New bank trojan detection on Android Red Alert

Network security researchers have discovered a new Android banking trojan called Red Alert 2.0 that has been developed for the past few months and has just been launched.

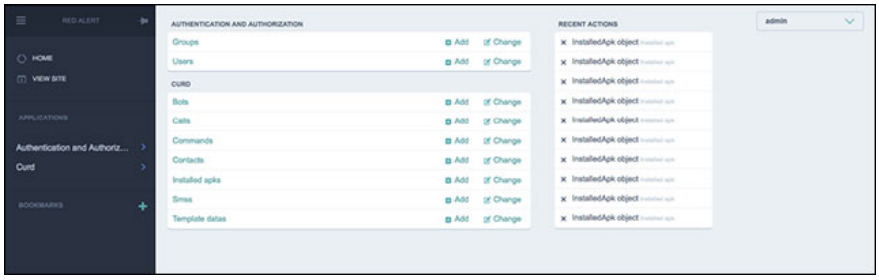
Network security researchers have discovered a new Android banking trojan called Red Alert 2.0 that has been developed for the past few months and has just been launched.

According to the report, researchers at SfyLabs first saw the ad for this trojan on a Russian-speaking hacking forum earlier in the year. Last week, they discovered the first applications affected and tracked by C&C servers.

Red Alert is not yet on Play Store

All Red Alert-infected applications are located on third-party Android app stores. SfyLabs said no malicious application has been available on the official Google Play Store at this time.

Red Alert is a new name but also works like other Trojans. It will silently wait until the user opens the banking application or social network. Meanwhile, the trojan will display as HTML inserted on the original application, warning users that there is an error and requesting authentication again.



Red Alert dashboard

Red Alert then collects user login information and sends it to the C&C server. This information can be used to log the victim's bank account, make a fake transaction, or log in to a social network to post spam or other content.

Red Alert also collects contacts on the device. To pass 2-factor authentication, it also takes over the phone's SMS function.

According to changelog on Red Alert advertising, its latest feature is to automatically block incoming calls from numbers associated with banks or financial institutions.

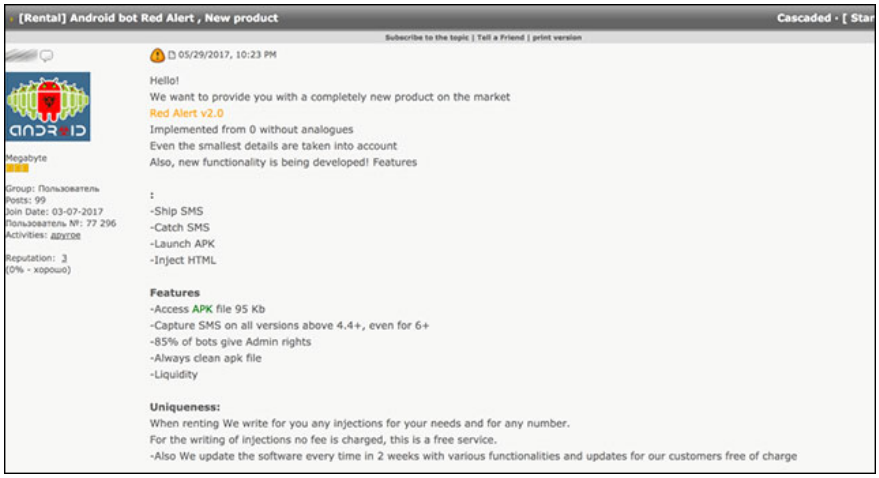
Red Alert rental for $ 500

Cengiz Han Sahin, CEO and founder of SfyLabs said the Red Alert author hired the trojan for only $ 500. The development process is also very positive. 'HTML Overlay was created almost twice a day,' Sahin said. Red Alert's works also work with SOCKS and VNS to add remote control capabilities on the device, improving Red Alert with the characteristics of SV.

Sahin said that Red Alert caught his attention because it was one of the few bank trojans that were written completely from the beginning in the past few years. Most recent Trojans like Exobot, BankBot or AgressiveX AndroBot are written based on previous malware.

Red Alert runs on all Android versions to 6.0

Sahin said that Red Alert's goal is that all versions of Android are available until version 6.0 (Marshmallow). It supports HTML Overlay display for more than 60 banks and social networking applications.



Advertise about Red Alert on hacking forums

The Trojan does not target a specific country but will initially target well-known banks. It chooses the target randomly by way of leasing trojans, Red Alert author focuses on providing attractive features for many potential buyers.

The post on SfyLabs's blog at this address *https://clientsidedetection.com/new_android_trojan_targeting_over_60_banks_and_social_apps.html* provides a list of targeted applications and IOC information. As usual, users can avoid malware by only using the application on Play Store, though not perfect but still safer.

You finished reading the article "**New bank trojan detection on Android Red Alert**" 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.