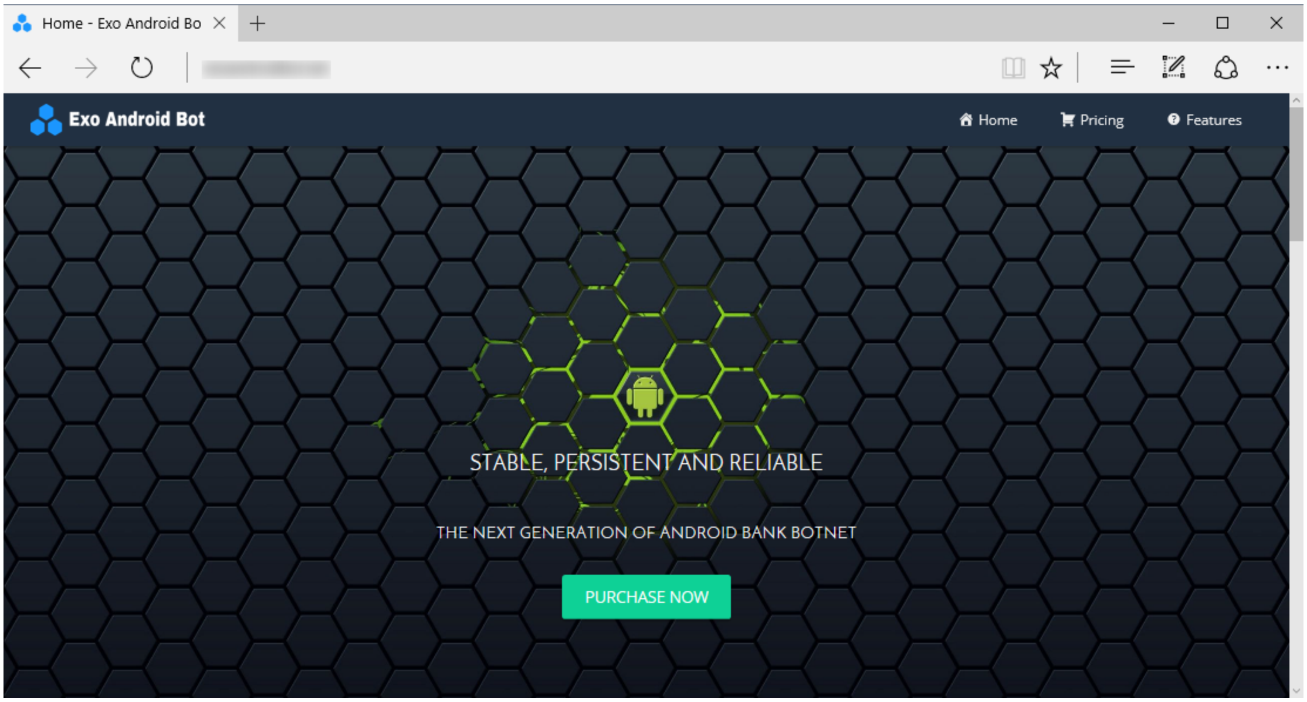
Exobot Author Calls It Quits and Sells Off Banking Trojan Source Code

bleepingcomputer.com/news/security/exobot-author-calls-it-quits-and-sells-off-banking-trojan-source-code/

Catalin Cimpanu

By
Catalin Cimpanu

- January 17, 2018
- 05:07 PM
- 0


Home - Exo Android Bo
Exo Android Bot
Home
Pricing
Features
STABLE, PERSISTENT AND RELIABLE
THE NEXT GENERATION OF ANDROID BANK BOTNET
PURCHASE NOW

Things are about to get a lot worse for Android users after the source code of a highly advanced Android banking trojan has been sold to different parties on a well-known hacking forum.

The trojan at the center of this worrisome news is called Exobot, an Android malware strain that first appeared on the malware scene in June 2016.

Just like most of today's professionally coded desktop or mobile banking trojans, Exobot has always been rented to customers on a monthly basis.

Customers never have access to the trojan's source code, but they can use configuration panels provided by the Exobot author to compile malicious apps with per-client custom settings. Renters then have to distribute these apps to victims, each using its own methods and means.

Exobot has been one of the most active Android mobile trojans in the past two years, together with BankBot, GM Bot, Mazar Bot, or Red Alert.

Initially, some security firms called it Marcher, but eventually everybody started calling it by the name its author had given it. Business was good as initial profits spurred Exobot's author to create Exobot v2 by late 2016.

Bleeping Computer covered Exobot v2's rise when the trojan was heavily advertised on the Dark Web, hacking forums, XMPP spam, and even on the public Internet.

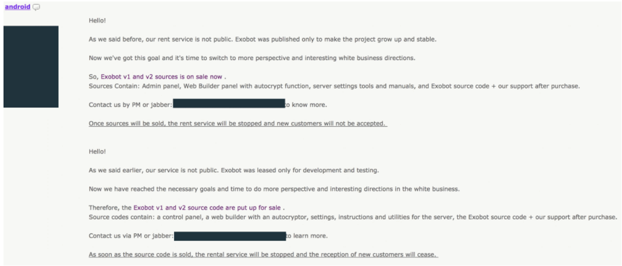
Based on the evidence this reporter gathered in past conversations with numerous security researchers, Exobot looked like a lucrative business for its author and was used to target users in many countries around the world.

