# Tema 4a – Malware e Ingeniería Social

## Atacantes:

### ¿Quiénes son los atacantes?

**Hackers:** Sustituida por atacante independientemente de los motivos.

**Espías:** Atacante bajo contrato (mercenario), el objetivo es mucho más específico, nivel excelente de conocimientos.

**Script Kiddies:** Atacantes sin conocimientos que utilizan herramientas automatizadas (scripts), las herramientas actuales tienen UI gráfica (más fáciles), Anonymous emplea este enfoque habitualmente.

**Interno (insiders):** Alrededor del 48% de los ataques son de origen interno (empleados, contratistas y empresas aliadas), suelen consistir en sabotaje o robo de propiedad intelectual, casi todos provienen de empleados recién despedidos.

## Propagación:

### Virus

**Biológico:** Infecta una célula o La controla para producir copias de sí mismo

**Informático:** Se inserta (infecta) en el código de un programa o Se reproduce infectando otros ficheros o Cada vez que arranca intenta reproducirse y/o llevar a cabo una acción maliciosa o Depende del usuario para saltar de máquina.

**Acciones:** Acciones de los virus o Colgar el ordenador de forma repetida o Borrar ficheros o Consumir todo el espacio libre copiándose a sí mismo o Desactivar los sistemas de seguridad o Formatear el disco duro, etc.

### Tipos de Virus

**Apéndice:** Se inserta al final, salto inicial al virus y cede el control al programa tras el virus.

**Queso Suizo:** Se inserta dentro del código del programa, se almacena el código sobrescrito para ejecutar el programa original correctamente.

**Fraccionado:** Se divide en muchas partes, se intercalan de forma aleatoria, se almacena el código sobrescrito.

**Programa**: Infecta ficheros ejecutables, se activa al ejecutar el programa. (Puede que tenga 70 extensiones de Windows)

**Macro:** Una serie de instrucciones para la automatización de tareas repetitivas que se almacenan en un fichero de datos. Se activa al abrir el documento.

**Arranque:** Infecta el Master Boot Record (MBR) del disco duro. Se activa al arrancar el ordenador (antes del sistema operativo)

**Asociado:** Suplanta a una herramienta legítima del sistema operativo.

### Gusanos

Programa malicioso que explota una vulnerabilidad para entrar en una máquina, una vez ha infectado una máquina, busca otros objetivos potenciales. Utiliza la red para enviar copias de sí mismo. Los gusanos originales simplemente se copiaban y producían un ataque de denegación de servicio. (Borrar ficheros, control remoto)

### Diferencia

**Virus:** Requiere que una persona o agente externo transfiera archivos infectados a otros sistemas, se insertan en ficheros ejecutables, requiere acción externa.

**Gusano:** Utiliza la red para transferirse de forma autónoma entre sistemas, explotan las vulnerabilidades de aplicaciones o SO, se puede controlar de forma remota.

## Ocultación:

### Troyanos

Un programa que oficialmente hace una actividad, pero tiene otra actividad oculta.

### Rootkits

Un grupo de herramientas que sirve para esconder la actividad o presencia de otro malware, actúan escondiendo registros, logs y procesos asociados. Modifican el SO para forzarle a ignorar actividad maliciosa. (“Todo aparenta ser normal”) Cambio de ficheros del SO, difíciles de eliminar una vez detectados.

### Bombas lógicas

Programas que permanecen dormidos hasta que se satisface cierta condición. Pueden producir cualquier tipo de actividad maliciosa. Son muy difíciles de detectar antes de activarse. (No son “easter egss”) Ejemplos: borrar datos críticos, trabajadores descontentos.

### Puertas traseras

Código que permite el acceso a un programa o servicio sin las restricciones de seguridad normales. Es una práctica normal en el desarrollo de muchos programas para obtener un acceso rápido o de depuración al mismo. A veces se olvida de eliminar antes del lanzamiento. Malware puede dejar una puerta trasera para que el atacante vuelva después sin pasar por los sistemas de seguridad.

## Beneficio:

### Botnets

Cuando cientos, miles o cientos de miles de zombies (robot con malware que permite su control remoto) forman una red de ordenadores bajo control de un atacante se llama botnet. Difícil de detectar dada la capacidad de cómputo y multitarea de las máquinas actuales, sigiloso, ataques encubiertos, activas durante años, gran porcentaje de máquinas disponibles.

