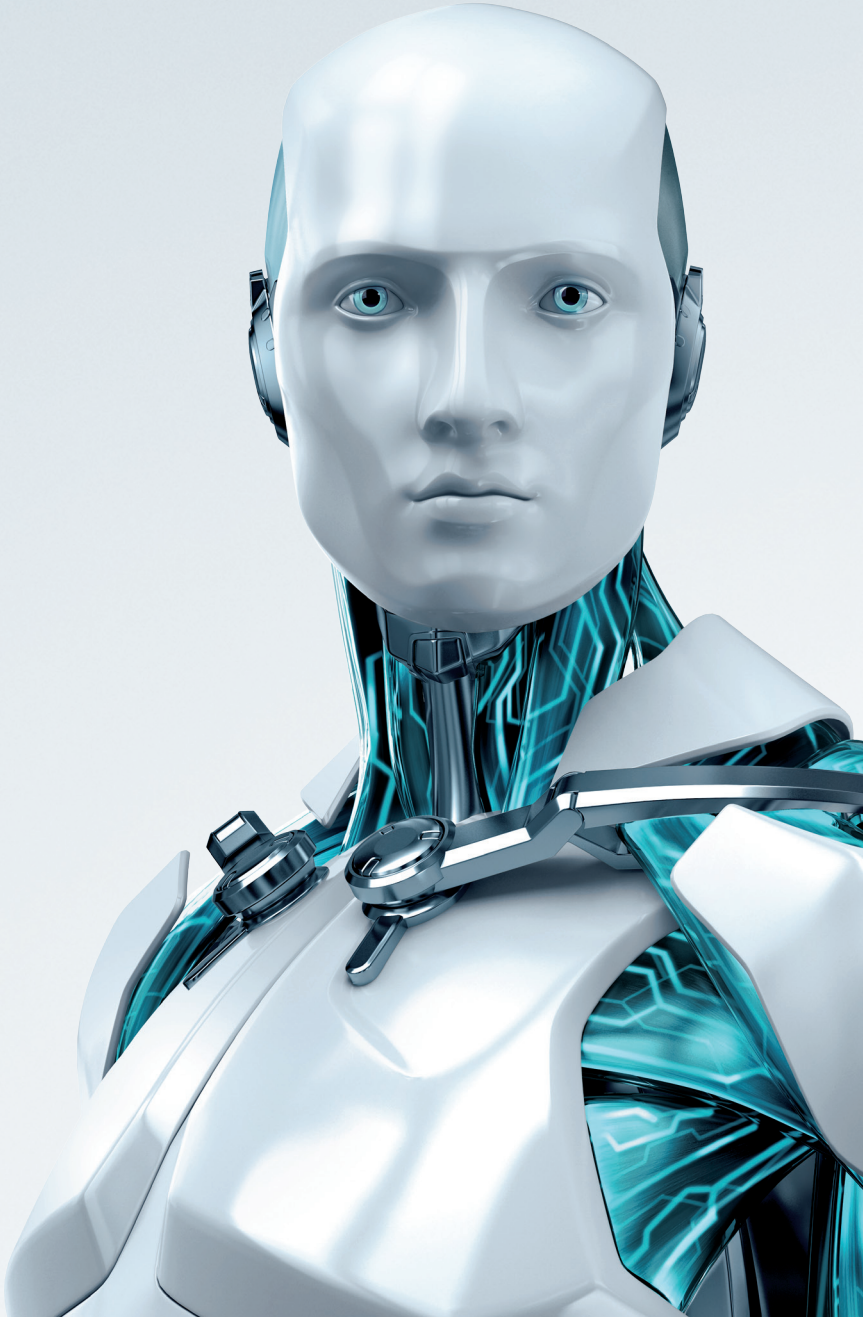
Boxer SMS Trojan

The first threat of the kind targeting Latin American countries



André Goujon / *ESET Awareness & Research Specialist* /
Pablo Ramos / *ESET Security Researcher* /

Android/TrojanSMS.Boxer.AA

Introduction

After several queries from users in the Latin America region, the ESET Latin America's Research Lab team analyzed the Boxer Trojan for the Android platform and found that the threat, detected by ESET Mobile Security as Android/TrojanSMS.Boxer.AA[1] targets nine Latin American countries out of total of more than 60 countries. An SMS Trojan targeting users across this region is unprecedented.

