EXPOSING ANDROID WHITE COLLAR CRIMINALS

Luis Corrons
Panda Security, Spain

Email luis.corrons@pandasecurity.com

ABSTRACT

Android has grown to become the most popular mobile operating system, and cybercriminals are taking advantage of this. One of the main ways for them to make money easily with the use of malware is through SMS premium services – using trojans to turn our mobile devices into slot machines and causing our monthly phone bills to skyrocket. Until now, most such trojans have managed to reach *Google Play* simply by posing as popular apps, such as *Angry Birds*, etc., but recently some new techniques have emerged, even reaching a point where the trojan indicates that it is going to subscribe you to a premium SMS service... and users happily agree.

In this paper, we will look at two different attack vectors used by two different Spanish criminal gangs. We will show what social engineering techniques are used to gain permission to activate the premium SMS services (to [try to] avoid being prosecuted) and provide an analysis of the two trojan families, uncovering the different techniques used to perform their actions.

Taking advantage of their main weakness (trying to do things legally), we will also unmask the real people behind these attacks.

INTRODUCTION

In February 2014, we came across a new *Android* malware attack. It was using a very popular monetization technique (premium SMS), but with a very different approach from all other premium SMS trojans known about until then. A few days later, another malware family was spotted using a similar approach, although the distribution vectors for the two new families were completely different.

1. ATTACK THROUGH GOOGLE PLAY

We found four different malicious apps that were spreading through *Google Play*. After finding the first app, we went to *Google Play* and found another three (all labelled as similar apps) that belonged to the same malware family, uploaded by two different developers. The main surprise was the number of downloads. Two of the apps had been published in December 2013 (they were less than two months old when we found them) and the other two were uploaded in January 2014 (they were less than one month old when we found them), and according to official figures from *Google Play*, in total they had been downloaded between 300,000 and 1,200,000 times(!).

Let's take a look at one of the apps, what it says it does, how it really works, and the tactic used to steal the victim's money.

This app poses as a step-by-step diet app. When you install the application, you open it and it will start loading, as shown in Figure 1.

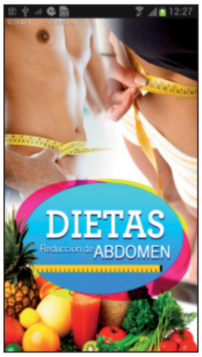


Figure 1: The application starts loading.

After it has finished loading, it will display the screen shown in Figure 2.

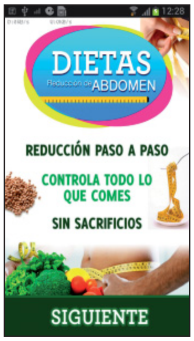
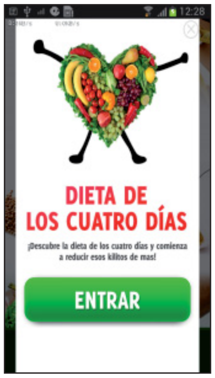


Figure 2: After the app has finished loading.

When you click on 'Siguiente' ('Next'), it will offer you access to one of the diets, as shown in Figure 3.

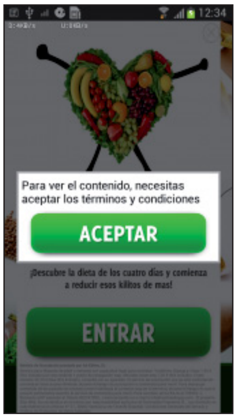


¡Descubre la dieta de los cuatro días y comienza a reducir esos kilitos de mas!

Figure 3: Access is offered to one of the diets.

It is hard to see the 'close window' cross in the upper-right corner of the screen – they want to make sure you click on 'Entrar' ('Enter'). When you click on it, a new message will be shown on top of the last screen, as shown in Figure 4.