(Spam, distribuir malware, manipular encuestas, delegación de servicios)

Las botnets originales usaban IRC para controlar las máquinas. Recientemente, se ha sustituido IRC por HTTP. De esta forma es más difícil de detectar y bloquear además de permitir más independencia entre el atacante y la botnet.

### Spyware

Software que espía a los usuarios obteniendo información sin su consentimiento: Uso de recursos del sistema, instalación de programa, recolección y distribución de información personal o sensible, cambios en la experiencia del usuario, privacidad o seguridad del sistema.

**Efectos adversos**: Reducir el rendimiento, inestabilidad del sistema, barras de navegador, enlaces o página de inicio, Pop-ups.

### Adware

Proporciona publicidad de manera inesperada e indeseada. Puede provenir de otro malware. Contenido inapropiado, afecta a la productividad, puede provocar que la maquina deje de responder. Intención comercial. Similar a Spyware.

(Muestra banners o Pop-ups o Abre páginas web)

### Keyloggers

Captura y almacena cada pulsación en el teclado. Puede ser recuperado más adelante o transmitido a una localización remota. Objetivo de contraseñas o información personal. Puede ser un dispositivo hardware intercalado entre el teclado y el ordenador, un receptor inalámbrico o un software.

### Ransomware

**Cifrado:** Cifrado en ficheros en disco, uso de criptografía de clave.

**No cifrado:** Restringe el acceso al sistema con imágenes pornográficas, imita la activación de Windows, ofrecer fotos de famosos desnudos.

## Ingeniería Social:

### Caso verídico

**1.** Antes de entrar en el edificio, llaman a recursos humanos para obtener el nombre de ciertos empleados clave.

**2.** Al acercarse al edificio, un atacante simula haber perdido la llave. Un empleado les permite entrar.

**3.** Saben que el CFO está fuera por su buzón de voz. Entran en su oficina y obtienen información de su ordenador y documentos en papel.

**4.** Llaman a los técnicos desde la oficina del CFO suplantándole. Solicitan su contraseña puesto que la ha olvidado y está de camino a una reunión importante.

### Suplantación de identidad

**Suplantación:** Actuar como un personaje ficticio, personajes estándar o alguien de autoridad y esperar a solicitud de información.

**Phishing:** Enviar un e-mail o mostrar un anuncio que simula provenir de una fuente legítima con el objetivo de engañar al usuario para que proporcione información privada o El atacante copia logos, colores, texto, url y direcciones de e-mail para incrementar autenticidad.

### Spam y Hoax

**Spam:** E-mail no solicitado con fines comerciales, es uno de los vehículos primarios para otro malware, el beneficio económico es sorprendentemente alto. (Spim: mensajería instantánea)

**Hoax:** Aviso falso que proviene de los técnicos informáticos indica una alerta por un virus especialmente malicioso. Insta a modificar ciertos ficheros o cambiar los ajustes de seguridad, así como reenviar a otros empleados. El atacante tiene, de esta forma, vía libre para atacar el sistema. Otro enfoque consiste en solicitar cambios que hagan inestable el sistema para que el usuario llame al teléfono falso proporcionado en el hoax.

# Tema 4b – Ataques de aplicación y de red

## Ataques de Aplicación:

### Aplicaciones Web

Requiere enfoque alternativo puesto que no se protege 100% la aplicación de forma tradicional. Protección del servidor web, la entrada del usuario se procesa en la aplicación. Protección de la red, el bloqueo o control se realiza a nivel de servicio, el contenido HTTP no se examina.

### Cross Site Scripting (XSS)

Se inyectan scripts en un servidor de aplicaciones web con el objetivo de atacar el cliente. (inyección JavaScript). Cuando la víctima visita el web “inyectado”, se descarga un script malicioso que se ejecuta en su navegador. Se requiere un sitio web que acepte entrada sin validar y use esa entrada en una respuesta sin filtrarla.

### Inyección SQL

El objetivo es insertar comandos en servidores SQL. Surge por una falta de filtrado de la entrada. El atacante prueba a introducir una apóstrofe al final de la entrada, comprobando su efecto.

### Inyección XML

El ataque es similar a la inyección SQL, aprovechando una vía de entrada sin filtrar para introducir nuevo XML.