Once the sample was analyzed and its operation was understood as an SMS Trojan which uses commands to send SMS messages to Premium-rate numbers, we could also identify Internet users asking about and claiming for "mysterious" charges that appeared in their invoices or accounts. In all these cases, the Premium number causing this inconvenience was identified in the Boxer analysis.

The present report explains the nature of the threat, the technical characteristics of this malicious code in particular and the way in which the malware identified as Android/TrojanSMS.Boxer.AA and why it was designed in such a way to affect more than 60 countries all over the world.

SMS Trojans

The SMS Trojan is a category of malicious code for mobile phones whose main purpose is to subscribe the victim to Premium-rate messaging numbers. Since this type of service usually informs the user that he has been successfully subscribed, some Trojans of this category filter the SMSs from those Premium telephone numbers so that the user remains unaware of the infection; therefore, messages from other users or services are visible except the ones connected to the Premium-rate number. This represents a serious financial problem for the user: if he fails to check his balance or statement account, he could incur expensive charges.

The diagram in the following page shows the behavior of an SMS Trojan.

As can be seen, the user starts the malicious application and an SMS is sent; consequently, an attack by this type of malware, designed exclusively to target mobile devices, generates profit for the attacker.

[1] http://www.virus-radar.com/en/Android_TrojanSMS.Boxer.AA/description

Image 1: How an SMS Trojan operates

The Malicious Code

Generally speaking, the SMS Trojans have a limited range of action, i.e., they are only able to affect particular countries due to the fact that, in most cases, the Premium-rate numbers vary according to each operator and nation. Nevertheless, Boxer has the ability to affect a total of 63 countries, from America, Europe, Africa, Asia and Oceania. This turns it into an SMS Trojan that has great propagation potential across a wide geographic range (the exact parameters of this range are not entirely clear although it is probably arrived at by discarding countries seen as less profitable and retaining the most profitable ones).

Infection and Propagation

Being a Trojan, Boxer cannot propagate for itself; therefore, the people responsible of this kind of threat are those who upload it to a site or repository. In addition to the above, they also employ Social Engineering techniques to manipulate the potential victim and induce him to execute the malware.

Twenty-two applications infected with Boxer where found in Google Play[2] in December 2011 (formerly Android Market). Game titles such as Sim City Deluxe Free, Need for Speed Shift Free, Assassin Creed, and some Angry Birds accessories were used to deceive the users and get them infected with this malware. Although such trojanized applications were removed from Google a long time ago, the non-official stores or repository sites are still the main propagation vectors

[2] For more information, see the Limpieza en el Android Market report (Android Market Clean Up), available at ESET Latin America's Blog page.

of malicious codes targeting Android; for this reason, it would not be surprising for this Trojan to keep on getting new victims through this kind of web sites.

For the purposes of this analysis and the development of the present document, we have used a sample identified as Android/TrojanSMS.Boxer.AA, which appeared in an application known as "Urban Fatburner" (Md5: 962078fba0bca8cda4fe39c516d21ffc). If the user downloads and installs the malicious software, the following permissions are required to carry on with the process:

- Send text messages
- Receive text messages
- Make telephone calls
- Receive WAP PUSH
- Internet access

If the user notices all the permissions requested by the application, he will realize that there are some suspicious aspects, since a game or an application to "burn fat" should not need to send or receive SMSs in order to function. Afterwards, a license agreement is shown stating that the user could be subscribed to Premium-rate SMS numbers; however, some aspects are omitted, for instance, the fact that messages will continue to be sent to the user at an associated cost. Furthermore, the creators of this kind of threat usually take advantage of the fact that almost no user reads the terms and conditions of license agreements, in spite of the fact that they may be disadvantageous or suspicious.

The two screenshots below show the Android system (2.3 version) being infected: The first one (1) corresponds to the warning a user would see after executing Boxer. The second one (2) shows part of the license agreement of the SMS Trojan. This information is only shown if the user presses the "Rules" button.

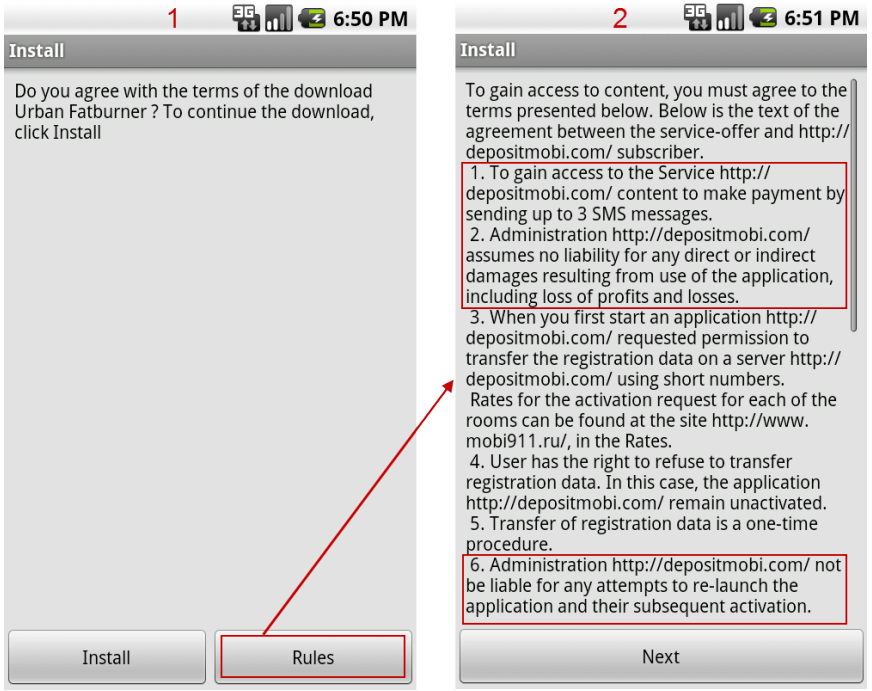


Image 2: Alleged license agreement

If the person is cautious enough to read the license agreement, he would notice some suspicious and abusive clauses, such as the limited liability of the provider in case the user's finances are affected in some direct or indirect way (point 2), or the omission of the Premium-rate numbers to be contacted and the cost associated with them.

At the same time, in point 1 it is possible to observe that, in order to access the content, up to three text messages must be sent; however, in point 6 it is mentioned that, if the application is executed one more time, it could be reactivated. That implicitly means that the user will have to pay again for the three Premium-rate SMS messages each time the threat is opened. Besides, a legitimate application in normal use conditions should not have to be activated more than once.

Payload: Subscription to Premium-Rate SMS Numbers

If the license agreement is accepted by the user, the Trojan proceeds to get the identification number codes by country and operator MCC (Mobile Country Code) and MNC (Mobile Network Code); in this way, it determines the country where the smartphone is located as well as the telephone company it belongs to. Subsequently, it sends SMSs to Premium-rate numbers in accordance with the information previously gathered.

The analysis of the Trojan allowed us to identify the code sections where the list of MCC codes is stored; these codes are used later on to identify each country:

```
private static final String ARAVIA_MCC = "420";
private static final String ARGENTINA_MCC = "722";
private static final String ARMENIA_MCC = "283";
private static final String AVSTRIA_MCC = "232";
private static final String AZ_MCC = "400";
private static final String BELGIA_MCC = "206";
private static final String BELORUS_MCC = "257";
private static final String BOLGARIA_MCC = "284";
private static final String BOSNIAGERC_MCC = "218";
private static final String BRAZILIA_MCC = "724";
private static final String CHEHIA_MCC = "230";
private static final String CHERNOGORIA_MCC = "297";
private static final String CHILI_MCC = "730";
```

Image 3: Partial list of MCC codes contained in Boxer

In total, there are 63 different MCC codes for countries all over the world. This information is used by Boxer to determine the phone number to which it will send an SMS of subscription to the Premium message service according to the user's country. In order to identify the country, this SMS Trojan reads the device's information and obtains the system codes, comparing them and configuring itself to communicate with the correct number.

Once the country has been identified, the execution of Boxer continues and it proceeds to activate the recent installation in the user's device, thus managing to send a series of text messages to the Premium number with all the information the cybercriminals need to gain financial profit.

Affected Latin American Countries

As mentioned above, the analysis of the threat identified that, out of the 63 countries that were affected by this threat, 9 correspond to Latin America, which can be seen in the following map:

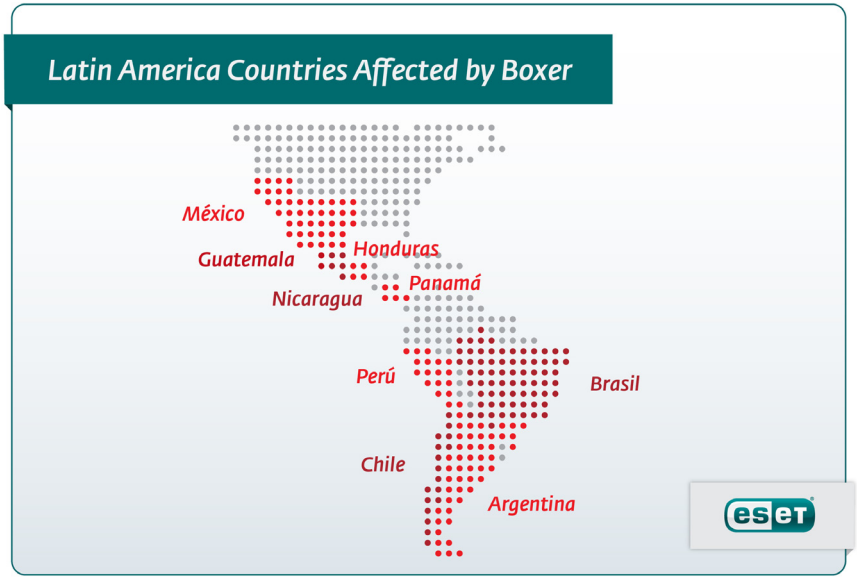


Image 4: Nine Latin American countries affected by Boxer

Below there is a table with the Premium-rate numbers and MCC codes corresponding to the nine Latin American countries affected by Boxer:

Table 1 - List of MCC and Premium-rate numbers by country

Country	SMS Premium-rate Number	MCC
Argentina	22588	722
Brazil	44844	724
Chile	3210	730
Peru	2447	716
Panama	1255	714
Nicaragua	1255	710
Honduras	1255	708
Guatemala	1255	704
Mexico	37777	334

Throughout the research, the ESET team has identified users in different forums claiming to have been charged unidentified fees in their accounts and, as can be seen below, the indicated numbers are the same ones used by Boxer.

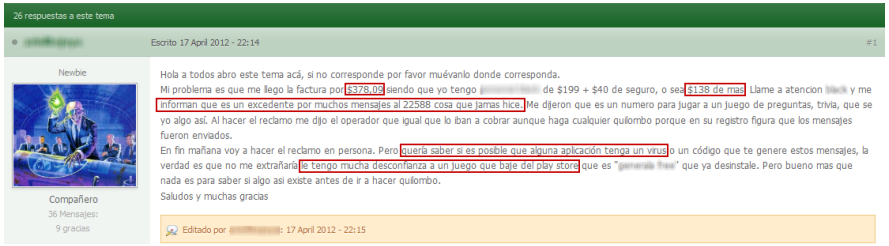


Image 5: User in a forum asking about "mysterious" charges

As can be seen in the preceding screenshot, a person claims for an excess of AR$ 138 charged to his account. When he called to customer service, he was told that those were the costs for sending messages to the **Premium number 22588**. The user claims not being aware of having sent those SMSs. At the same time, he discusses the possibility of being infected with a malware, since he was suspicious of an application he had downloaded from Google Play.

According to the Boxer analysis performed by ESET, the Premium-rate SMS number 22588 corresponds precisely to the one used by this threat to affect users in Argentina. Another similar case is the following one:

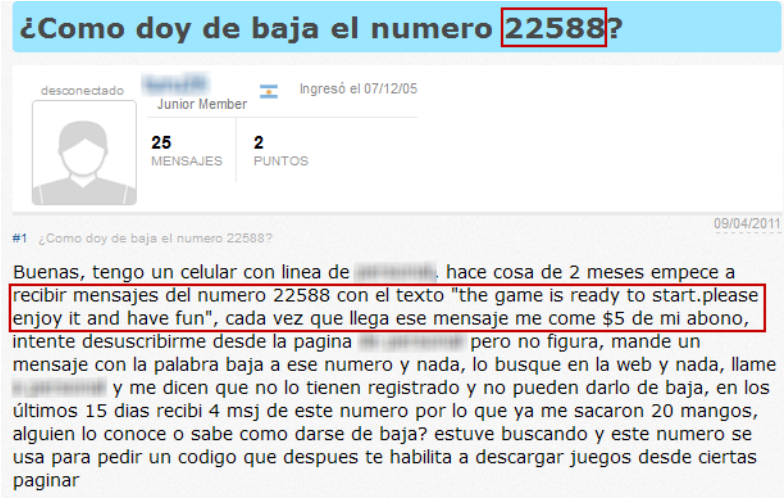


Image 6: Another user asking about the Premium-rate number "22588"

In this case, the user makes a claim regarding the same Premium messaging number 22588. In addition, he explains he has tried to unsubscribe the service through some mechanisms like sending a message with the word "unsubscribe", but he was not successful. Both cases involve an economic loss for the user, in the first case of AR$ 138 and in the second one of AR$ 20.

World impact

During this investigation we focused on the effect that this SMS Trojan had in Latin America because we were able to access reports from affected users in this region. Nevertheless from the total of 63 countries targeted 60% of them belong to Europe, 16% to Asia, 14 % to North and Latin America, 7% to Africa and 3% to Oceania.

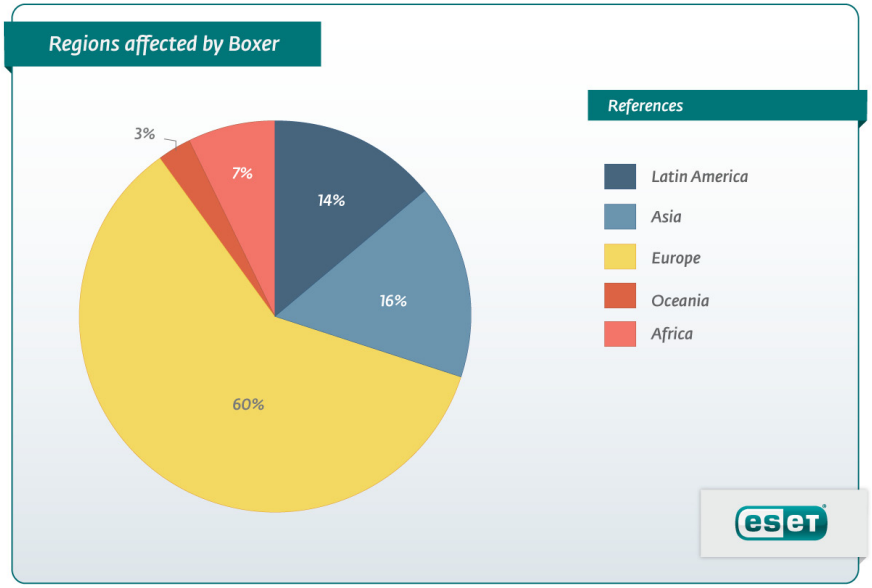


Image 7: Targeted countries distribution

The spectrum that is being targeted is quite wide, and might lead to further investigations about how this environment could be profitable to cybercriminals. As it has been reported previously, Pay Per Install markets are growing in relation to mobile devices[3]. Boxer is one of the wider threats that we have seen so far using this kind of business model.

Europe is the region with most targeted countries including Russia, France, Germany, Czech Republic and Poland among others. In order to clarify the distribution defined by Boxer around the world we can appreciate targeted countries in the following map:

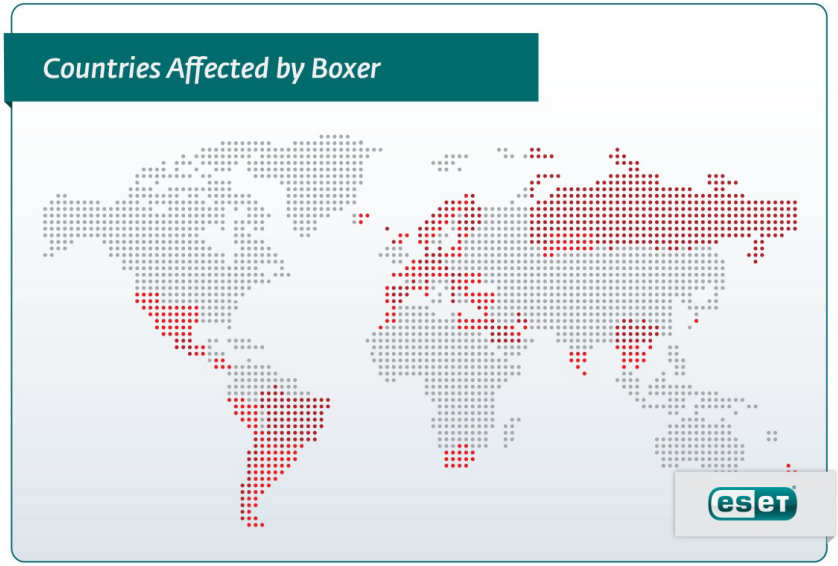


Image 8: Countries affected by Boxer

[3] http://blog.eset.com/2012/09/12/dancing-penguins-a-case-of-organized-android-pay-per-install

The full list of the 63 countries targeted around the world by this SMS Trojan is:

Africa	Hong Kong	Croatia	Portugal
Algeria	Israel & Palestine	Cyprus	Republic of Montenegro
Egypt	Jordan	Czech Republic	Republic of Serbia
Morocco	Kyrgyz Republic	Denmark	Romania
Republic of Macedonia	Lebanon	Estonia	Russia
South Africa	Malaysia	Finland	Slovenia
America	Qatar	France	Spain
Argentina	Saudi Arabia	Germany	Sweden
Brazil	Taiwan	Greece	Switzerland
Chile	United Arab Emirates	Hungary	Turkey
Guatemala	**Europe**	Kazakhstan	Ukraine
Honduras	Armenia	Latvia	United Kingdom
México	Austria	Lithuania	**Oceania**
Nicaragua	Azerbaijani Republic	Luxembourg	New Zealand
Panama	Belarus	Moldova	
Peru	Belgium	Netherlands	
Asia	Bosnia and Herzegovina	Norway	
Cambodia	Bulgaria	Poland	

Later variants for this malware have been reported and the list of targeted countries is not so big. Probably some countries were discarded due to certain issues involved with payment or effectiveness.

The variant we analyzed was published in 22 different applications in Google Play, where the probability of affecting a huge amount of users is more likely. After the impact they had and Google removing those malicious app, Boxer appeared in third applications repositories where there is no need to target so many countries due to the low probability of success.

Capabilities and malware functionalities can be used for other cybercriminals in order to inject the malicious payload in more applications and post them in regional

More Information

Apart from subscribing the victim to Premium-rate SMS numbers, Boxer tries to establish connection to two URL addresses. The first one has been blocked by the ESET products since September 2011 because it is related to another malware for mobile devices: J2ME/TrojanSMS.Konov.AB. When the site is visited, it is possible to see some fields for the user to fill in with his phone number and the subscription data that he supposedly will receive through a text message.

Information stored inside the malicious file will be used to subscribe the infected phone to Premium SMS numbers, but no information is being shown to notify users how to disable this service. If victims are not able to deactivate the service, their mobile number will still be charged with Premium SMS messages rates.

We have seen previous reports about Pay Per Install activities involving Android devices in which per every infected device cybercriminals got paid between 2 and 5 dollars. In the case of Boxer this Russian web page seems to be strongly related to the malicious activities executed by this threat.

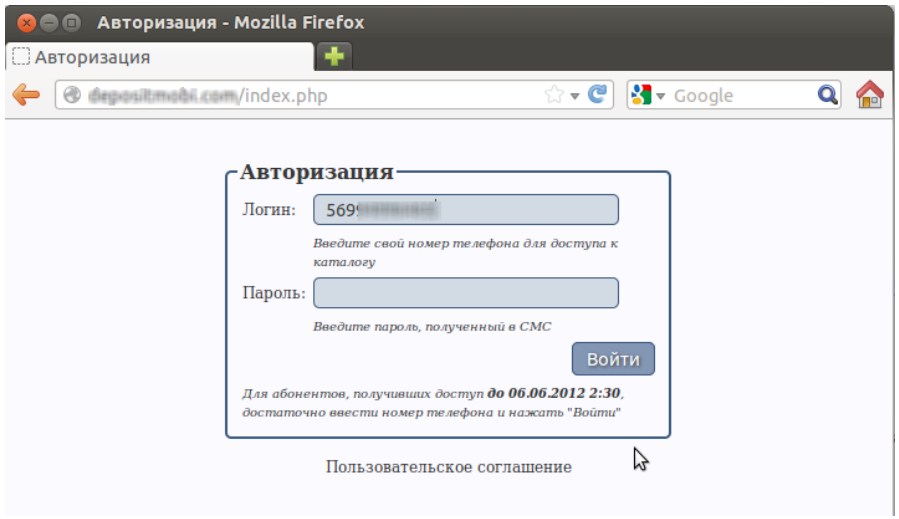


Image 8: SMS access pane

Afterwards, it tries to connect itself to another address. At the time of the analysis and of writing of this report, that website was offline; therefore, it was not possible to determine its content. On the other hand, the malware also includes a third website in the sms.cfg file, which is unavailable as well.

Conclusion

As time goes by, smartphones are getting more and more accessible and popular for users who, in many occasions, are unaware of the threats they may face if they do not adopt the necessary preventive and security measures. Although there are SMS Trojans for other platforms such as Symbian and for mobile devices compatible with Java Micro Edition, during 2012 it was possible to observe a rise of this kind of threats exclusively designed for Android, as is the case of Boxer.

In general, SMS Trojans affect a very limited number of countries. There are also other cases in which they are capable of working in several nations belonging to a particular continent, as in Europe. However, Boxer is able to transcend and surpass this barrier by contemplating within its malicious routine 63 countries belonging to regions in America, Asia, Africa, Europe and Oceania. Out of this list of countries, nine are Latin American. Consequently and taking into account the fact that this threat was found in several malicious applications through Google Play, Boxer is placed among the most important SMS Trojans of the last year, and is the first one trying to impact so many countries at the same time.

This also tends to confirm that cybercriminals are not only focusing their resources on the creation of increasingly complex malware for mobile devices, but that they are also starting to concentrate on how to expand their threats worldwide. It is likely that in the near future more malicious codes targeting Android will be detected and that, at the same time, they will be built to affect users as many regions as possible.

Finally, it is important to mention that simple actions like reading the license agreements and the permissions an application requests when it is being installed are crucial factors to reduce the malware infection risk. If you, or someone you know, has experienced unidentified mobile phone charges, we recommend checking whether they reference the numbers in the table shown earlier in this report. Also, check the device for malware because Boxer is the first case of this magnitude in the region and many users in the affected countries could already be infected with this potentially costly SMS Trojan.