Ernesto Aranda del Valle
Antonio Jiménez Rodríguez

Ataques Man In The Middle

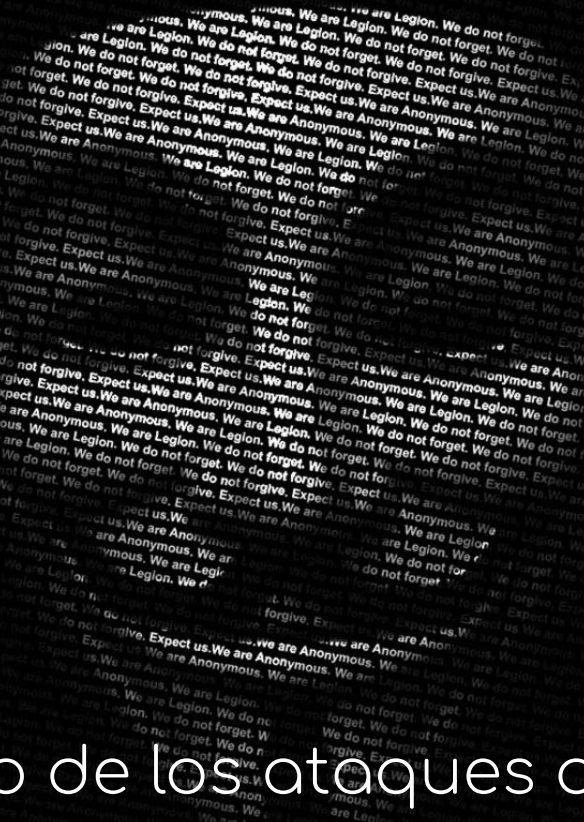
Concepto de ataque MITM

Ataque MITM

Es un tipo de ataque donde cierto usuario altera la comunicación entre dos partes de manera secreta. Por ejemplo el 'eavesdropping.'

'Eavesdropping'

Es un tipo de ataque MITM en el que el atacante intercepta los mensajes entre los dos usuarios pudiendo insertar los mensajes que le convenga.



Funcionamiento de los ataques de intermediario

1. Interceptación

Lo primero que hacen los atacantes es interceptar el tráfico de internet antes de que llegue a su destino.

Suplantación de IP

Los cybercriminales falsifican la fuente real de los datos que envían desde su equipo y la camuflan como si fuera una fuente fiable.

