Researchers Discover New Android Banking Trojan

By Catalin Cimpanu

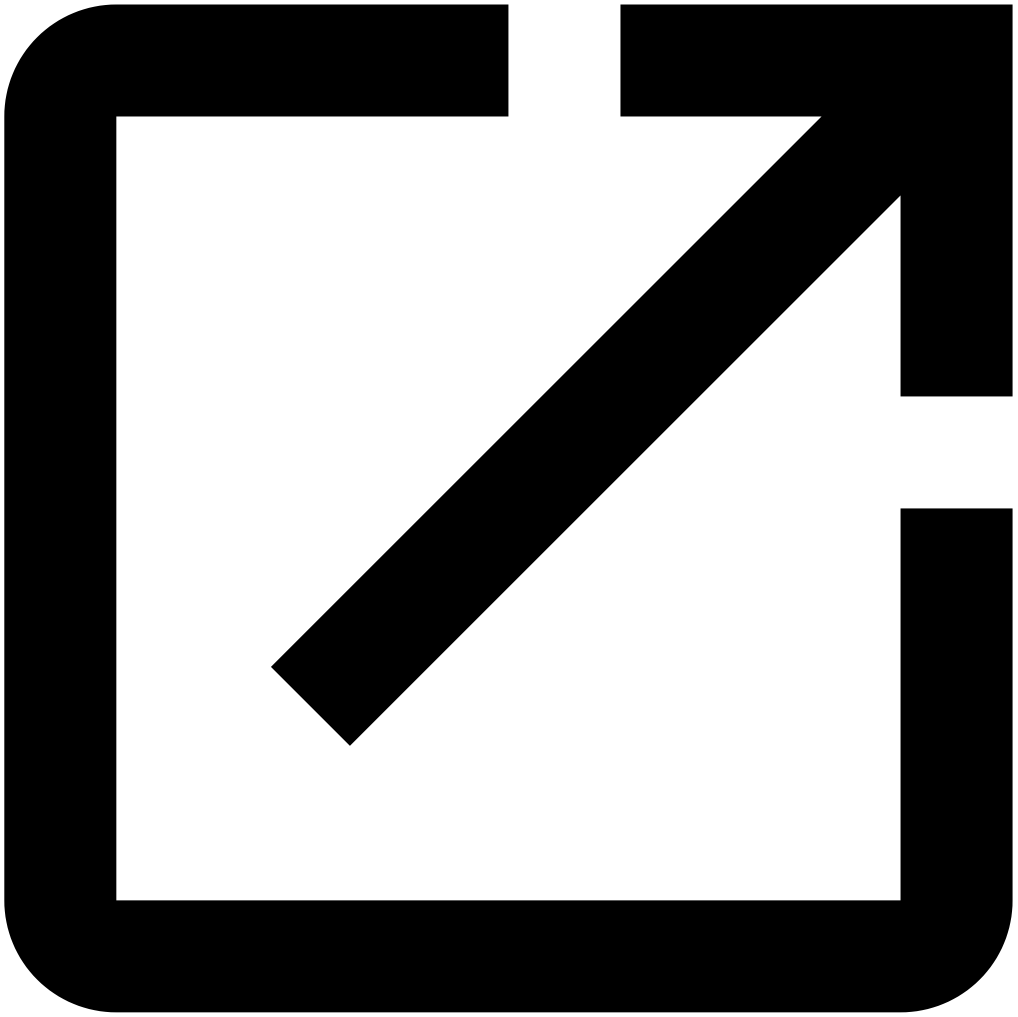
Published: 2017-09-18 · Archived: 2026-04-05 14:02:34 UTC

Security researchers have detected a new Android banking trojan by the name of Red Alert 2.0 that was developed during the past few months and has been recently rolled out into distribution.

According to a report shared with Bleeping Computer before publication, security researchers from SfyLabs first saw ads for this trojan on a hacking forum for Russian-speaking criminals during the spring.

During the past weeks, researchers have identified the first apps infected with this new threat and have tracked down C&C servers used to manage the banking trojan.


DIE LINKE.
0:00

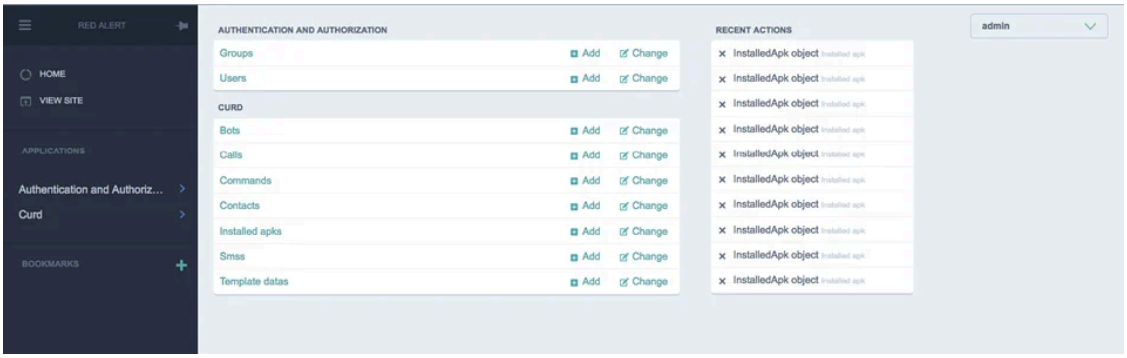


Red Alert has not made it on the Play Store (yet)

All the apps spreading Red Alert were hosted on third-party Android app stores. SfyLabs told *Bleeping Computer* that no Red Alert app made it on the official Google Play Store at the time of writing.

