



ADWARE

Paulo Mantilla
Aldo González
Diego Cano
Ferdinand Miranda

DEFINICION

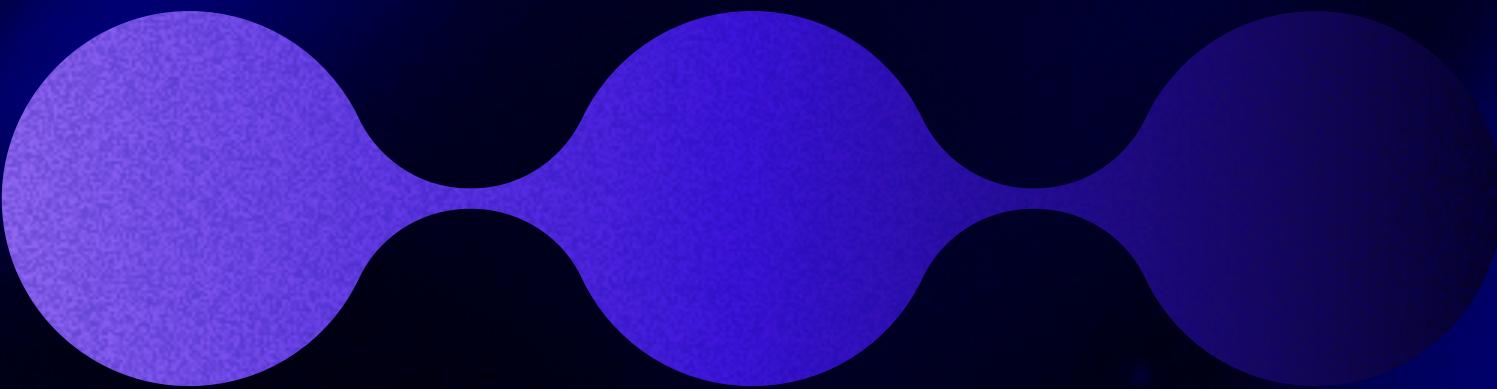
El adware (advertising-supported software) es un tipo de software no deseado que muestra publicidad intrusiva en dispositivos, como ventanas emergentes, banners o redirectiones a sitios web. Su objetivo principal es generar ingresos para sus desarrolladores a través de la publicidad, a menudo sin el consentimiento del usuario.



CASO FAMOSO: SUPERFISH

Superfish fue un adware preinstalado en computadoras Lenovo entre 2014 y 2015. Este software insertaba anuncios en los resultados de búsqueda de los usuarios, incluso en conexiones HTTPS (que deberían ser seguras).

Superfish comprometía la seguridad de los usuarios al interceptar el tráfico encriptado, lo que permitía a los atacantes realizar ataques de "man-in-the-middle" (hombre en el medio) y robar información sensible, como contraseñas o datos bancarios.



COMO IDENTIFICARLO?

Anuncios intrusivos

APARECEN VENTANAS
EMERGENTES, BANNERS O
REDIRECCIONES
CONSTANTES, INCLUSO
CUANDO NO ESTÁS
NAVEGANDO EN
INTERNET.

Rendimiento lento

LA COMPUTADORA SE
VUELVE MÁS LENTA DE LO
NORMAL DEBIDO AL
CONSUMO DE RECURSOS
POR PARTE DEL ADWARE.

Tráfico inusual

SI NOTAS UN AUMENTO
EN EL USO DE DATOS O
ACTIVIDAD EN LA RED,
PODRÍA SER SEÑAL DE
ADWARE.

COMO AFECTA MI COMPU?

ESTAS SON LAS AFECTACIONES QUE HACE A TU ORDENADOR ESTE TIPO DE SOFTWARE MALICIOSO

RENDIMIENTO

EL ADWARE CONSUME RECURSOS DEL SISTEMA (CPU, MEMORIA RAM), LO QUE RALENTIZA LA COMPUTADORA.

SEGURIDAD

ALGUNOS ADWARES ABREN PUERTAS PARA MALWARE MÁS PELIGROSO, COMO SPYWARE O RANSOMWARE.

PRIVACIDAD

RECOPILA DATOS PERSONALES, COMO HÁBITOS DE NAVEGACIÓN, Y LOS ENVÍA A TERCEROS SIN TU CONSENTIMIENTO.

SOLUCION

1. Usar un antivirus o antimalware:

- Herramientas como Malwarebytes, Avast, Windows Defender o AdwCleaner pueden detectar y eliminar adware.
- Ejecuta un análisis completo del sistema.

2. Desinstalar programas sospechosos:

- Ve a Panel de Control > Programas > Desinstalar un programa (en Windows) o Aplicaciones (en macOS).
- Busca y elimina cualquier software que no reconozcas o que parezca sospechoso.

3. Mantener el sistema actualizado:

- Instala las últimas actualizaciones del sistema operativo y del navegador para evitar vulnerabilidades.

4. Evitar descargas sospechosas:

- Descarga software solo de fuentes oficiales y evita hacer clic en anuncios o enlaces dudosos.