AHEAD

Bezpečnost a mobilní aplikace

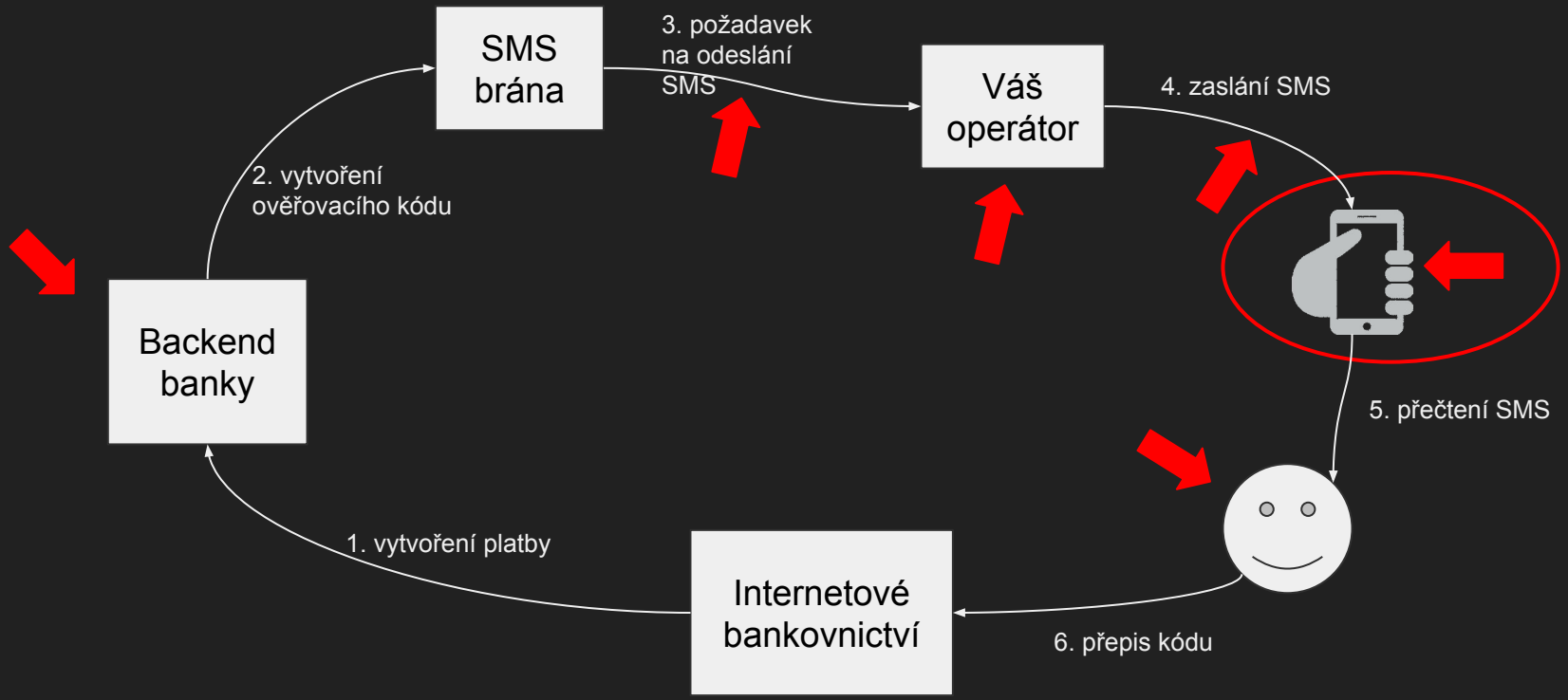
18. 4. 2018

Jakub Jeřábek
jakub.jerabek@ahead-itec.com

Co nás dnes čeká

1. Důvěřujete SMS zprávám od své banky?
2. Jak zabezpečit kód aplikace před okopírováním
3. Jak zabezpečit aplikaci před zneužitím
4. Antiviry a útoky na mobilní telefony

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 Telefónica 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 právo k přístupu na internet
**server pro sběr SMS byl vypnut

