January 2017

ANDROID MALWARE IN 2016:
THE EMERGENCE OF A PROFESSIONAL ECOSYSTEM

Cyber Threat Intelligence Team

σtratégic notes

INTELLIGENCE
IN DECISION-MAKING

PREAMBLE

This document was produced by CEIS Cyber Threat Intelligence Team as part of the missions and reflects the activities observed on underground cybercriminal platforms during the past year.

The aim is to shed light on the cybercrime threat coming from the platforms – private forums and blackmarkets – present on the Deep and Dark Web. The team is monitoring on a daily basis:

- 10 French-speaking platforms;
- 12 English-speaking platforms;
- 15 Russian-speaking platforms;
- 5 Arabic-speaking platforms.

All of the information available on this document is provided for purely informational purposes only. The analysis and conclusions in this report are the sole responsibility of the authors and do not necessarily represent the CEIS' views.

1. Introduction

2016 has seen the development of a professional Android malware ecosystem that revolves around two notorious families – **Mazar** and **EXO** – and a much less industrialized family of small bots, inspired by them.

Each of the big ones presents a list of very advanced features; they are also constantly supported by their developers and cleaned at least twice a week to avoid anti-virus detection.

How did they arrive to those positions? It is worth knowing how the situation came about.

2. A major event: leak of a powerful malware source code

Since February 2016, many global newspapers alert on the wave of attacks implemented with the help of a robust Android malware called **Mazar Bot**[1]. Installed on the phone as an APK file downloaded either on Google Play or on alternative applications markets, it allows the cybercriminal to:

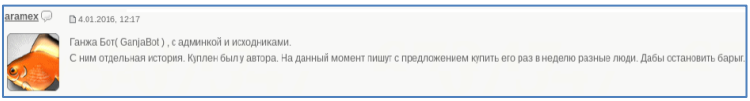
- Gain total control over the smartphone;
- Steal banking card information;
- Intercept SMS texts;
- Erase the phone's content;
- Block the work of famous anti-virus solutions.

Dubbed **GM Android VBV Grabber Bot** and available on a private Russian underground platform since October 2014, the malware was traded in January 2016 at a price of 10 Bitcoins ($4,200 at the time). **GM** stood for ***Ganja_Man***, the nickname of the official malware distributor, who had a "Seller" status (reserved to a few members) on the platform. Screenshots provided by the sale topic starter showed statistical

[1] http://www.bbc.com/news/technology-35586446 + http://www.forbes.com/sites/ewanspence/2015/02/04/android-malware-apps-deleted

information by country and by infected machine, as well as phones' IMEI and operators, texts of sent and received SMS and the grabbed banking card information. The author of the topic specified that it was possible to grab various data directly from applications, such as Google Play and WhatsApp, but also from "*nearly any bank*".

In fact, the first version of the malware, **Mazar Android Bot**, had been sold at $5,000 from 29 October, 2014. But in the same month of January 2016, a user named ***aramex*** released a pack containing the source code of this malware for public use:



aramex's release

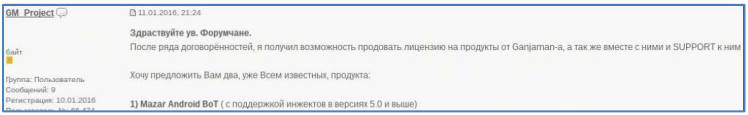
Aramex: "*Ganja Bot, with admin panel and sources. I bought it from the author. Now tons of people are trying to commercialize it. I make it public to stop those resellers.*"

Transcription of aramex's release

Members of the platform started to panic, asking ***aramex*** how could he leak something that was still sold by the developer. To this he answered: "*Ok, first of all, this version has been reworked by my coder team, many bugs have been corrected, so I do think I can release and share it with people. Second, the support for this bot has ended half a year ago and new versions have appeared since, which the author supports. Third, every second guy on this forum sends me messages asking me to sell it for $500 or $100. Therefore, I am convinced that releasing this bot will only help the author to finally be relieved from all those people who ask to support*

this semi-public bot. Fourth, people who'll start working with this bot will be able to get what they want from it and clarify it when they will buy a new awesome version from the author, since no one, except Ganja, is able to write that kind of software on our boards."