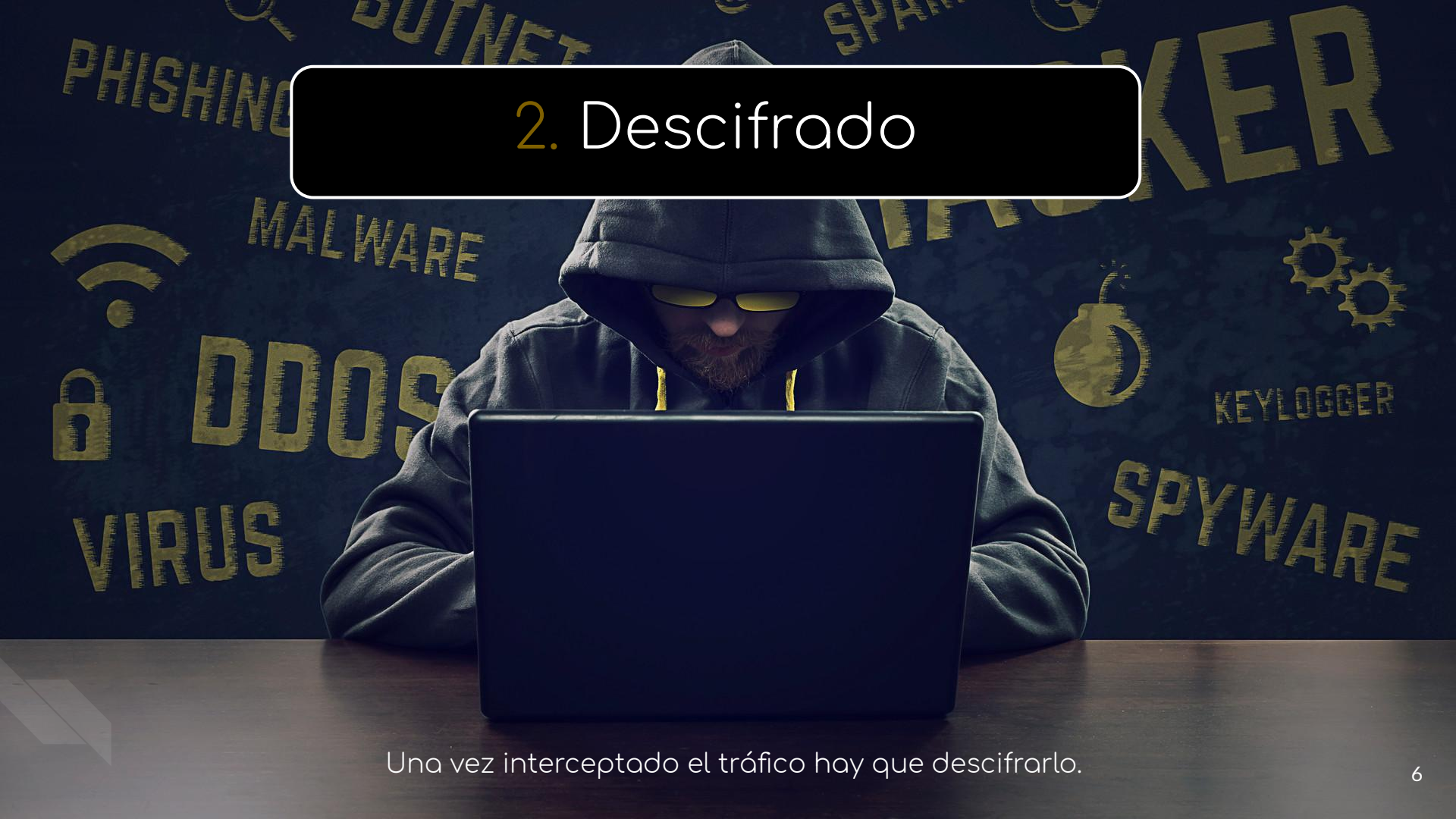
Suplantación de ARP

Los cybercriminales envían un ARP falso a una LAN para que la dirección del MAC del atacante pueda vincularse a su IP y recibir todos los paquetes de datos de la víctima.

Suplantación de DNS

Los cybercriminales acceden a esta caché y cambian las traducciones que hay en el propio DNS redirigiendolos así a un lugar vulnerable.

2. Descifrado



Una vez interceptado el tráfico hay que descifrarlo.

Suplantación de HTTPS

- HTTPS es la clave del certificado de un sitio web que indica que los envíos de datos están cifrados, por lo tanto es un lugar seguro.
- Sin embargo un atacante puede instalar un certificado raíz de seguridad falso para que su navegador crea que es uno de confianza

BEAST en SSL

Permite a los atacantes aprovecha los puntos débiles cifrado por bloques, pudiendo atrapar y descifrar los datos que se mueven entre un navegador y un servidor web.

Secuestro de SSL

- En este caso se cambia se cambia la conexión del usuario de HTTPS en un sitio web a HTTP.
- El atacante se sitúa entre el atacante y una conexión segura y le ofrece una versión HTTP mediante un servidor proxy u otros métodos.

Stripping de SSL

- Al conectarnos a un sitio web el navegador se conecta primero a la versión HTTP y el servidor lo redirige a la HTTPS
- El secuestro de SSL se produce en mitad y se dirige el tráfico al equipo del atacante

Es difícil detectar que estás siendo atacado...