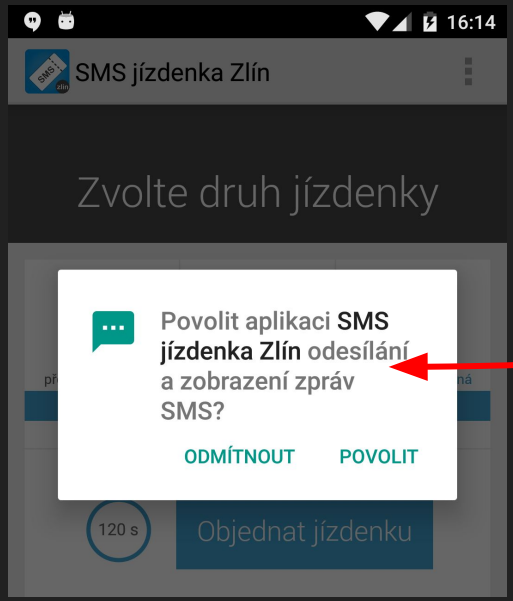
Potřebujeme oběť

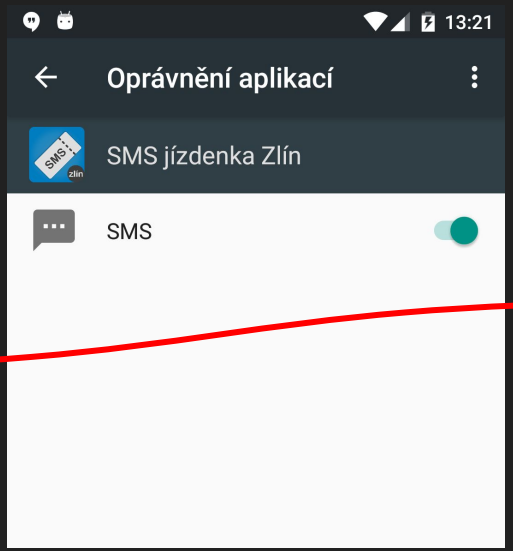
+420 *** *** *** :)

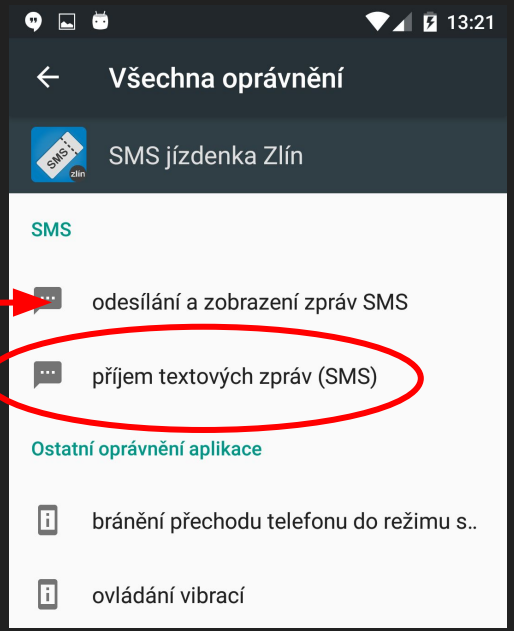
Oprávnění na Androidu 6 a vyšších

- krok vpřed
- `targetSdkVersion 23`
- rozdělení na *normal* a *dangerous*
  - https://developer.android.com/guide/topics/permissions/normal-permissions.html
  - https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous
- ale...

