# Co když zavirování telefonu není nejhorší věc, která se vašemu mobilnímu společníkovi může stát?

Filip Chytrý
Malware Analyst

# Už jste slyšeli o Androidu?

# O čem že to všechno bude?

- Trendy mobilních útoků
- Ztráty mobilních zařízení a rizika z toho plynoucí
- BYOD
- Avast AntiTheft
- NFC
- Cílená reklama

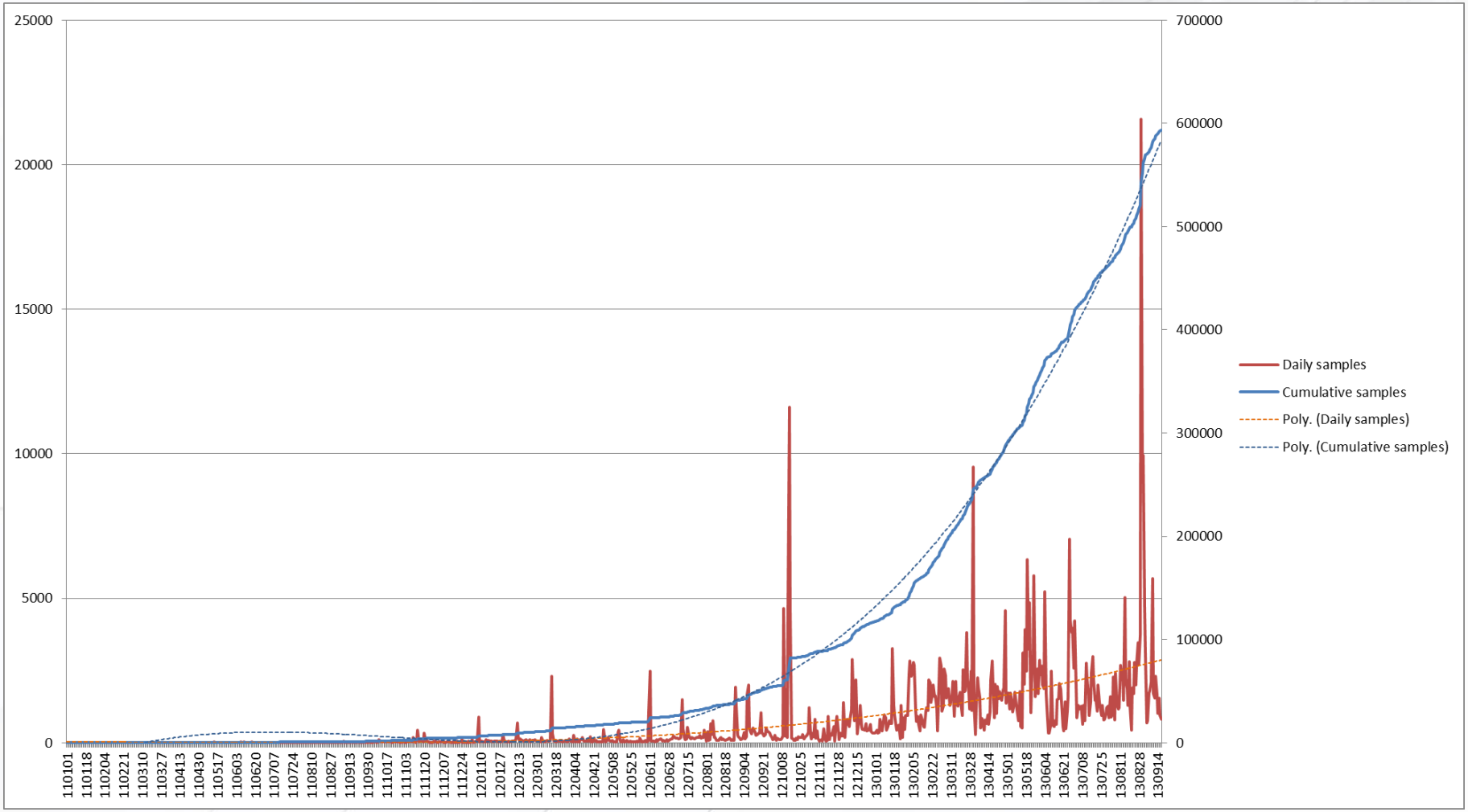
# Trendy mobilních útoků #1

- Mobilní boom pokračuje
  - 1.000.000.000 Android zařízení v roce 2013
  - iOS, Windows Mobile
  - Nízké povědomí uživatelů
  - Výkon a technická složitost zařízení
  - Rizika připojení do internetu
  - Soukromí