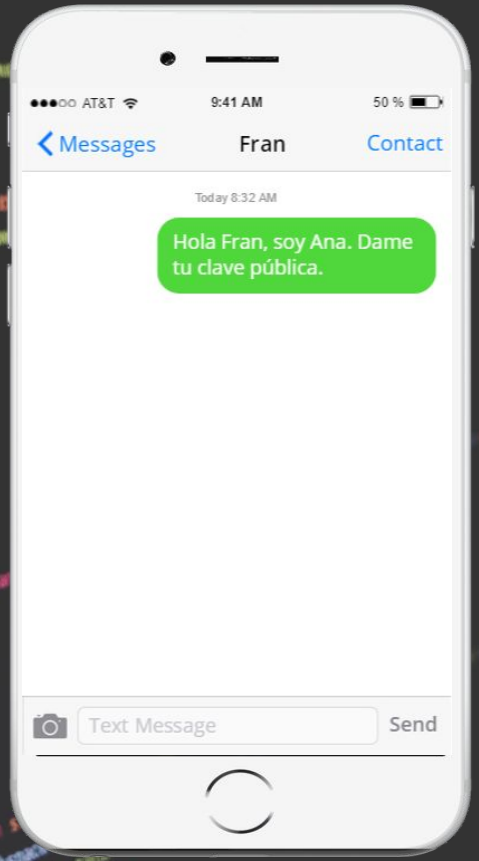
...Por lo que la mejor defensa es una buena prevención

Como defenderse de un ataque MITM

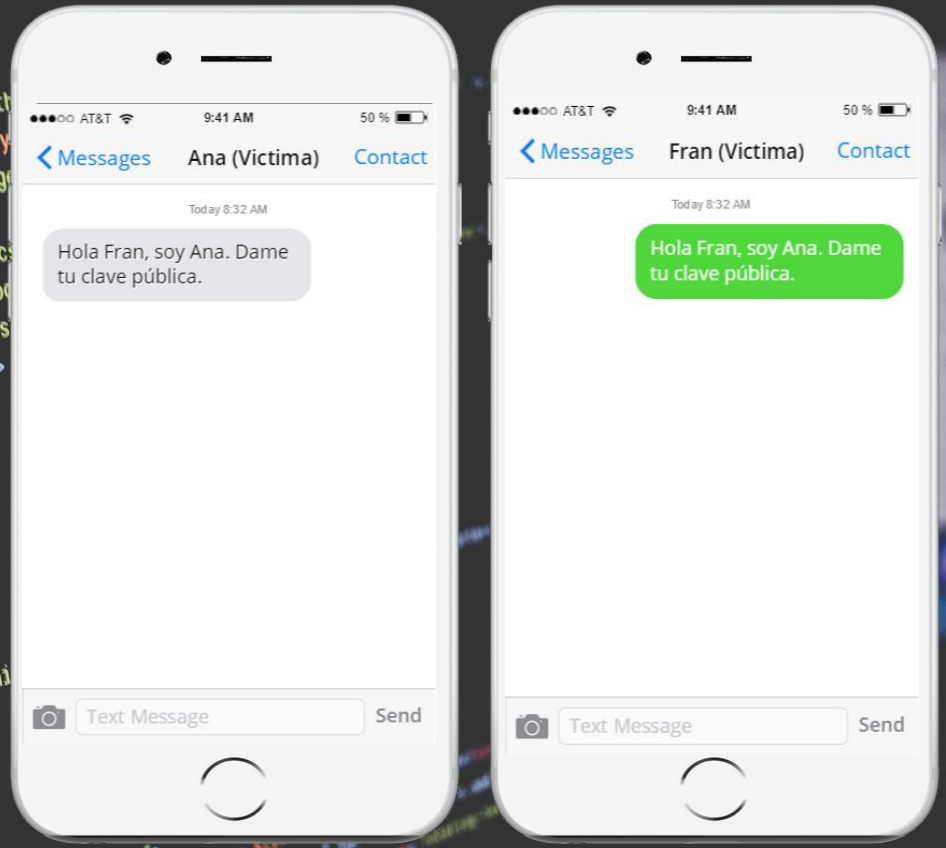
Defensa contra MITM

- Activar la verificación en dos pasos.
- Detectar y evitar estafas de phishing.
- Evitar conectarse a redes públicas.
- Usar HTTPS para al menos ponérselo más difícil al atacante.
- Usar redes VPN para crear túneles de comunicación seguros

