

A H E A D

Bezpečnost a mobilní aplikace

10. 4. 2019

Jakub Jeřábek
jakub.jerabek@ahead-itec.com

Co nás dnes čeká

1. Důvěřujete SMS zprávám od své banky? Realita 2FA
2. Jak zabezpečit kód aplikace před okopírováním
3. Jak zabezpečit aplikaci před zneužitím
4. Hackování mobilní aplikace - praktická ukázka
5. Antiviry a útoky na mobilní telefony

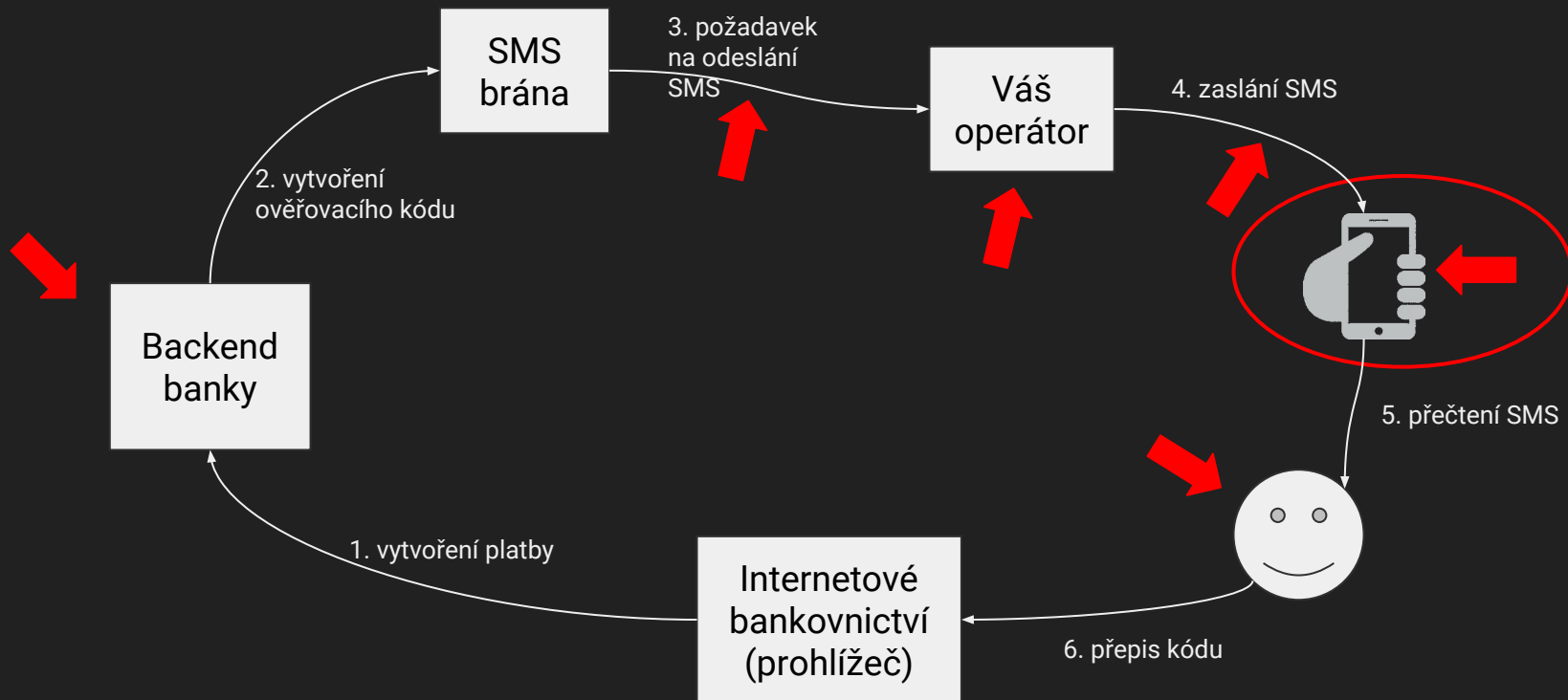
Vícefaktorová autentizace - co to je a co to není