Basically they are asking you to accept ('Aceptar') the terms of service in order to be able to see the content. This is the third time in a row the user has had to press a button – thus it's likely the user will just click on it without thinking. However, even if you want to be cautious, there is nothing special you need to pay attention to. Or is there? Take a look again at the picture. The



Para ver el contenido, necesitas aceptar los términos y condiciones

¡Descubre la dieta de los cuatro días y comienza a reducir esos kilitos de mas!

Figure 4: A new message is shown on top of the last screen.

previous screen is still behind the new pop-up, however there is a 'minor' difference: beneath the green 'Entrar' button there is a paragraph of small text – completely unreadable – that wasn't there before. Figure 5 shows the same image zoomed in a bit.

These are the terms of service you are accepting if you click on 'Aceptar'. They state that you will be subscribed to a service to obtain content for your mobile phone. Of course, it is all completely illegible in its original size.

Once you accept the terms of service and click on enter ('Entrar'), you will have access to the different diets advertised. But that's not all – there are a number of other things that the user won't see, which are happening in the background.

The first time the app is opened, it will create a GUID (Global Unique Identifier), and obtain the mobile operator's name:

```
ServicesLog.informLog(this, this.guid, “OPERADORA” +
localTelephonyManager.getSimOperatorName() + “ | “ +
localTelephonyManager.getSimOperator());
```

It will also obtain the mobile phone number, and all of this information will be uploaded to a log server where it is stored and used by the criminal gang behind the malware to track the different infection campaigns.

It is worth mentioning the method used to obtain the telephone number. The usual way for an app to do this is to take the number from the SIM card – there is a function in the operating system to do that – however, due to security issues, a number of providers do not store the number there. To get around this, the app 'steals' the number from one of the most popular mobile apps in the world: *WhatsApp*. When you open *WhatsApp* for the first time, you are asked for your mobile phone number. *WhatsApp* uses your phone number as part of your user account – and this is how the trojan app obtains the number:

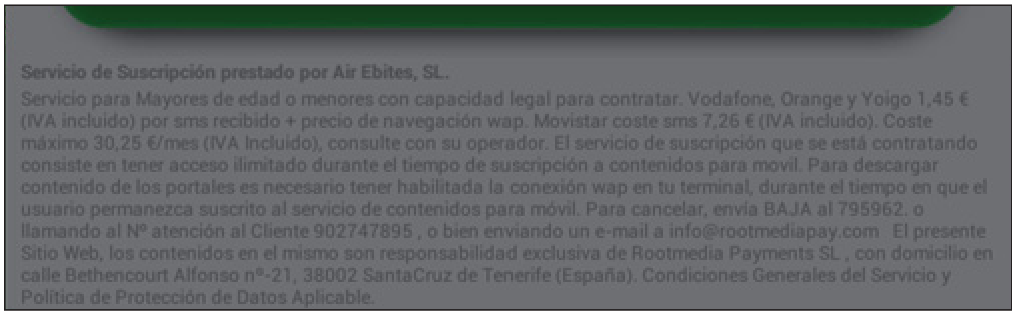
```
public static String getPhoneNumber(Context
paramContext)
{
   Account[] arrayOfAccount = AccountManager.
get(paramContext).getAccounts();
   String str1 = “”;
   int i = arrayOfAccount.length;
   for (int j = 0;; j++)
   {
      if (j >= i) {
         return str1;
      }
      Account localAccount = arrayOfAccount[j];
      String str2 = localAccount.name;
      String str3 = localAccount.type;
      Log.i(“milog”, “Accounts : “ + str2 + “, “ + str3);
      if (str3.equals(“com.whatsapp”)) {
         str1 = localAccount.name;
      }
```

The trojan app will download a configuration file which contains, among other things, the premium number that it will subscribe the phone to. The malware itself already has a hard-coded premium number, but the configuration file is used as a safeguard in case there is some change in the future. By doing this, the gang avoids having to release new versions of the malware just because there is a change in the premium SMS provider. The configuration file is downloaded not only the first time the app is opened, but also if the last time it was opened was more than three hours ago.