Some days afterwards, ***Ganja_Man*** offered the rights to sell his last version of the **Mazar Android Bot** to another user, registered under the nickname ***GM_Project***. On the 11th January 2016, ***GM_Project*** started his own trade topic:

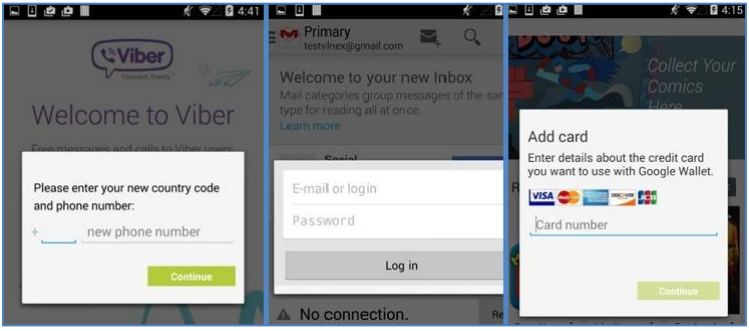


GM_Project advertisement

GM_Project: "*Hello dear forum members. After a series of negotiations, I have been provided the opportunity to sell the licenses of Ganjaman's products, as well as provide the support.*
I would like to present you two products that everybody knows already:
1) Mazar Android Bot (supports injections for versions 5.0 and above)
Sources of admin panel, bot apk, instructions for installation, free installation on your server (the 1st one)
2) GM Loader
Sources of admin panel, apk sources, instructions for installation, free installation on your server (the 1st one)
Price: Mazar Android Bot - $500, GM Loader - $350"

Transcription of GM_Project advertisement

And ***Ganja_Man*** confirmed in the same topic: "*This is exact. I am no longer selling this software!*" However, he still sold his **VBV Card Grabber** for 10 Bitcoins, which experts of Kaspersky Lab named **Acecard** in their reports. According to their first analysis, **Acecard** introduced a new advanced feature: application injects. Thanks to this feature, it was able to overlay screens in a number of applications (Gmail, Facebook, Skype, WhatsApp, Instagram, Paypal, Twitter, Goggle Play, Google Music, as well as a number of banking applications) with a fake copy, which automatically sent the registered credentials to the hacker server panel in real-time.

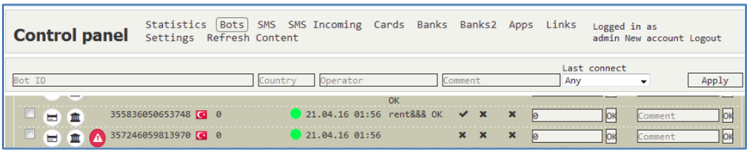


Example of an application inject

But the fame and success of ***Ganja_Man*** did not last long. In March 2016, he disappeared without giving money back to some members and was banned from the underground market. His status switched from an elegant "Seller" to a "Ripper" status.

3. A disputed hegemony

In March 2016, only one Android malware was still sold on the market: **Android KNL Bot ($4,000)**, distributed by ***Rashe***, the only long-standing competitor to ***Ganja_Man*** from before 2014, also with a "Seller" status, without counting **GM_Project's Mazar Android Bot ($500)**, which also remained available for purchase.



Rashe's Android KNL Bot – Admin Panel

The same week, another malware emerged from nowhere on both Russian and English-speaking platforms: the so-called **Bilal's Bot**.

It is important to understand that only some weeks after ***aramex*** released the source code of **Mazar Android Bot in January 2016**, Android malware popped up like mushrooms on different underground forums, with one new product appearing every two weeks. They may not have been as sophisticated as the ***Ganja_Man***'s product, but they were all advertised as such.

