TRANXFER - Como previene ataques “Man in the middle”?

tranxfer

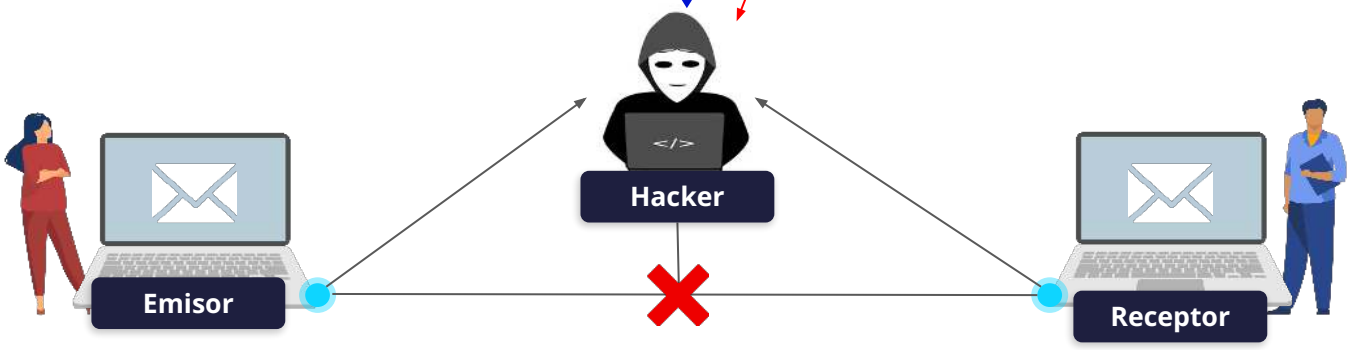
¿Qué es el “Man in the middle”?

El “Man in the Middle” o ataque por intervención, són aquellos ataques en los cuales un hacker interviene las comunicaciones entre dos personas, y modifica los mensajes sin que nadie se de cuenta

Lo más frecuente es que los ciberdelincuentes creen una red maliciosa intentando suplantar una red segura e intervenir todas las comunicaciones que pasen por ella.

Una vez las víctimas se conectan a su red, los ciberdelincuentes tienen control total sobre sus comunicaciones, y pueden intervenirlas, modificarlas y enviarlas a su destinatario, siendo uno de los ciberdelitos más difíciles de detectar.

Estructura de los ataques “Man in the middle”



¿Qué tipos de ataques Man in the middle” existen?

Hay varios tipos de ataques “MITM”, estos són los principales:

- Ataques basados en servidores DHCP o DNS
- ARP cache poisoning
- Simulación de un punto de acceso inalámbrico
- “Man-in-the-browser”
- “Human assisted attack”

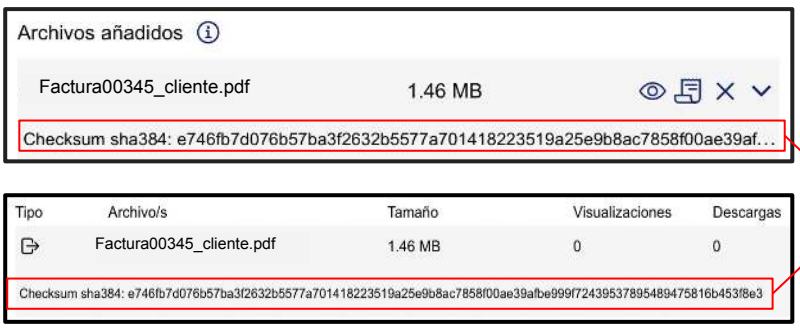
¿Qué es el “Man in the middle”?

¿Cómo Tranxfer elimina este tipo de ataques?

Tranxfer propone a sus clientes un canal seguro para la transferencia de archivos y certificación del contenido original mediante un hash o checksum

Cómo aseguramos que el contenido es original y que no hay posibilidad de modificar el archivos mediante un ataque “**man in the middle**:

- Los archivos viajan encriptados por un canal seguro
- Las transferencias encriptadas se identifican con un código checksum único que se valida a la salida y a la recepción para asegurar que el contenido no ha sido modificado



El Checksum certifica la veracidad e integridad del documento enviado y recibido.

Checksum cómo método seguro de verificación de los archivos

El Checksum es una suma de comprobación que se obtiene de un origen de datos. Sirve para comprobar que el fichero que nos hemos descargado mantiene su identidad original.
Mediante un algoritmo matemático, cuándo se sube el archivo a Tranxfer, se calculan una serie de números, que se vuelven a calcular cuándo el remitente abre la transferencia. Si són iguales, significa que el fichero es original.

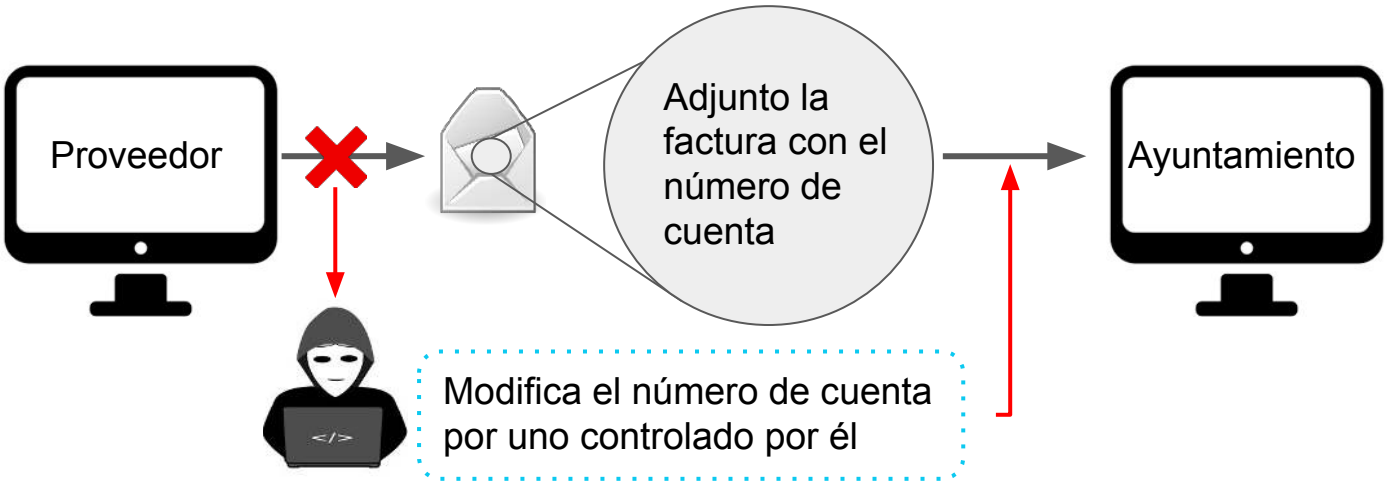
¿Cómo funciona?

- Se adjuntan los archivos, y se encriptan mediante “**AES 256**”.
- Cuando se encriptan, **se les da una identidad original mediante un checksum único**
  Se envían los ficheros, y cuándo el receptor los recibe
- Se **vuelve a calcular el código checksum** y se valida que sea el mismo.
- El destinatario puede **desencriptar el fichero y visualizarlo o descargarlo sabiendo que es el original**
- **En caso de que el documento hubiera sido modificado durante el viaje, el checksum no coincidira y por tanto se impediría la descarga**

tranxfer

Ataque “Man in the middle”

Un ciberdelincuente robó casi 1 millón de euros al modificar el número de cuenta de la factura del proveedor de iluminación navideña mediante “Man in the middle”



¿Cómo intentar evitar este tipo de ataques?

Este tipo de ataques no són fáciles de detectar, mientras que en otros malware, la víctima detecta que ha sido atacada, en el caso de “Man in the middle” pueden pasar semanas hasta que no se detecta el ataque. Por eso, lo más importante es la prevención.

- Código de descarga en los archivos
- Validación de dos factores (2FA)
- Encriptación End to End (E2E)
- Trazabilidad de los archivos

o

Contar con un canal seguro cómo **Tranxfer** para el intercambio de información

El 93% de los ciberataques entran por correo electrónico, Utiliza Tranxfer cómo canal seguro para el intercambio de información en tu empresa.

Solicita tu demo gratuita en tranxfer.com

Con la confianza de: Naturgy, Crèdit Andorrà, PROSEGUR

Certificaciones: ens Esquema Nacional de Seguridad

Aprobado por: GDPR