Ana envía un mensaje no cifrado a Fran, que es interceptado:

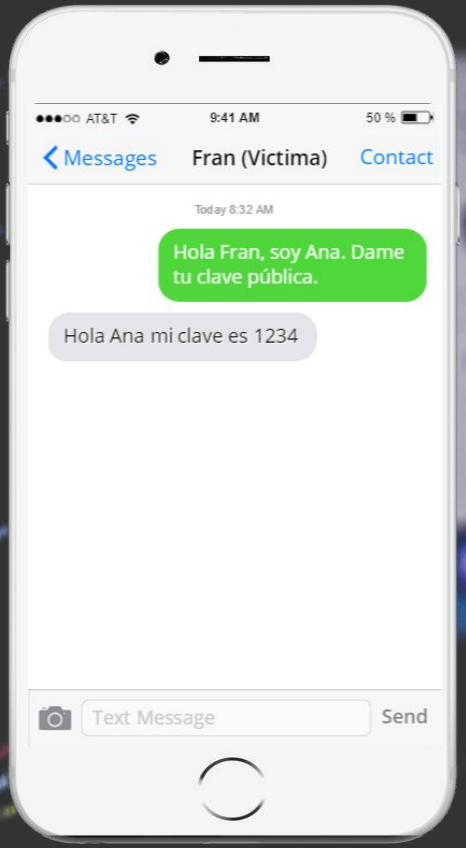


El atacante reenvía este mensaje a Fran con su clave pública; Fran no puede decir que no es realmente de Ana:

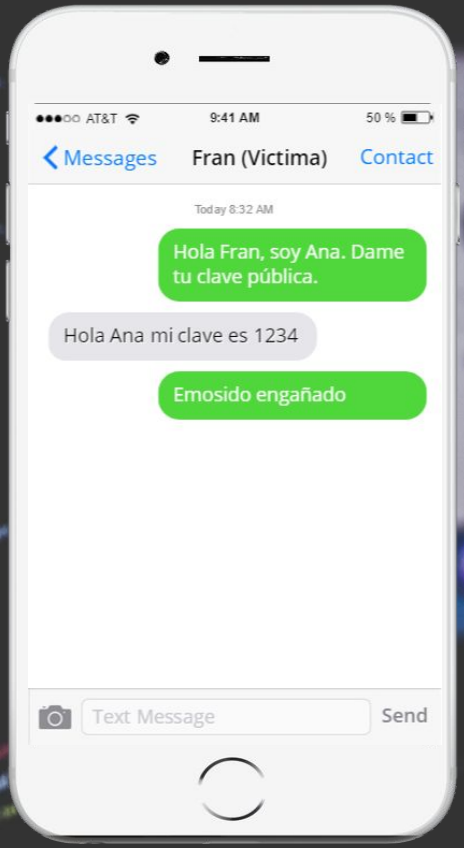


Fran responde con su clave pública:

El atacante reemplaza la clave de Fran por la suya, y transmite la clave a Ana, afirmando que es la clave de Fran



Sin embargo, debido a que en realidad el mensaje estaba cifrado con la clave del atacante, este puede descifrarlo, leerlo, si desea, modificarlo, y posteriormente cifrarlo con la clave de Fran, remitiéndoselo al mismo:



Demostración Práctica

Ataque ARP con Ettercap

Gracias!

¿Alguna pregunta?