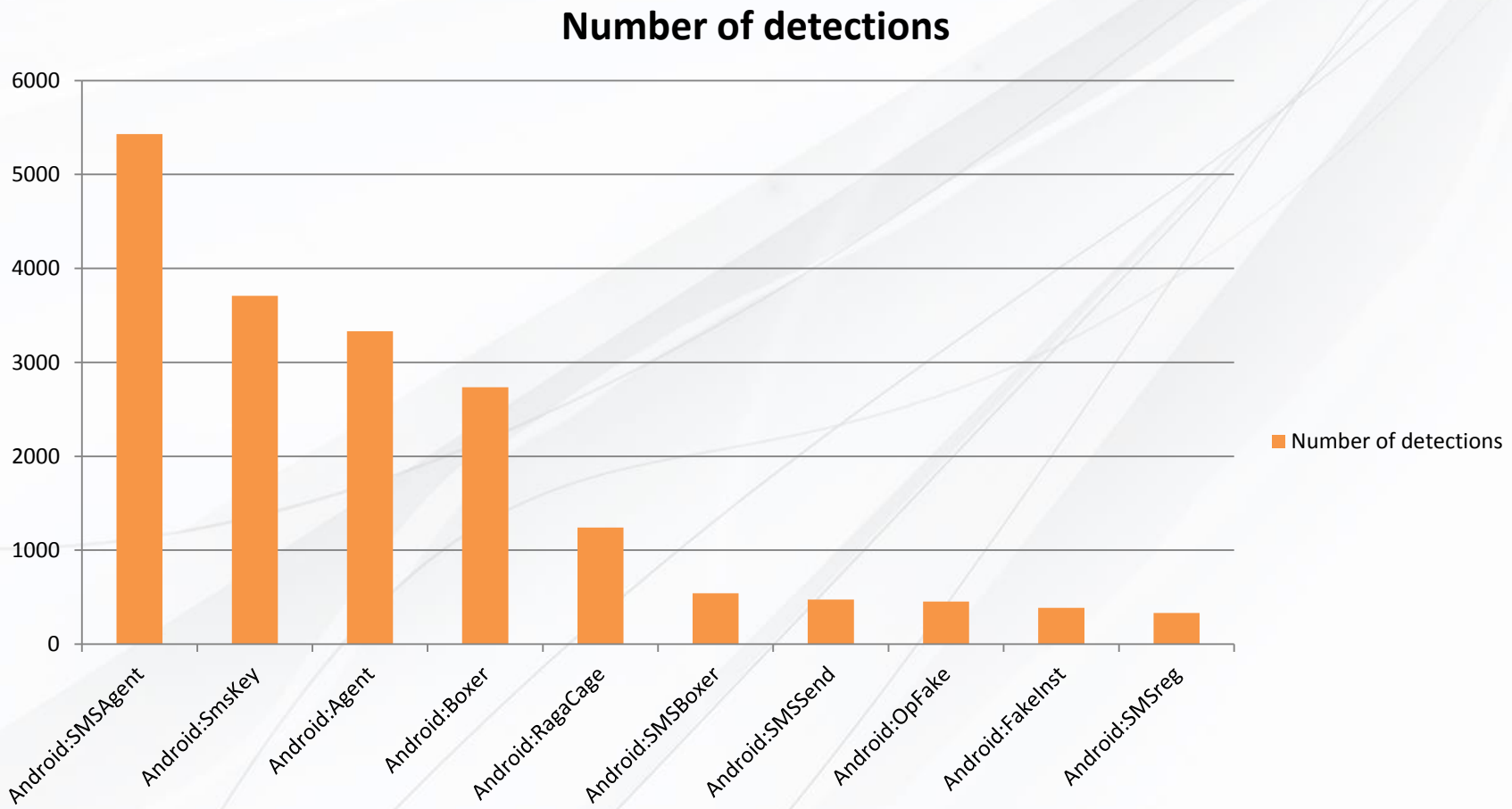
# Trendy mobilních útoků #2

- Útoky mířené na získání peněz či osobních informací
- Sofistikovaný malware poslední doby
  - Ransomware
  - Android:Obad
  - CVE-2013-4787
  - Hesperbot
- Malware z originálních marketů

# Rozvoj malwaru na Android v posledních letech



# Nejvíce viděné detekce



# Typy malwaru #1 – „FAKE APPS“

- **Fake apps – falešné aplikace**
  - Originální aplikace infikované malware kódem
  - Často schované za dobře známými aplikacemi (Avast, Angry Birds, Bad Piggies atd.)
  - Velké možnosti zneužití
  - Spam
  - Krádeže dat
    - Kontakty, telefonní čísla, hesla atd.

# Typy malwaru #2 – „SMS SENDERS“

- **SMS sender – odesílání SMS bez vědomí uživatele**
  - Mohou být součástí Fake apps
  - Odesílání placených SMS
  - Často kompletně skrytý proces
    - V některých případech je nutná interakce uživatele
  - Často si uživatel všimne, že je něco špatně až při měsíčním vyúčtování

# Typy malwaru #3 – „SPY APPS“

- **Spy apps – špehovací aplikace**
  - Některé mohou být i legální
    - Potencionální riziko
  - Monitorují chování uživatele během používání telefonu
  - Zaznamenávají GPS souřadnice
  - Zneužití dat při cílené reklamě

# Sofistikovanější Malware

- Nové možnosti malwaru
- Obdobný vývoj jako historicky na platformě Windows
- Snadnější zneužitelnost
- Nemožnost mazání „normální“ cestou
