Troyano SMS Boxer

Primer amenaza de este tipo para países de Latinoamérica

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autor:
André Goujon
Especialista de Awareness & Research

Pablo Ramos
Security Researcher

Fecha:
Octubre de 2012

Índice

Introducción

En el último tiempo, se ha venido observando un aumento en la cantidad de familias de códigos maliciosos diseñados para plataformas móviles, especialmente para el sistema operativo Android. Luego de varias consultas de los usuarios en la región, el equipo del Laboratorio de Investigación de ESET Latinoamérica analizó el troyano *Boxer* para dispositivos que utilizan esta plataforma, identificando que esta amenaza (detectada por ESET Mobile Security como *Android/TrojanSMS.Boxer.AA)* afecta a **nueve países de América Latina**. Este es un hecho del cual no se tenían registros previos, ya que no se había encontrado un troyano SMS que afectara a usuarios de la región.

Luego del análisis de la muestra y habiendo comprendido su funcionamiento y los comandos que utiliza para enviar mensajes SMS Premium, se pudo también identificar usuarios en Internet consultando en foros por cobros "misteriosos" en sus saldos o cuentas. En todos estos casos, el número Premium por el cual presentaban este inconveniente estaba identificado en el análisis de *Boxer*.

Aunque en ninguna de estas situaciones se pudo determinar de forma concluyente que se trataba de una infección provocada por este troyano móvil, los usuarios indicaban recurrentemente no haber enviado los mensajes y en muchos casos, operadores de soporte de compañías de telefonía móvil respondían a los afectados que "la única forma de suscripción [a dichos mensajes SMS Premium] es manual".

En el presente informe se explica qué es este tipo de amenazas, las características técnicas de esta código malicioso en particular, y cómo el malware identificado como *Android/TrojanSMS.Boxer.AA* se transformó en el primer troyanos SMS para Android conocido en poder afectar también a usuarios de países latinoamericanos.

Troyanos SMS

Los troyanos SMS son una categoría de códigos maliciosos para teléfonos móviles cuyo objetivo principal es suscribir a la víctima a números de mensajería Premium. Como este tipo de servicios suelen informarle al usuario que ha sido suscrito, algunos troyanos de esta categoría filtran los SMS provenientes de dichos números con el fin que el usuario no se percate de la infección. De este modo, aquellos mensajes de otros usuarios o servicios sí aparecen, pero los relacionados al número Premium no. Esto representa un grave problema financiero para el usuario, quien de no consultar su saldo o estado de cuenta a tiempo, podría incurrir en costosos cargos.

Por otro lado, los troyanos SMS son una de las categorías de códigos maliciosos para teléfonos móviles más antigua, cuyas primeras apariciones datan de 2004. Actualmente, existen algunos capaces de funcionar en varias plataformas al estar desarrollados en Java Micro Edition (Java ME). Otros, en cambio, se ejecutan en sistemas operativos específicos como el caso de *Boxer* en Android.

En la siguiente página, se presenta un esquema del funcionamiento de los troyanos SMS:

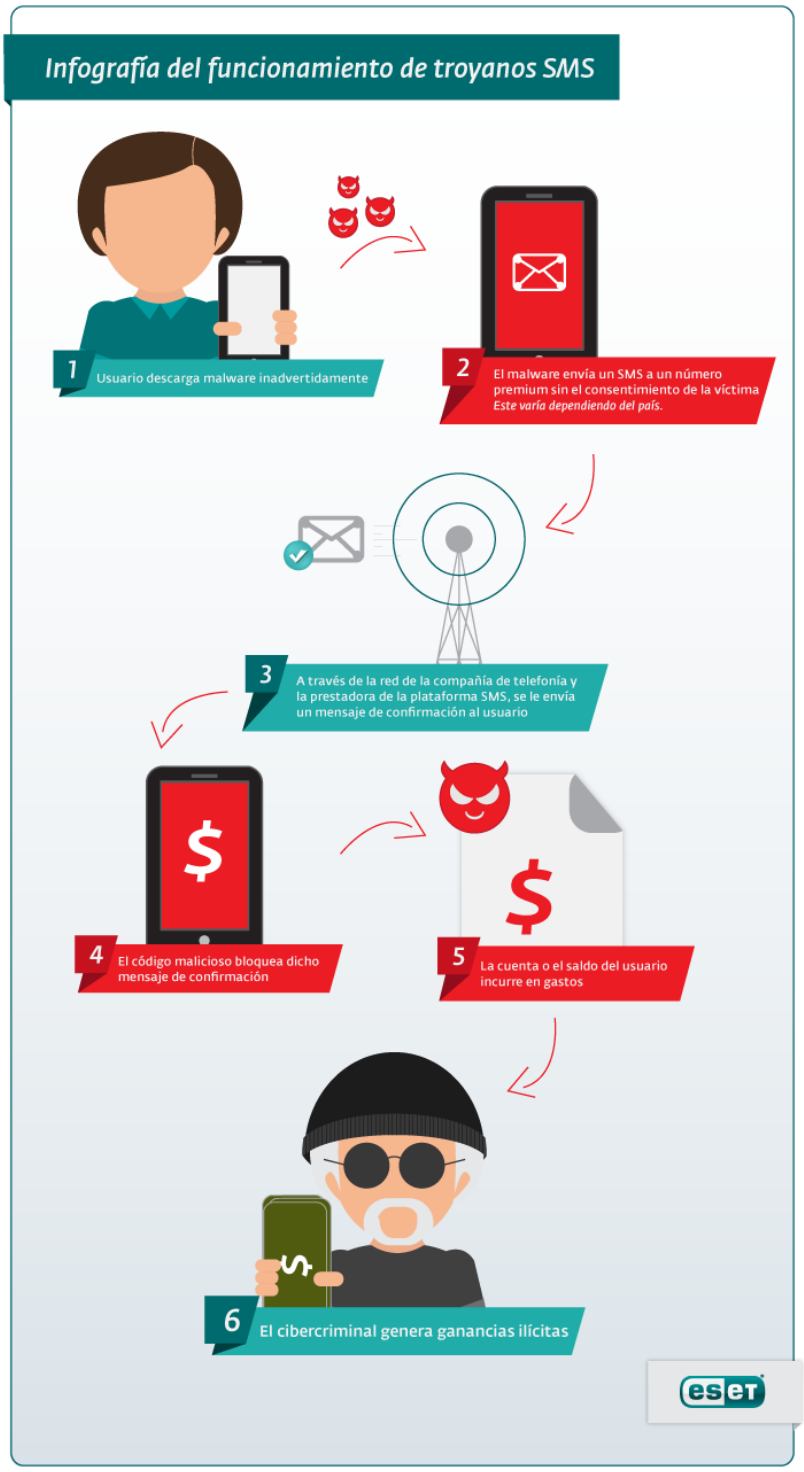

Imagen 1 Funcionamiento de un troyano SMS

Como se puede observar, los usuarios comienzan a incurrir en gastos y en consecuencia, el ataque se transforma en una ganancia para el cibercriminal.

¿Por qué Android?

En la actualidad, los teléfonos inteligentes se han transformado en una herramienta cada vez más utilizada por las personas, quienes a diario suelen realizar una amplia gama de tareas que abarcan leer y escribir correos electrónicos, revisar redes sociales, estados bancarios, compra de productos, pagos de cuentas, y en general, cualquier servicio web que necesite de un nombre de usuario y contraseña para funcionar. Frente a este escenario de interconectividad y almacenamiento de información confidencial, los cibercriminales invierten cada vez más recursos en crear malware para este tipo de dispositivos.

Según la consultora Gartner, Android representa en la actualidad el 64.1%[1] del mercado de sistemas operativos móvil, por lo tanto, resulta atractivo para los ciberdelincuentes crear amenazas que funcionen bajo este sistema operativo. De esta manera, se aseguran de poder llegar a la mayor cantidad de víctimas posibles y así poder maximizar sus ganancias ilícitas.

