New Exo Android Trojan Sold on Hacking Forums, Dark Web

bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/

Catalin Cimpanu

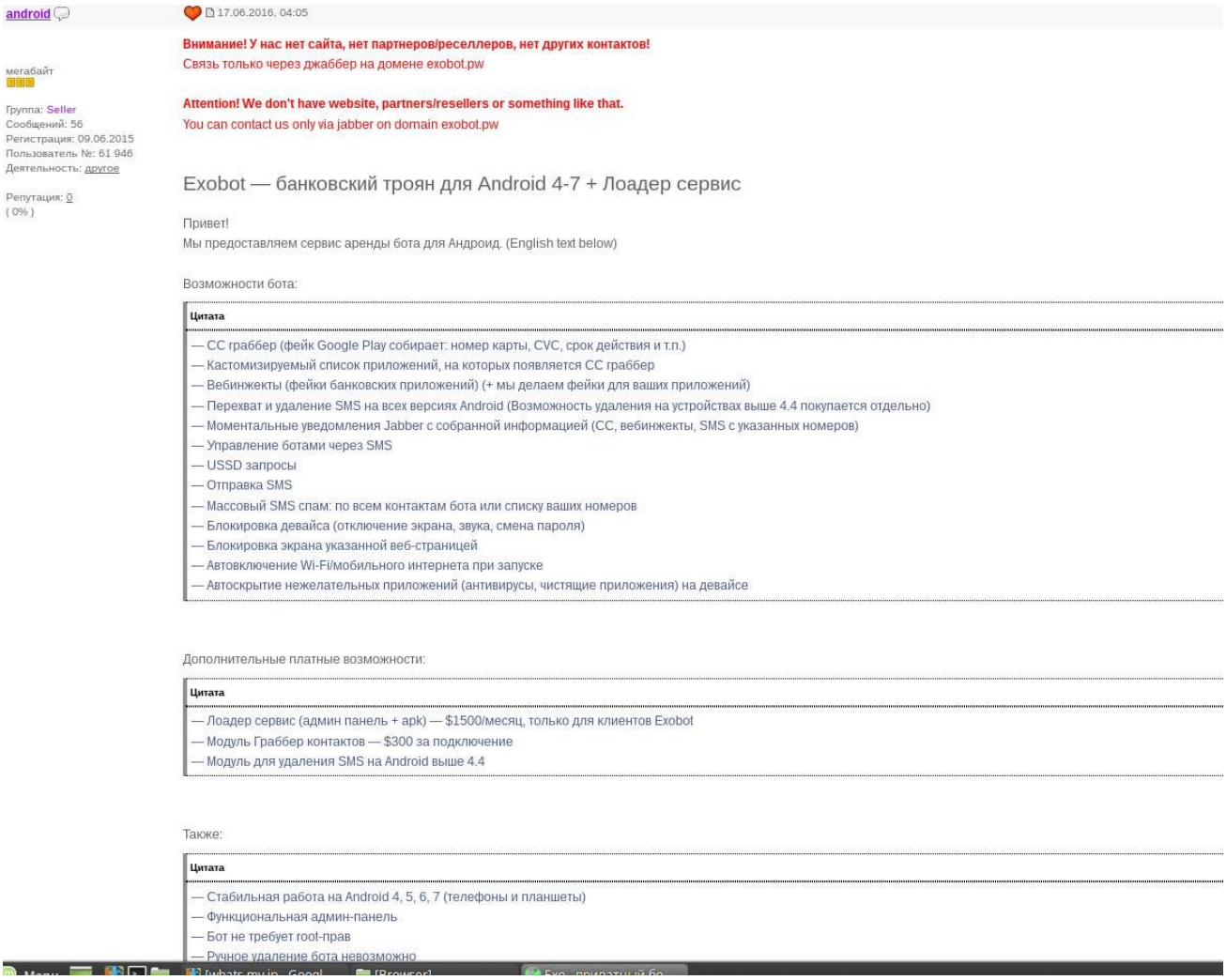
By
Catalin Cimpanu

- December 9, 2016
- 11:20 AM
- 0

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).



android

17.06.2016, 04:05

мегабайт

Группа: Seller
Сообщений: 56
Регистрация: 09.06.2015
Пользователь №: 61 946
Деятельность: другое

Репутация: 0
(0%)

Внимание! У нас нет сайта, нет партнеров/реселлеров, нет других контактов!
Связь только через джаббер на домене exobot.pw

Attention! We don't have website, partners/resellers or something like that.
You can contact us only via jabber on domain exobot.pw