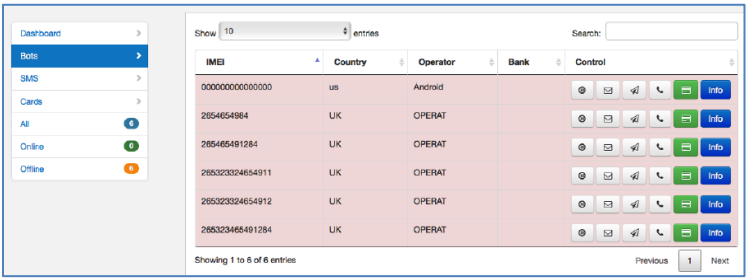
Bilal's Bot price was originally $4,000, but soon passed to $3,000 and then to $2,500. The developer of this malware was originally looking for 5 people to work with. The malware was

said to be able to receive and send SMS, forward calls, provide custom-made app injections and full bot statistics. Furthermore, customers were given the possibility to edit overlay screens right in the control panel before they infected the victim.

Bilal: "*The most valuable functions are the phishing windows that are popping out when the target is trying to access apps, such as WhatsApp, Viber, Google Play. When they enter into these applications you get full info (Full name, CVV, Exp. Date, VBV password, Billing Address). It is then easy to cash-out money having this information.*"

Bilal said he was working hard every day in order to make this product the best on the market. And he indeed updated it at least twice a week, making the bot fully undetectable by anti-virus solutions. ***Bilal*** also explained that having fewer functions guaranteed a longer life for the botnet: "*We are aware that there are several bots on the market already, which have these functions and can do even more things, but all of them are 2 years old* (reference to **Mazar Android Bot** and **Android KNL Bot**, first versions of which were released in 2014)*, and are detected even if you provide a strong encryption. The support is poor, the updates cost more than the bot itself, they are coded hurriedly and bugs are not even fixed these days, they are unstable, bots are dying fast. Our bot does not have a lot of functions, and most likely we will keep it that way. Too much useless functions kill the Trojans, make them detected and investigated. This is why we have implemented only some of the most necessary functions which will bring you money (Cards + VBV Grabbing, getting all necessary info to do bank transfers easily). If you want to see nude pictures of some random faggot, you should buy subscription to https://www.mspy.com/. If you are looking for a*

bot that brings you money, lasts long and stays stable, then you have to get this one. Purchasing this, you will also receive tutorials on how to use it, where to get traffic/installs, how to spread and many more things."



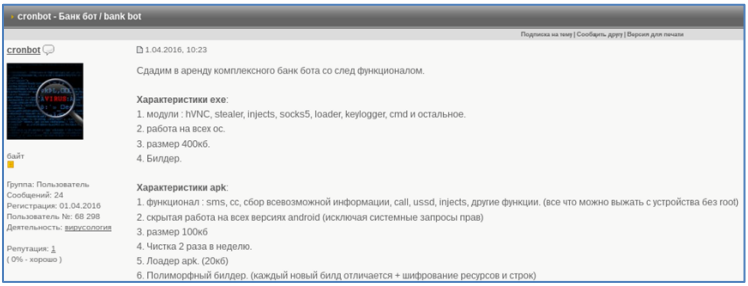
Bilal's Bot – Admin Panel

The coder behind this team actively collaborated with various players of the Russian malware market, notably one of the best designers and providers of banking injections, ***Kaktys***. Soon, Bilal's bot offer sharply improved due to the coder's ability to provide new shiny "*injects for any bank, any country*".

Bilal's Bot did not last long either. The author filled the 5-spots-for-rent and then surprisingly started to commercialize the source code version. As a result, he has not even been able to provide support for the original renters, since his server was not up to this task, and ***Bilal*** had to vanish from black markets.