… lze získat oprávnění bez povšimnutí







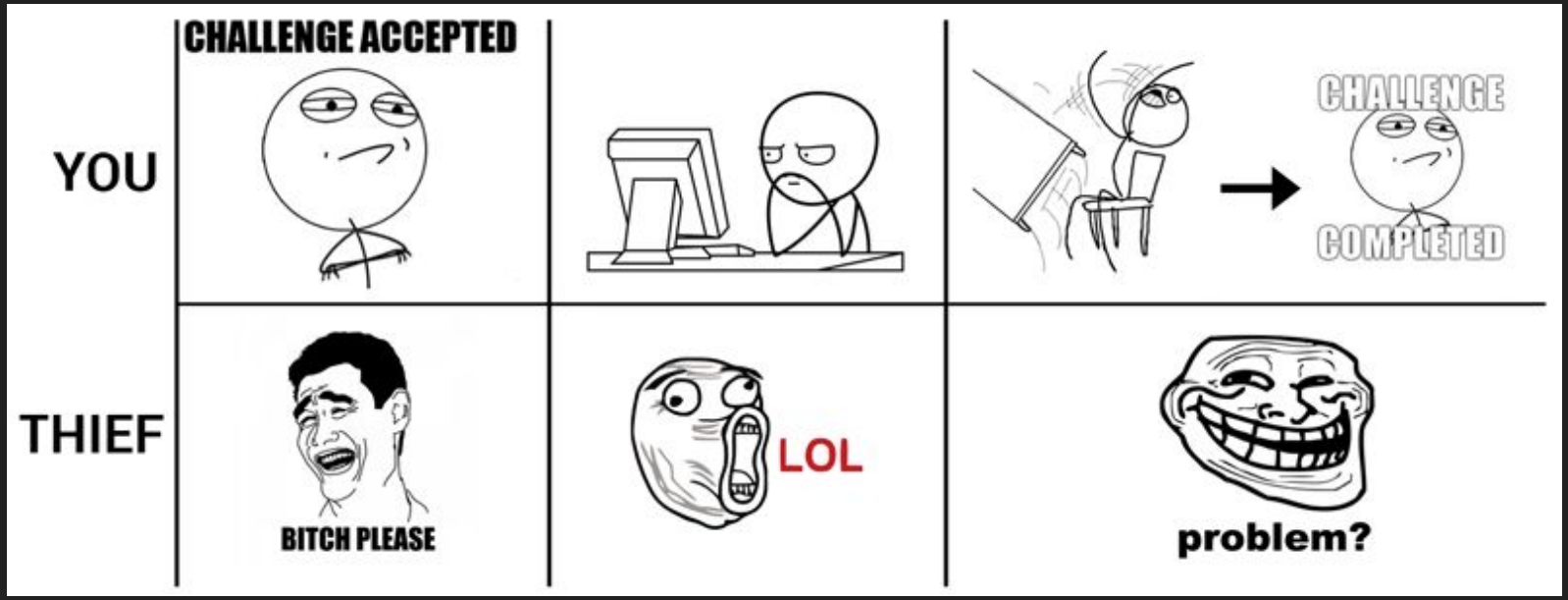
Jak je to možné?