The app won't do anything else until the user presses the button accepting the terms and conditions. Once the user accepts them, it will register the phone number to activate the premium SMS subscription and install an SMS receiver in the phone. This receiver has a high priority, which means it will intercept an SMS before any other app, including the default operating system message controller.

This SMS receiver will wait for any message that:

- Comes from the short number that is hard coded in the trojan.
- Comes from the short number that is in the previously downloaded configuration file.



Servicio de Suscripción prestado por Air Ebites, SL.
Servicio para Mayores de edad o menores con capacidad legal para contratar. Vodafone, Orange y Yoigo 1,45 € (IVA incluido) por sms recibido + precio de navegación wap. Movistar coste sms 7,26 € (IVA incluido). Coste máximo 30,25 €/mes (IVA Incluido), consulte con su operador. El servicio de suscripción que se está contratando consiste en tener acceso ilimitado durante el tiempo de suscripción a contenidos para movil. Para descargar contenido de los portales es necesario tener habilitada la conexión wap en tu terminal, durante el tiempo en que el usuario permanezca suscrito al servicio de contenidos para móvil. Para cancelar, envía BAJA al 795962. o llamando al Nº atención al Cliente 902747895 , o bien enviando un e-mail a info@rootmediapay.com El presente Sitio Web, los contenidos en el mismo son responsabilidad exclusiva de Rootmedia Payments SL , con domicilio en calle Bethencourt Alfonso nº-21, 38002 SantaCruz de Tenerife (España). Condiciones Generales del Servicio y Política de Protección de Datos Aplicable.

Figure 5: Looking more closely at the small print.

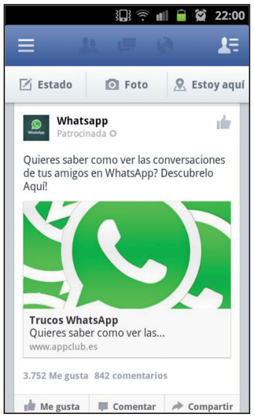
- Contains specific text in the SMS body.

Once the trojan has used a web service to activate the subscription, an SMS message containing a PIN code will be sent to the phone number that has been subscribed. The user is supposed to enter that PIN code into the website of the premium SMS service in order to confirm that he wants to be subscribed to it. However, the trojan takes care of all of this for him.

It will parse the SMS to get the PIN code and enter it into the website in order to activate the service. Straight after that, it will perform an abortBroadcast(). The user will never see the SMS, which won't appear on his mobile phone. The trojan uses the same technique to intercept all messages received from the premium SMS service, and the user will only recognize the 'issue' when his monthly bill arrives. Any other SMS messages will reach the phone without problems.

2. ATTACK THROUGH FACEBOOK

The other attack we are going to look at does not use *Google Play* to spread, but uses another very successful approach: *Facebook* ads are used to attract victims and trick them into installing the malicious apps. As shown in Figure 6, when you access *Facebook* from your *Android* mobile device, you will see a 'suggested post' (*Facebook*'s subtle euphemism for an advertisement), which advertises tools for *WhatsApp*.

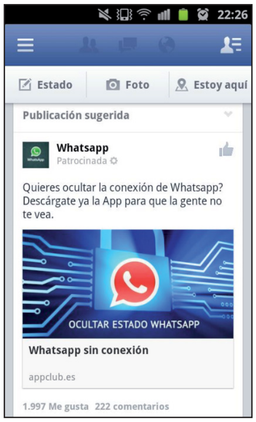


Quieres saber como ver las conversaciones de tus amigos en WhatsApp? Descubrelo Aquí!

Trucos WhatsApp
Quieres saber como ver las...
www.appclub.es

3.752 Me gusta 842 comentarios

Figure 6: Facebook 'suggested post' advertising a tool for WhatsApp that allows the user to spy on their contacts' conversations.



Quieres ocultar la conexión de Whatsapp? Descárgate ya la App para que la gente no te vea.

Whatsapp sin conexión
appclub.es

1.997 Me gusta 222 comentarios

Figure 7: Another 'suggested post', advertising an app that lets you hide your WhatsApp status.