El código malicioso

Por lo general, los troyanos SMS tienen un rango de acción limitado, es decir, solo son capaces de afectar determinados países porque en la mayoría de los casos, estos números Premium varían de acuerdo a cada operador y nación. Sin embargo, *Boxer* es capaz de afectar un total de 63 países dentro de los cuales se encuentran nueve latinoamericanos: **Argentina, Brasil, Chile, Perú, Panamá, Nicaragua, Honduras, Guatemala y México**. Esto no sólo lo convierte en un troyano SMS capaz de afectar usuarios de Latinoamérica, sino que también se trata de una amenaza con un amplio potencial de propagación y gran rango de acción.

[1] Fuente: Ventas de smartphones a usuarios finales por sistemas operativos 2Q12, Gartner.
Disponible en http://www.gartner.com/it/page.jsp?id=2120015.

Infección y propagación

Boxer, al ser un troyano, no posee capacidad de propagarse por sí mismo, por lo tanto son los responsables de este tipo de amenazas quienes deben subirlas a algún sitio web o repositorio. Luego de realizar esto, emplean técnicas de Ingeniería Social para manipular a la potencial víctima y provocar que ésta ejecute el código malicioso.

En el caso de *Boxer*, se encontraron 22 aplicaciones infectadas con esta amenaza en Google Play[2] (anteriormente Android Market). Títulos de juegos como "Sim City Deluxe Free", "Need for Speed Shift Free", "Assassin Creed", y algunos accesorios para "Angry Birds", fueron utilizados para engañar a los usuarios y provocar que resulten infectados con este malware. Aunque dichas aplicaciones troyanizadas fueron removidas por Google hace bastante tiempo, los repositorios o tiendas no oficiales siguen siendo los principales vectores de propagación de códigos maliciosos para Android, por lo tanto, no sería extraño que este troyano siga consiguiendo nuevas víctimas a través de este tipo de sitios.

Para efectos de este análisis y el desarrollo del presente documento, se ha utilizado una muestra identificada como *Android/TrojanSMS.Boxer.AA* contenida en una aplicación denominada "Urban Fatburner", una aplicación que aparentement sirve para acompañar los ejercicios físicos del usuario. Si el usuario descarga y luego procede a instalar el programa malicioso, se le solicitan los siguientes permisos para continuar con el proceso:

- Enviar mensajes de texto
- Recibir mensajes de texto
- Realizar llamadas de teléfono
- Recibir PUSH de WAP
- Acceso a Internet

Si el usuario presta atención a todos los permisos que solicita dicha aplicación, podrá percatarse que existen algunos aspectos sospechosos puesto que un juego o aplicación para "quemar grasas", no tendría por qué necesitar enviar o recibir SMS para funcionar. Luego, se le muestra un contrato de licencia en donde se especifica que podría ser suscrito a números SMS Premium, sin embargo, se omiten ciertos aspectos como el hecho que se le seguirán enviando mensajes a la persona con un costo asociado. Asimismo, los creadores de este tipo de

[2] Más información disponible en la publicación Limpieza en el Android Market del Blog de ESET Latinoamérica.

amenazas suelen aprovecharse del hecho que casi ningún usuario se detiene a leer las condiciones de un contrato de licencia aunque las mismas sean desfavorables o sospechosas.

A continuación, se muestran dos capturas de pantalla de sistema Android (versión 2.3) en el proceso de infección. La primera (1) corresponde a la advertencia que vería un usuario con tan solo ejecutar *Boxer*. La segunda imagen (2) muestra parte del contrato de licencia del troyano SMS. Esta información es desplegada únicamente si el usuario presiona sobre el botón "Rules".