- Faktor znalosti (něco co znám jen já - PIN, heslo)
- Faktor vlastnictví (něco co vlastním jen já - karta, security token)
- Faktor inherence (něco co jsem - hlas, duhovka, otisk prstu, obličej)
- *Faktor polohy (kde jsem - restrikce přístupu z určitých IP adres)*
- 2FA - libovolná podmnožina prvních tří faktorů
 - příklady:
 - výběr z bankomatu (vlastnictví - platební karta, znalosti - PIN)
 - přihlášení do IB s využitím mobilní aplikace (George/Smart/KB klíč, My Air, aj.)
- 2-kroková (2-step) autentizace



Platbu kartou 51*****0
ve výši 159,00 CZK prosím
potvrďte kódem 672677.

Důvěřujete SMS zprávám od své banky?



Útok na SMS v Německu 2017

Hackerům se podařilo zneužít chyby v technologii SS7, kterou používají mobilní sítě ke komunikaci a získali přístup k SMS napadených uživatelů. Ve spojení s e-mailovým phishingem tak byli schopni za posledních několik měsíců v rámci německé mobilní sítě O2 Telefonica získat ověřovací SMS pro přihlášení i provedení platby a doslova vysát peníze z bankovních účtů napadených uživatelů. Kvůli přesměrování neměl daný majitel účtu celou dobu o ničem ani ponětí.

Zdroj:

<https://connect.zive.cz/clanky/hackeri-vyuzili-chyby-vmobilni-siti-o2-telefonica-vybrali-lidem-bankovni-ucty/sc-320-a-187540/default.aspx>

Jak Android zpracovává příchozí SMS

1. OS Android přijímá SMS zprávu
2. OS Android posílá zprávu všem aplikacím*
3. Aplikace, se samy rozhodují, jak s SMS zprávou naloží

*Všem, které mají zaregistrovaný receiver `android.provider.telephony.SMS_RECEIVED` a oprávnění `android.permission.RECEIVE_SMS`.

Krádež SMS - praktická ukázka

Potřebujeme:

- zdánlivě neškodnou aplikaci
- sběrné místo SMS
- oběti

Máme:

- SMS jízdenka Zlín
 - http://bit.ly/GPlaySMSJizdenka*
- http://bit.ly/StolenSMS**
- Počet stažení: 1-5 tisíc

