Danger lurks in third-party Android app stores

By A Prasad

Published: 2016-02-19 · Archived: 2026-04-05 19:24:42 UTC

As the adoption of smartphones and the reliance on mobile apps increases, security has become a critical issue depending on where the apps are downloaded from. Security firms have found that third-party app stores harbour dangers of malware capable of rooting victims' devices, delivering malicious ads and collecting sensitive user data from the mobile phones.

Recent Google data shows that devices of users who have sideloaded or installed apps from third- party app stores have a higher chance of getting infected than those of users who install apps only from Google's Play store.

Speaking at a Kaspersky Lab Security Analyst Summit, Elena Kovakina of Google's Android security team said Google scans more than two million apps every week for its 1.4 billion Android users, and collects a lot of data from its users. She stressed that using the Play store is much safer than using third-party app stores. "It turns out that using only Play is ten times safer than side-loading too," she said.

She added that countries like Iran, India, and Indonesia typically have the highest rates of PHA (potentially harmful app) installation, so much that about 2%-2.5% of devices have at least one PHA installed.

The apps from these stores often appear legitimate and function normally, but may contain malware that tricks the user into downloading malicious code that can take complete control of the user's device by gaining root access. The malware can then collect all sensitive and personal user data on the device. The apps also mimic popular apps, increasing the chances of getting selected and downloaded. These include mobile games, mobile security apps, camera apps and music streaming apps. Some known third party app stores are Nineapps, Mobogenie, Getjar, Aptoide, Vshare, and Onemobile.

One of the most recent malware families spread through these types of third party app stores is ANDROIDOS_LIBSKIN.A. Another malware doing the rounds is the Mazar Bot that gives attackers full administrative rights to monitor and control users' phones. Another one is the "trojanised adware" known as Shuanet, Kemoge and Shudun. The malware could insert adware into 20,000 commonly-used apps like Facebook, Candy Crush Saga, Twitter, WhatsApp and Snapchat.