As you can see, not only do the criminal gangs use the most popular platforms to attract users, they also appeal to the users' curiosity by offering them the chance to spy on their contacts' conversations. You can see how successful this is by looking at the number of 'Likes' (3,725) and comments (842) it has. Yet this is not the only lure they've used. Figure 7 shows another suggested post, advertising an app that lets you hide your *WhatsApp* status.

Facebook offers targeted advertising for advertisers: you can specify which type of users you want to see your ads, where they appear (e.g. in the right-hand column), whether they appear as suggested posts, etc. In this case, it seems that the ad is only shown to Spanish *Facebook* users who are accessing the social network from an *Android* mobile device – because these are the types of victims that the cyber-crooks behind this scam are after. In fact, all of the screenshots in this paper are taken from a Spanish *Facebook* account via an *Android* mobile device. I also tried using the same account from a PC, an *iPad* and an *iPhone*, and in none of these cases were the ads displayed.

If you click on the image shown in any of the ads, you'll be redirected, as shown in Figure 8.

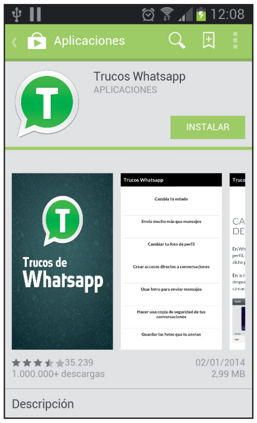

12:08
Aplicaciones
Trucos Whatsapp
APLICACIONES
INSTALAR
Trucos de Whatsapp
Trucos Whatsapp
Cambia tu estado
Envía mucho más que mensajes
Cambiar tu foto de perfil
Crear accesos directos a conversaciones
Usar Intro para enviar mensajes
Hacer una copia de seguridad de tus conversaciones
Guardar las fotos que te envían
35.239
1.000.000+ descargas
02/01/2014
2,99 MB
Descripción

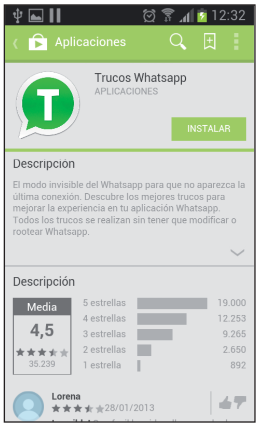
Figure 8: If you click on the image in any of the ads, you'll be redirected here.

As any *Android* user will be able to tell, this is *Google Play* – specifically, a page for an app. It has the option to install it, and shows over one million downloads and a 3.5-star user rating (out of 5). If you scroll down the screen you can see numerous positive comments, and the votes of over 35,000 users who have rated it (see Figure 9).

However, a keen eye will note that the numbers do not all add up:

- The app has a score of 4.5, yet the number of stars is 3.5.
- You can see that the score is calculated on the basis of the votes from 35,239 users. Yet, if you add up all of the votes that appear on the right, the total is 44,060 votes.

How can this be happening in *Google Play*? Well, it's happening because it is *not Google Play*. In fact, it is a web page designed to look like *Google Play*, so that users think they are visiting a



12:32

Aplicaciones

Trucos Whatsapp
APLICACIONES

INSTALAR

Descripción

El modo invisible del Whatsapp para que no aparezca la última conexión. Descubre los mejores trucos para mejorar la experiencia en tu aplicación Whatsapp. Todos los trucos se realizan sin tener que modificar o rootear Whatsapp.

Descripción

Media		
4,5	5 estrellas	19.000
★★★★☆	4 estrellas	12.253
35.239	3 estrellas	9.265
	2 estrellas	2.650
	1 estrella	892

Lorena
★★★★☆ 28/01/2013

Figure 9: You can see numerous positive comments, and the votes of over 35,000 users who have rated it.

trusted site. As you can see in the screenshots, the browser address bar is hidden at all times.

If you click on the 'Install' button, a file called 'whatsapp.apk' is downloaded and the user has to install it manually. When it runs, the app displays the screen shown in Figure 10.