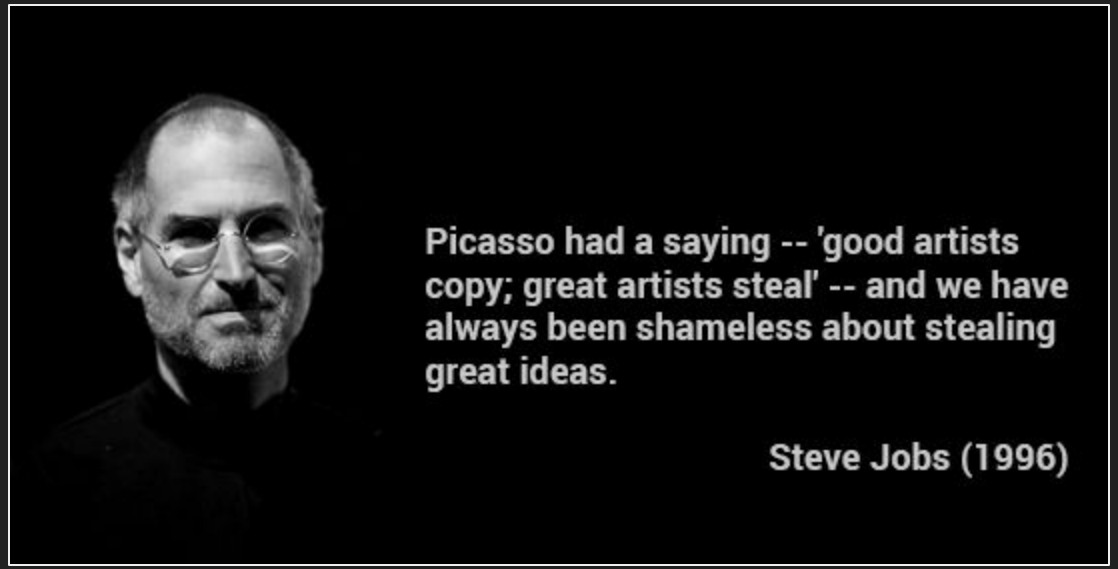
```
6     <uses-permission android:name="android.permission.SEND_SMS" />
7     <uses-permission android:name="android.permission.RECEIVE_SMS" />
8     <uses-permission android:name="android.permission.WAKE_LOCK" />
9     <uses-permission android:name="android.permission.VIBRATE" />
10    <uses-permission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


YOU
CHALLENGE ACCEPTED
CHALLENGE
COMPLETED
THIEF
BITCH PLEASE
LOL
problem?


Picasso had a saying -- 'good artists copy; great artists steal' -- and we have always been shameless about stealing great ideas.
Steve Jobs (1996)

Ochrana kódu - proč?

- Softwarové patenty?
  - https://webshop.ffii.org/
- 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!

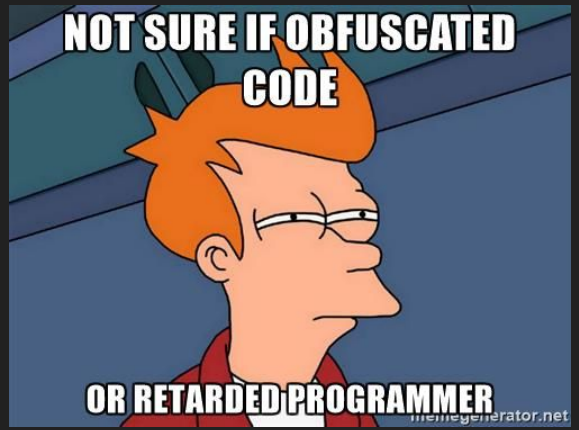
Pro zájemce: https://www.fi.muni.cz/research/laboratories/crocs.xhtml.cs

Ochrana kódu - jak?

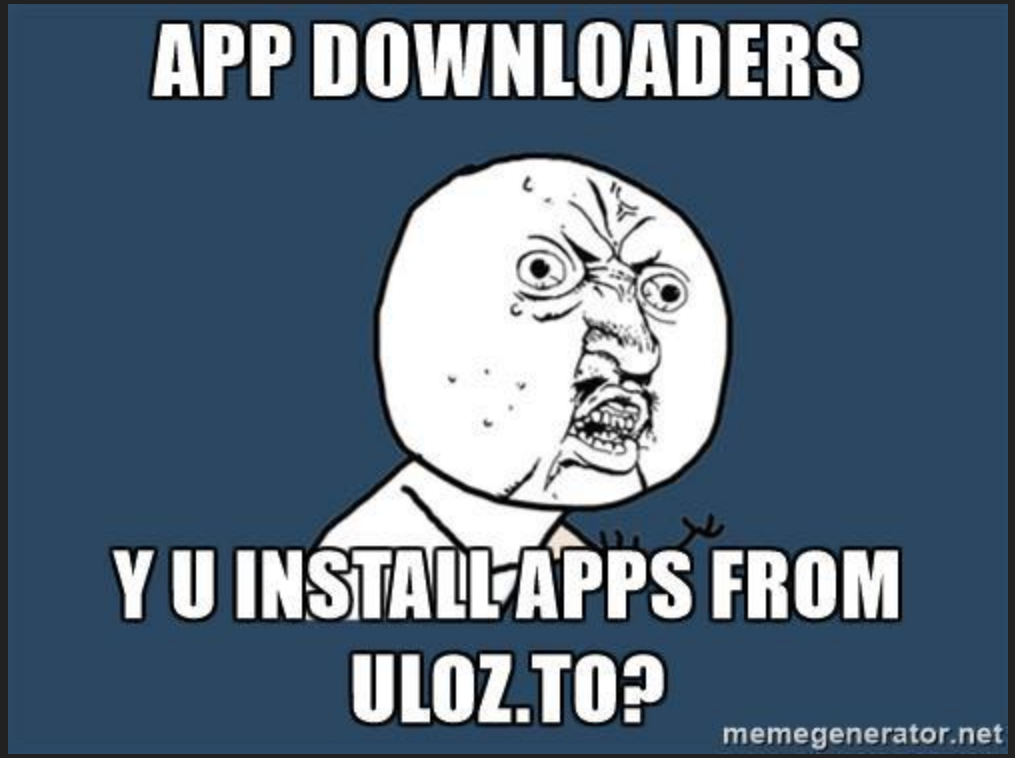
- Obfuskace při buildu [1]
  - SDK/tools/proguard/proguard-android.txt