On the 1st of April, a fourth Android malware arrived: the **Cron Bot.** Quite interestingly, it was possible to buy the malware as a bot for Windows (EXE) or for Android (APK) or as both. **Cron Bot for Windows** offered a wide variety of options that duplicated those of PC Trojans, including a bunch of modules

(loader, VNC, keylogger, stealer, etc.) and a polymorphic builder. The Android version had traditional features and was able to obtain most of the data without getting root rights on the infected device.



Cron Bot advertisement

cronbot: "*Complex banking bot for rent.*

Exe characteristics:

1. *Modules: hidden VNC, stealer, injects, socks5, loader, keylogger, cmd etc.*
2. *Works on all OS*
3. *Weight: 400 kB*
4. *Builder*

Apk characteristics:

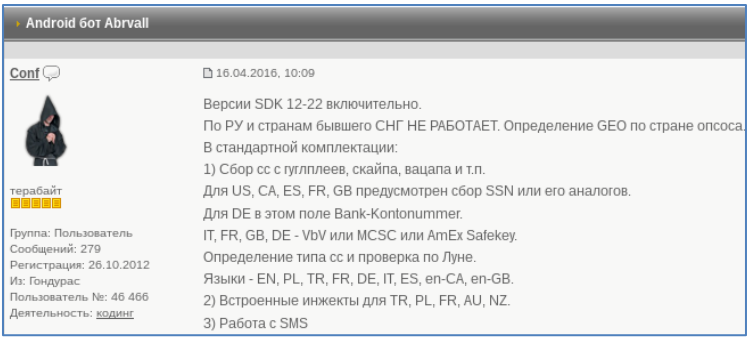
1. *Functionalities: SMS, credit card, collecting all possible information, calls, ussd, injects, other functions (everything that can be obtained from a device without root rights)*
2. *Hidden work on any version of Android*
3. *Weight: 100 kB*

4. Apk loader (20 kB)
5. Polymorphic builder (every new build is different + encrypting resources)"

Transcription of Cron Bot advertisement

The price depended on the chosen version: either exe or apk cost $4,000, while both were given for $7,000. The latter included unlimited encryption and a server. **Cron Bot** was one of the most dangerous products at the time. The user, ***cronbot***, earned the long-expected Seller status and developed a loader for Android systems, **C2H5OH** ($250/month), and a stealer, **Fox v1.0** ($250/month). After a period of success, he vanished in thin air without apparent reason (around October 2016).

Conf, an old user with a strong reputation and undisputable technical skills, who had long specialized in selling loaders and droppers, began marketing his Android malware called **Abrvall** on the 16th of April. This product was from the outset equipped with banking injections for Turkey, Poland, France, Australia and New Zealand. The developer made it clear that the malware would not function in Russia or CIS countries and refused working with strangers or analyzing Google-translated messages. **Abrvall** had a very unique feature – SMS Spam Bot – successfully implemented by its creator a few days after he conducted a positive market study. The Spam Bot functionality allowed sending hidden SMS from the infected device to all of the victim's contacts and numbers in SMS history. ***Conf*** also worked on implementing an extortion function for US smartphones, based on the camera use, but in the end of April he suddenly disappeared. The support for the bot was cut, while the server remained operational. According to some forum members, ***Conf*** died from a heart attack.



Abrvall advertisement

Two new Android malware appeared in August 2016 and are still distributed: **Catelites Android Bot (rent: $1800/month** and **Alien Bot (rent: $2000/month)**. They seem to be quite sophisticated but limited to a few buyers. To be continued…

4. A confirmed supremacy of historical malware

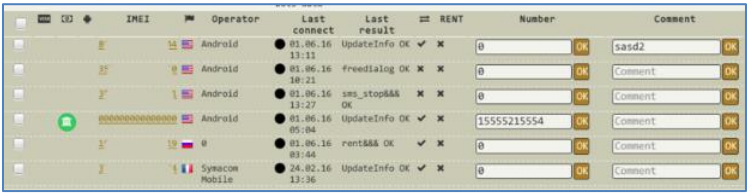
Rashe had been around for at least as long as ***Ganja_Man***, selling his **Android KNL Botnet**. On the 21st of April, after a two-week break in his activities, he successfully presented a new version of this malware: **Marcher Android Banking Trojan**. The malware was the closest to ***Ganja_Man***'s in terms of functionalities. It allowed:

- A total control over the infected device;
- Getting online banking and credit card data;
- Intercepting and sending messages;
- Making and forwarding calls;
- Turning off the phone's sound, vibration and screen;
- Blocking anti-viruses;
- Killing the device;
- Getting jabber notifications about fresh stolen data.