*verze publikovaná neobsahuje škodlivý kód a nemá přístup k SMS

**server pro sběr SMS byl vypnut

Potřebujeme oběť

+420 *** **

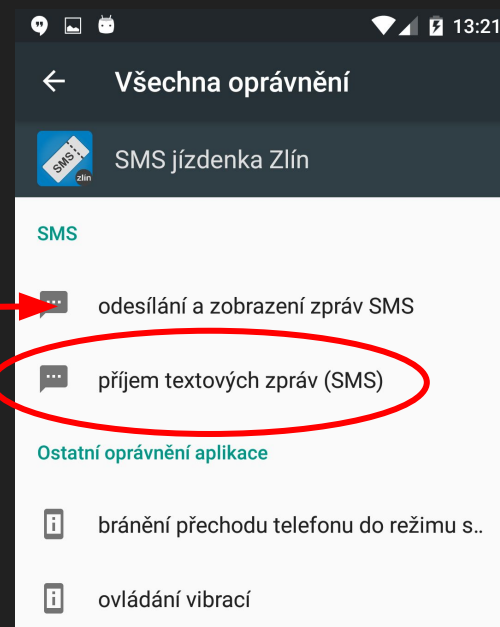
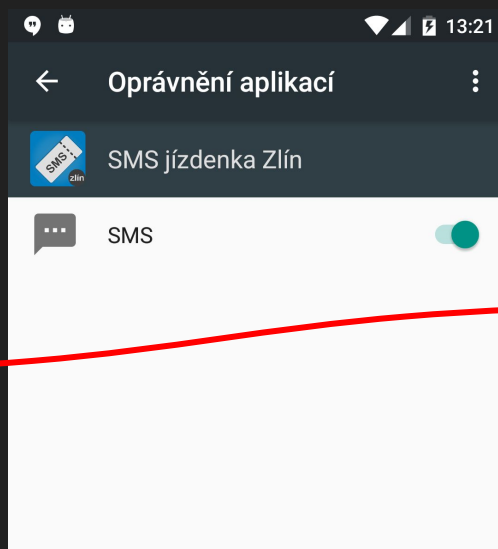
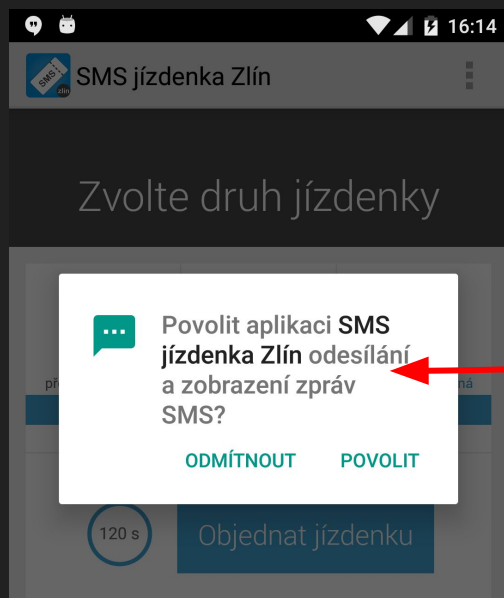
Jak se bránit?

- používat 2. faktor

Oprávnění na Androidu 6 a vyšších

- krok vpřed
- `targetSdkVersion 23` (GPlay vyžaduje minimálně 26 (8.0))
- rozdělení na *normal* a *dangerous*
 - https://developer.android.com/guide/topics/permissions/overview#normal_permissions
 - <https://developer.android.com/guide/topics/permissions/overview#permission-groups>
- ale...

... lze získat oprávnění bez povšimnutí



Jak je to možné?

```
6 <uses-permission android:name="android.permission.SEND_SMS" />
7 <uses-permission android:name="android.permission.RECEIVE_SMS" />
8 <uses-permission android:name="android.permission.WAKE_LOCK" />
9 <uses-permission android:name="android.permission.VIBRATE" />
10 <uses-permission android:name="android.permission.INTERNET" />
```

SMS

- SEND_SMS
- RECEIVE_SMS
- READ_SMS
- RECEIVE_WAP_PUSH
- RECEIVE_MMS

- If an app requests a dangerous permission listed in its manifest, and the app already has another dangerous permission in the same permission group, the system immediately grants the permission without any interaction with the user. For example, if an app had previously requested and been granted the `READ_CONTACTS` permission, and it then requests `WRITE_CONTACTS`, the system immediately grants that permission.

Jak zabezpečit kód aplikace před okopírováním

Ochrana kódu - proč?

- Softwarové patenty? Nefungují
 - https://ddd.uab.cat/pub/vivataca/vivataca_a2001m9n28/index.html
- Flappy Birds
 - 300 klonů, 238 infikovaných
 - posílání SMS, hovory, GPS, adresáře [1]

Praktická ukázka

Potřebujeme:

- vytáhnout APK z telefonu
- dekompilovat APK
- umět číst v cizím kódu

Máme:

- TCMD, APK extractor, ...
- APK Tool [\[1\]](#)
- ???

