

ATAQUES SOBRE SISTEMAS

WEB Y MOVILES

SISTEMAS MOVILES

1. *filtración de datos*

Por regla general, se trata de aplicaciones gratuitas que es posible encontrar en tiendas oficiales y que se ejecutan según su descripción, pero que también envían información personal

En este caso, el malware móvil utiliza un código de distribución nativo en sistemas operativos móviles populares, como iOS y Android, para difundir datos valiosos en redes corporativas sin levantar sospechas.



2. *Wi-fi no segura*

las redes Wi-Fi gratuitas generalmente son inseguras.

Procura usar las redes Wi-Fi con prudencia en tu dispositivo móvil y no te conectes nunca a ellas para acceder a servicios confidenciales o personales, como sitios web de banca o información de tarjeta de crédito.



3. *Suplantación de red*

(conexiones que parecen redes Wi-Fi, pero que en la práctica son una trampa) en ubicaciones públicas concurridas, como cafeterías, bibliotecas y aeropuertos.

demás de recurrir a la prudencia cuando te conectes a cualquier red Wi-Fi gratuita, no proporciones nunca información personal y, si te solicitan crear credenciales de inicio de sesión, crea siempre una contraseña única, por si acaso.



4. *Ataques de phishing*

Como los dispositivos móviles están siempre encendidos, son las primeras líneas de cualquier ataque de phishing.

Según [CSO](#), los usuarios móviles son más vulnerables porque a menudo son los primeros en recibir correos electrónicos aparentemente legítimos y caer en la trampa.



5. *Spyware*

Existe una amenaza clave más cercana: el [spyware](#). En numerosos casos, no es el malware lo que debe preocuparles, sino el spyware instalado por cónyuges, compañeros de trabajo o empleadores para rastrear sus desplazamientos y patrones de uso.

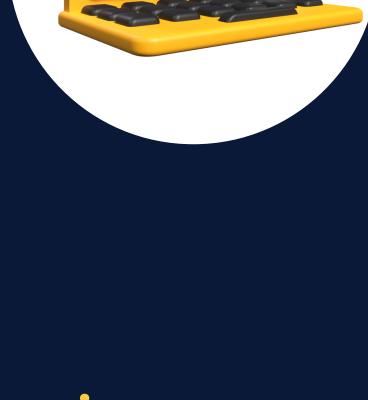


6. *Criptografía quebrada*

En el primer caso, los desarrolladores utilizan algoritmos de cifrado que ya poseen vulnerabilidades conocidas para acelerar el proceso de desarrollo de aplicaciones y el resultado es que cualquier atacante decidido puede descifrar las contraseñas y obtener acceso.

En el segundo ejemplo, los desarrolladores utilizan algoritmos altamente seguros, pero dejan abiertas otras "puertas traseras" que limitan su eficacia.

los hackers puedan no llegar a necesitar las contraseñas para provocar estragos.



6. *Gestión inadecuada de las sesiones*

Según el [Proyecto de seguridad de aplicaciones](#) de The Open Web, la gestión inadecuada de las sesiones se produce cuando las aplicaciones comparten involuntariamente tokens de sesión con entidades maliciosas, lo que les permite hacerse pasar por usuarios legítimos.



SISTEMAS WEB

1. Inyección SQL

Los atacantes insertan código SQL malicioso en formularios web u otras entradas para manipular las consultas de bases de datos y obtener acceso no autorizado a la información almacenada en la base de datos.



2. Cross-Site Scripting (XSS):

Los atacantes injecan scripts maliciosos en las páginas web que luego se ejecutan en el navegador de los usuarios. Estos scripts pueden robar información del usuario o realizar acciones no autorizadas en su nombre.



Cross-Site Request Forgery (CSRF):

Los atacantes engañan a los usuarios para que realicen acciones no deseadas en un sitio web sin su conocimiento. Esto se logra a través de enlaces o formularios falsificados que aprovechan la sesión activa del usuario en el sitio objetivo.



Ataques de inyección de comandos:

Similar a la inyección SQL, en este caso los atacantes insertan comandos maliciosos en entradas de la aplicación web para ejecutar código en el sistema subyacente.



Fuga de información sensible

Los atacantes buscan y explotan fallos en la configuración del servidor o en la aplicación para acceder a información sensible, como contraseñas almacenadas en texto plano.



Fuerza bruta y ataques de diccionario:

Los atacantes intentan adivinar contraseñas probando diferentes combinaciones de nombres de usuario y contraseñas hasta que encuentran la correcta.



Exposición de directorios y archivos:

Los atacantes buscan y acceden a archivos o directorios que no deberían ser públicos, exponiendo así información confidencial.



Denegación de servicio (DoS) y Distributed Denial of Service (DDoS):

Los atacantes intentan abrumar un servidor o servicio web con una gran cantidad de tráfico falso, lo que hace que el sistema sea inaccesible para los usuarios legítimos.

Ataques de manipulación de sesiones:

Los atacantes intentan robar o manipular las credenciales de sesión de los usuarios para obtener acceso no autorizado a sus cuentas.

Ataques de manipulación de sesiones:

Los atacantes intentan adivinar las credenciales de acceso al probar diferentes combinaciones de nombres de usuario y contraseñas.



UNIVERSIDAD AUTONOMA DE
CHIAPAS

ALUMNO: TOMÁS ÁLVAREZ GÓMEZ
MATERIA: ANALISIS DE VULNERABILIDADES
ACT 1.4