### Inyección de comandos

Consiste en escapar del directorio raíz del servidor web. El atacante puede utilizar esta vulnerabilidad para leer documentos ocultos o ejecutar comandos arbitrarios.

## Ataques en el Cliente

Explotar vulnerabilidades en las aplicaciones del cliente. Se activa al interactuar con un servidor comprometido o procesar datos maliciosos. (Drive-by download)

### Manipulación de cabeceras

**Referer:** El atacante modifica este campo para ocultar el hecho de que la petición no proviene de una página de ese sitio. Permitiría almacenar, modificar y realojar una página web

**Accept-Language:** Algunas aplicaciones pasan este valor de forma directa a la base de datos. El atacante puede intentar una inyección SQL modificando esta cabecera. Si la aplicación utiliza este valor para crear un nombre de fichero, el atacante podría lograr acceso a un directorio restringido.

### Cookies

HTTP no soporta controlar visitas previas, utiliza cookies para almacenar información en el cliente en relación con un usuario.

**Problemas de privacidad y seguridad:** explotadas por atacantes para otros fines, las cookies de terceros permiten monitorizar los hábitos de navegación del usuario a lo largo de muchas webs, las cookies de primera mano pueden ser robadas y utilizadas para hacerse pasar por el usuario.

### Tipos de Cookies

**Primera mano:** Se crea en el sitio que el usuario está visitando.

**Tercero:** Provienen de otros sitios web: anunciantes, etc.

**Sesión:** Se almacena en RAM y está activa únicamente durante la visita.

**Persistente:** Se almacena en el disco y pervive entre sesiones.

**Segura:** Se utiliza cuando el cliente visita un servidor por un canal seguro (SSL/TLS).

**Flash:** Permiten regenerar cookies borradas o bloqueadas, ocupan 25 veces más de tamaño.

### Asalto de sesión

Cuando un usuario entra con su usuario y contraseña el servidor le asigna un identificador de sesión (token). El ataque consiste en suplantar al usuario utilizando su token.

### Extensiones maliciosas

Programas que proporcionan funcionalidad adicional a los navegadores web (plugins). Una de las extensiones más conocidas son los controles Microsoft ActiveX que permiten gran funcionalidad.

**Problemas de seguridad:** ActiveX tiene acceso absoluto al disco y el sistema operativo. Un usuario puede descargar un control que esté activo para los demás usuarios de la máquina. Los controles pueden ser ejecutados de forma independiente al navegador. Proporciona un sistema de firma digital, pero no hay garantías de que no tenga vulnerabilidades.

### Desbordamiento

Ocurre cuando un proceso intenta almacenar datos en RAM más allá de los límites de un búfer de tamaño finito. Estos datos extra se desbordan a las posiciones de memoria adyacentes. Bajo algunas condiciones, la memoria sobrescrita contiene la dirección de retorno y permite que se ejecute código arbitrario en la máquina comprometida.

## Ataques en Red:

### Denegación de servicio (DoS)

Requiere un recurso finito y capacidad de extinción más rápida que reposición. DS distribuido (DDoS), permite a un grupo realizar ataques masivos.

**Posibles objetivos:** Sobrecargar servidores Web, sobrecargar enlaces de red, colgar servidores o atacar una dependencia.

**Propagación:** Inclusión de carga, descarga posterior.

**Ataque:** Preplanificado con objetivo de cuelgue o reinicio, rotura o sobrecarga.

**Tipos:** Ping Flood (obligación de respuesta), Amplificación de DNS (Respuesta mucho más grande que la petición) y DDoS a nivel de servicio (Gran volumen de peticiones correctas)

**Consejos:** Guardar logs, observaciones y pasos dados, estar al día en los ataques DDoS y defensas, monitorizar la red en busca de sistemas vulnerables, comprobar regularmente que las máquinas no pertenecen a una botnet, monitorizar logs en busca de actividad sospechosa (IDS), establecer una rutina de actualización, escaneo y monitorización

### Intercepción

**Man-in-the-Middle:** Un atacante se intercala entre dos interlocutores que no sospechan de su existencia. Puede ser pasivo (Los datos se capturan y retransmiten sin modificaciones) y activo (Los datos se alteran antes de ser retransmitidos).

