www.komando.com

These flashlight apps contained malware

By James Gelinas, Komando.com

4-5 minutes

Are you using a flashlight app on your phone? Still? While these apps were incredibly popular during the earliest days of the smartphone boom, software updates and later models of phones granted users access to the flashbulb to use as a torch in the dark. As such, these apps have mostly fallen out of style but a staggering amount is still available for download on Google Play.

Like many other third-party apps on Google Play, a number of these flashlight apps have proven themselves to be rather suspicious in their behavior. In addition to requesting unusual permissions like location tracking, several were even found to contain malware that infects the users who install them.

If you have any of these flashlight apps installed on your phone, it's time you removed them for the sake of your privacy and security. We have more details on which apps are compromising users' phones, as well as what these shady programs might have been up to behind the scenes.

A not-so-bright idea

According to new reports from security researchers at Avast, a large number of flashlight apps on the Google Play store were found to contain numerous sketchy permissions requests, and in some cases, outright malware.

Avast looked at nearly 1,000 of these apps and found that a large amount requested access to things like the phone's microphone, location data and the ability to make calls. Nine of the selected apps had malicious software that would hijack some features of the phone. Nearly all, however, subjected users to low-quality advertisements for revenue.

Your daily dose of tech smarts

Learn the tech tips and tricks only the pros know.

Ever since flashlight features became more commonplace on smartphones, apps enabling the flashbulb outside of the normal system settings have mostly fallen out of favor.

Unfortunately, the fact that these apps are so overlooked made them a perfect place to hide malware and tracking software. This takes advantage of the least tech-savvy users, who may not know how to use the flashlight feature on their phone and resort to an app for the option instead.

With so many apps that do the same thing crowding the Google Play Store, here is a list of the worst offending apps. We're advising users to delete them from their phone as soon as possible:

- **Ultra Color Flashlight**
- **Super Bright Flashlight**
- **Flashlight Plus**
- **Brightest LED Flashlight — Multi LED & SOS Mode**
- **Fun Flashlight SOS mode & Multi LED**
- **Super Flashlight LED & Morse code**
- **FlashLight – Brightest Flash Light**
- **Flashlight for Samsung**
- **Flashlight – Brightest LED Light & Call Flash**
- **1Free Flashlight – Brightest LED, Call Screen**

For that matter, it would be advisable to delete *any* flashlight app from your phone, as all versions of Android have had access to flashlight features since as early as 2014. There is no need to have any app that does this on your device.

I used one of these apps. Is my personal data at risk?

Most likely not at this point. The researchers were quick to point out that only nine out of nearly 1,000 apps examined appeared to have any malicious function.

Still, the sheer amount of unusual permissions requests in the remaining apps raises questions. Most likely, these apps were laying the groundwork for an update to more malicious activity at a later time, but for the time being, most were benign if invasive.

Right now, the best thing you can do is go through all of your installed apps (even the ones you don't pay much attention to) and make sure no flashlight apps remain on your phone.

More importantly, users should continue to tread cautiously when downloading apps from the Google Play Store. Time and time again, we've seen malicious or fraudulent apps slip through the cracks.

What’s stopping even more bad actors from infecting peoples’ phones if the platform’s moderation is this ineffective?

The answer, sadly, is nothing at all.