```
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      }
```

- Obfuskace při psaní



Jak zabezpečit aplikaci před zneužitím


APP DOWNLOADERS
Y U INSTALL APPS FROM ULOZ.TO?
memegenerator.net

Ochrana aplikace - proč?

- Reputace
- Ochrana klientů / komunity

Ochrana aplikace - jak?

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

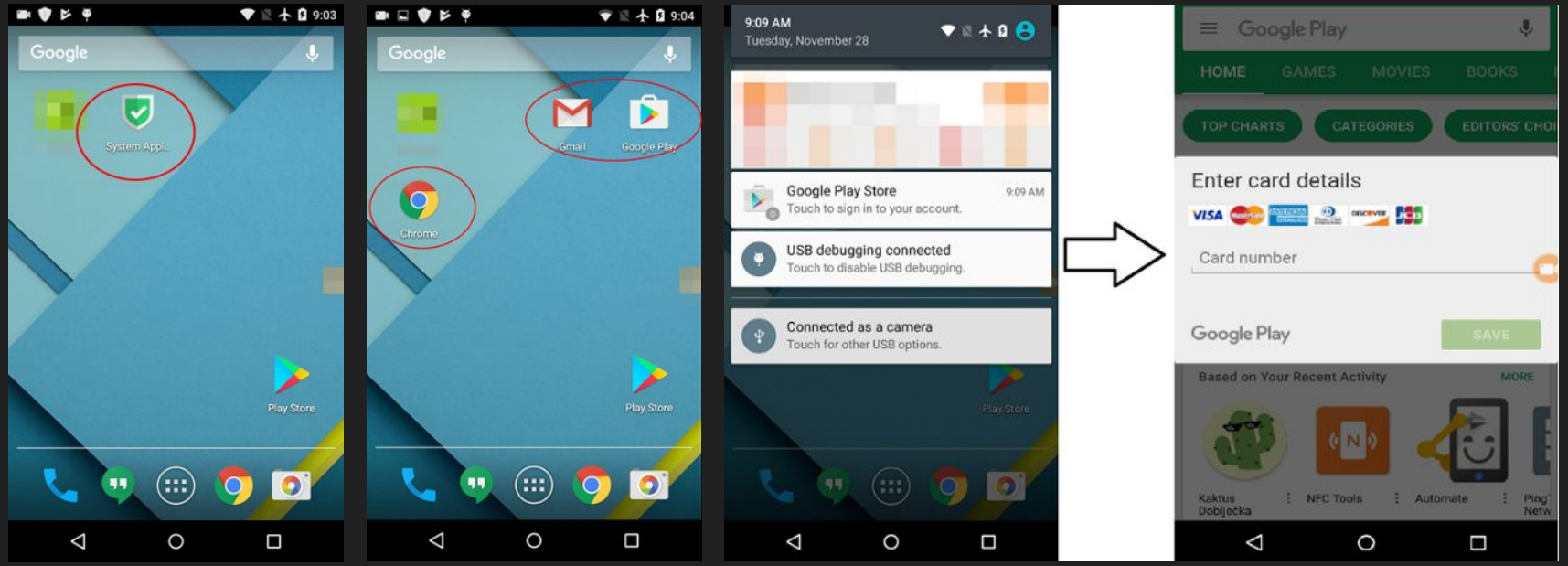
Antiviry a útoky na mobilní telefony

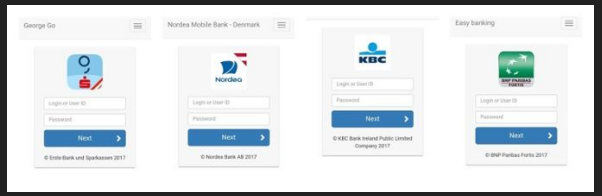
Mobilní vs. desktopový svět

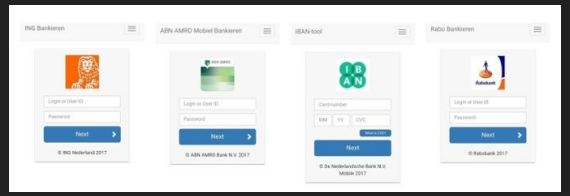
- Možnosti virů
- Možnosti antivirů
- Virus vs. malware

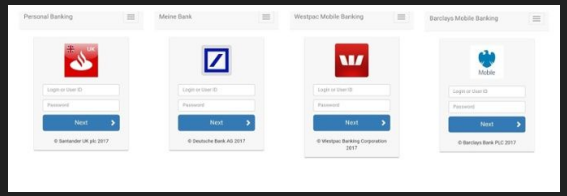
Ukázka reálných útoků

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


9:03
Google
System Appl...
Play Store
9:04
Google
Gmail
Google Play
Chrome
Play Store
9:09 AM
Tuesday, November 28
Google Play Store
9:09 AM
Touch to sign in to your account.
USB debugging connected
Touch to disable USB debugging.
Connected as a camera
Touch for other USB options.
Play Store
Google Play
HOME
GAMES
MOVIES
BOOKS
TOP CHARTS
CATEGORIES
Enter card details
Card number
Google Play
SAVE
Based on Your Recent Activity
MORE
Kaktus Doblječka
NFC Tools
Automate







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.sdvrz.ihb.mobile.app
enbd.mobilebanking
es.bancosantander.apps
es.cm.android
es.ibercaja.ibercajaapp

BankBot - ukázka

Děkuji za pozornost

Prostor pro vaše dotazy