Google Play Protect

Android anti-RE choosing a different path

Łukasz Siewierski, Kaspersky SAS 2018

Three malware families - three different approaches

1. Failing based on the execution environment
2. Policy compliance based on the C&C response
3. Taking it one step further

Failing based on the execution environment

A case of an unusual exception

Exception below was thrown in the native code.

SIGSEGV is not something that should usually happen.

```
pid: 4002, tid: 4002  >>> com.tempus.spatium <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 00000000
r0 00000000  r1 00000007  r2 0000f2c0  r3 496d4e68
r4 0000f2c0  r5 00000001  r6 00000000  r7 00000001
r8 be9516a0  r9 44b96d28  10 49545682  fp be9516b4
ip 0000000f  sp be9515e8  lr 4080f85b  pc 49618b60  cpsr 60000030
[...]
        #00  pc 0000fb60  /data/data/com.tempus.spatium/lib/libStoras.so
        #01  pc 0000fc76  /data/data/com.tempus.spatium/lib/libStoras.so (Java_com_tempus_introitum_bealach_glaonna)
```

A case of an unusual exception

Exception below was thrown in the native code.

SIGSEGV is not something that should usually happen.

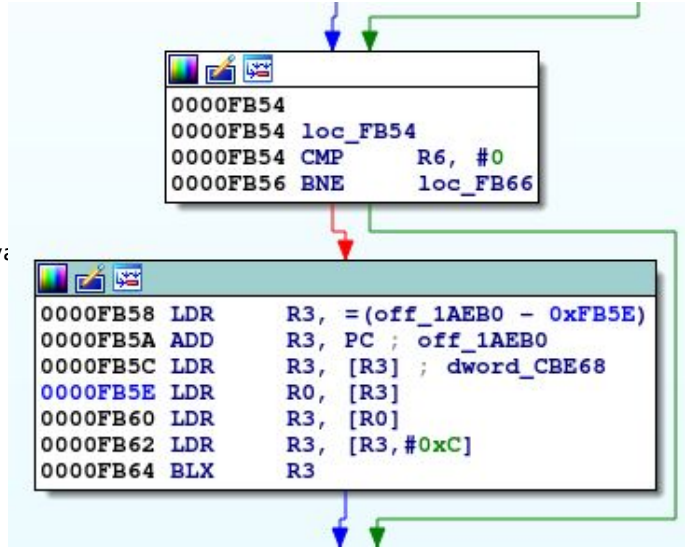
```
pid: 4002, tid: 4002  >>> com.tempus.spatium <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 00000000
r0 00000000  r1 00000007  r2 0000f2c0  r3 496d4e68
r4 0000f2c0  r5 00000001  r6 00000000  r7 00000001
r8 be9516a0  r9 44b96d28  10 49545682  fp be9516b4
ip 0000000f  sp be9515e8  lr 4080f85b  pc 49618b60  cpsr 60000030
[...]
        #00  pc 0000fb60  /data/data/com.tempus.spatium/lib/libStoras.so
        #01  pc 0000fc76  /data/data/com.tempus.spatium/lib/libStoras.so (Java_com_tempus_introitum_bealach_glaonna)
```

A case of an unusual exception

Exception below was thrown in the native code.

SIGSEGV is not something that should usually happen.

```
pid: 4002, tid: 4002  >>> com.tempus.spatium <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 00000000
r0 00000000  r1 00000007  r2 0000f2c0  r3 496d4e68
r4 0000f2c0  r5 00000001  r6 00000000  r7 00000001
r8 be9516a0  r9 44b96d28  10 49545682  fp be9516b4
ip 0000000f  sp be9515e8  lr 4080f85b  pc 49618b60  cpsr 60000030
[...]
        #00  pc 0000fb60  /data/data/com.tempus.spatium/lib/libStoras.so
        #01  pc 0000fc76  /data/data/com.tempus.spatium/lib/libStoras.so (Java
```



Policy compliance based on the network

Google Play policy regarding monitoring apps

Apps that monitor or track a user's behavior on a device must comply with these requirements:

(...)

- *Apps and app listings on Google Play must not provide any means to activate or access functionality that violate these terms, such as linking to a non-compliant APK hosted outside Google Play.*

- *Present users with a persistent notification and unique icon that clearly identifies the app.*

(...)

A case of a missing “u”

App makes a GET request to

`http://www.website.ro/app/test_net.php`

This is the response:

```
{"net":"ok","test":"uuu"}
```

A case of a missing “u”

```
android.util.Log.d("check user", response);
if (!json_response.getString("net").equals("ok")) {
  this.step1 = 0;
} else {
  if (!json_response.getString("test").equals("uu")) {
    this.step1 = 0;
  } else {
    this.step1 = 1;
  }
}
```

Google Play Protect

A case of a missing “u”

```
android.util.Log.d("check user", response);
if (!json_response.getString("net").equals("ok")) {
  this.step1 = 0;
} else {
  if (!json_response.getString("test").equals("uu")) {
    this.step1 = 0;
  } else {
    this.step1 = 1;
  }
}
```

Google Play Protect

A case of a missing “u”

App makes a GET request to

`http://www.website.ro/app/test_net.php`

This is the response:

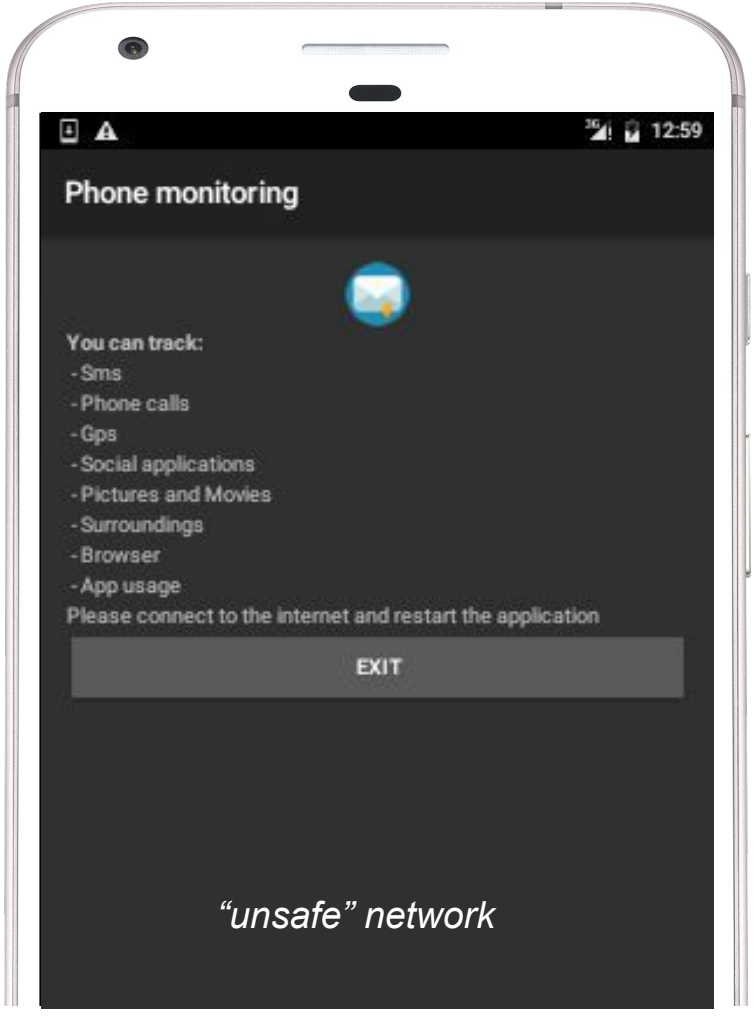
```
{"net":"ok","test":"uuu"}
```

Is it a “safe” network?

So, what's the difference?

```
if (!this.step1) {
  AppMain.access$002(new java.util.Timer());
  AppMain.access$000().schedule(
    new StartCls1(this.context), 2900L);
  AppMain.access$102(1);
} else {
  AppMain.access$002(new java.util.Timer());
  AppMain.access$000().schedule(
    new StartCls(this.context), 2900L);
  AppMain.access$102(1);
}
```

Yes, but do you have the pictures?



Google Play Protect

Sidebar: interesting string obfuscation

```
MyActivity.down_pls =
"0101000001101100011001010110000101110011011001010010000
0011001000110111011101110111011011001101100011011110110000
1011001000010000001110100011010000110010100100000110000
1011100000111000 0";
```

“Please download the app”

Evaluating the device

Device evaluation

App makes a POST request with the following information:

```
action          =firstcheck
website         =64.140.xxx.xxx
typeapp         =2
imei            =0069320xxxxxxxx
appid           =85
langphone       =en
time            =1500575690929
minname         =5
maxname         =15
minpass         =5
maxpass         =20
timesend        =1500575690936
```

C&C response

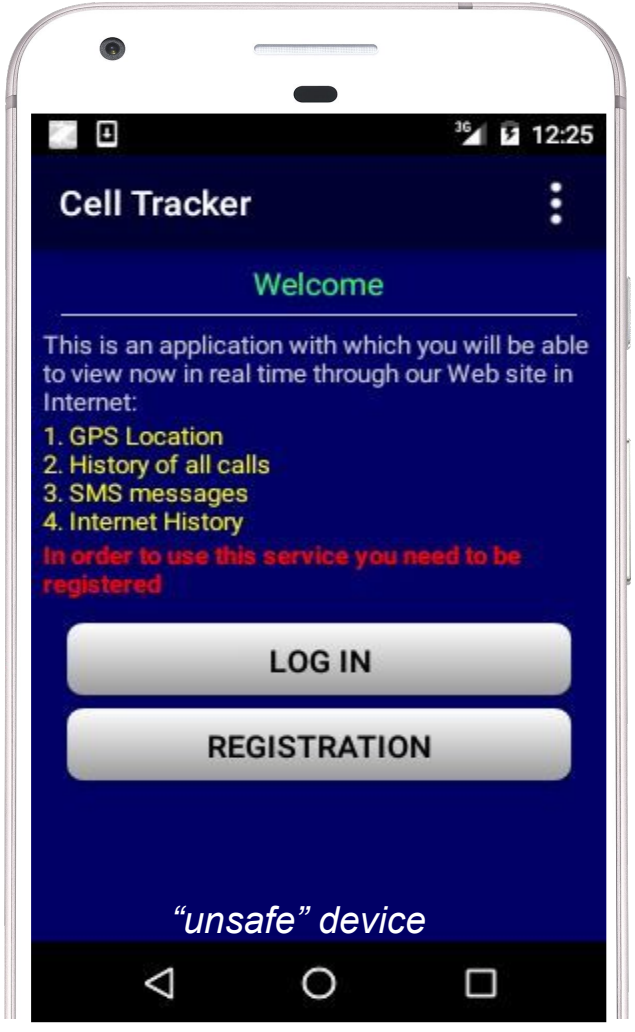
```
[["super_ok","85"],
…
<HTML code for a screen>]
```

```
[["super_no","85"],
…
<Different HTML code for a
different screen>]
```

The outcome of the device evaluation

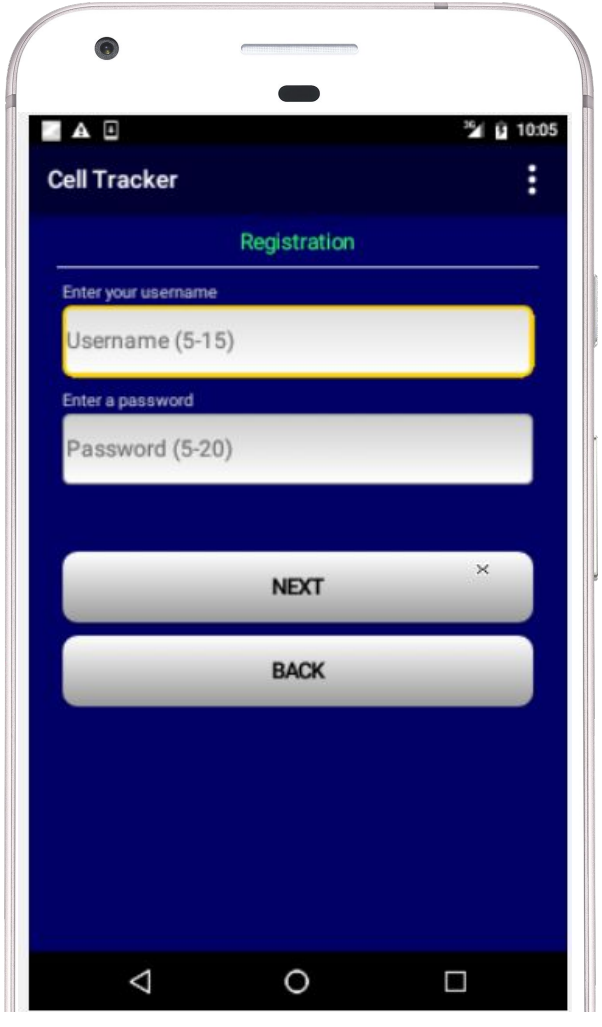
	Any Pixel / Nexus device	Other device
Google network		
Other network		

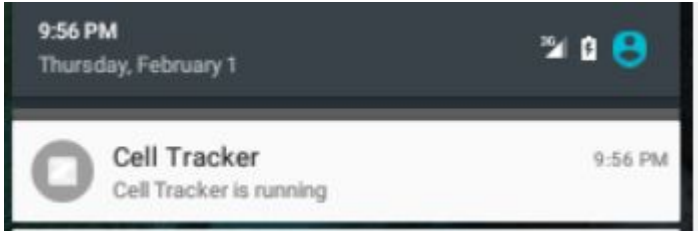
Yes, but do you have pictures?



Google Play Protect

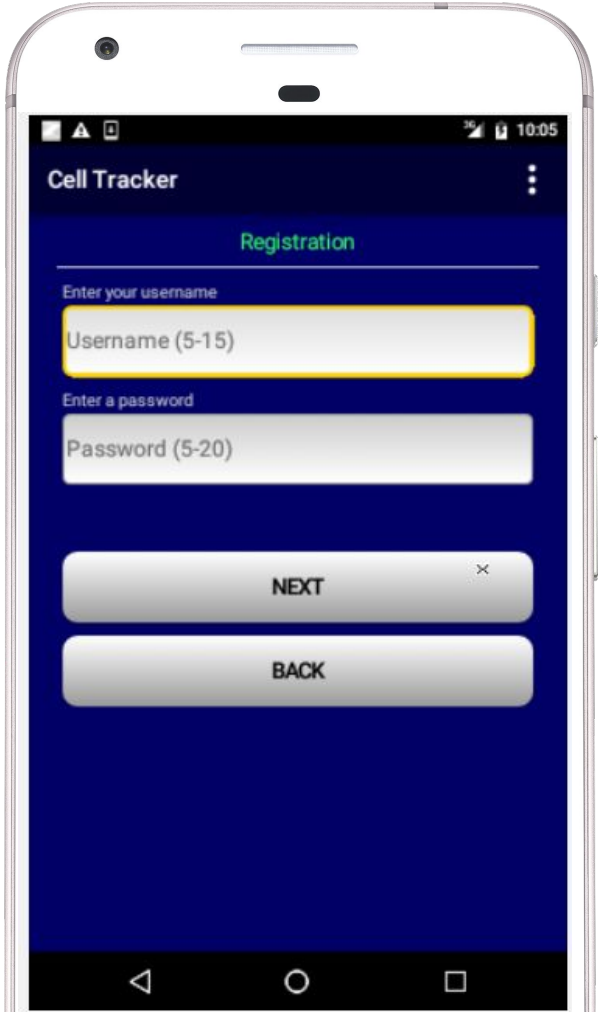
Yes, but do you have pictures?

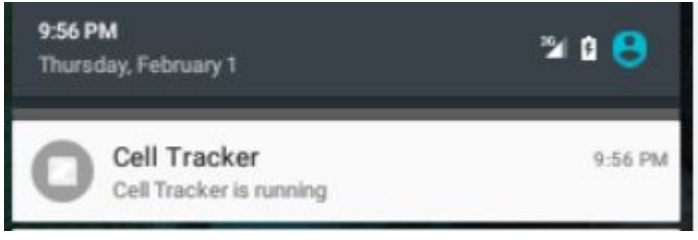




Google Play Protect

Yes, but do you have pictures?

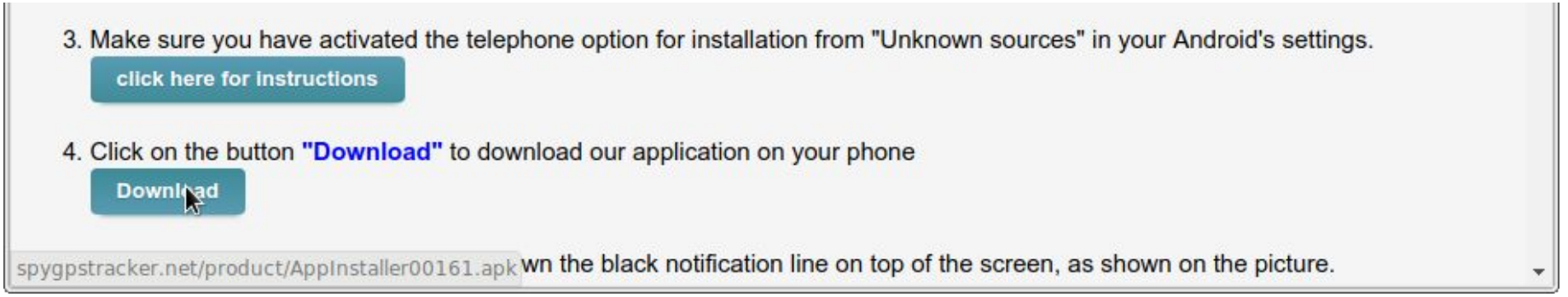


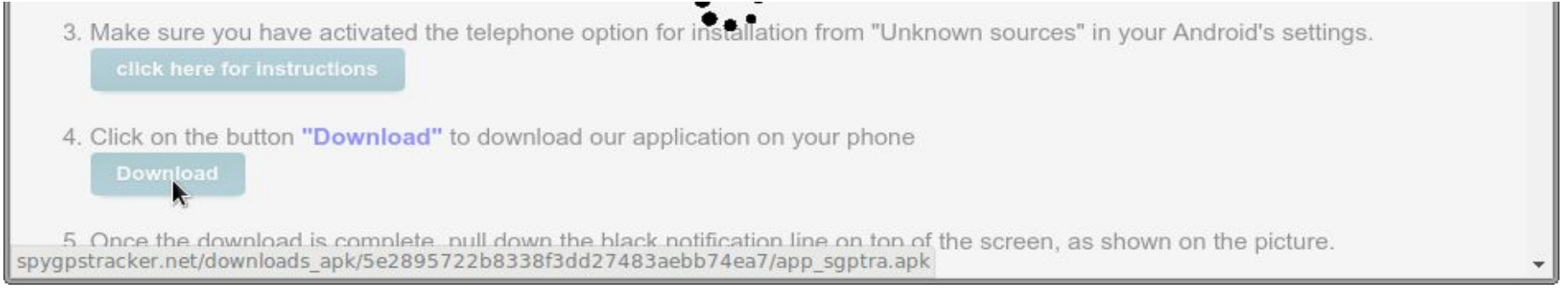


No actual spying is done!

Google Play Protect

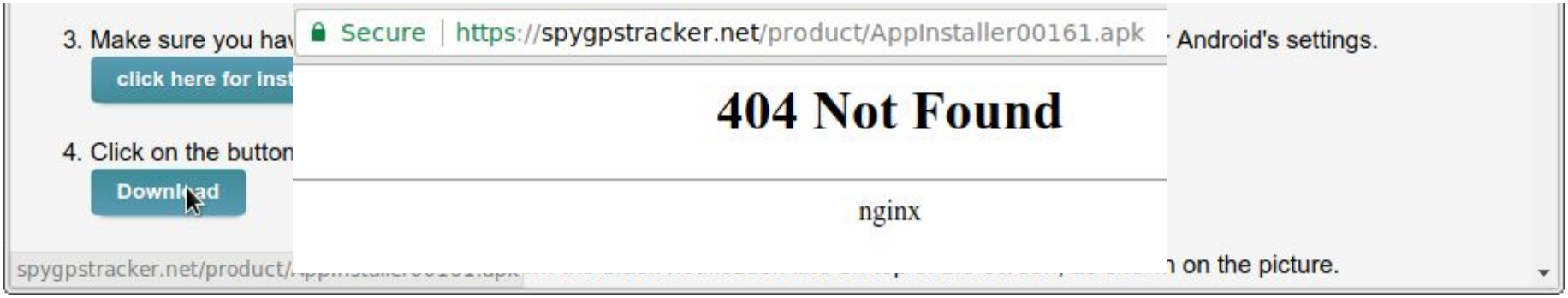
Let’s download the app from the website...

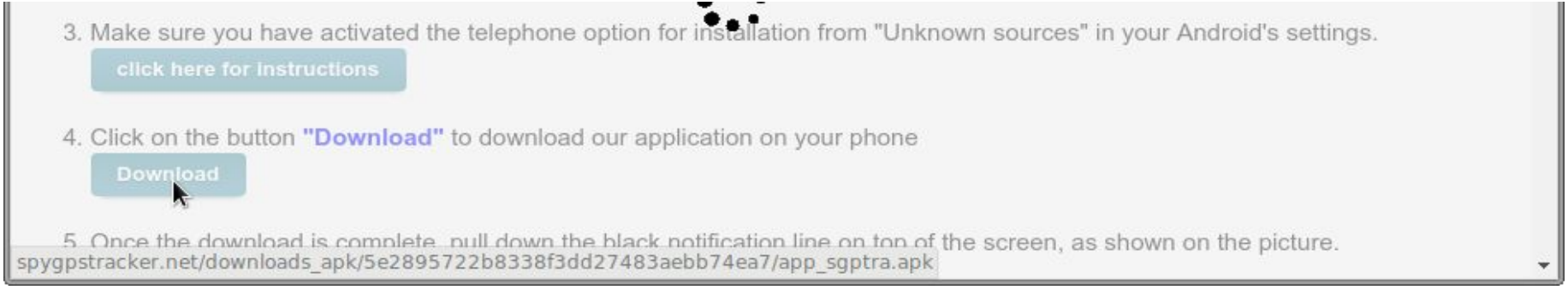




Google Play
Protect

Let’s download the app from the website...





Google Play
Protect

Sidebar: obfuscation of names

```
es.cell.apiece.speeches.Rediscovered.spine =
 es.bled.warehousing.tinder.Rehearsed.miniseries("d3858fa8e8b3e10961cab096afd96b6c");
es.cell.apiece.speeches.Rediscovered.hiss = 0;
es.cell.apiece.speeches.Rediscovered.photography =
 es.bled.warehousing.tinder.Rehearsed.miniseries("4ffc4c3d55615445b7ecf48d7fc937cf");
es.cell.apiece.speeches.Rediscovered.loneliness =
 es.bled.warehousing.tinder.Rehearsed.miniseries("3e8ad8fc5546d188c5ac306b3e852978");
es.cell.apiece.speeches.Rediscovered.misspell =
 es.bled.warehousing.tinder.Rehearsed.miniseries("495d8ba92fbf878d2b2b31b2f1419149");
```

Some final thoughts

1. Apps don't like to be repackaged
2. You shouldn't prioritise only evaluation failures
3. Apps don't like your networks (and devices), devs don't like them too

Some final thoughts

1. Apps don't like to be repackaged
2. You shouldn't prioritise only evaluation failures
3. Apps don't like your networks (and devices), devs don't like them too
4. Malicious authors have really interesting obfuscation ideas

More about the actual spyware...

https://team-sik.org/sideloading-malware-googleplay-2017/

Thank you, TeamSIK from Fraunhofer!

THANK YOU

Google Play
Protect