Detecting fake 2FA security apps that can steal bank accounts on Android phones

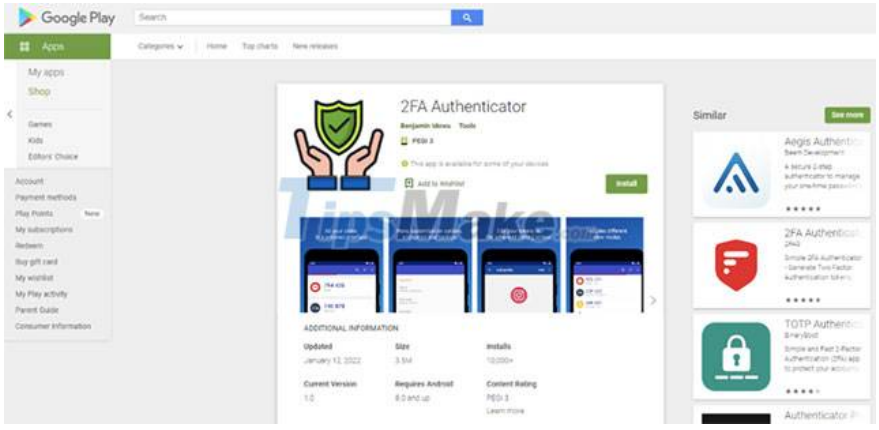
International security researchers have just discovered a dangerous fake two-factor authentication application on the Android platform.

Two-factor authentication (2FA), which is a simple and effective form of security, is therefore widely used in today's digital verification activities. However, it is that popularity that gives hackers the idea of ????using 2FA to serve their malicious purposes.

International security researchers have just discovered a dangerous fake two-factor authentication application on the Android platform. Inside this application hides a type of malicious code in the form of a banking trojan, capable of stealing financial data and other personal information when successfully installed on the victim's device.

Pradeo was the first security team to detect this malicious application. It is aptly named 2FA Authenticator to make itself more 'reputable', which contains a type of trojan called Vultur. This Trojan can infect Android phones as soon as the 2FA Authenticator app is successfully installed. According to the investigation of security experts, this malicious application has existed for more than a year, and has received no less than 10,000 installs on Google Play.

> 'Our analysis shows that the app automatically installs a piece of malware called Vultur, which targets financial services to steal users' banking information.



The interface of this fake application is generally quite well designed, looking exactly like a legitimate 2FA tool, enough to fool the majority of ordinary users. According to the Pradeo team, '2FA Authenticator looks legit and offers a real 2-factor security service. To do so, its developers used the open source code of the official Aegis authentication app, and injected malicious code into it'.

The 2FA Authenticato app works in two phases. First, it profiling the user, by collecting and sending the victim's application list and location data. During this phase, the malware disables the keylock and any associated form of password security, then downloads other third-party apps disguised as updates.

In stage two, researchers discovered that the attack depends on information the application finds about the user in phase 1. When certain conditions are met, Vultur is installed, the The malware primarily targets online banking interfaces to steal credentials and financial information'.

This is not a piece of malware disguised as a security tool and taken lightly. If you already have this app installed (removed from Google Play but still available on some third-party app stores), you need to remove it immediately. If the app starts to relaunch itself when you try to close it, restart your phone and remove it from the system.