjunto:

Factura_detalle.zip (archivo comprimido que contiene un archivo ejecutable malicioso, como Factura_detalle.exe).

Pasos del Ataque de Phishing:

1. Recepción del Correo:

El usuario recibe el correo en su bandeja de entrada y nota que proviene de un supuesto servicio de atención al cliente de su banco. El asunto es urgente, indicando una "actividad sospechosa en su cuenta", lo cual genera un sentido de urgencia.

2. Análisis del Correo:

Al examinar el correo, el usuario observa:

El remitente: servicio@bancomex.com. Aunque parece legítimo, una revisión más cercana muestra que el dominio es ligeramente incorrecto. El dominio real del banco es bancomex.com, pero en este caso, el atacante ha utilizado una versión modificada.

El enlace: El texto del enlace dice "Confirmar cuenta", pero si el usuario coloca el cursor sobre el enlace, la URL real muestra http://www.bancomex-login.com. Este es un sitio web falso creado por los atacantes para robar las credenciales.

El archivo adjunto: El correo incluye un archivo comprimido Factura_detalle.zip. Los archivos ZIP son un método común de distribución de malware. Al abrir el archivo comprimido, se encuentra un archivo ejecutable llamado Factura_detalle.exe.

3. Acción del Usuario:

Si el usuario hace clic en el enlace, será redirigido a una página de inicio de sesión falsa que imita el sitio real del banco, donde se le pedirá ingresar su nombre de usuario y contraseña. Al hacerlo, las credenciales serán enviadas a los atacantes.

Si el usuario decide abrir el archivo adjunto, el archivo ejecutable Factura_detalle.exe se ejecutará en su máquina, posiblemente instalando un malware como un troyano o keylogger que permite a los atacantes obtener acceso remoto a su dispositivo y robar información sensible.

4. Detección del Ataque:

El ataque se puede detectar mediante varios métodos, tales como:

Análisis de los correos electrónicos recibidos: la revisión de los correos electrónicos muestra una fuente sospechosa (dominio alterado) y un enlace a un sitio web falso.

Monitoreo de acceso web: Si se monitoriza el tráfico de la red, se podría ver que el usuario accede a un sitio web falso con un dominio sospechoso.

Análisis de logs: En los logs de correo, se pueden encontrar registros de correos electrónicos provenientes de dominios no oficiales o desconocidos. Además, se pueden identificar intentos de inicio de sesión a sitios web falsos o servicios de banca en línea.

5. Respuesta ante el Incidente:

Confirmación del incidente: Al comprobar que el ataque de phishing ha tenido éxito, se confirma que el vector de ataque es el phishing con un archivo adjunto malicioso.

Revisión de seguridad: Verificar los sistemas comprometidos, realizar un análisis de malware en los dispositivos afectados, y cambiar las credenciales de acceso al banco y otros servicios sensibles.

Notificación a los usuarios afectados: Informar a los usuarios sobre el ataque y cómo evitarlo en el futuro. También se pueden ofrecer pasos de recuperación, como restablecer contraseñas y activar la autenticación de dos factores (2FA).

Medidas de Prevención para el Futuro:

Educación continua: Entrenar a los empleados sobre cómo reconocer correos electrónicos sospechosos y no hacer clic en enlaces o abrir archivos adjuntos de fuentes no confiables.

Análisis de correos electrónicos entrantes: Utilizar filtros de correo electrónico avanzados para detectar y bloquear posibles ataques de phishing antes de que lleguen a los usuarios.

Autenticación de dos factores (2FA): Implementar 2FA en cuentas bancarias y otras cuentas críticas para añadir una capa extra de seguridad.

Monitoreo de actividad: Implementar un sistema de monitoreo de actividad para detectar accesos inusuales o intentos de acceso no autorizados.

Paso 2: Análisis de los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

2.1 Recolección de Logs

Logs del servidor de correo electrónico:

Buscar registros de entrada con dominios sospechosos (@bancomex-login.com).

Revisar encabezados del correo para verificar el servidor SMTP original.

Verificar si otros usuarios recibieron correos similares.

Logs del sistema de bases de datos:

Verificar accesos inusuales desde IPs desconocidas.

Revisar consultas SQL inusuales que podrían indicar extracción o modificación no autorizada.

Logs de seguridad del sistema operativo:

Detección de ejecución de archivos .exe fuera de lo habitual.

Cambios en permisos o creación de nuevos procesos por Factura_detalle.exe.

Alertas generadas por antivirus, EDR o firewall.

2.2 Análisis de la Actividad Maliciosa

Análisis de patrones:

Correlacionar hora de recepción del correo con actividad en el sistema (p. ej. ejecución del .exe).

Identificar intentos de conexión saliente a IPs externas inusuales.

Revisión de tráfico DNS y HTTP que apunten al sitio falso (bancomex-login.com).

Herramientas recomendadas:

ELK Stack (Elasticsearch, Logstash, Kibana)

Splunk

Wireshark (para análisis de tráfico de red)

Sysinternals (para analizar procesos en Windows)

VirusTotal (para validar el .exe)

Paso 3: Determinar el Alcance del Compromiso y Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos

Escaneo de endpoints que hayan descargado o ejecutado el archivo malicioso.

Evaluar conexión entre el equipo afectado y otros sistemas en la red local (compartición de archivos, sesiones abiertas).

Verificar si hubo propagación del malware mediante mecanismos automáticos (p. ej. ejecución en red compartida o RDP).

3.2 Evaluación del Impacto

Disponibilidad: Evaluar si algún sistema quedó inutilizado o si se ralentizó la red o los servicios por el ataque.

Integridad: Verificar si se alteraron archivos, registros o configuraciones.

Confidencialidad: Analizar si hubo fuga de credenciales, accesos no autorizados o exfiltración de datos.

Paso 4: Medidas de Contención y Recuperación

4.1 Medidas de Contención Inmediatas

Desconexión del equipo afectado de la red.

Cambio de credenciales de todos los usuarios afectados y sistemas potencialmente comprometidos.

Actualización de sistemas con los últimos parches de seguridad.

Reforzar reglas del firewall para bloquear acceso a dominios como bancomex-login.com.

4.2 Plan de Recuperación

Restaurar el sistema afectado desde una copia de seguridad limpia.

Aplicar escaneos exhaustivos con antivirus actualizado.

Monitoreo activo de todos los endpoints y tráfico de red en busca de reinfección.

Revisión completa de la configuración del correo para asegurarse que no hay reglas maliciosas (como redirecciones ocultas).

4.3 Comunicación

Informar al equipo de TI y usuarios afectados con transparencia.

Notificar al proveedor de correo o banco real si se está usando su marca para phishing.

Si se comprometen datos personales, cumplir con regulaciones de notificación de incidentes (como GDPR o normativas locales).

Preparar informe técnico y ejecutivo con:

Causa del incidente

Acciones realizadas

Recomendaciones futuras