certin Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2018-0033

Security issues of Fake mobile applications

Original Issue Date: November 16, 2018

Severity Rating: Low

Description

Fake mobile apps are Android or iOS applications that mimic the look and/or functionality of legitimate applications to trick unsuspecting users to install them. Once installed on a smartphone/mobile device, the fake app can perform a variety of malicious actions. Some fake applications are built to persistently push advertisements to rake in advertisement revenue, other apps are designed to harvest credentials, track and report location, intercept sensitive data, divert revenue or infect devices.

Some fake apps can install malware to steal personal information, lock personal files and demand money and they can even delete all your personal data. Fake apps can harm your device in many possible ways. It will eventually steal your information and destroy your device.

Be aware about threats associated with fake game apps and pirated video games as they can harm your mobile devices by installing embedded malicious programs.

Some of the apps take advantage of the absence of an official mobile app for the targeted service, while others attempt to fool users by impersonating existing official apps.

Best practices for users

- Unsolicited texts, emails, or sudden notifications that appear to be from a bank, retailer, or other known institution may not always be what they seem. Use caution with any link delivered to you and always read the message first.
- Do not download and install applications from untrusted sources [offered via unknown websites/ links on unsolicited messages or emails]. Ensure to turn off the "Unknown Source" option in the Security Settings page. Install applications downloaded from reputed application markets only.
- Prior to downloading/installing apps on mobile devices (even from trusted application stores):
  - Always do some research on the developer of the app you plan to install. Search the developers name and scan through the results. A genuine developer is most likely to have a website and other details on the net. Apps that have the tags "Editor's Choice" or "Top Developer" are more than likely to be a genuine legitimate app.
  - Read all app permissions carefully. When in doubt the best rule of thumb to abide by is to ensure that the permissions asked by an app must comply with its functions/features. For example, if a flashlight app is requesting permission to access SMS, call logs, media files, etc., then this is definitely a red flag and not an app you should be downloading.
  - It is important to note that not all apps in the application markets are in fact "apps", rather they are just meant to redirect to mobile websites. Developers that create genuine apps are typically useful to the user and not to the mobile websites that try to scam you into clicking on ads or other links.
  - Always pay attention to user ratings and reviews prior to downloading an app. If there are hundreds of reviews, you will know that the app has stood the test of time. Be cautious of exaggerated reviews that praise the app for those too could be an indicator of a fraudulent app. A real app should have a sizable number of reviews. A fake one will likely have very few, often all 5-star reviews.
  - Check to see how many times the app has been downloaded. This may not be the most accurate way, but if an app gets 10,00,000 downloads and many positive reviews, it's more likely to be legitimate.
- Visual things such as spelling errors, shoddy logos, and poorly formatted interfaces are pointers that the app may be fake.
- Do not use "jailbroken" or "rooted" devices for mobile banking or other financial transactions. A rooted phone just gives the user the ability to become superuser (and give that privilege to apps). The security level of the device depends on that user's vulnerability to social engineering.
- Install updates and patches as and when available from device vendors/service providers.
- Always run a reputable mobile security app for your device, and keep it up to date regularly. A mobile security app can help to scan the apps you download for malware and spyware, and protects you from unsafe websites.
- Report any fakes you find in app stores and/or inform respective brand owners. On Google Play Store, there is an option to report the app by clicking the option "Mark as inappropriate" in the description. An Apple user could navigate on their "Report a Problem" page.

Best practices for Organizations/Developers

- Organizations could monitor the official app stores and report any abuse of their brands to reduce the negative impact of fake apps.
- Implementing code hardening and runtime applications self-protection (RASP) can prevent mobile applications from being cloned and tampered with.
- Advise customers regarding availability of legitimate apps.

References

https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/fake-apps-taking-over-phone/
https://blogs.quickheal.com/aware-hiddad-malware-present-google-play-store/
https://support.google.com/accounts/answer/2812853?hl=en

Disclaimer

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India