¿Qué es el malvertising?

¿Qué es el malvertising?

El malvertising, una combinación de las palabras «malicious» (malicioso) y «advertising» (publicidad), se refiere a la práctica de distribuir software malicioso a través de anuncios digitales. Esta táctica explota las plataformas publicitarias legítimas para infectar los dispositivos de los usuarios con malware, sin que ellos tengan que hacer clic en los anuncios. Es una forma insidiosa de ciberataque que aprovecha la confianza que los usuarios depositan en sitios web populares y plataformas de publicidad.

¿Cómo funciona?

El malvertising se lleva a cabo al insertar código malicioso en anuncios que se distribuyen a través de redes publicitarias. Estos anuncios pueden aparecer en sitios web respetables y bien conocidos, lo que hace que los usuarios no sospechen de la amenaza. Cuando un usuario visita una página que contiene un anuncio malicioso, el código puede redirigir el navegador a sitios web peligrosos o directamente descargar malware en el dispositivo del usuario.

Tipos de ataques comunes en malvertising:

1. **Redirecciones automáticas:** El usuario es redirigido automáticamente a una página web que intenta instalar malware en su dispositivo o a un sitio de phishing.
2. **Exploits de vulnerabilidades:** Los anuncios maliciosos aprovechan vulnerabilidades en el software del dispositivo (como el navegador o plugins) para ejecutar código malicioso sin ninguna interacción por parte del usuario.
3. **Descargas de drive-by:** Sin necesidad de que el usuario haga clic, el simple hecho de cargar la página infectada

puede iniciar la descarga de malware.

Ejemplo notable: El caso de The New York Times (2009)

Uno de los casos más conocidos de malvertising ocurrió en 2009, cuando el sitio web de **The New York Times** fue víctima de este tipo de ataque. Unos cibercriminales compraron espacio publicitario en el sitio utilizando credenciales falsas. Durante un fin de semana, los anuncios que se mostraban en la página principal del sitio redirigieron a miles de usuarios a un sitio malicioso que intentaba instalar software de seguridad falso (también conocido como «scareware») en sus computadoras. Este ataque generó un gran escándalo debido a la reputación de la plataforma afectada y la cantidad de usuarios expuestos.

Prevención y protección:

Para protegerse contra el malvertising, tanto los usuarios como los administradores de sitios web deben adoptar prácticas de seguridad robustas:

- **Usuarios:** Mantener el software actualizado, usar bloqueadores de anuncios confiables, y contar con un antivirus actualizado.
- **Administradores y editores:** Verificar la legitimidad de los anunciantes, monitorear regularmente las campañas publicitarias y utilizar sistemas de detección de fraudes.