Back Door

It is any method that allows someone to remotely access devices without the user's permission or knowledge. Hackers can install a backdoor on the device using malware, exploiting software vulnerabilities, or even directly installing hardware/firmware on the device.

How does it work?

In order for hackers to install a backdoor on the device, they must first gain access to it, either through physical access, a malware attack, or by exploiting system vulnerabilities. Some of the vulnerabilities can be: open ports, weak passwords, outdated software, weak firewalls.

Examples

DoublePulsar Cryptojacker

In 2017, security researchers discovered that the DoublePulsar backdoor malware (which was originally developed by the NSA) was used to monitor Windows PCs by installing a cryptojacker on computers with enough memory and CPU power. The cryptojacker stole the processing power of infected computers to mine Bitcoin.

PoisonTap

It's a backdoor malware that allows hackers to access almost any website that's logged in (including sites protected with two-factor authentication). PoisonTap is a pretty scary malware, but luckily it can only be installed by directly connecting a Raspberry Pi computer to the victim's USB port.