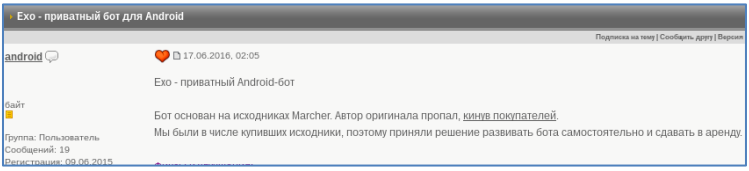
It was also equipped with a special feature, called "*Entice the holder into the bank*". The malware was offered at $4,000 plus $500 per month for "cleaning" to always keep it fully undetectable by anti-viruses. Only ***Rashe*** was not going to clean the files. After selling several licenses and getting over $30,000, he disappeared as a watch in the night in the same direction than ***Ganja_Man***, obtaining a "Ripper" status.

His work has not been vain, since another user has had the time to buy and rework his malware. Now this user, who calls himself ***android***, is marketing on English and Russian-

speaking platforms his **Exo Android Bot**, which clearly inherited the **Marcher and Android KNL Botnet** panel:



Exo Android Bot – Admin Panel



Exo Android Bot advertisement

android: "*Exo: Private Android bot.*

The bot is based on Marcher Bot sources. The author behind the original Bot has disappeared, letting his customers down. We were among those who were the first buyers of the sources, which is why we have taken the decision to develop the bot independently and rent it out."

Transcription of Exo Android Bot advertisement

The differences between **Marcher** and **Exo** were:

"*Android 6 support added*
Functionality and stability of web injects improved
Jabber notification system improved and extended

Some bugs such as eating CPU services in background were fixed
Admin panel improvements
The apps installed on the phone are verified every X time to ensure the injections work even on the newly installed target apps
Documentation for Admin Panel in English/Russian
Multi-domain system for robust bot work"

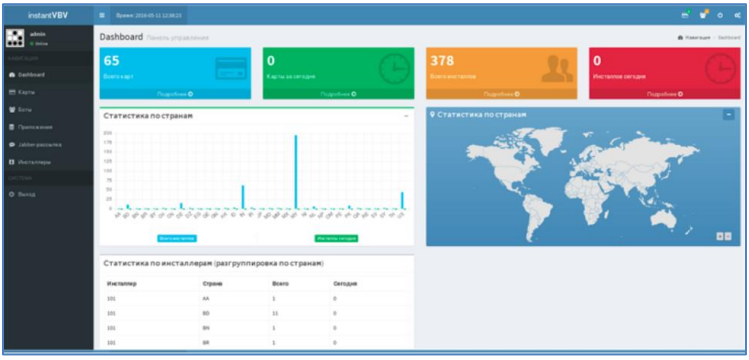
This new malware, which is traded at $2,500/month, has the possibility to:

- Intercept SMS to admin panel or a specified phone number,
- Send SMS,
- Overlay screens with injections,
- Grab banking card information including VBV password,
- Send immediate jabber notifications when new CC/webinjection data or SMS from specified phone numbers are collected,
- Lock/unlock the device with a password,
- Activate Wi-Fi/mobile data,
- Lock screen with a specified webpage,
- Send mass SMS spam (to contacts or by number list).