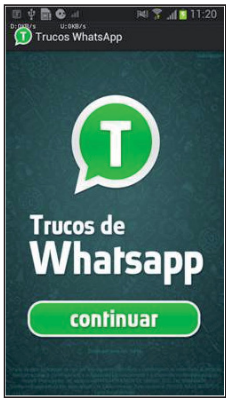


Figure 10: Screen shown when the app runs.

If you look carefully, you can see at the bottom of the screen, beneath the 'Continue' ('continuar') button, there is a barely legible chunk of text. Figure 11 shows a zoomed in image.

In English, the text reads:

> 'Cost per SMS received €1.45
>
> 'The use of this application is subject to the following terms and conditions: On subscribing to the service you will have access to periodically updated content and multimedia content for your phone. The service provider is MICAMOSA MON DE SERVEI. SLU. Tel 900844456. contacto@appclub.es. Cost of the subscription service €1.45 per minute. Subscription to 797025. UNSUBSCRIBE to 797025 to unsubscribe.'

The trojan starts by going through the list of registered user accounts, searching for the user's *WhatsApp* account in order to obtain the mobile phone number (in exactly the same way as the other malware family we have analysed). If *WhatsApp* is not installed, or it fails to get the phone number, it uses an API to access the system services in order to get the information.

It then randomly selects one of the following short numbers:

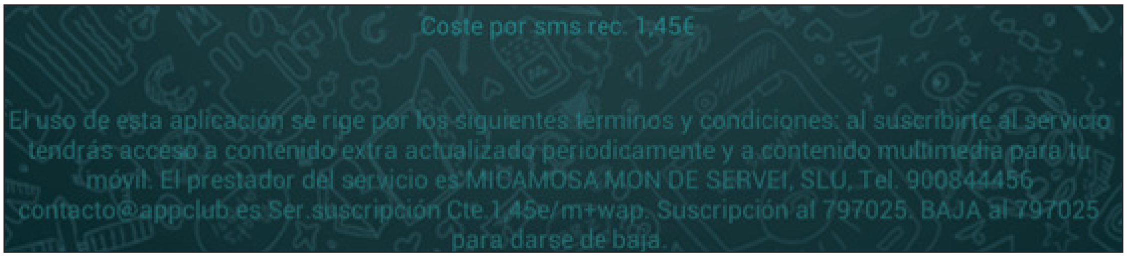
- 797024
- 795964
- 797025

This is to select which of the three premium SMS services it will subscribe the user to. The text of the service terms and conditions (the illegible text that appears when you open the application, as shown in Figure 11) will vary depending on the number that has been selected. Depending on the number selected, the text will show the names of either one of the following two companies:

- LINEAS DE RED INTELIGENTE S.L
- MICAMOSA MON DE SERVEI, SLU

It then installs an SMS receiver to manage inbound text messages. What is interesting is the technique used to prevent users from realizing they have received text messages from any of the three numbers mentioned above. If everything goes according to plan, the SMS receiver will abort the communication process and the user will never see those SMS messages, as in the previous case. However, *Google* made some changes in *Android KitKat* (4.4), which no longer allows the use of the abortBroadcast() function. The developers of this app are aware of this, and decided to solve the issue using a witty technique to try to hide the messages: the trojan switches the device into silent mode for a couple of seconds, so the user won't hear the notification sound when an SMS arrives, and then it marks the message in the inbox as read.

The app has an SMS counter, so when the first message arrives from the premium-rate SMS service, it reads it to obtain the necessary PIN code, and registers on the corresponding website to activate the premium-rate service. Another interesting feature we've come across is that it also hides messages from the



Coste por sms rec. 1,45€

El uso de esta aplicación se rige por los siguientes términos y condiciones: al suscribirte al servicio tendrás acceso a contenido extra actualizado periodicamente y a contenido multimedia para tu móvil. El prestador del servicio es MICAMOSA MON DE SERVEI, SLU, Tel. 900844456 contacto@appclub.es Ser.suscripción Cte.1,45e/m+wap. Suscripción al 797025. BAJA al 797025 para darse de baja.

