Puerta trasera

Es cualquier método que permite a alguien acceder remotamente a los dispositivos sin el permiso o conocimiento del usuario. Los hackers pueden instalar una pueta trasera en el dispositivo utilizando malware, explotando vulnerabilidades del software o incluso instalado directamente en el hardware/firmware en el dispositivo.

¿Cómo funciona?

Para que los hackers pueden instalar una puerta trasera en el dispositivo, primero deben de obtener acceso al mismo, ya sea por medio de un acceso físico, un ataque de malware o explotando vulnerabilidades del sistema. Algunas de las vulnerabilidades pueden ser: puertos abiertos, contraseñas débiles, softwares obsoletos, firewalls débiles.

Ejemplos

Cryptojacker DoublePulsar

En 2017, los investigadores de seguridad descubrieron que el malware de puerta trasera DoublePulsar (que fue desarrollado originalmente por la NSA) se utilizaba para vigilar los PC con Windows, instalando un cryptojacker en los ordenadores con suficiente memoria y potencia de CPU. El cryptojacker robaba la capacidad de procesamiento de los ordenadores infectados para minar Bitcoin.

PoisonTap

Es un malware de puerta trasera que permite a los piratas informáticos acceder a casi cualquier sitio web en el que se haya iniciado sesión (incluidos los sitios protegidos con autenticación de dos factores). PoisonTap es un malware bastante aterrador, pero afortunadamente sólo puede instalarse conectando directamente un ordenador Raspberry Pi al puerto USB de la víctima.