While Red Alert is a new addition to the mobile banking scene, the trojan works similarly to past threats. The trojan waits in hiding until the user opens a banking or social media app. When this happens, the trojan shows an HTML-based overlay on top of the original app, alerting the user of an error, and asking him to reauthenticate.

Red Alert then collects the user's credentials and sends them to its C&C server.



People in command of Red Alert's control panel take these credentials and access their victims' bank accounts to make fraudulent transactions, or the victim's social media apps, to post spam or give surreptitious likes to other content.

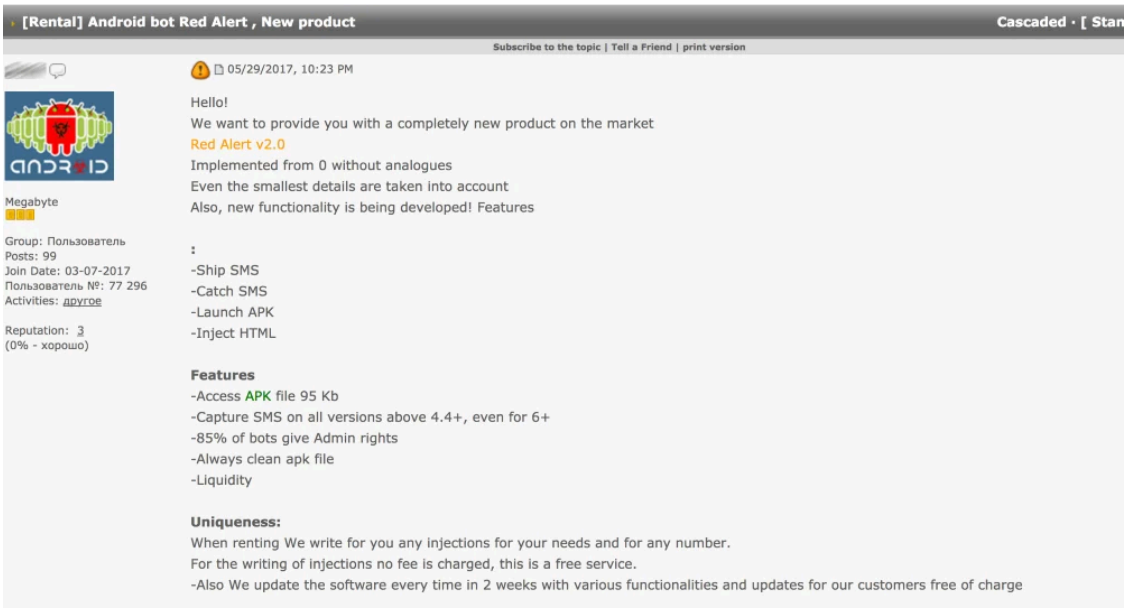
Red Alert also includes a feature to collect the contact lists from infected devices. In addition, to bypass two-factor authentication and suppress any notifications, the trojan also takes over the infected phone's SMS function.

According to a changelog in Red Alert's forum ads, the most recent feature added to trojan's codebase is its ability to automatically block incoming phone calls from numbers associated with banks and financial institutions.

Red Alert rented on hacking forums for $500

Cengiz Han Sahin, CEO and founder of SfyLabs, tells *Bleeping Computer* that the Red Alert author is renting the trojan for the lowly price of $500.

Development is also very active. "New HTML overlays are created almost every 2 days," Sahin told *Bleeping*. In addition, Red Alert's author is also working on SOCKS and VNC modules that would add remote control features to infected devices, enhacing Red Alert with RAT-like features.


[Rental] Android bot Red Alert , New product

Cascaded · [Stan

Subscribe to the topic | Tell a Friend | print version

05/29/2017, 10:23 PM

Megabyte

Group: Пользователь
Posts: 99
Join Date: 03-07-2017
Пользователь №: 77 296
Activities: другое

Reputation: 3
(0% - хорошо)

Hello!
We want to provide you with a completely new product on the market
Red Alert v2.0
Implemented from 0 without analogues
Even the smallest details are taken into account
Also, new functionality is being developed! Features

:
-Ship SMS
-Catch SMS
-Launch APK
-Inject HTML

Features
-Access APK file 95 Kb
-Capture SMS on all versions above 4.4+, even for 6+
-85% of bots give Admin rights
-Always clean apk file
-Liquidity

Uniqueness:
When renting We write for you any injections for your needs and for any number.
For the writing of injections no fee is charged, this is a free service.
-Also We update the software every time in 2 weeks with various functionalities and updates for our customers free of charge

Sahin said the Red Alert caught his team's eye because it's one of the few Android banking trojans that's been written from scratch in the past few years.

Almost all recent Android banking trojans such as Exobot, BankBot, or AgressiveX AndroBot, are based on malware that was previously available on the malware market.

Red Alert works on all Android versions up to 6.0

Sahin tells Bleeping that Red Alert can target smartphones running Android versions up to and including 6.0 (Marshmallow).

Experts say that Red Alert comes with support for showing HTML overlays for over 60 banking and social media apps.

The trojan doesn't seem to target users in a particular country but uses a shotgun approach, providing overlays for the most well-known banks and financial institutions.

This random targeting is most likely because of the trojan's rental system, as Red Alert's author focuses on providing enticing features for a wide group of potential buyers.

A SfyLabs blog post will be made available later today at this URL and will include a list of targeted apps and IOCs.

As always, users can avoid most Android malware by not using third-party app stores and sticking to apps only available on the Play Store. Google's official app store may not be perfect, but it's way better than any shady Android app store.

Image credits: SfyLabs

Source: https://www.bleepingcomputer.com/news/security/researchers-discover-new-android-banking-trojan/