Exobot author puts banking trojan up for sale

But out of the blue, the Exobot author —going by the generic pseudonym of "android"— made a major move, which in hindsight might cause a lot of problems for users in the upcoming future.

The Exobot author decided to shut down the Exobot rental scheme and sell the source code to a small number of clients.

Below are two images of the Exobot's author sale ad, courtesy of Cengiz Han Sahin, a mobile security researcher at SfyLabs.



android

[redacted]

Hello!

As we said before, our rent service is not public. Exobot was published only to make the project grow up and stable.

Now we've got this goal and it's time to switch to more perspective and interesting white business directions.

So, Exobot v1 and v2 sources is on sale now .
Sources Contain: Admin panel, Web Builder panel with autocrypt function, server settings tools and manuals, and Exobot source code + our support after purchase.

Contact us by PM or jabber: [redacted] to know more.

Once sources will be sold, the rent service will be stopped and new customers will not be accepted.

Hello!

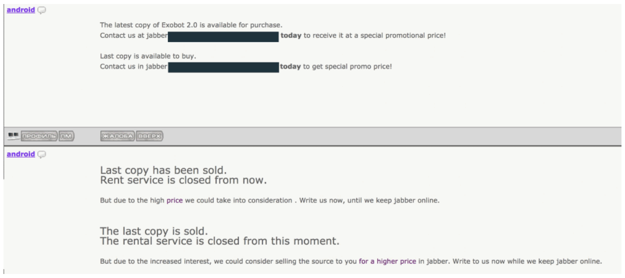
As we said earlier, our service is not public. Exobot was leased only for development and testing.

Now we have reached the necessary goals and time to do more perspective and interesting directions in the white business.

Therefore, the Exobot v1 and v2 source code are put up for sale .
Source codes contain: a control panel, a web builder with an autocryptor, settings, instructions and utilities for the server, the Exobot source code + our support after purchase.

Contact us via PM or jabber: [redacted] to learn more.

As soon as the source code is sold, the rental service will be stopped and the reception of new customers will cease.



android

The latest copy of Exobot 2.0 is available for purchase.
Contact us at jabber [redacted] **today** to receive it at a special promotional price!

Last copy is available to buy.
Contact us in jabber [redacted] **today** to get special promo price!

android

Last copy has been sold.
Rent service is closed from now.

But due to the high price we could take into consideration . Write us now, until we keep jabber online.

The last copy is sold.
The rental service is closed from this moment.

But due to the increased interest, we could consider selling the source to you for a higher price in jabber. Write to us now while we keep jabber online.

"According to his statement, he became very rich," Sahin says. "Such a statement in the malware world generally means one of the following two things: Either the actor notices the surge of interest from law enforcement and/or competitors fighting back their market share, either his business has indeed been very fruitful and its ratio of risk/gain is no longer of interest."

Many fear Exobot source code will become public

But despite the reasons, the sale of Exobot will have deep repercussions on the Android malware scene, even if not right away.

This reporter has covered many such incidents in the past. Based on this reporter's experience, and Sahin's own predictions, which he penned in a blog here, it's only a matter of time until this source code gets leaked online for everybody to enjoy.

Such sales almost never remain secret, and at one point or another, a dissatisfied customer will leak the source code when Exobot's author won't provide the support the buyer needs. This is how many families of desktop-based banking trojans have been leaked in the past decade.

Once it gets leaked, the Exobot code will follow the same fate of Slempo, BankBot, and the GM Bot Android banking trojans, and will be tweaked and remastered into hundreds of offshoot trojans, reducing the costs and technical skills needed to enter the mobile malware scene.

Exobot sale leads to new malware campaigns

But before low-skilled actors get their hands on leaked versions of Exobot, the trojan's new customers are already putting it to good use.

"Less than a month after the actor started selling the Exobot source code, new campaigns in Austria, England, Netherlands, and Turkey where discovered," Sahin says. Of all, Turkey is the most affected by these campaigns, with over 4,400 devices in total, based on Sahin's investigation.

This rise in malicious Exobot apps was caused by a few private sales of the Exobot source code. We don't need to imagine the scale of Exobot attacks if the source code leaks, mainly because we already have an example in BankBot.

Leaked online in late 2016, this trojan has been at the heart of a recent wave of malicious apps spread via the Google Play Store, in what appears to be a losing battle for Google engineers, who are having a harder and harder time detecting the initial apps that spread these threats.

The fragmented Android OS market, the annoying mobile carriers that never deliver patches in time, and the Google Play Store team that can't seem to keep up with malware authors puts Android users at a serious disadvantage when it comes to mobile malware. The only methods that can safeguard most users are mobile antivirus solutions and the use of common sense not to install apps from untrusted sources or not to install Play Store apps that require unnecessary permissions.

Related Articles:

Top 10 Android banking trojans target apps with 1 billion downloads

Mobile trojan detections rise as malware distribution level declines

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

SMSFactory Android malware sneakily subscribes to premium services

FluBot Android malware operation shutdown by law enforcement

- Android
- Android Exo Bot
- Banking Trojan
- Exobot
- Malware
- Source Code

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: