

New Exo Android Trojan Sold on Hacking Forums, Dark Web

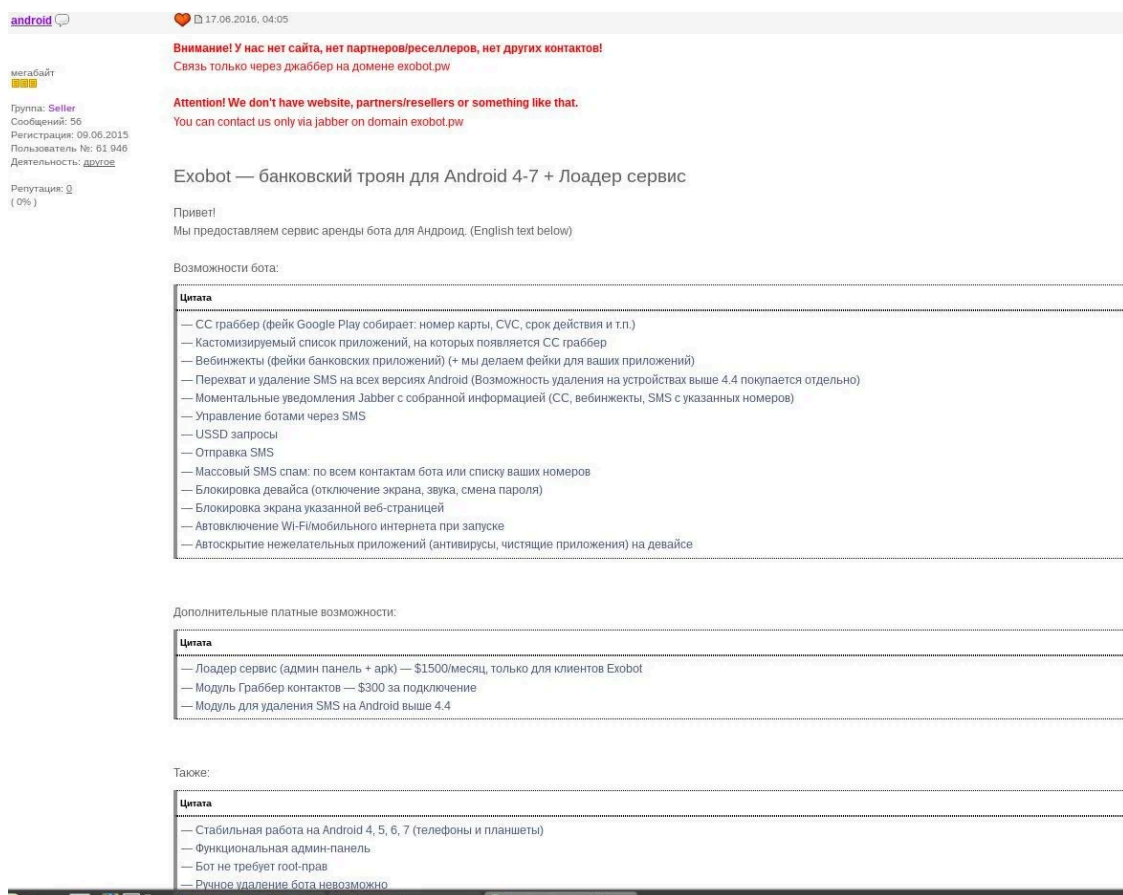
By Catalin Cimpanu

Published: 2016-12-09 · Archived: 2026-04-05 14:21:31 UTC

Malware coders are advertising a new Android trojan that can be used for phishing banking credentials, intercepting SMS messages, locking devices with a password (ransomware-like behavior), and more.

The trojan's name is Exo Android Bot, or Exobot, and is being advertised and sold via Jabber/XMPP spam, via hacking forums, Dark Web marketplaces, and even on the public Internet via a dedicated website.

According to the information we were able to unearth, the trojan has been sold as early as mid-June 2016, when its creator (or one of its creators) had opened a topic on a Russian-speaking hacking forum (image below).





Visit Advertiser website [GO TO PAGE](#)

Shortly after, a listing appeared on AlphaBay, the largest Dark Web marketplace for illegal products.

The screenshot shows the AlphaBay Market interface. At the top, there's a navigation bar with 'HOME', 'SALES', 'MESSAGES', 'ORDERS', 'LISTINGS', 'BALANCE', 'FEEDBACK', 'FORUMS', 'API', and 'SUPPORT'. A user is logged in as 'Autoshop' with a balance of BTC 0.0000 and XMR 0.0000. The main navigation includes 'Software & Malware', 'Botnets & Malware', and 'Exo Android Bot'. The listing for 'Exo Android Bot' is the central focus. It includes a product image, a description, and a list of features. The product is sold by 'exosales' for USD 1,500.00. The listing also features a 'Product Description' section with detailed information about the bot's capabilities and usage.

AlphaBay Market Logged in as Autoshop
Balance: BTC 0.0000 / XMR 0.0000
Autoshop Logout

USD 769.20 CAD 1015.82 EUR 725.16 AUD 1031.29 GBP 611.24

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT

Software & Malware Botnets & Malware Botnets & Malware Exo Android Bot

LISTING OPTIONS

Contact Seller
Favorite Listing
Favorite Seller
Alert when restock
Report Listing

BROWSE CATEGORIES

- Fraud 32377
- Drugs & Chemicals 174302
- Guides & Tutorials 11822
- Counterfeit Items 6297
- Digital Products 14243
- Jewels & Gold 1415
- Weapons 2750
- Carded Items 2995
- Services 6439
- Other Listings 3019
- Software & Malware 2443
- Security & Hosting 609

SEARCH OPTIONS

Search terms:
Listing type: All Fixed Price Auction
Product type: All Digital Physical
Price range: USD 0.00 to USD 99999.99
Origin country: Any
Ships to: Any
Order by: Most popular item
Active vendor: Active vendor listings
Automatic fulfillment: All listings
Multisig options: All listings
Bulk discounts:

Exo Android Bot

Exo Android Bot its a recoding work which we ve bought the source code from author before dissappear on february. Now we worked during 4 months day after day to add new feature and bug fixes and stability. Main features list

Sold by exosales - 0 sold since Jul 8, 2016 Vendor Level 1 Trust Level 3

Product class	Quantity left	Ends in	Origin country	Ships to	Payment	Features
Digital goods	Unlimited	Never	Worldwide	Worldwide	Escrow	

Default - 1 days - USD +0.00 / Item

Purchase price: USD 1,500.00
Qty: 1 Buy Now Queue
1,9501 BTC / 190,3553 XMR

Description Bids Feedback Refund Policy

Product Description

Exo Android Bot its a recoding work which we ve bought the source code from author before dissappear on february. Now we worked during 4 months day after day to add new feature and bug fixes and stability.

Main features list

- SMS intercept (send the sms content to admin panel in real time. If is desired with jabber notifications too, can be configured for a target or by sender phone numbers)
- Send SMS for a specified phone number
- Hide/delete incoming sms (this feature works upto android 4.4 version)
- USSD requests
- Web injects (show phishing over targeted app names to steal data, username,password,telepin whatever you want)
- Custom injects could be made under customer request
- CC Stealer (Steal CCs data Including VB/MSC/SAFEKEY) (CCs stealer can target the desired apps. Example: Whatsapp, Viber, the Google the Play Store)
- Jabber notifications for incoming new CCs or Webinject data or the SMS from specified phone numbers Collected
- Lock / unlock device with a password / disable screen and phone use also can show a custom page on locked screen
- Uninstall the bot manually (without the PC / cable) is impossible
- Wi-Fi access / mobile data automatic enabler, if detect stored wifi networks on range
- Send Mass SMS to all contacts from the infected phone
- Control the bot with SMS too in case no internet access
- Exo Android Bot do not need Root privileges to work Correctly
- Admin panel to manage your bots
- Our bot works from 2.3 to 6.0.1 Android versions

FAQ and answers

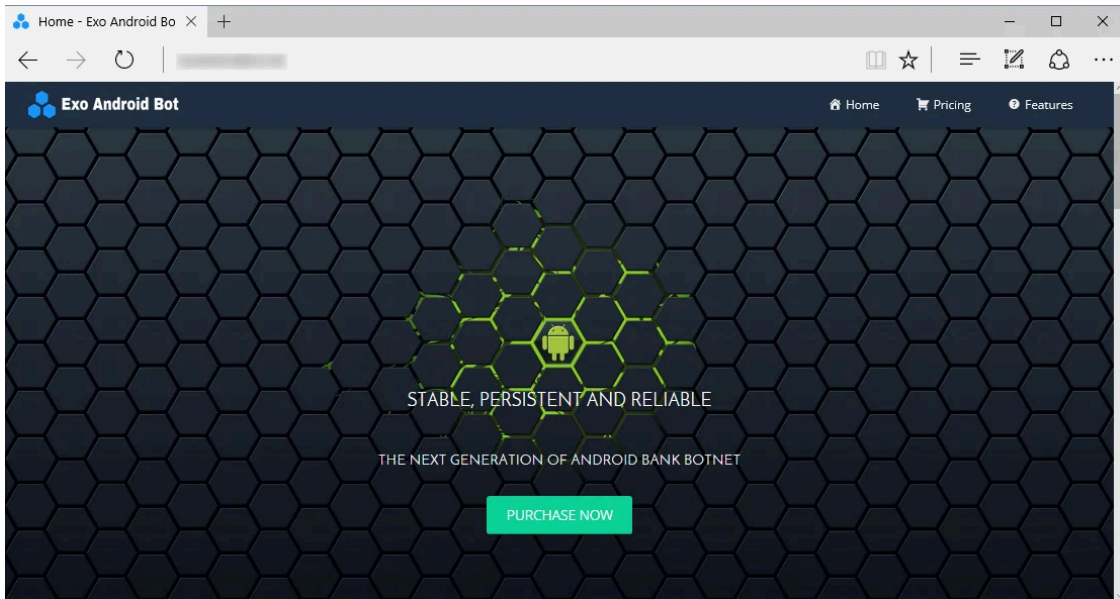
- we dont install admin panel files outside our servers , the customer will need to provide us a vps/server root access to install frontend/proxy script
- Customer must provide from 1 to 3 domains names where the bot be pointing to
- we are noob friendly , which means we may guide you to setup all the necessary stuff for a fast start on this android scene
- if you consider our product is expensive and no worth , is not our problem if you dont have money, or dont have the intention to use our services and just want troll around
- we are here to make happy our customers and be sure all the features which we are offering it works and continue working offering a good support
- this project was made from scratch ? answer : No, we purchased a base source code 4 months ago directly from his developer before he vanish from internet, and we began our own project and development/improvements/new features
- what if i rent your product and your disappear? Answer : No definitely we are not going to disappear or run away least for the next year
- what other features are planned for the incoming months? Answer: VNC/Geo Fencing / File Manager Browser and others
- Why you are renting this if is stable and good as you say to be? Answer : Direct Financial to keep improving this project and be sure will be alive during many time, so we dont need to use our parallels earnings to use on this.
- Where can i contact you? Answer : you may contact us directly on our sales jabber id : sales@exobot.pw (Serious people with serious deal only, Haters.Time waster pls stay away)
- we dont provide apk builder
- cleaning service? Answer : we delivery the apk file cleanaed and include free cleaning 1 time monthly, for other cleaning services can be discussed

Prices and Coverage

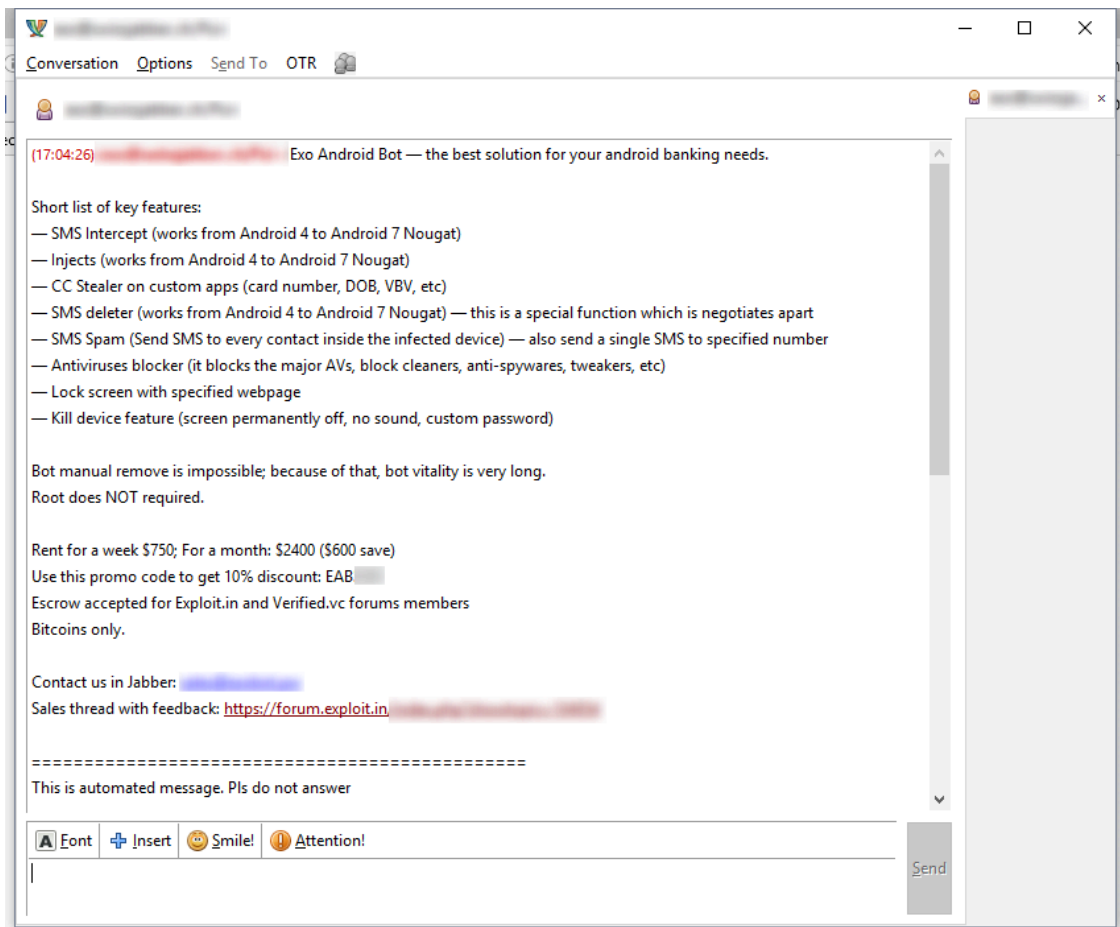
Monthly rent price promotion for next 6 customers will be 1500 dollars after we will ask for the normal price which is 2500 dollars monthly
Weekly Rental for those curious which want to try with low budget. Price 500 dollars with same requirements for the installation

android bot android bot private bto sms sms interception trojan android trojan

In October, someone had also registered a domain on the public Internet, where he now hosts a website, peddling the malware.



In November, we also came across Jabber/XMPP spam advertising Exo.



The trojan is currently sold at different prices, depending where you see an ad for it, but Exo is rented out on a weekly, monthly, or yearly basis.

According to its creator(s), Exo is worth its price. First of all, Exo works on Android versions 4, 5, and 6. In some ads, it's also advertised as working on Android 7, but this may be just false advertising, since not all listings advertise this feature.

Furthermore, crooks boast that the trojan doesn't need root access to work and that users can't uninstall it manually, meaning they need to do a complete phone reflashing to get rid of Exo.

Other features, taken from the AlphaBay listing are embedded below [original, unaltered text]:

- SMS intercept (send the sms content to admin panel in real time. If is desired with jabber notifications too, can be configured for a target or by sender phone numbers)
- Send SMS for a specified phone number
- Hide/delete incoming sms (this feature works upto android 4.4 version)
- USSD' requests
- Web injects (show phising over targeted app names to steal data, username,password,telepin whatever you want)
- Custom injects could be made under customer request
- CC Stealer (Steal CCs data Including VBV/MSV/SAFEKEY) (CCs stealer can target the desired apps. Example: Whatsapp, Viber, the Google the Play Store)
- Jabber notifications for incoming new CCs or WebInject data or the SMS from specified phone numbers Collected
- Lock / unlock device with a password / disable screen and phone use also can show a custom page on locked screen
- Uninstall the bot manually (without the PC / cable) is impossible
- Wi-Fi access / mobile data automatic enabler, if detect stored wifi networks on range
- Send Mass SMS to all contacts from the infected phone
- Control the bot with SMS too in case no internet access
- Exo Android Bot do not need Root privileges to work Correctly
- Admin panel to manage your bots
- Our bot works from 2.3 to 6.0.1 Android versions

The same AlphaBay listing provides a short FAQ section, which also provides a hint on Exo's origins [original, unaltered text] [text in bold]:

- we dont install admin panel files outside our servers , the customer will need to provide us a vps/server root access to install frontend/proxy script
- Customer must provide from 1 to 3 domains names where the bot be pointing to
- we are noob friendly , which means we may guide you to setup all the necessary stuff for a fast start on this android scene
- if you consider our product is expensive and no worth , is not our problem if you dont have money. or dont have the intention to use our services and just want troll around
- we are here to make happy our customers and be sure all the features which we are offering it works and continue working offering a good support
- **this project was made from scratch ? answer : No, we purchased a base source code 4 months ago directly from his developer before he vanish from internet, and we began our own project and development/improvements/new features**
- what if i rent your product and your dissappear? Answer : No definetly we are not going to dissappear or run away least for the next year
- what other features are planned for the incoming months? Answer: VNC/Geo Fencing / File Manager Browser and others
- Why you are renting this if is stable and good as you say to be? Answer : Direct Financial to keep improving this project and be sure will be alive during many time, so we dont need to use our parallels earnings to use on this.
- Where can i contact you? Answer : you may contact us directly on our sales jabber id : [REDACTED] (Serious people with serious deal only, Haters.Time waster pls stay away)
- we dont provide apk builder
- cleaning service? Answer : we delivery the apk file clenaed and include free cleaning 1 time monthly. for other cleaning services can be discussed

As you can see, the Exo author is providing a control panel for managing infected bots, but which buyers can access only via a proxy client installed on their own servers. Below are two GIFs depicting the Exo control panel, included in some of the ads.

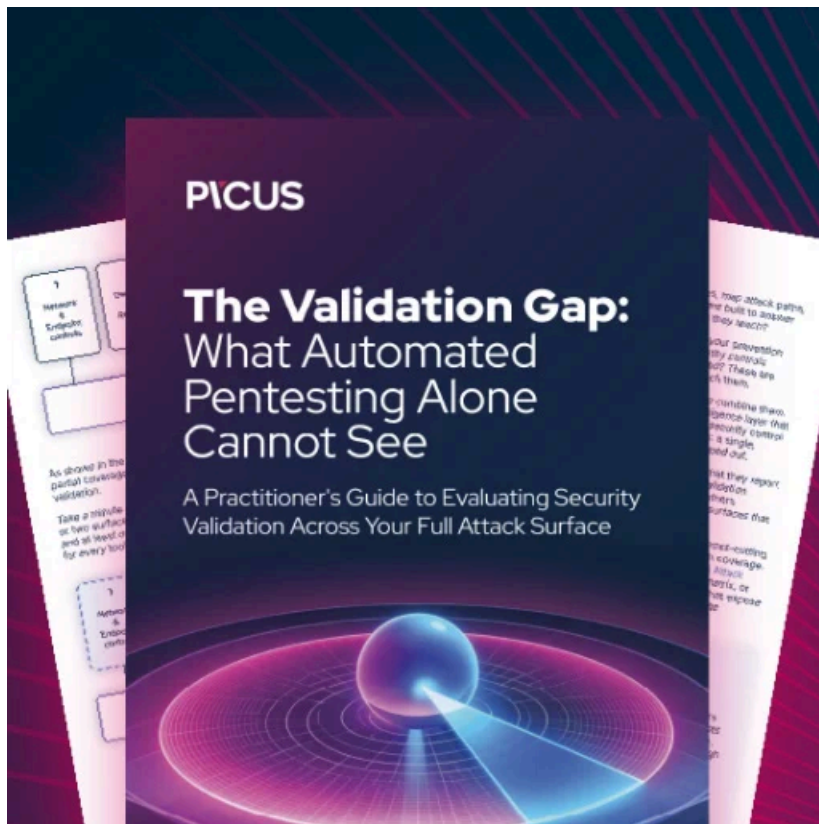
Bleeping Computer reached out to one of the contacts listed in many of the ads, and we stumbled upon a person that admitted he was only a reseller, meaning Exo already runs its own affiliate system.

Bleeping Computer also reached out to Exo's creator(s), but we have not received any reply at the time of publishing.

In the original hacking forum ad, Exo's creator had listed the times of day during which he wanted to be contacted: "14:00 — 20:00 MSK". MSK stands for Moscow Time, which is a pretty reliable (not definitive) clue on the hacker's location, taking into account the ad was initially listed on a forum for Russian-speaking hackers.

Furthermore, Exo includes a feature that prevents the trojan from executing on devices from users located in former Soviet states, and the US. This filter is likely there so the author may avoid getting on the radar of Russian or US law enforcement agencies.

Bleeping Computer has reached out to several security providers and inquired about campaigns distributing Exo, as to assess the status of this current malware family, either as a marginal player or as an active threat.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/>