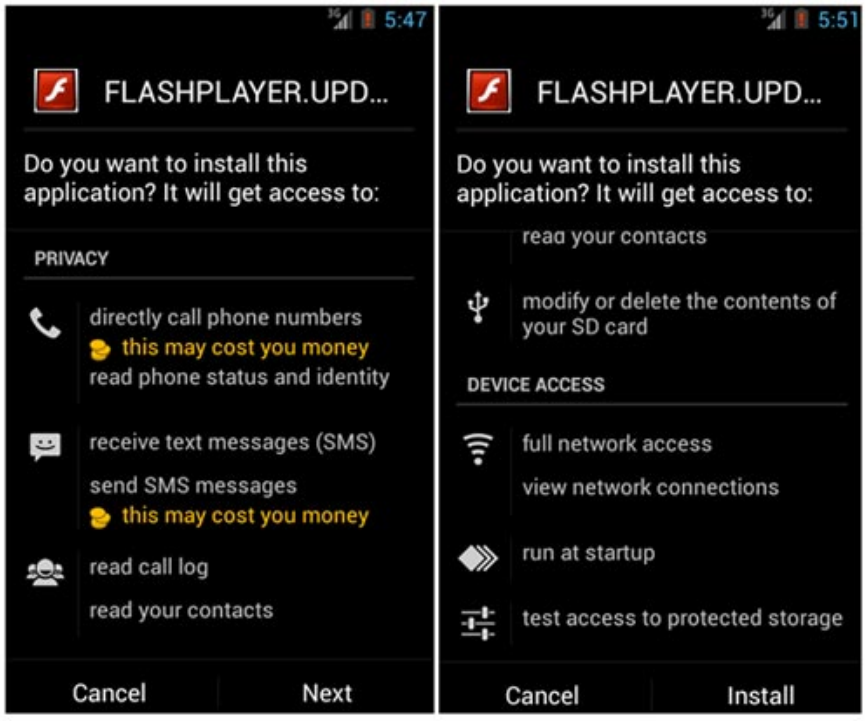
New Android Trojans lead users to phishing websites by notification on the application

Security researchers have found that a dangerous Trojan appears on Android platforms, using the same web messages to redirect users to sophisticated phishing sites.

Recently, Google Play Store security researchers have discovered a dangerous Trojan named Android.FakeApp.174, which appears on Android platforms, uses web notifications itself to redirect users to Sophisticated scam sites.

Many of these fake brand-name applications for malicious distribution of Android.FakeApp.174 were removed in early June after being discovered and reported to Google by security experts at Doctor Web.

1. Discovery of Trojan scattering steals virtual money through YouTube



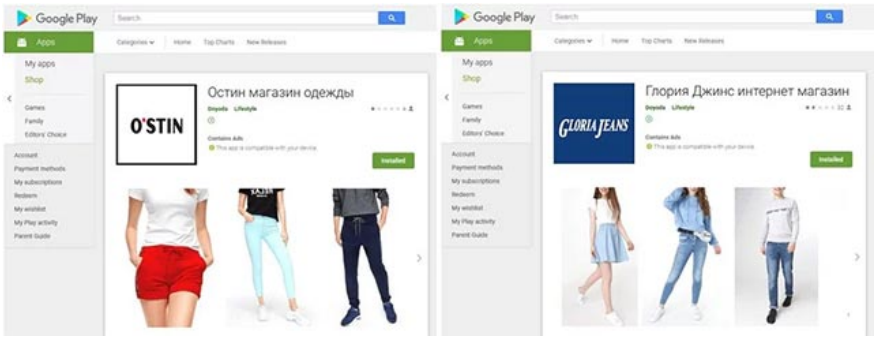
Fake notice

Although statistically, these fake applications have only been installed about 1000 times - the number cannot cause significant damage, but malware exploiters can publish applications completely. Similar applications at any time on Play Store, and can also switch to using some more powerful attack methods such as redirecting

victims to malicious payloads, launching phishing attacks spend on banking system - currency, or spread fake news.

For example: "Users who are distracted, caught off guard and lacking in knowledge may think that false messages sent to their phones are real, and if they click on that message, they will be transferred. Here, the victim will continue to be tricked into providing names, login information, email addresses, bank card numbers and many other valuable personal information ", home Doctor Web study explained.

