PEGASUS

Spyware:

Spyware is a type of malicious software that penetrates your system, gathers data about you, and transmits it to a third party without your knowing. Spyware is also a legal term for software that monitors your data for commercial purposes such as advertising. Malicious spyware, on the other hand, is designed to profit from content which has been stolen. The monitoring operations of spyware, whether legitimate or fake, expose you to data breaches and exploitation of your sensitive data. Spyware also has an impact on network and device performance, which slows down normal user activity.

Pegasus:

Pegasus is also a spyware that attacks your computer, gathers the data from your system and send it to some other remote system located to anywhere in the world. It was developed by NSO Group. It is arguably the strongest spyware ever developed. Its purpose is to infiltrate Android and iOS phones and turn them into spying devices. Israeli corporation sells it as a tool for tacking criminals and terrorists — not for mass surveillance, but for specific snooping. NSO Group seems to be the only company that offers the software to governments. A single licence may cost up to Rs 70 lakh and infect multiple phones. NSO Group charged $650,000 for infecting 10 devices, plus a $5000 installation fee, according to a price sheet from 2016.

How it works:

Pegasus takes use of Android and iOS flaws that have yet to be disclosed. This implies that even if a phone has the most recent security patch installed, it might be compromised. Most recently the fact that Pegasus, spyware, can achieve zero-click installations in various ways makes it so effective and dangerous at the same time. It uses one over-the-air (OTA) option to send a push message covertly that makes the target device load the spyware, with the target unaware of the installation over which he/she anyway has no control. An earlier version of the malware, launched in 2016, used a technique known as "spear-fishing," which entailed sending the victim text messages or emails containing a harmful link. It was conditional on the target clicking the link, which was eventually deleted in later versions.

Pegasus was claimed in 2019 to be able to enter a device with a missed WhatsApp call and even remove the record of the missed call, making it difficult for the user to notice they were being monitored. According to WhatsApp in May 2019, Pegasus used a flaw in WhatsApp's code to infect over 1,400 Android and iPhone phones, including even government officials, journalists, and human rights activists. Pegasus also exploits weaknesses in the iMessage system to get backdoor access to a wide range of iPhones. Installing malware with a wireless transceiver (radio transmitter and receiver) near a target is also possible.