Trojan root Android device bypasses Google's security mode on Play Store

A new malware rooted the Android device with the ability to turn off the device's security settings and try to perform a standalone task in the background that was detected on Play Store.

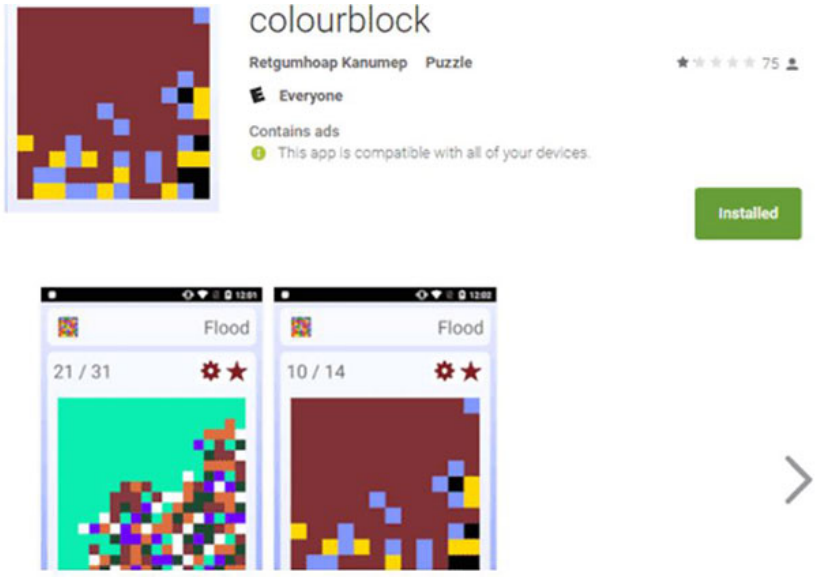
The malicious code hidden in this application is so smart that it deceives Google's security mechanism, pretending to be a clean application, then replacing it with a poisoned version for a short time. Security researchers at Kaspersky Lab discovered that the new malware was released in the form of a Google Play Store game application, hidden behind the colorful block puzzle game that was downloaded at least 50,000 times before being removed.

Named Dvmap, this Android root malware disables the device's security settings to install a third-party malicious application and inserts a malicious code and system runtime library device to gain root access. phone.

> "To overcome the security of Google Play Store, this malware creator used a very interesting method. They downloaded a clean application to the Store at the end of March 2017, then updated with the poisoned version in a short period of time, "the researchers said. "Normally, they will upload a clean version later on the same day. They did it at least 5 times between April 18 and May 15."

How it works Dvmap malware

The Trojan works on both 32-bit and 64-bit versions of Andorid, once installed, it will attempt to gain root access to the device and install some modules on the system, including some written in Chinese. together with standalone application named com.qualcmm.timeservices.



The root of the Android phone is in the puzzle game application

To ensure that the infected module can be run by the system, the malware overwrites the system's runtime library, depending on the version of the user's Android device. To complete the installation of the stand-alone application, the system's authorized trojan will turn off **Verify Apps** and adjust the system settings, allowing applications to be installed from third parties.

"In addition, it can give the com.qualcmm.timeservices application the Administrator Administrator administrative rights without user intervention, just by running the command. That's a very different way to gain administrative rights." This third-party application will connect the infected device to the attacker's server, giving complete control of the device to the hacker.

However, researchers still do not know which Android device is infected with the command, so it is unclear what kind of file it is executing, but it could be an ad file or a poison.

How to protect the phone from the Dvmap malware?

Researchers are still testing the malware, but users who have installed the game are advised to back up phone data and perform data reset to avoid malware attacks.

To protect your phone from such applications, always be cautious of untrusted applications, especially when downloading from Google Play Store. Remember to only grant application verification rights when the content is relevant to the purpose of the application. Don't forget to read the user comments section before installing. In addition, anti-malware applications on your phone can detect and block malware before they infect your phone.

You finished reading the article "**Trojan root Android device bypasses Google's security mode on Play Store** " edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.