1. Azorult Trojan steals user passwords while running in the background like Google Update



2 of the malicious applications found

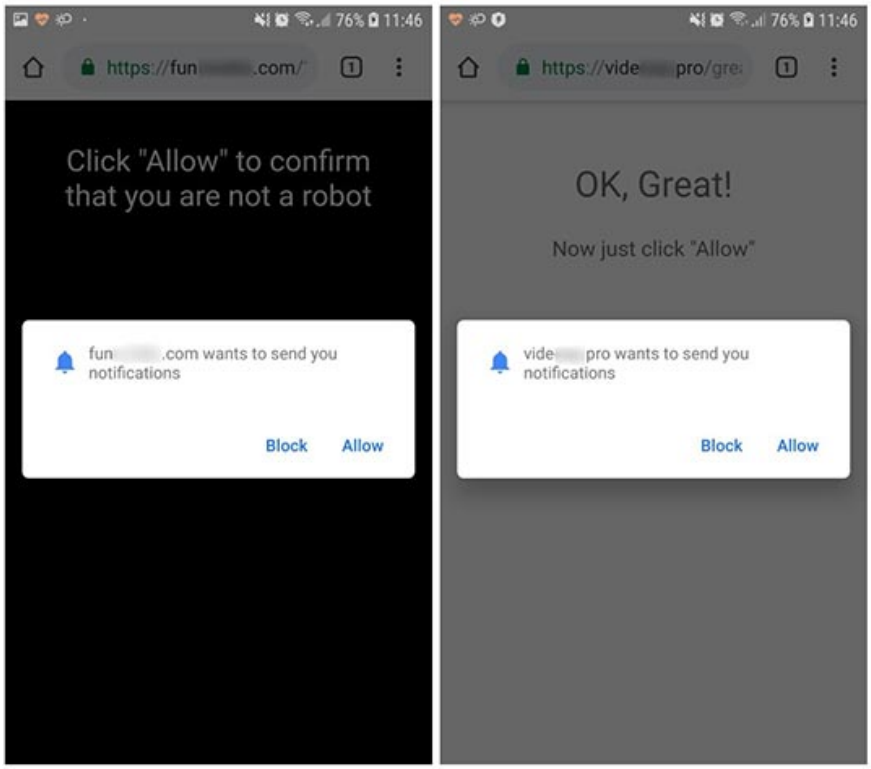
When malicious phishing applications launch for the first time, Trojan Android.FakeApp.174 will silently download a hard-coded website in its settings via the Google Chrome web browser. This site is responsible for asking target systems to allow fake notifications to appear under the guise of questions verifying that the user is not a bot.

When agreeing to enable web redirect notifications for "verification purposes," the owner of the compromised device accidentally registered the site's notification and will be spammed with dozens of fake notifications sent through Chrome with Web Push technology.

When agreeing to enable web push notifications for "verification purposes," the owner of the compromised device has 'accidentally' subscribed to the site's notification without knowing it, and will be spammed with dozens of notifications. Chrome sent with Web Push technology.

According to Doctor Web's explanation, this technology allows sending notifications even when the web browser is closed, or when the website is not opened in the browser, and even after the Trojan has been completely deleted from the system. The victim's system.

1. The official GandCrab 5.2 decoder was released, ending the bad nightmare called GandCrab Ransomware

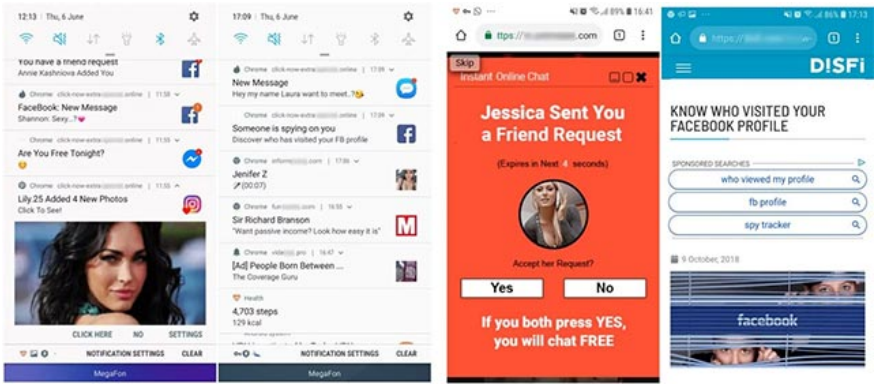


The verification dialog requires permission to send notifications

"But this fake notification message is displayed on the notification panel of the device and can be mistaken for system messages. They may look like notifications sent from pages. social networks, dating sites, news agencies and many other popular online services ".

The crook uses these perfectly disguised phishing messages to redirect the victim to various types of phishing sites such as "online gambling websites, betting shops, various Google Play applications, Discount codes and coupons, as well as fake online polls depending on the user's country of residence, "explained Doctor Web experts.

1. Microsoft warned about malicious spam campaigns using vulnerabilities in Office and Wordpad



Notify spam and phishing sites that they redirect to

Doctor Web researchers predict that those who create Trojan Android.FakeApp.174 "will use this method more aggressively to promote malicious services, so Android mobile device users should be careful It is important to access websites, and absolutely do not register to receive notifications from a strange or suspicious site ".

Android users who have been tricked into signing up for this spam web navigation notification should take the following steps to remove them:

1. Visit the installation section of Google Chrome, select the **Site Settings** option, and then the **Notifications** .
2. On the list of websites that send notifications, look for the suspicious website address, click on the website address and select **Clear & reset.**