New Trojan SpyNote Installs Backdoor on Android Devices

By Tom Spring

Published: 2016-07-29 · Archived: 2026-04-05 18:42:18 UTC

A new SpyNote Trojan can give bad guys control over your phone from the camera, microphone to eavesdropping on phone calls.

A new Android Trojan called SpyNote has been identified by researchers who warn that attacks are forthcoming.

The Trojan, found by Palo Alto Networks' Unit 42 team, has not been spotted in any active campaigns, but it is now widely available on the Dark Web and that it will soon be used in a wave of upcoming attacks.

Unit 42 discovered the Trojan while monitoring malware discussion forums. Researchers say that's where they found a malware builder tool specifically designed to be used to create multiple versions of SpyNote Trojan.

SpyNote has a wide range of backdoor features that include the ability to view all messages on a device, eavesdrop on phone calls, activate the phone's camera or microphone remotely or track the phone's GPS location. The APK (Android application package file) containing the remote access tool (RAT) SpyNote, gives an attacker complete access to a victim's phone.

SpyNote is similar to other remote administration tools such as OmniRat and DroidJack. Droidjack made news earlier this month when researchers at Proofpoint found a rigged version of the massively popular game Pokémon Go with the Trojan. OmniRat is similar in function and was first spotted in Germany in November by researchers who said targeted victims received a text message asking them to download an app to view an image.

Once installed, SpyNote is hard to get rid of; it removes the SpyNote application icon from the victim's phone and install new APKs and update the malware.

"The SpyNote APK requires victims to accept and give SpyNote many permissions, including the ability to edit text messages, read call logs and contacts, or modify or delete the contents of the SD card," according to a technical description of malware.

Palo Alto has gleaned important details of SpyNote from what it identifies as a video demonstrating the capabilities of the malware. In the video hacking tutorial a user appears to be running SpyNote through its paces showing a remote takeover of an Android device.

https://www.youtube.com/watch?v=E9OxlTBtdkA

"The uploader might be following the instructions described in YouTube videos on using SpyNote, considering the port number used is exactly the same as in the videos and the uploader only changes the icon of the APK file," wrote Jacob Soo.

SpyNote is configured to communicate with a command and control server via IP address via TCP using hard-coded SERVER_IP and SERVER_PORT values. That has given researchers the ability to extract C2 information from the malware.

Unlike the closely related RATs OmniRat and DroidJack, researchers say they have not seen SpyNote in the wild therefore determining how attackers might lure victims into downloading the Android APK is still an unknown.
