Probably a couple of years ago, if you asked a security expert if risk from mobile malware could be real, you would get a mixed response. But the same question asked today will draw consensus on the fact that risk of mobile malware is real and evolving. Since malware has proven successful on traditional platforms, it has subsequently found its way to mobile devices. Let us have a look at mobile malware, and how it is different from malware attacks on traditional devices.

One of the early mobile malware, a virus named as Timofonica, was discovered back in the year 2000. Malware found in modern devices, however, is far greater in strength than it was almost two decades back. For example, Ghost Push, an Android malware discovered in 2015, gets privileged control over your Android device and cannot be removed unless you flash your firmware. It can also install other malicious software programs into your system, send push advertisements and drain your battery life, etc.

Similarly, malware programs XcodeGhost and XcodeGhost S are modified versions of Xcode, a development environment of Apple. This malware not only steals user device information, but also opens specific URLs upon opening an infected app, reads and writes from clipboard, and infects other apps. One of the greatest threats put forth by this malware is that it can be controlled remotely by an attacker through HTTP from a command and control server. A developer could develop an app with XcodeGhost without knowing so and once the app makes it to the App Store, the Ghost begins to perform its malicious duties.

*Mobile apps pose major malware threat*

And this is why mobile malware is different from conventional platforms. Just like traditional computer systems, clicking malicious links can infect a mobile device with malware. But it is the mobile application that poses real danger to mobile devices. When it comes to installing apps, we have many options, but not every option is safe. One such option is sideloading; a process where Android users can install apps from sources other than the Play Store. Third parties such as Mobogenie, Amazon, Appbrain, etc. offer applications that may not be available to users on the Play Store. Another option is to look for Android.apk files and find a multitude of applications. These options may seem convenient, but they also open doors for malicious software and compromise your mobile devices. For iOS, a device can invite malware once you install a malicious app from a source other than AppStore. Even if you don’t jailbreak your iPhone and don’t sideload your Android device, you can still give way to malware inside your device. The latest example of this is AceDeceiver, a malware that was spread in early 2016 by apps downloaded from the AppStore.

Enterprises need to invest in mobile app security testing and security awareness training of its employees to follow best practices. Best practices also include mandating the installation of apps from official application stores only, such as Google’s Play Store and Apple’s AppStore. They can also use market-leading solutions. However, not all apps require the same level of mobile app security testing and organizations need to identify the ones that require additional security.