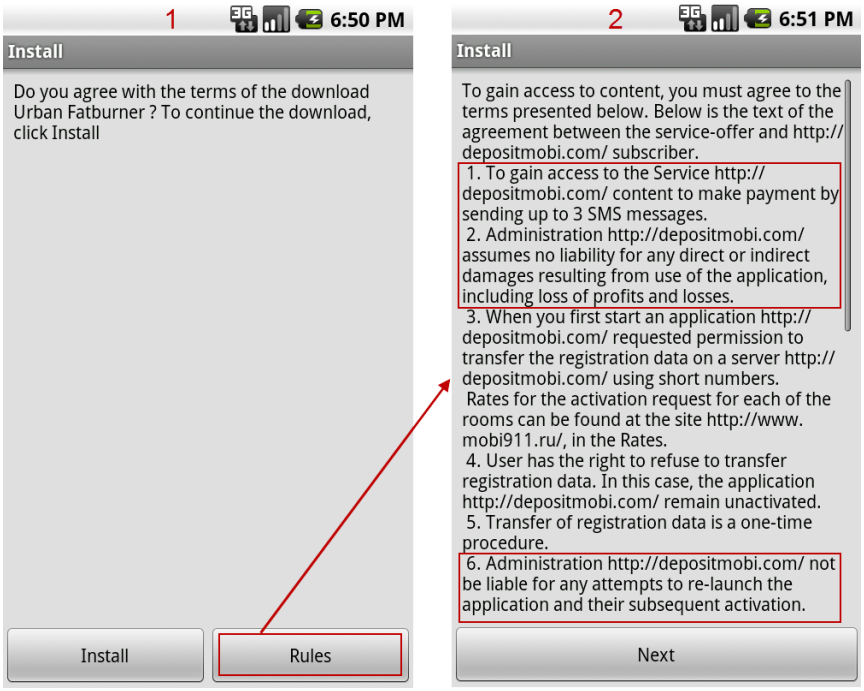

Imagen 2 Supuesto contrato de licencia

Si la persona es precavida y lee este contrato de licencia, podría notar ciertas cláusulas sospechosas y abusivas como el desligamiento de responsabilidad por parte del proveedor si las finanzas del usuario se ven afectadas de algún modo directo o indirecto (punto 2). Además no se advierte sobre la existencia de los números Premium a los cuales la aplicación contacta y el costo asociado a estos.

Asimismo, en el punto 1 es posible observar que para acceder al contenido, se deben enviar hasta tres mensajes de texto. Sin embargo, en el punto 6 se menciona que si la aplicación es ejecutada nuevamente, podría volver a reactivarse. Implícitamente significa que el usuario deberá volver a pagar por tres mensajes Premium SMS cada vez que la amenaza es abierta. Además, una aplicación legítima en circunstancias normales de uso no tendría porqué ser activada en más de una ocasión.

Payload: suscripción a números SMS Premium

Si el contrato de licencia es aceptado por el usuario, el troyano procede a obtener los códigos numéricos de identificación por país y operador MCC (*Mobile Country Code*) y MNC (*Mobile Network Code*). De este modo, determina el país del smartphone en cuestión así como la compañía telefónica a la cual pertenece. Posteriormente procede a enviar SMS a números Premium de acuerdo a la información recopilada anteriormente.

El análisis del troyano permite identificar sus secciones de código en dónde se almacena el listado de códigos de MCC que luego es utilizado para identificar cada uno de los países:

```
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";
```

Imagen 3 Listado parcial de códigos MCC contenidos en *Boxer*

En total se cuentan 63 códigos diferentes de MCC para países alrededor del mundo. Esta información es utilizada por *Boxer* para decidir a qué número de teléfono enviar un SMS de suscripción al servicio de mensajes Premium según el país del usuario afectado. Para lograr identificar el país, este Troyano SMS lee la información del dispositivo y obtiene sendos códigos del sistema para luego compararlos y configurar a qué número comunicarse:

```
else
{
  localObject3 = new ArrayList();
  localObject1 = new Pair("22588", "7665895");
  ((ArrayList)localObject3).add(localObject1);
  localObject2 = this.activationSchemes;
  localObject1 = CURRENT_ACTIVATION_SCHEME;
  localObject3 = new ActivationScheme(1, (ArrayList)localObject3);
  ((HashMap)localObject2).put(localObject1, localObject3);
}
```

Imagen 4 - Identificación y configuración del mensaje para Argentina

Una vez identificado el país, continúa la ejecución de *Boxer* y se procede a activar la reciente instalación en el dispositivo del usuario, logrando así enviar una serie de mensajes de texto al

número Premium con toda la información necesaria para que los cibercriminales obtengan un beneficio económico.

