Issued 1/23/17

Android Users Under Attack As Banking Malware Source Code Was Posted Online

Security firm Dr. Web reveals that it has already discovered one malware developed with this leaked source code, adding that it's distributed as popular applications either directly injected in APKs available online or in third-party stores.

The malware has been flagged as Android.BankBot.149.origin and tries to get administrator privileges on compromised computers. Once it's granted full privileges, the malware removes the app's icon from the home screen, trying to trick people into believing it was removed.

But on the other hand, it remains active in the background, and it connects to a command and control server to await for commands. It can perform a wide array of tasks, such as send and intercept SMS messages, steal contacts, track devices, make calls, show phishing dialogs, and steal sensitive information, such as banking details and credit card data.

Once popular applications are launched, including here Facebook, Instagram, WhatsApp, YouTube, and even the Google Play Store, the malware launches a phishing dialog similar to the one showing

up when you make purchases on Google Play, asking for credit card information.