**Reproducción:** Similar a un ataque MITM pasivo, la información se almacena y se reproduce después (no de forma inmediata), puede ser una herramienta valiosa en credenciales y otros servicios y protocolos.

### Envenenamiento ARP

ARP permite obtener la dirección MAC de una determinada IP. El atacante modifica la dirección MAC en la caché ARP para que la IP correspondiente apunte a un ordenador distinto. Aunque se puede realizar de forma manual, existe gran cantidad de herramientas automatizadas.

Es un ataque satisfactorio puesto que ARP no soporta autentificación para verificar el origen de las peticiones y respuesta.

**Ataques asociados:** Robo de datos, denegación de acceso, MITM y denegación de servicio.

### Envenenamiento DNS

DNS es un sistema jerárquico para asociar nombres a máquinas en una red IP. El atacante sustituye una IP fraudulenta para un nombre en el sistema DNS.

Se puede realizar en dos sitios: Tabla de hosts local o servidor DNS externo.

Se puede utilizar zone transfers para convencer al servidor DNS de que acepte la IP fraudulenta [error en protocolo].

El gobierno chino usa envenenamiento DNS para filtrar contenidos no apropiados.

### Derechos de acceso

**Escalado de privilegios:** Consiste en explotar una vulnerabilidad local para obtener acceso a recursos restringidos.

**Ejemplos:** Un usuario sin privilegios escala para acceder servicios que requieren privilegios mayores. Un usuario utiliza escalado para obtener acceso a través de otra cuenta que sí tiene los privilegios adecuados.

**Acceso transitivo:** Consiste en utilizar una tercera parte para obtener acceso.

**Ejemplo:** A puede ofrecer servicios de backupa B, pero A implementa su backup en base a los servicios de C. ¿Qué credenciales se han de usar? B tendría acceso a los recursos de C.

# Tema 4c – Seguridad en wireless

## Ataques Wireless:

### Car Hacking

Irrumpir en el sistema electrónico del coche. Se puede cambiar ajustes y settings o desactivar sistemas de seguridad. Vías de ataque: Red bluetooth, 3G a bordo, Troyano en mp3. Hacer que el coche transmita marca/modelo y posición GPS. Tiene vulnerabilidades y son el objetivo de atacantes.

### Bluetooth

Es una tecnología PAN.

**Bluejacking:** Envío de mensajes no solicitados a dispositivos activos. Consiste en texto, imágenes o sonido. Es más molesto que dañino (spam). Ha sido utilizado por anunciantes.

**Bluesnarfing:** Acceder información no autorizada a través de conexiones bluetooth. El atacante puede copiar e-mails, calendario, contactos, etc. Se ha usado contra celebridades. El bluetooth debe estar desactivado cuando no se utilice.

## Ataques WiFi

Las transmisiones Wireless (o Puntos de acceso) no están sujetas a los mismos límites que las cableadas. Un atacante puede interceptar, fácilmente, transmisiones no cifradas recuperando contraseñas, información privada e incluso modificar el mensaje. También se puede producir un ataque de interferencia remoto mediante un inhibidor de frecuencias (DoS)

## Descubrimiento

**Beaconing:** Transmisión cada 100µS para anunciar la presencia de una red WiFi. Los atacantes usan esta información para encontrar y catalogar redes WiFi.

**WarDriving**: Consiste en buscar redes en coche o a pie usando un dispositivo móvil.

## Ataques mediante espectro RF

Se puede analizar el tráfico capturado de igual forma que se hace en conexiones cableadas. Es necesario el modo monitor para que pueda capturar paquetes sin estar asociado a un punto de acceso. Un atacante puede provocar interferencias (Microondas, teléfonos, etc.) para evitar que un dispositivo se comunique con el punto de acceso.

## Ataques con Puntos de Acceso

**No autorizado:** Instalación no autorizada de un punto de acceso por un empleado. Generalmente mal configurado o sin seguridad. Permite el acceso a la red interna desde el exterior de las instalaciones sin control del firewall.

**Gemelo maligno:** Punto de acceso instalado por un atacante. Emula un punto de acceso legítimo por lo que los dispositivos se conectan al mismo. El atacante puede capturar el tráfico que proviene de los usuarios conectados.

