BIZCOMMUNITY

Cyber attacks moving to mobile

By Colin Thornton

7 Jul 2017

With individuals and businesses becoming increasingly dependent on mobile devices for everything from email to banking, cyber criminals have turned their attention to mobile platforms as a new target for attack.

Colin Thornton

One of their most common strategies is mobile phishing, which is different from the regular definition of phishing. Hackers are predominantly using applications as the hook or entryway. Mobile apps are an independent entity, yet they are increasingly leaving users vulnerable to attack.

Two main ways

As it stands, there are two main ways that a hacker can create a false sense of trust in the mobile environment.

The first approach is via an illegitimate application “acting” as a legitimate application. So although that iOSor Android app file may look like the real deal, be wary! This doesn’t only apply to Android - a jailbroken iPhone is also at risk. This is mainly an issue for users who want to download apps from places other than the Google Play Store.

The second and increasingly common approach is to tamper with or modify the content within an application. Many mobile apps will display web-based content via an internal browser. Because of that web-based content, exploits like man-in-the-middle can be leveraged to modify the content that is being shown.

Over 800 apps on Google Play that infect

Recently, Trend Micro identified over 800 apps on Google Play that infect your smartphone or tablet with Xavier Spyware.

“Xavier’s impact has been widespread. Based on data from Trend Micro Mobile App Reputation Service, we detected more than 800 applications embedded the ad library’s SDK that have been downloaded millions of times from Google Play,” the company stated.

© Dmitriy Shironosov via 123RF

Apps containing the virus range from data watching apps to ringtone modifiers. The most dangerous element here is that once an infected app is installed, it can download malicious software onto your device without your authorisation.

Be vigilant!

Arguably, the best way to protect your devices is to only install from verified app developers and always use legitimate stores. In addition, always take note of what permissions these platforms ask for when you are installing an app. It also helps to read the reviews posted by other users. Finally, keep your devices update with the latest software.

Phishing is just one example of how a traditional attack can be adapted to the mobile environment. It's a newer category for security professionals to consider in their ever-evolving fight, and one that IT players are all watching closely…

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...