Figure 11: Barely legible text.

number 22365. It turns out that *Orange* sends a warning SMS to users who have activated this kind of premium service, and that warning message comes from the number 22365. The trojan deletes messages from this number so the user won't know he has been subscribed to the premium service.

Going back to the 'visible' part of the app, after clicking 'Continue' you will see some supposed 'tricks' for *WhatsApp*.

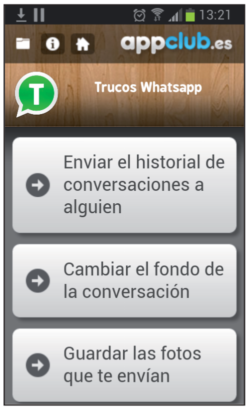

13:21
appclub.es
Trucos Whatsapp
Enviar el historial de conversaciones a alguien
Cambiar el fondo de la conversación
Guardar las fotos que te envían

Figure 12: 'Tricks' for WhatsApp.

As you can see in the complete list, there is absolutely nothing special about these, and they can't reasonably be referred to as 'tricks':

- How to tell if you've been blocked
- How to block a contact
- Change your status
- Send much more than just messages
- Change your profile image
- Create shortcuts to chats
- Use Enter to send messages
- Make a backup of your chats
- Save the pictures you've been sent
- Change the chat background
- Send someone the chat history.

In fact all of these 'tricks' are readily available from the page that hosts the app, and without having to subscribe to a premium-rate service.

If you go to the main website, you can see that not only are the criminals using *WhatsApp* as bait, but also many other popular apps and topics (see Figure 13).

The method of operation in each case is identical: you are taken to an imitation of *Google Play*, where you can download the relevant app, which has the same hidden functions as described above (see Figure 14).

As shown in Figure 15, you look closely, you can see that some of the data from the first case we described has been re-used (user rating, number of downloads, and the number of votes).

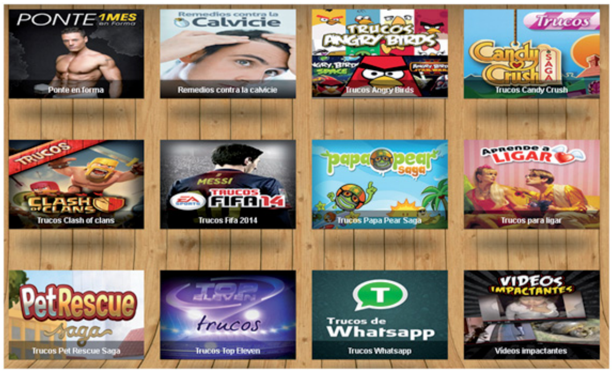


Figure 13: They are not only using WhatsApp as bait, but also many other popular apps and topics.

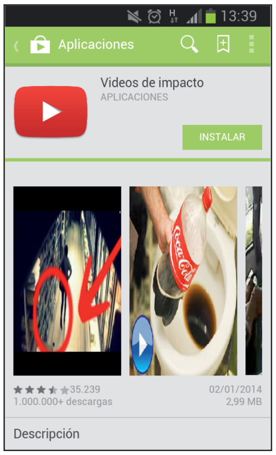
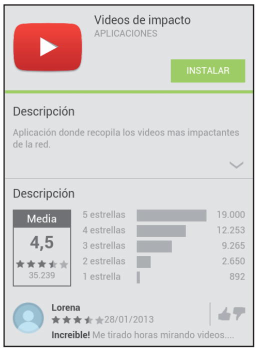


Figure 14: An imitation of Google Play, where you can download the app.



Aplicación donde recopila los videos mas impactantes de la red.

Increible! Me tirado horas mirando videos....

Figure 15: Some of the data is reused.

During the presentation at VB2014, I will describe the legal issues that law enforcement officers are currently facing in the fight against these criminal gangs. I will also use information provided by both malware families to identify who is behind each attack.