Red Alert 2.0 Android Trojan Spreads Via Third Party App Stores

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/red-alert-2-0-android-trojan-spreads-via-third-party-app-stores

A spate of new attacks targeting the Android operating system have been discovered using a banking trojan named after a video game. Dubbed Red Alert 2.0 (Detected by Trend Micro as ANDROIDOS_BANKER) by its creators, this new malware tricks users into downloading it by hiding in third-party app stores as fake versions of legitimate applications such as WhatsApp, Viber, and updates for both Android and Flash Player.

Once a user downloads one of these malicious apps into their devices and opens it, a popup overlay will appear prompting the user to enter their login credentials. The credentials are then sent to a command-and-control (C&C server) that the attackers control.

Red Alert 2.0 will block incoming calls from banks, presumably to block verification attempts. The malware also intercepts SMS text messages, sending messages to the attackers for future use. By disrupting the device's actual communication capabilities, the attackers can maximize the time spent doing malicious activities.

According to its researchers, Red Alert 2.0 is being peddled on hacking forums for $500—a low price that could make it attractive to a large number of potential attackers.

Red Alert 2.0 can target mobile devices that are running Android versions of up to 6.0, which was released two years ago, but it is currently confined to third party app stores. No versions of the malicious apps carrying the malware have been detected on the official Google Play Store as of the time of publication.

This is not the first time that malware is being spread via third party app stores, as seen in last year's Fobus attack involving Super Mario Run. Users are advised to avoid third party-app stores, as the lack of security regulations could expose them to malware. In addition, users should also disable the "Allow installation of apps from unknown sources" as a further

security measure, and only enable it when they are sure of the legitimacy of the download source. In general, Android users should be wary of whatever they download—whether from third party app stores of even the official Google Play Store itself. If an app seems to be suspicious, perhaps it is best to refrain from downloading it.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Mobile Malware