Este accionar se ejecuta cuando se invoca al método *activate()* que será el encargado de llevar a cuenta el estado de todos los mensajes de texto enviados a los número pagos, evitando llamar la atención del usuario y manteniendo oculta a la aplicación maliciosa. En la siguiente imagen se detalla la información obtenida luego de analizar minuciosamente el código:

```
private void activate()
{
  registerReceiver(new BroadcastReceiver()
  {
    public void onReceive(Context paramContext, Intent paramIntent)
    {
      switch (getResultCode())
      {
      default:
        Main.this.dialog.dismiss();
        Toast.makeText(Main.this.getBaseContext(), 2131099655, 0);
        break;
      case -1:
        Object localObject = Main.this;
        ((Main)localObject).sendedSmsCounter = (1 + ((Main)localObject).sendedSmsCounter);
        SharedPreferences localSharedPreferences = Main.this.getSharedPreferences("Activator_preferences", 0);
        localObject = localSharedPreferences.edit();
        ((SharedPreferences.Editor)localObject).putInt("sendedSMS", Main.this.sendedSmsCounter);
        ((SharedPreferences.Editor)localObject).commit();
        if (((ActivationScheme)Main.this.activationSchemes.get(Main.CURRENT_ACTIVATION_SCHEME)).smsQuantity != Main.this.sendedSmsCounter)
          break;
        localObject = localSharedPreferences.edit();
        ((SharedPreferences.Editor)localObject).putString("appIsActivated", Main.this.url);
        ((SharedPreferences.Editor)localObject).commit();
        Main.this.showLink(true);
      }
    }
  }
```

Imagen 5- Envío de mensajes a números Premium

Afectados en Latinoamérica

Como se indicó anteriormente, el análisis de la amenaza identificó que de los 63 países afectados por esta amenaza, 9 de ellos corresponden a Latinoamérica tal como se puede observar en el siguiente mapa:

Imagen 6 Nueve países latinoamericanos afectados por Boxer

A continuación se muestra una tabla con los números Premium y códigos MCC correspondientes a los nueve países de América Latina que afecta *Boxer*:

Tabla 1 - Lista de MCC y número Premium por país

País	N° SMS Premium	MCC
Argentina	22588	722
Brasil	44844	724
Chile	3210	730
Perú	2447	716
Panamá	1255	714
Nicaragua	1255	710
Honduras	1255	708
Guatemala	1255	704
México	37777	334

Durante la investigación, el equipo de ESET ha identificado en diversos foros en Internet usuarios reclamando gastos no identificados en sus cuentas y, como se puede visualizar a continuación, los números indicados son los mismos que utiliza *Boxer*.

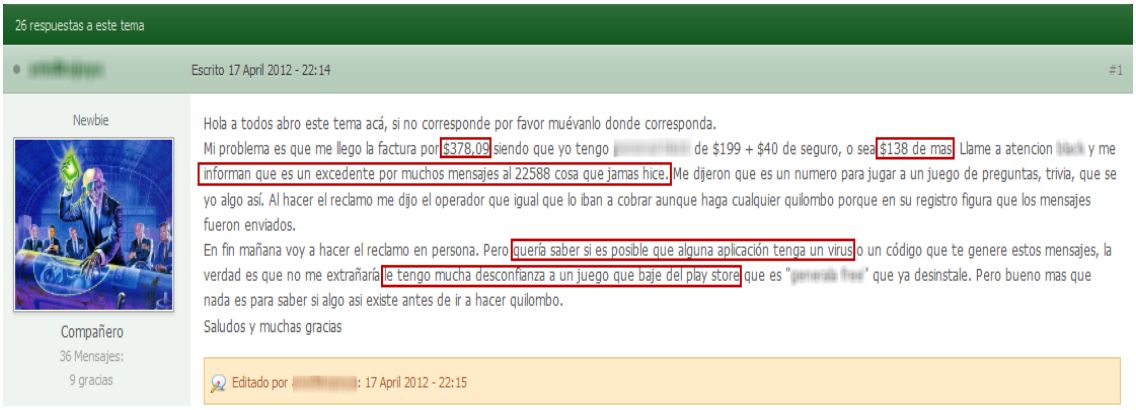

Imagen 7 Usuario consultando en foro por cobros "misteriosos"