## Vulnerabilidades de IEEE 802.11

**Filtrado de MAC:** Es un esquema de seguridad que limita el acceso a ciertas MAC legítimas. Permite bloquear o autorizar direcciones. Es susceptible de ataque puesto que se intercambian en abierto. Resulta muy difícil gestionar grandes cantidades de usuarios de esta forma.

**Retransmisión SSID**:

- **Autentificación abierta**: Sólo es necesario el SSID correcto. El atacante puede obtener el SSID de diversas formas.
- **Ocultar SSID:** El SSID se transmite también en otros paquetes de gestión. Puede evitar el roaming. No siempre se puede ocultar. En Windows XP siempre se conecta al dispositivo con retransmisión de SSID.

### WEP

Proporciona un cierto nivel de confidencialidad. Se basa en una **clave precompartida** entre el punto de acceso y los dispositivos. La clave puede ser de 64 o 128 bits

Al atacante le basta con descubrir el texto en claro de uno de los paquetes (o parte) para descubrir el texto en claro de todos los paquetes que usen el mismo IV

**¿Cómo puede el atacante encontrar suficiente texto en claro del paquete 1 para obtener el paquete 222?**

Conoce ciertos campos de los paquetes, el cuerpo del paquete suele contener ASCII, un atacante puede capturar un paquete de 28 bytes sabiendo que es una petición ARP, se puede enviar datos desde fuera de la red (Internet) al dispositivo.

## Soluciones de Seguridad Wireless:

### WPA

**Cifrado TKIP:** Utiliza claves de 128 bits y cambian en cada paquete, evitando las colisiones. Sustituye el CRC por un Message Integrity Check (MIC) ~ Hash.

**Autentificación PSK:** Autentificación WPA usando 802.1x, La clave debe estar precompartida en el punto de acceso y todos los dispositivos. Al contrario que en WEP la PSK no se utiliza para el cifrado, se utiliza como punto de inicio para la función generadora de claves de cifrado.

**-Vulnerabilidades:** Gestión incorrecta de claves PSK (La distribución de claves PSK se realiza de forma manual y sin seguridad añadida: cualquier usuario que obtenga la clave es considerado auténtico) y las contraseñas PSK (Uso de contraseñas débiles).

### WPA2

El objetivo es evitar las vulnerabilidades basadas en autentificación y el sistema de cifrado en WLANs

**Cifrado AES-CCMP**: AES en modo contador (CTR) para la privacidad y en CBC-MAC para la integridad de datos. Necesario realizar las operaciones de AES en hardware para poder atender la demanda de múltiples dispositivos.

**Autentificación IEEE 802.1x:** Diseñado para redes cableadas, implementa seguridad por puerto. Bloquea el tráfico puerto a puerto hasta que el cliente se ha autentificado mediante las credenciales almacenadas en un servidor de autentificación o De esta forma se evita que un dispositivo sin autorización reciba ningún tráfico hasta que su identidad pueda ser verificada.

### EAP

Es un framework que define los mensajes a utilizar por los protocolos de autentificación definidos sobre el mismo.

**Lightweight EAP (LEAP)**: Creado por CISCO (propietario), no soportado en Windows, vulnerable.

**Protected EAP (PEAP)**: Diseñado para utilizar logins y passwords de Windows, crea un canal cifrado entre el cliente y el servidor de autentificación: más flexible.

## Otros factores

**Disposición de antenas:** Los puntos de acceso deben ser colocados en el centro del área a cubrir. Idealmente se colocarán en el techo para evitar interferencias y robo del dispositivo. Se debe minimizar la cantidad de señal que alcanza fuera del edificio o campus

**Control de potencia:** Algunos puntos de acceso permiten ajustar la potencia para restringir la señal a la zona requerida.

**Descubrimiento de puntos de acceso no autorizados:** Es un problema delicado para las organizaciones de cierto tamaño. Existen varios métodos para detectar estos puntos de acceso. (Manual/Automatizado) Hay 4 tipos de sensores Wireless (Dispositivo Wireless, PC con USB, PA y sensor dedicado).

**WVLANs:** Consiste en segmentar las redes Wireless para aumentar la seguridad.

Muchas organizaciones establecen 2 redes virtuales: Una para acceso de empleados que tiene acceso a la base de datos y ficheros y otra para invitados con acceso limitado a Internet o archivos públicos

Existen 2 enfoques: División en switch con varios puntos de acceso y puntos de acceso con soporte para VLAN.