¿Por qué hablar de malware?


Emprendimiento
para Jóvenes
Fomentando la Innovación y la
Creatividad

Isaac Ruiz


Recorrido de Incibe Emprende
incibe emprende 2023-2026
Charlas - Talleres Eventos
Incubadora de proyectos
Aceleradoras Express

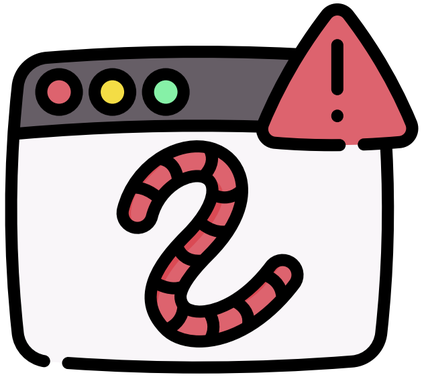
Tipos comunes de malware

Virus informáticos

- **Necesitan un archivo huésped (documentos, programas).**
- **Se activan cuando el usuario abre o ejecuta ese archivo.**

Gusanos (worms)

- Se autorreplican sin intervención del usuario.
- Se propagan por redes, correos o vulnerabilidades del sistema

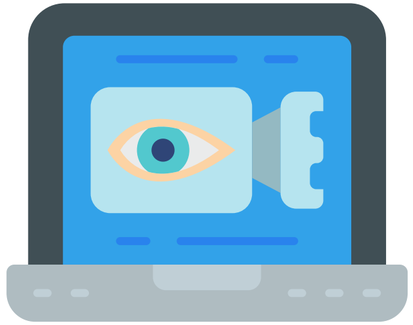


Ransomware

- Secuestra archivos o el dispositivo completo.
- Exige un pago para recuperar el acceso.

Spyware

- Espía la actividad del usuario.
- Roba contraseñas, pulsaciones del teclado, datos personales.



Troyanos

- Se disfrazan de software legítimo.
- El usuario los instala voluntariamente sin saberlo.

Adware

- Muestra publicidad invasiva.
- Aunque parece inofensivo, suele recolectar datos.

Vías de infección más comunes

Correos electrónicos sospechosos

Correos electrónicos sospechosos

Descargas desde sitios no seguros

Correos electrónicos sospechosos

Descargas desde sitios no seguros

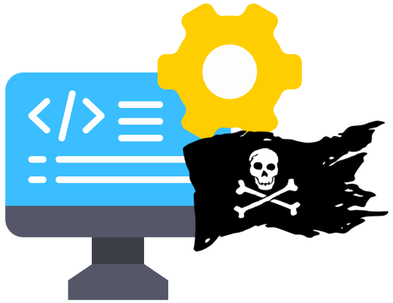
Dispositivos USB infectados

Correos electrónicos sospechosos

Descargas desde sitios no seguros

Dispositivos USB infectados

Software pirata



Objetivos del malware

1. **Robo de credenciales y dinero**

1. **Robo de credenciales y dinero**
2. **Secuestro de dispositivos**

1. **Robo de credenciales y dinero**
2. **Secuestro de dispositivos**
3. **Uso del equipo para delitos**

Prevención y buenas prácticas

1. **Antivirus y software de seguridad**

1. **Antivirus y software de seguridad**
2. **Sistema operativo actualizado**

1. **Antivirus y software de seguridad**
2. **Sistema operativo actualizado**
3. **Desconfiar de enlaces y archivos**

1. **Antivirus y software de seguridad**
2. **Sistema operativo actualizado**
3. **Desconfiar de enlaces y archivos**
4. **Autenticación de doble factor**

Mensaje final

- **El malware es real.**
- **No distingue entre expertos y usuarios normales.**
- **La mayoría de infecciones se producen por errores humanos, no técnicos.**

Malware: Amenazas y Cómo Protegerte

El malware es software malicioso diseñado para dañar o espiar dispositivos sin permiso. Afecta a cualquier persona, no solo a expertos, y la mayoría de las infecciones ocurren por acciones cotidianas como abrir un correo o descargar un archivo.

La Amenaza: Conoce al Enemigo Digital

Ransomware: El Secuestrador

Ofre tus archivos o bloques tu dispositivo y exige un pago para llberarlos.

Troyano: El Faiso Regalo

Se diefraza de programa útil para que lo instales, abriendo una puerta a los atacantes.

Spyware: El Espía Sliencioso

Registra tu actividad, roba contraseñas y datos personales sin que te des cuents.

¿Cómo Llega a Tus Dispositivos?

Las vías de infección más comunes son simples y se basan en el engaño.

Correos Electrónicos (Phishing): Enlaces y adjuntos que suplantan a entidades de confianza (bancos, empresas).

Descargas Inseguras: Software "gratuito", pirata o de páginas web no oficiales que oculta el malware.

Dispositivos USB: Un pendrive encontrado o prestado que contiene archivos infectados.

La Defensa: 4 Pasos Clave para tu Seguridad

1. Mantén Todo Actualizado

Un antivirus y sistema operativo al día corrigen las vulnerabilidades que usa el malware.

2. Desconfía por Defecto

La regla de oro: si un enlace, archivo o correo te genera la más mínima duda, no hagas clic.

3. Activa el Doble Factor de Autenticación (2FA)

Es una segunda llave para tus cuentas; aunque roben tu contraseña, no podrán entrar.

4. Descarga Solo de Fuentes Oficiales

Evita el software pirata o de sitios extraños; usa siempre las tiendas y webs legítimas.