Como puede apreciarse en la captura anterior, una persona pregunta sobre un excedente de $138 ARS que registró su cuenta. Al llamar al servicio de atención a clientes de su empresa telefónica, le dijeron que esos cobros correspondían al envío de mensajes Premium al número 22588. Según relata el usuario, nunca envió premeditadamente dichos SMS. Asimismo, plantea la posibilidad de estar infectado por un código malicioso al sospechar de una aplicación que habría descargado de Google Play.

De acuerdo al análisis de *Boxer* realizado por ESET, el número SMS Premium 22588 corresponde precisamente al que utiliza esta amenaza para afectar a usuarios pertenecientes a Argentina. Otro caso similar es el que se puede observar a continuación:

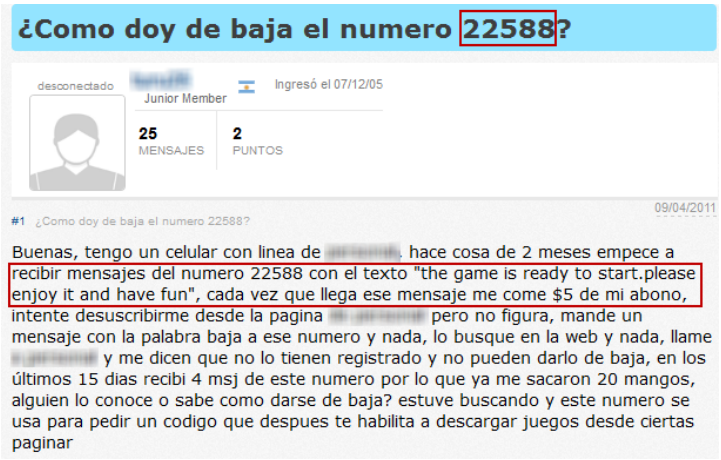

Imagen 8 Otro usuario preguntando por el número Premium "22588"

En esta ocasión, el usuario reclama por el mismo número de mensajería Premium 22588. Además explica que ha intentado darse de baja a través de algunos mecanismos como el envío de un mensaje con la palabra "baja", y que sin embargo no ha tenido éxito. Si se observan ambos casos, se puede notar que en los dos existe un perjuicio económico para el usuario. En el primero ha sido de $138 ARS (casi 30 USD) y en el segundo, de $20 ARS (4 USD aproximadamente).

Más información

Además de suscribir a la víctima a números SMS Premium, *Boxer* intenta conectarse a dos direcciones URL. La primera es bloqueada por los productos de ESET desde septiembre de 2011 por estar relacionada con otro código malicioso para dispositivos móviles, *J2ME/TrojanSMS.Konov.AB*. Al visitar dicho sitio, se pueden observar algunos campos en donde se le solicita al usuario ingresar su número telefónico y los datos de suscripción que supuestamente recibe a través de un mensaje de texto.