Exobot — банковский троян для Android 4-7 + Лоадер сервис

Привет!
Мы предоставляем сервис аренды бота для Андроид. (English text below)

Возможности бота:

Цитата

— CC граббер (фейк Google Play собирает: номер карты, CVC, срок действия и т.п.)
— Кастомизируемый список приложений, на которых появляется CC граббер
— Вебинжекты (фейки банковских приложений) (+ мы делаем фейки для ваших приложений)
— Перехват и удаление SMS на всех версиях Android (Возможность удаления на устройствах выше 4.4 покупается отдельно)
— Моментальные уведомления Jabber с собранной информацией (CC, вебинжекты, SMS с указанных номеров)
— Управление ботами через SMS
— USSD запросы
— Отправка SMS
— Массовый SMS спам: по всем контактам бота или списку ваших номеров
— Блокировка девайса (отключение экрана, звука, смена пароля)
— Блокировка экрана указанной веб-страницей
— Автовключение Wi-Fi/мобильного интернета при запуске
— Автоскрытие нежелательных приложений (антивирусы, чистящие приложения) на девайсе

Дополнительные платные возможности:

Цитата

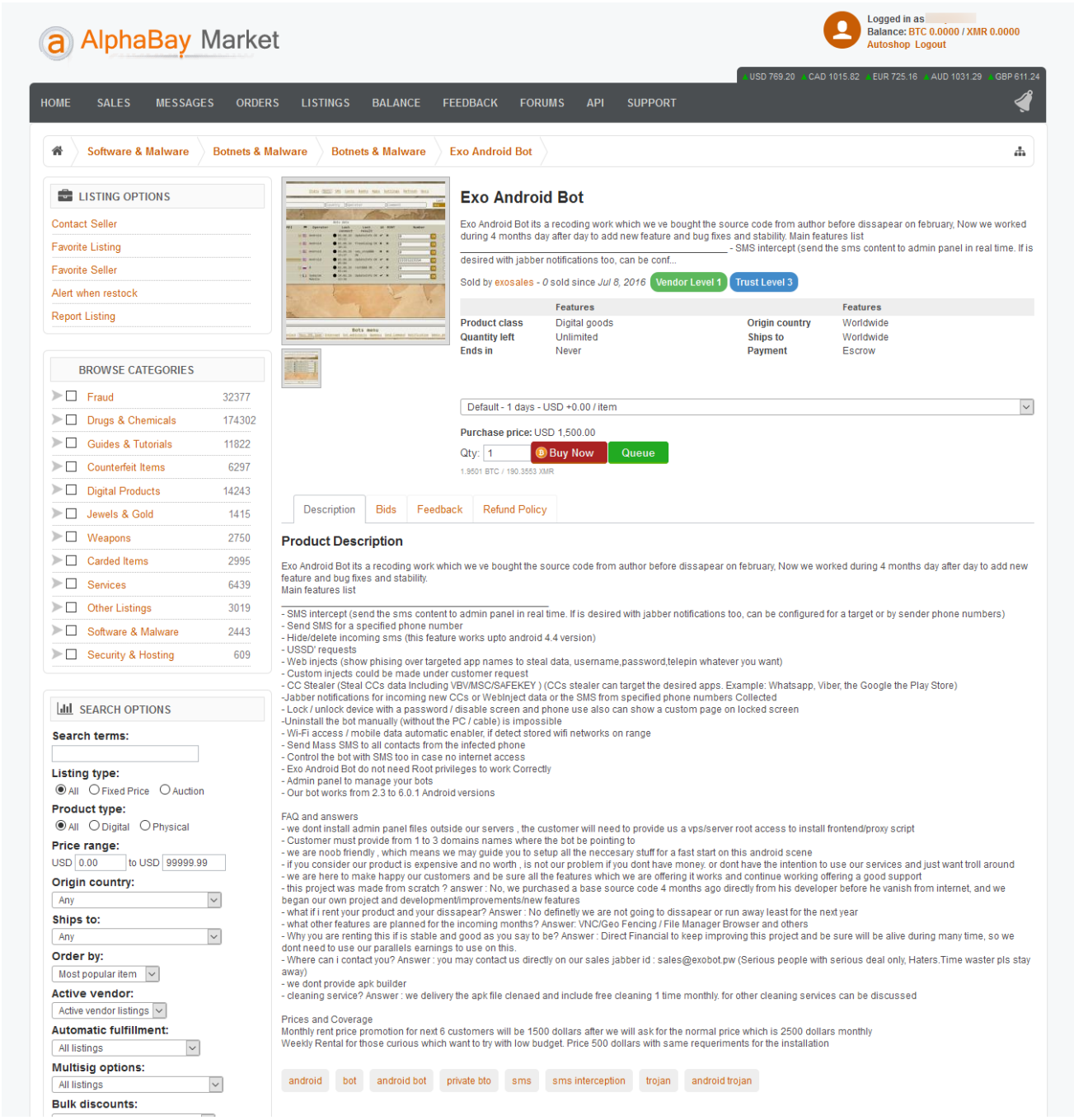
— Лоадер сервис (админ панель + apk) — $1500/месяц, только для клиентов Exobot
— Модуль Граббер контактов — $300 за подключение
— Модуль для удаления SMS на Android выше 4.4

