Scareware

Normalmente se utilizan tácticas de ingeniería social basadas en el miedo para engañar a los usuarios. Se presenta a menudo como un software legitimo (antivirus, limpiadores del sistema, etc.) y utiliza alertas falsa para asustar a las victimas y persuadirlas para comprar o instalar software inútil o malicioso.

¿Cómo funciona?

Aparecen ventanas emergentes para "advertir" que se encontraron archivos pornográficos o peligrosos en el dispositivo y seguirán apareciendo hasta que no se haga clic en los botones que "eliminan las amenazas". Se diseñaron para verse como mensajes genuinos de advertencia, mediante el uso de tácticas de ingeniería social, Estas tácticas se diseñaron para incitar sentimientos de pánico y temor. Se hace esto para que los usuarios tomen decisiones apresuradas e irracionales y engañarlos.
El resultado menos dañino sería una pérdida de dinero e instalar software inútil que no repare el dispositivo, por otro lado, la opción más dañina seria que el estafador use los números de tarjeta y datos personales para robar dinero y cometer robo de identidad. Incluso podría llegar a tomar como rehén el contenido del disco duro y se tenga que pagar un rescate.
Lo que los ciberdelincuentes quieren que el usuario haga es:

- Comprar software falso/inútil
- Descargar distintos tipos de software malicioso.
- Visitar sitios web que automáticamente descargan e instalan software malicioso en los dispositivos.

Ejemplos

Muchos programas de scareware copian elementos de interfaz de usuario de programas reales de protección contra malware y utilizan nombres que suenen legítimos. Algunos ejemplos son:

- XPAntivirus/AntivirusXP
- Antivirus360
- PC Protector
- Mac Defender
- DriveCleaner
- WinAntivirus