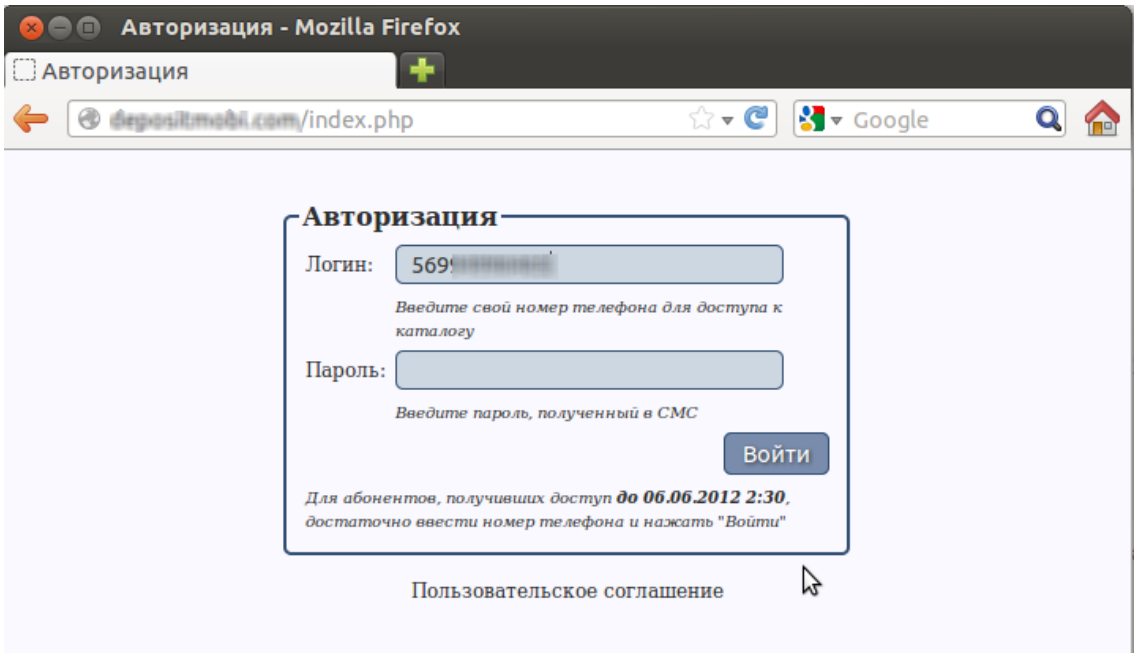

Imagen 9 - Panel de acceso de SMS

Posteriormente, intenta conectarse a otra dirección. Al momento del análisis y escritura de este informe, dicho sitio se encuentra fuera de línea, por lo tanto no se pudo determinar el contenido del mismo. Por otro lado, el código malicioso también incluye un tercer sitio dentro del archivo sms.cfg que tampoco está disponible.

Conclusión

A medida que pasa el tiempo, los smartphones se hacen cada vez más asequibles y populares dentro de los usuarios quienes, en muchas ocasiones, desconocen las amenazas a las cuales pueden verse enfrentados si no adoptan las medidas preventivas y de seguridad necesarias. Aunque existen troyanos SMS para otras plataformas como Symbian y dispositivos móviles compatibles con Java Micro Edition, durante 2012 se ha observado un aumento de esta clase de amenazas diseñadas exclusivamente para Android, como es el caso de *Boxer*.

Por lo general, los troyanos SMS afectan una cantidad muy limitada de países. También existen otros casos donde son capaces de funcionar en varias naciones pertenecientes a un continente en particular, como por ejemplo Europa. Sin embargo, lo novedoso de *Boxer* es su capacidad de trascender y superar esta barrera al contemplar dentro de su rutina maliciosa **63 países** pertenecientes a regiones como América, Asia y Europa. De esta lista de países, **nueve son de Latinoamérica**. Por lo mismo, y considerando que esta amenaza fue encontrada en varias aplicaciones maliciosas a través de Google Play, *Boxer* se ubica entre los troyanos SMS más importantes del último año, y el primero con tamaña relevancia para la región latinoamericana.

Esto también permite confirmar que los ciberdelincuentes no sólo están concentrando sus recursos en la creación de malware cada vez más complejo para dispositivos móviles, sino que también están comenzando a enfocarse en usuarios de América Latina. Es probable que un futuro cercano se detecten más códigos maliciosos diseñados para Android y que a la vez, estén diseñados para afectar a usuarios de la región.

Finalmente, es importante mencionar que acciones tan simples como la lectura de los contratos de licencia y los permisos que una aplicación solicita al momento de instalación, permiten disminuir el riesgo de infección producto de un código malicioso. Si el lector del presente artículo ha tenido incidentes de gastos no identificados en sus consumos móviles, se recomienda chequear si los números pertenecen a los listados antes expuestos y explorar el dispositivo en busca de malware, ya que Boxer es el primer caso de esta magnitud en la región, por lo que muchos usuarios en los países afectados pueden estar infectados sin saberlo.