Также:

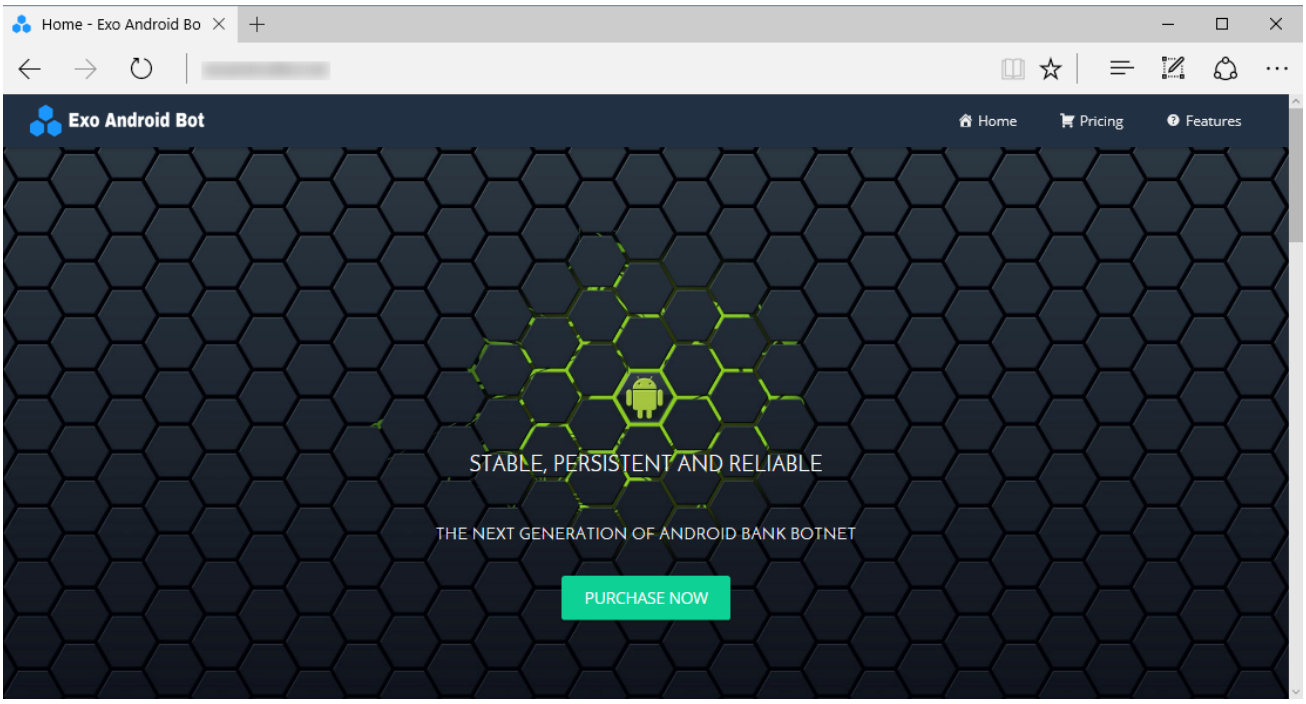
Цитата

— Стабильная работа на Android 4, 5, 6, 7 (телефоны и планшеты)
— Функциональная админ-панель
— Бот не требует root-прав
— Ручное удаление бота невозможно

