The growth in mobile industry has opened new doors for cyber criminals, and where technology has significantly advanced, security has taken a step back. This is because human error is a major factor in making a cyber-attack successful and because mobile devices are individually owned, most of them do not have any safety measures in place. According to a recent study, more than one third of mobile users do nothing to keep their devices secure. This is why the recent years have seen a considerable increase in the development of mobile malware.

Because Android runs on a sizeable majority of smart devices, Android app security is more challenged as compared to iOS-running devices. Let us look at some of the most malicious and most recent malware discovered on Android devices all over the world.

**HummingBad**

Developed by a famous Chinese advertising agency known as Yingmob, HummingBad tricks users into clicking advertisements, thus generating revenues for the agency in return. Though it has not yet been used by the ad agency for anything other than revenue-generating ads, it holds the capability to do all malicious activities such as stealing bank login details, etc.

**Stagefright**

Stagefright has been termed as perhaps the biggest threat to android app security and to mobile security in general. It seems as though the bug is back for the third time. Due to the ease with which it enters a tablet or phone and the fact that it does not require the victim’s involvement to infect their own device, it is more dangerous as compared to other malware types.

The most recent version of Stagefright has been named as Metaphor, and can take over your mobile device in as less as 15 minutes. Approximately one billion devices worldwide have Stagefright vulnerability. Metaphor infects a system when the victim receives a message that contains a link to a video which crashes the media player and restarts the phone.

**Ghost Push**

Another recent threat to Android app security, this malware has been around for two years. It mostly enters devices through third party apps and suspicious links, but recently it has been found to be making its ways through apps on the Google Play Store. Once it enters a system, it disguises itself as a built-in app and tricks the device into following its instructions. It can then take control of the device and display advertisements, load unsuitable content, etc.

Devices with android 6.0 Marshmallow and above are not affected by Ghost Push, but even then half of Android devices are still prone to this Malware because of outdated Android versions.