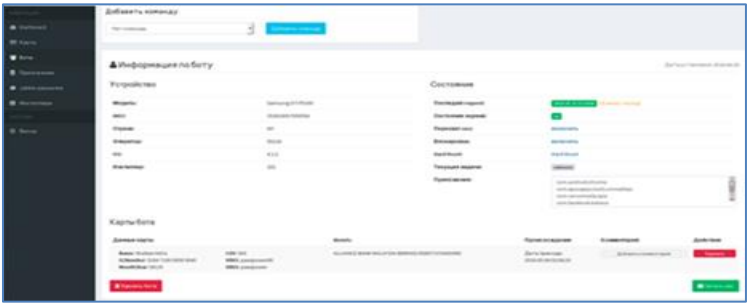
The difference is also in payment methods: unlike what happened with some scammers, here the escrow releases funds after one-month-use only if the customer has been happy with this product.

In the meantime, ***GM_Project*** began to sell a simplified version of **GM's VBV Cardgrabber**, which has been

exclusively conceived for stealing card information and VBV in real-time.



Instant VBV Admin panel (in blue: the total number of cards grabbed; in green: the number of cards grabbed today; in orange: the number of installs (victims' devices); in red: victims today; below: statistics by country and installs).



Bot information window (on the left: phone model, imei, country, operator, OS, installer; on the right: last request, screen state, on/off SMS interception, on/off blocking, on/off hard reset, current task, apps; below: bot card data – name,

credit card number, month/year, CVV, VBV1, VBV2, Bank info (name, country, type), the date and time of grabbing).

Unsatisfied with the sales, ***GM_Project*** finally launches the sale of "*A perfectly new product, with an old name*", on the 27th of October, which is called **Mazar 3** ($2,500). He claims that "*all errors of previous versions have been taken into account*" and that "*everything was rewritten from scratch*". Not even hiding that his "partnership" with ***GanjaMan*** (who was blacklisted as a ripper) still stands, he creates a topic in which he asks the population of the underground market if they accept his distribution of ***GanjaMan***'s products. The latest version of the malware has received a number of grabbing functionalities: contacts ("*around 100k from 1k bots"*), card numbers and phone numbers from a list of applications and has been said to bypass Android OS 6 Marshmallow security. The same week, **EXO Android Bot** is updated to be able to work on Android 7.1.1 version.

Mazar 3 – Admin Panel

5. Conclusion

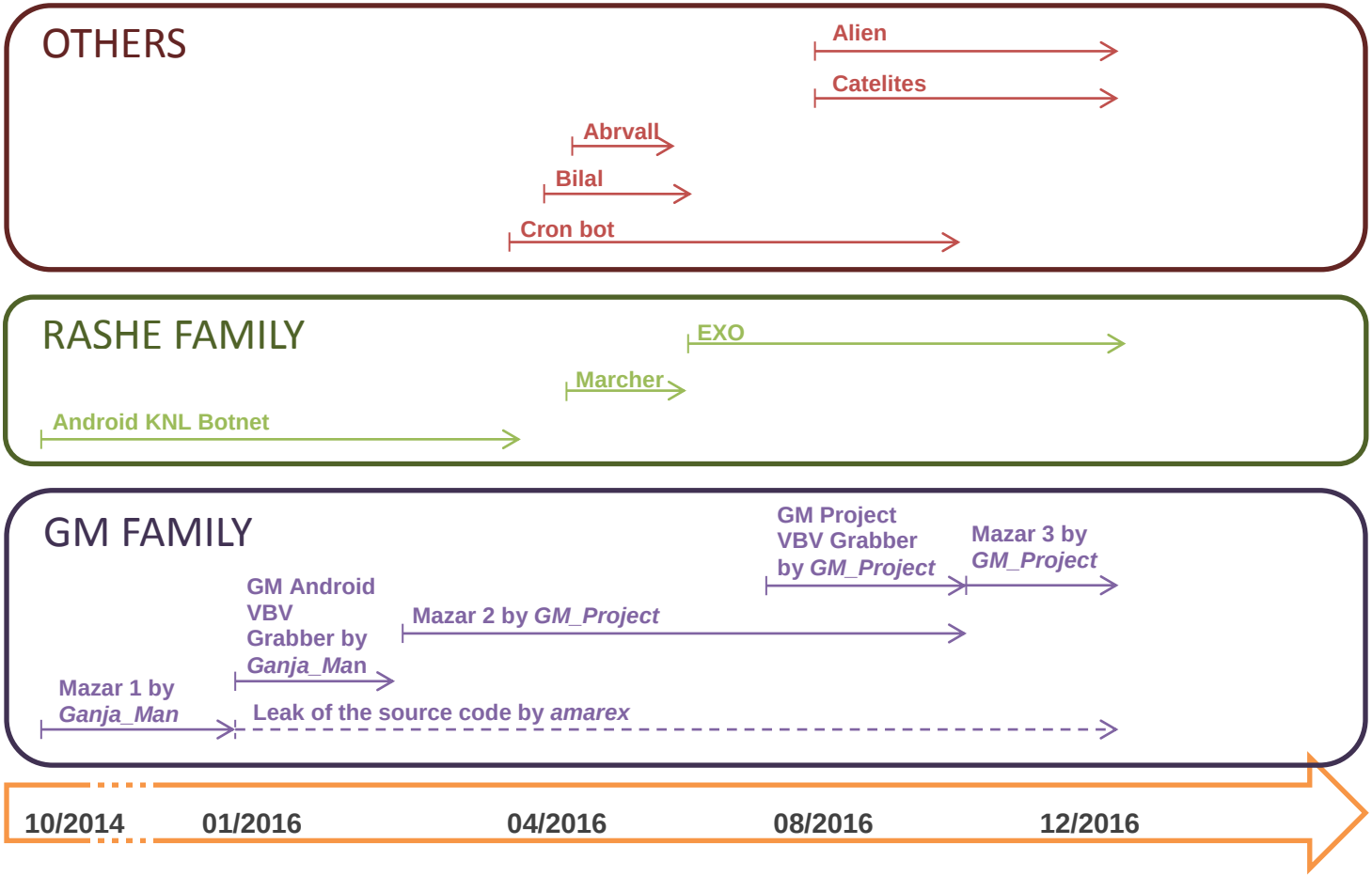
Despite a strong competition, the two historical Android malware are still on the top of the market. They are traded on the underground platforms: **EXO Android bot** (available only for rent) and **Mazar 3** (license purchase). Some malware were inspired by them (**Cron Bot**, **Bilal's Bot.**) and tried to offer some new functionalities to attract the market's favors: partnership with freelance injection coders (such as ***Kaktys*** for example) or new methods of distribution (EXE+APK versions).

A bunch of mobile malware can also be found on the same places for free: **Mazar Bot 1**, **SpyNote v2**, **Flex Bot**, **iBank**, **Droidjack**, **Dendroid** and others. Their technological capabilities are quite low and they are not supported by their developers against anti-virus detection. However, their functionalities still allow to ensure control over a device (remember that the first version of **Mazar** already had the possibility to kill an Android device).

The nature of underground markets is such that the most sounding products end up being detected by cyber security experts and anti-viruses, and that is why the creators of small bots tend to make a good showing, attract customers and then disappear in the wilderness. But the big ones are trying to always adjust to new realities and Android versions, a bit like Microsoft and Sony when they pop a new console.

Considering the buzz they made over the last year and the variety of Australian, US, European and Russian banks attacked, **Mazar** and **EXO** bots are sure to break the news again.

ANDROID MALWARE TIMELINE



ALREADY PUBLISHED

Available on ***www.ceis.eu***

MRO of military helicopter engines – Innovative solutions for a critical asset in military operations June 2015

The SIA Lab – Fostering Defence Innovation and Transformation June 2015

Anticipating Risks and Adopting Cloud Computing with Confidence May 2015

Société Anonyme au capital de 150 510 €
SIRET : 414 881 821 00022 - APE : 741 G
Tour Montparnasse – 33, avenue du Maine
BP 36 – 75 755 - Paris Cedex 15