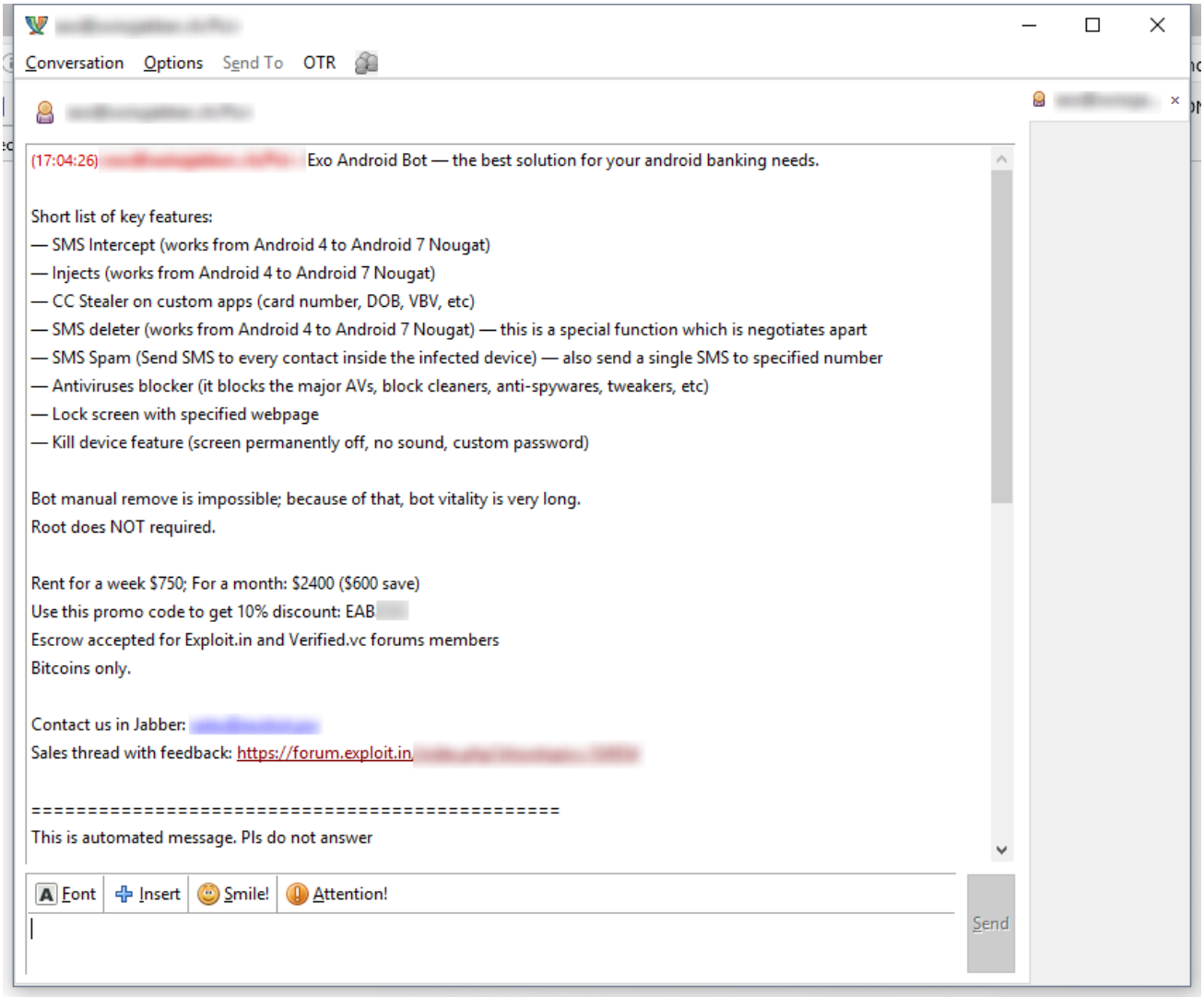
Shortly after, a listing appeared on AlphaBay, the largest Dark Web marketplace for illegal products.



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]:

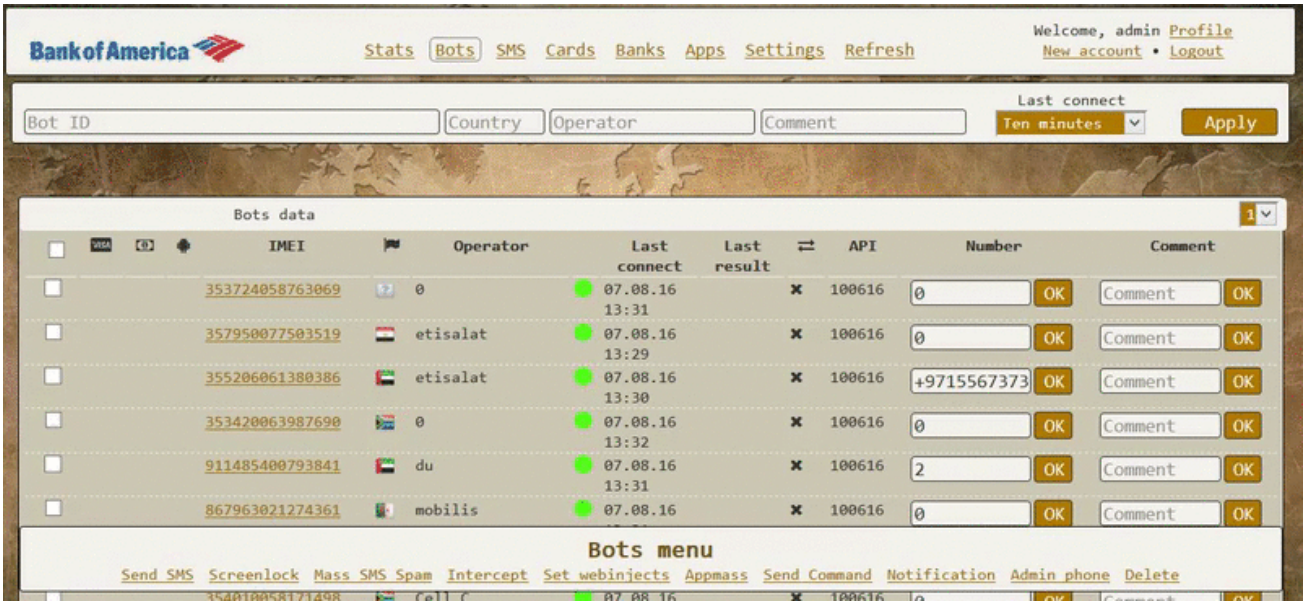
- SMS intercept (send the sms content to admin panel in real time. If is desired with jabber notifications too, can be configured for a target or by sender phone numbers)
- Send SMS for a specified phone number
- Hide/delete incoming sms (this feature works upto android 4.4 version)
- USSD' requests
- 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/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

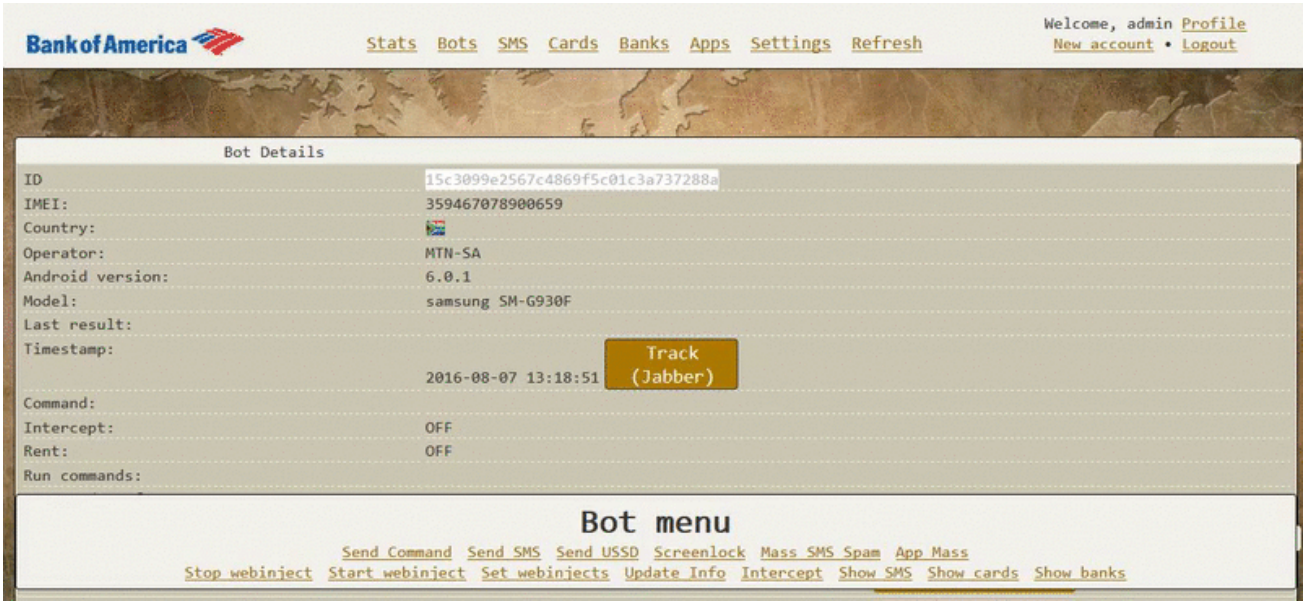
The same AlphaBay listing provides a short FAQ section, which also provides a hint on Exo's origins [original, unaltered text] [text in bold]:

- 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 neccesary 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 dissapear? Answer : No definetly we are not going to dissapear 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.

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

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

You may also like: