Ataque de hombre en el medio (MitM)

Un ataque de hombre en el medio (MitM) es una forma de ciberataque en el que los criminales que explotan protocolos débiles basados en la web se insertan entre entidades en un canal de comunicación para robar datos.

1. Secuestro de correo electrónico

Como su nombre lo indica, en este tipo de ataque, los cibercriminales toman el control de las cuentas de correo electrónico de bancos, instituciones financieras u otras empresas de confianza que tienen acceso a datos sensibles y dinero. Una vez dentro, los atacantes pueden monitorear las transacciones y la correspondencia entre el banco y sus clientes.

En escenarios más maliciosos, los atacantes falsifican o falsifican la dirección de correo electrónico del banco y envían a los clientes correos electrónicos que les indican que vuelvan a enviar sus credenciales, o peor aún, envían dinero a una cuenta controlada por los atacantes. En esta versión de ataque MitM, la ingeniería social o el desarrollo de confianza con las víctimas es clave para el éxito.

2. Espionaje Wi-Fi

En el espionaje Wi-Fi, los cibercriminales hacen que las víctimas se conecten a una red inalámbrica cercana con un nombre de sonido legítimo. Pero en realidad, la red está configurada para participar en actividades maliciosas. La red inalámbrica puede parecer propiedad de una empresa cercana a la que el usuario frecuenta o podría tener un nombre genérico, aparentemente inofensivo, como “Red Wi-Fi pública gratuita”. En algunos casos, el usuario ni siquiera necesita ingresar una contraseña para conectarse.

Una vez que las víctimas están conectadas al Wi-Fi malicioso, el atacante tiene opciones: monitorear la actividad en línea del usuario o raspar las credenciales de inicio de sesión, la información de la tarjeta de crédito o pago y otros datos sensibles.

Para protegerse contra este ataque, los usuarios siempre deben verificar a qué red están conectados. Con los teléfonos móviles, deben desactivar la función de conexión automática Wi-Fi al moverse localmente para evitar que sus dispositivos se conecten automáticamente a una red maliciosa.

3. Suplantación de identidad DNS

La suplantación de identidad del sistema de nombres de dominio (DNS), o envenenamiento de caché DNS, ocurre cuando los registros DNS manipulados se utilizan para desviar el tráfico legítimo en línea a un sitio web falso o falsificado creado para parecerse a un sitio web que el usuario probablemente conocería y en el que confiaría.

Al igual que con todas las técnicas de suplantación de identidad, los atacantes solicitan a los usuarios que inicien sesión involuntariamente en el sitio web falso y los convenzan de que deben realizar una acción específica, como pagar una tarifa o transferir dinero a una cuenta específica. Los atacantes roban tantos datos como puedan de las víctimas en el proceso.

4. Secuestro de sesiones

El secuestro de sesión es un tipo de ataque MitM en el que el atacante espera a que una víctima inicie sesión en una aplicación, como la banca o el correo electrónico, y luego roba la cookie de sesión. Luego, el atacante utiliza la cookie para iniciar sesión en la misma cuenta propiedad de la víctima, pero en su lugar desde el navegador del atacante.

Una sesión es un dato que identifica un intercambio de información temporal entre dos dispositivos o entre una computadora y un usuario. Los atacantes aprovechan las sesiones porque se utilizan para identificar a un usuario que ha iniciado sesión en un sitio web. Sin embargo, los atacantes deben trabajar rápidamente a medida que las sesiones finalizan después de una cantidad de tiempo establecida, lo que podría ser tan corto como unos minutos.

5. Secuestro de capa de sockets seguros (SSL)

La mayoría de los sitios web actuales muestran que están utilizando un servidor seguro. Tienen “HTTPS”, abreviatura de Protocolo de transferencia de hipertexto seguro, en lugar de “HTTP” o Protocolo de transferencia de hipertexto en la primera parte del Localizador uniforme de recursos (URL) que aparece en la barra de direcciones del navegador. Incluso cuando los usuarios escriben HTTP, o ningún HTTP en absoluto, el HTTPS o la versión segura se renderizarán en la ventana del navegador. Este es un protocolo de seguridad estándar y todos los datos compartidos con ese servidor seguro están protegidos.

SSL y su seguridad de capa de transporte (TLS) sucesora son protocolos para establecer la seguridad entre computadoras en red. En un secuestro SSL, el atacante intercepta todos los datos que pasan entre un servidor y la computadora del usuario. Esto es posible porque SSL es un protocolo de seguridad más antiguo y vulnerable que requirió su reemplazo, la versión 3.0 fue obsoleta en junio de 2015, con el protocolo TLS más sólido.

5. Envenenamiento de caché ARP

El Protocolo de resolución de direcciones (ARP) es un protocolo de comunicación utilizado para descubrir la dirección de la capa de enlace, como una dirección de control de acceso a medios (MAC), asociada con una dirección de capa de Internet determinada. El ARP es importante porque traduce la dirección de la capa de enlace a la dirección del protocolo de Internet (IP) en la red local.

En este esquema, la computadora de la víctima es engañada con información falsa del cibercriminal para que piense que la computadora del estafador es la puerta de enlace de la red. Como tal, la computadora de la víctima, una vez conectada a la red, envía esencialmente todo su tráfico de red al actor malicioso en lugar de a través de la puerta de enlace de red real. Luego, el atacante utiliza este tráfico desviado para analizar y robar toda la información que necesita, como la información de identificación personal (PII) almacenada en el navegador.

6. Suplantación de identidad IP

La falsificación de IP es similar a la falsificación de DNS en el sentido de que el atacante desvía el tráfico de Internet dirigido a un sitio web legítimo a un sitio web fraudulento. En lugar de falsificar el registro DNS del sitio web, el atacante modifica la dirección IP del sitio malicioso para que parezca como si fuera la dirección IP de los usuarios legítimos del sitio web que se pretende visitar.

7. Robo de cookies del navegador

En informática, una cookie es una pequeña información almacenada. Una cookie de navegador, también conocida como cookie HTTP, son datos recopilados por un navegador web y almacenados localmente en la computadora de un usuario. La cookie del navegador ayuda a los sitios web a recordar información para mejorar la experiencia de navegación del usuario. Por ejemplo, con las cookies habilitadas, un usuario no tiene que seguir completando los mismos elementos en un formulario, como el nombre y el apellido.

El robo de cookies del navegador se debe combinar con otra técnica de ataque MitM, como el espionaje Wi-Fi o el secuestro de sesiones, para llevar a cabo. Los cibercriminales pueden obtener acceso al dispositivo de un usuario utilizando una de las otras técnicas de MitM para robar cookies del navegador y aprovechar todo el potencial de un ataque de MitM. Con el acceso a las cookies del navegador, los atacantes pueden obtener acceso a contraseñas, números de tarjetas de crédito y otra información confidencial que los usuarios almacenan regularmente en sus navegadores.

Casos de ataques MitM

1. El Escándalo Superfish en Laptops Lenovo (2015)

Este es un caso icónico y técnicamente puro de un MitM implementado por el propio fabricante.

¿En qué consistió? Lenovo, uno de los fabricantes de PC más grandes del mundo, preinstaló un adware llamado Superfish Visual Discovery en ciertos modelos de laptops para consumidores entre septiembre de 2014 y febrero de 2015.

La Técnica MitM:

El software Superfish instalaba un certificado raíz autofirmado (un certificado falso) idéntico y con la misma contraseña en todas las máquinas afectadas.

Al navegar por sitios seguros (HTTPS), Superfish se interponía. Interceptaba el tráfico, eliminaba el certificado de seguridad original del sitio web y lo sustituía por su propio certificado falso.

Esto permitía a Superfish descifrar e inspeccionar el tráfico cifrado (incluyendo datos sensibles como contraseñas) para inyectar anuncios emergentes relacionados con el contenido que el usuario estaba viendo.

La Vulnerabilidad Crítica: Dado que Superfish usaba la misma clave de cifrado universal, si un atacante malicioso la descubría (lo que ocurrió rápidamente), este podría haber llevado a cabo un ataque MitM contra cualquier usuario de Lenovo en una red pública, interceptando sus credenciales bancarias y otra información altamente confidencial.

Consecuencias: Fue considerado un desastre de seguridad masivo, obligando a Lenovo a disculparse públicamente, proporcionar herramientas de eliminación y enfrentar una acción legal por parte de la Comisión Federal de Comercio (FTC) de EE. UU.

2. El Robo de Datos de Equifax (2017)

Aunque el fallo principal fue una vulnerabilidad en una aplicación web, las técnicas MitM jugaron un papel clave en la fase de explotación.

¿En qué consistió? Equifax, una de las agencias de crédito más grandes de Estados Unidos, sufrió una de las mayores filtraciones de datos de la historia, exponiendo la información personal y financiera de más de 147 millones de personas.

La Técnica MitM y Suplantación: Una parte clave del ataque involucró el uso de la suplantación SSL (SSL spoofing) y el robo de certificados. Los atacantes lograron robar más de 500 certificados digitales, incluyendo algunos utilizados por grandes empresas.

Propósito del MitM: Al obtener certificados de seguridad legítimos, los hackers podían hacerse pasar por sitios web y empresas de confianza (suplantación de identidad) para seguir espiando a los usuarios, robar credenciales y eludir las defensas de seguridad que verifican la identidad del sitio web.

3. Ataques de Intercambio de SIM (SIM Swapping) Dirigidos a Celebridades y Cuentas de Criptomonedas (2018-Actualidad)

Este es un ejemplo de MitM a nivel de comunicación móvil, aprovechando la ingeniería social.

¿En qué consistió? Los atacantes roban el número de teléfono de la víctima y obtienen un duplicado de su tarjeta SIM. En varios casos de alto perfil (incluyendo robos a figuras públicas y cuentas de criptomonedas), las operadoras (como T-Mobile en EE. UU.) han sido el punto débil.

La Técnica MitM:

Interceptación del Factor de Confianza: El atacante se interpone entre la víctima y sus servicios en línea (bancos, correo electrónico, criptomonedas) que utilizan el número de teléfono como segundo factor de autenticación (2FA).

Ingeniería Social: El atacante engaña al empleado de la compañía telefónica, haciéndose pasar por la víctima, para que transfiera el número de teléfono (y, por ende, el tráfico SMS y de llamadas) a una nueva tarjeta SIM en posesión del atacante.

Resultado: El atacante recibe los mensajes de texto del 2FA destinados a la víctima, lo que le permite restablecer contraseñas, vaciar cuentas bancarias o transferir criptomonedas. En esencia, el atacante se convierte en el "hombre en el medio" de las comunicaciones de autenticación.

0dayexploit

El tipo de exploit que se emplea para aprovecharse de una vulnerabilidad de día cero depende del fallo encontrado. Se pueden usar diversos exploits para aprovechar un mismo día cero. Por ejemplo, un ataque de intermediario podría usarse para interceptar datos y ejecutar un ataque de cross-site scripting (XSS).

El flujo de trabajo para un día cero comienza cuando el atacante halla una vulnerabilidad. La vulnerabilidad podría ser de hardware, firmware, software o cualquier otro sistema corporativo. Los pasos indicados a continuación ofrecen un flujo de trabajo general para un ataque de día cero:

Los desarrolladores implementan una aplicación o actualización a una aplicación que contiene una vulnerabilidad desconocida.

Un atacante escanea el software y detecta una vulnerabilidad, o un atacante encuentra un fallo en el código fuente después de descargarla del repositorio.

Un atacante usa herramientas y recursos para aprovechar la vulnerabilidad. Esto podría consistir en software creado a medida por el atacante, o en herramientas disponibles en el mercado.

Esta vulnerabilidad podría ser explotada durante años enteros antes de que se descubra, pero eventualmente ocurrirá que equipos investigadores, el público general o los profesionales de TI identificarán la actividad de los atacantes y notifiquen a los desarrolladores acerca de la vulnerabilidad.