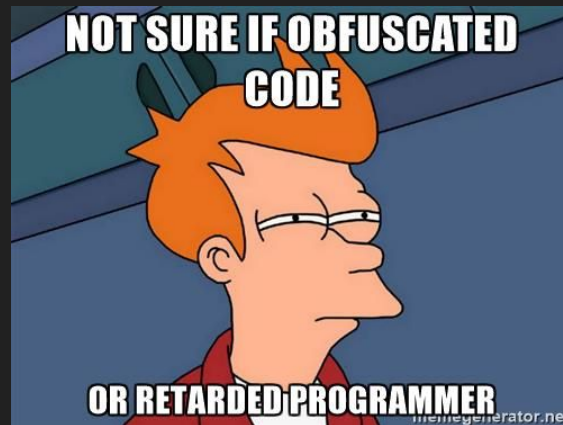
Pozor na řetězce!

Pro zájemce: <https://www.fi.muni.cz/research/laboratories/crocs.xhtml.cs>

Ochrana kódu - jak?

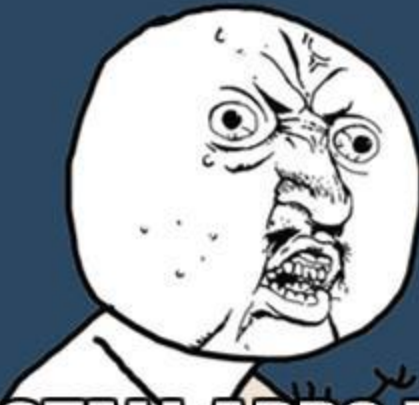
- Obfuskace při buildu [\[1\]](#)
 - SDK/tools/proguard/proguard-android.txt
- Obfuskace při psaní

```
14  buildTypes {  
15      debug {  
16          minifyEnabled false  
17          proguardFiles 'proguard-rules.pro'  
18      }  
19      release {  
20          minifyEnabled true  
21          proguardFiles 'proguard-rules.pro'  
22      }  
23  }
```



Jak zabezpečit aplikaci před zneužitím

APP DOWNLOADERS



**Y U INSTALL APPS FROM
ULOZ.TO?**

memegenerator.net

Ochrana aplikace - proč?

- Reputace
- Ochrana klientů / komunity

Hacknutí aplikace - praktická ukázka

- obejití ochrany (Authentication Bypassing)
- modifikace logických podmínek

Použité příkazy

Dekompilace APK (-r nedekompiluje resources)

```
apktool d -r fimuni-release.apk
```

Re-kompilace

```
apktool b -o fimuni-hacked.apk fimuni-release
```

PATH: C:\Program Files\Android\Android Studio\jre\bin

Vytvoření keystore pro podpis APK

```
keytool -genkey -v -keystore fimuni.keystore -alias fi -keyalg RSA -keysize  
2048 -validity 10000
```

Podepsání APK (klíč v keystore je "fi", heslo "fimuni")

```
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore  
fimuni.keystore fimuni-hacked.apk fi -storepass fimuni
```

Použité příkazy

Vypsání podpisu APK

```
jarsigner -verbose -verify -certs fimuni-hacked.apk
```

ADB

- instalace APK do připojeného telefonu či emulátoru:

```
adb install fimuni-hacked.apk
```

- otevření aktivity, která má parametr exported=true:

```
adb shell
```

```
am start -n com.aheaditec.fimuni/.DegreeActivity
```

Ochrana aplikace - jak?

- Kontrola certifikátu APK
- Kontrola původu APK
 - Google Play
 - odjinud
- Knihovna: <https://github.com/SandroMachado/AndroidTampering>

Antiviry a útoky na mobilní telefony

Typické znaky malwaru

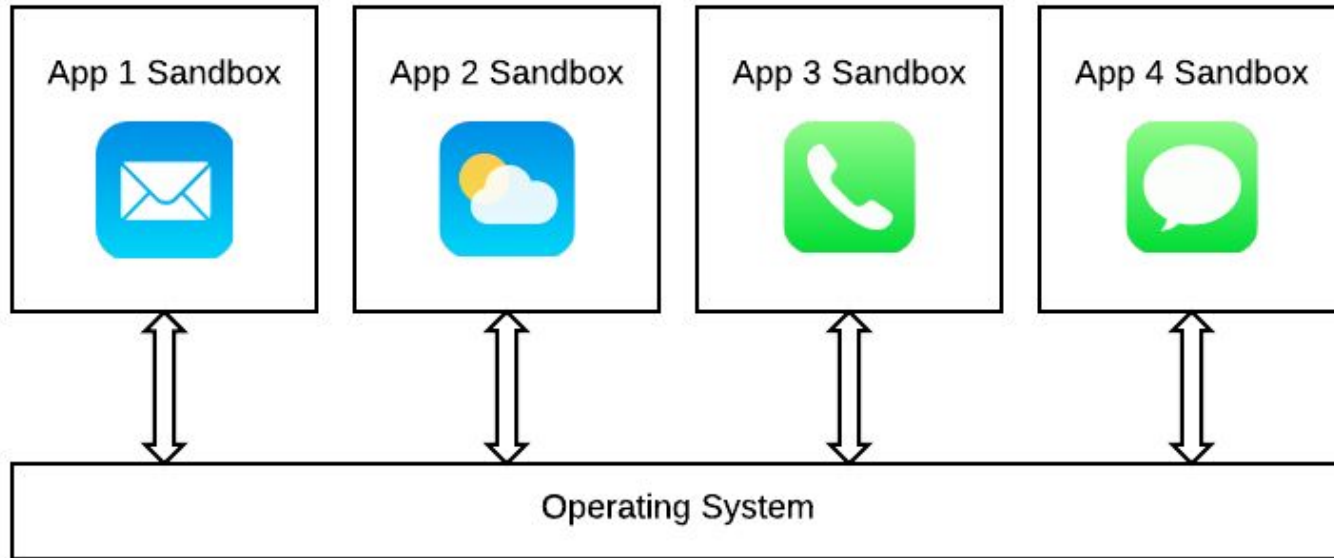
- snaha být nenápadný
- přístup na internet + monitoring nabíjení + citlivá data
- používání broadcast receivers
- opožděné spuštění škodlivého kódu

Manifest nikdy nelže!

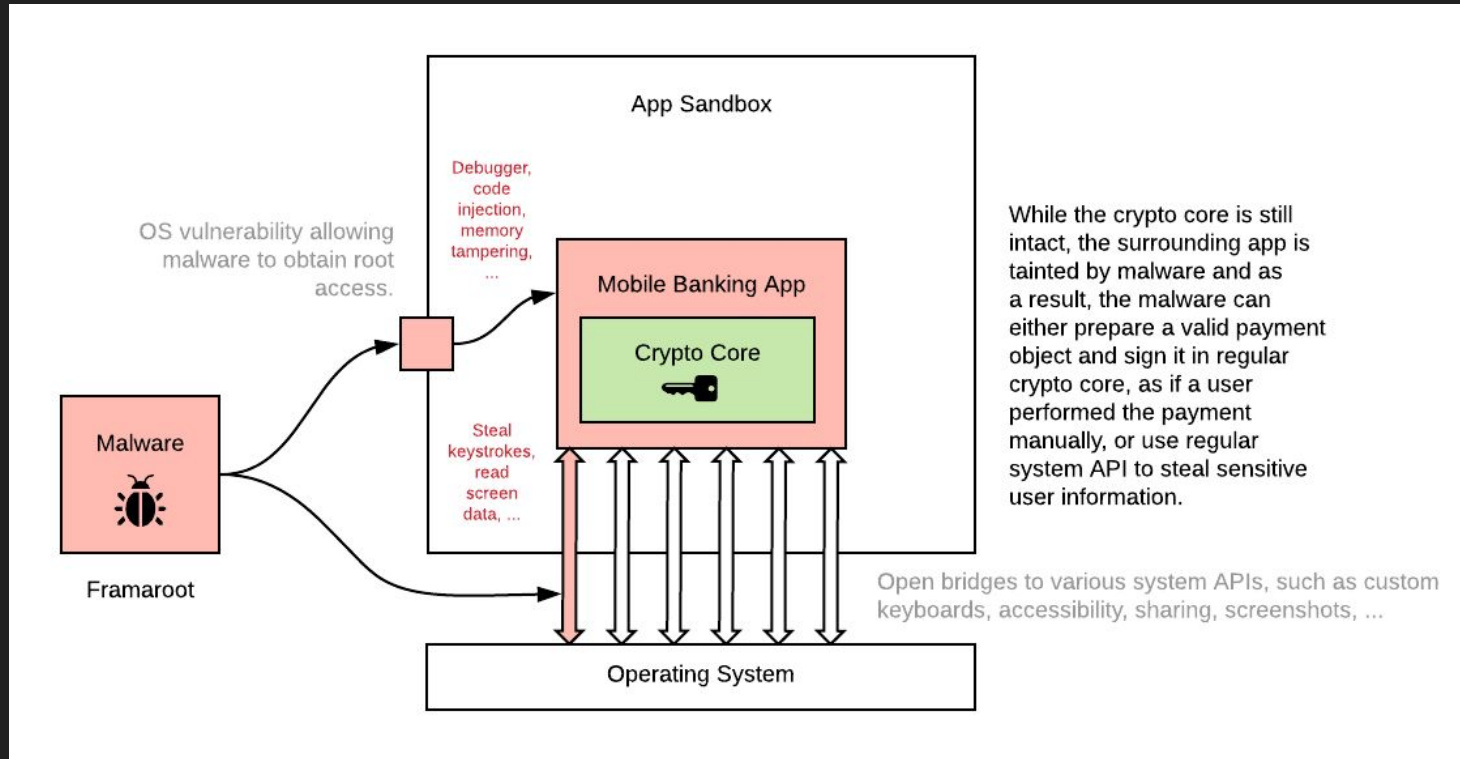
Mobilní vs. desktopový svět

- Možnosti virů
- Možnosti antivirů
- Virus vs. malware

Sandboxing



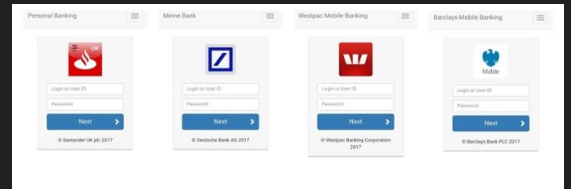
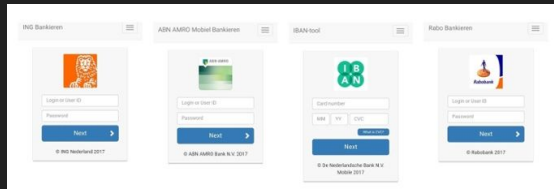
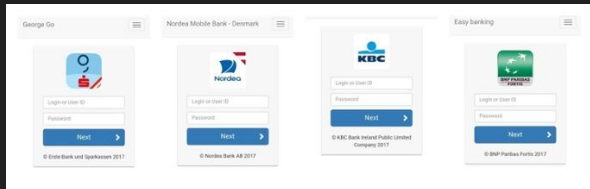
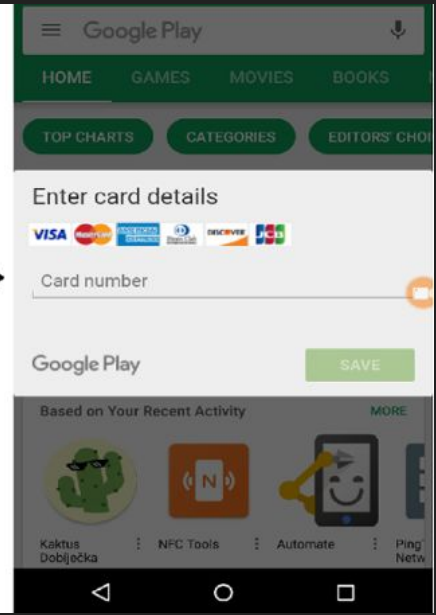
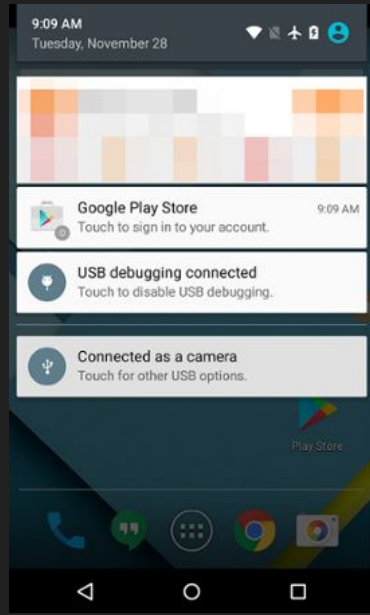
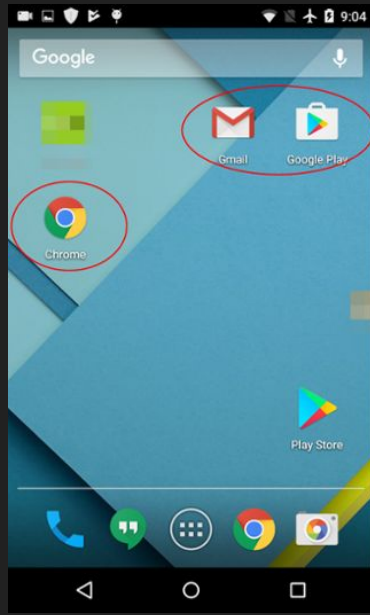
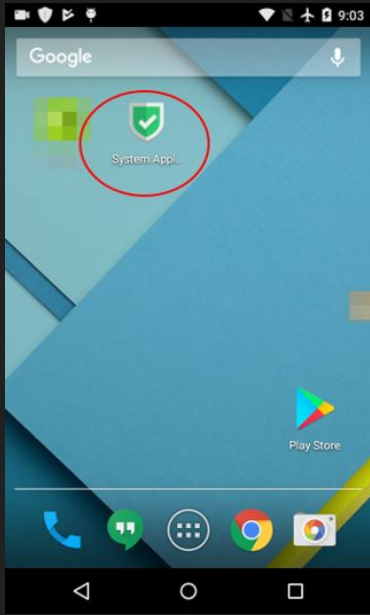
Sandboxing



Ukázka reálných útoků

Zdroje:

<https://blog.avast.com/new-version-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang>
<https://blog.avast.com/mobile-banking-trojan-sneaks-into-google-play-targeting-wells-fargo-chase-and-citibank-customers>

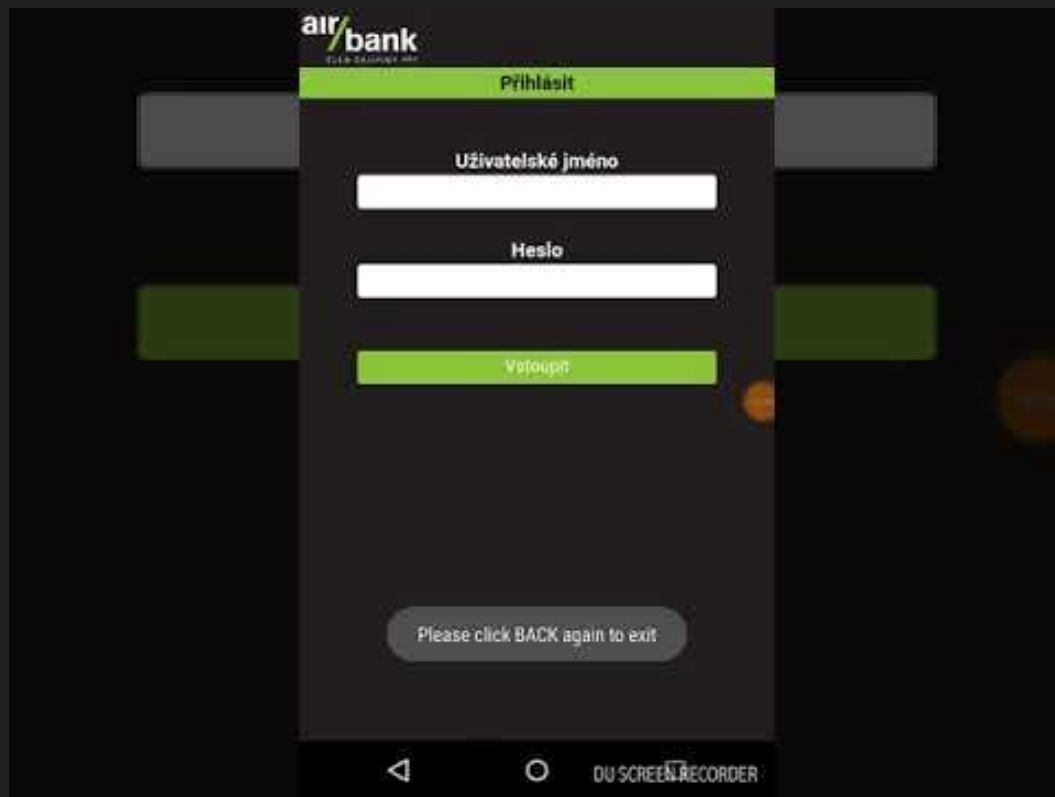


BankBot

```
private static boolean b(Context arg7) {
    boolean v0 = true;
    String[] v2 = new String[]{"U", "A"};
    String[] v3 = new String[]{"R", "U"};
    String[] v4 = new String[]{"B", "Y"};
    String v5 = arg7.getResources().getConfiguration().locale.getCountry();
    if((v5.equalsIgnoreCase(TextUtils.join("", ((Object[])v3)))) || (v5.equalsIgnoreCase(TextUtils
        .join("", ((Object[])v2)))) || (v5.equalsIgnoreCase(TextUtils.join("", ((Object[])v4))))
        ) {
        v0 = false;
    }
    return v0;
}
```

```
com.ubs.swidKXJ.android
com.unicredit
com.unionbank.ecommerce.mobile.android
com.usaa.mobile.android.usaa
com.usbank.mobilebanking
com.vakifbank.mobile
com.vipera.ts.starter.FGB
com.vipera.ts.starter.MashreqAE
com.wf.wellsfargomobile
com.ykb.android
com.ziraat.ziraatmobil
cz.airbank.android
cz.csob.smartbanking
cz.sberbankcz
de.comdirect.android
de.commerzbanking.mobil
de.direkt1822.banking
de.dkb.portalapp
de.fiducia.smartphone.android.banking.vr
de.postbank.finanzassistent
de.sdvz.ihb.mobile.app
enbd.mobilebanking
es.bancosantander.apps
es.cm.android
es.ibercaja.ibercajaapp
```

BankBot - ukázka



QRecorder



QRecorder

- 10 000+ instalací
- plnila svůj účel
- škodlivý kód vložen s aktualizací
- krádež přihlašovacích údajů, by-passing SMS overení

Zdroj:

<https://lukasstefanko.com/2018/09/banking-trojan-found-on-google-play-stole-10000-euros-from-victims.html>

QRecorder



Děkuji za pozornost

Prostor pro vaše dotazy