- Možnosti správce zařízení

# Ransomware – Fake Avast! #1

- Social engineering
- Objeven v září 2013
- Vydává se za Avast Antivirus!

```
</application>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.UPDATE_DEVICE_STATS" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
anifest>
```

# Ransomware – Fake Avast! #2

- Název balíku com.avastmenow

```
GC_CONCURRENT freed 1243K, 44% free 5826K/10375K, external 3125K/3
ms
DexInv: --- BEGIN '/data/app/com.avastmenow-1.apk' ---
DexOpt: load 116ms, verify+opt 485ms
DexInv: --- END '/data/app/com.avastmenow-1.apk' (success) ---
 73):    Receivers: core.StartBooRec
 73):    Activities: com.avastmenow.StartActivity com.avastmenow.Li
```

- Obsah .Apk balíku
  - AndroidDefender
  - Dr.Web


adef_icon

android_defender

blue_button_pressed.9

cat

# Ransomware – Fake Avast! #2

- Dekompilujeme

```
ArrayList localArrayList = new ArrayList();
localArrayList.add("Android/TrojanSMS.Agent.NB.Gen");
localArrayList.add("Android-Trojan/Agent");
localArrayList.add("Android:Agent-AHS [Trj]");
localArrayList.add("Android.Lijo.A");
localArrayList.add("AndroidOS/GenBl.147C189D!Olympus");
localArrayList.add("UnclassifiedMalware");
localArrayList.add("Android.SmsSend.730.origin");
localArrayList.add("a variant of Android/TrojanSMS.Agent.NB");
localArrayList.add("Trojan:Android/SmsSend.AE");
localArrayList.add("Android/SMSSend.AZ");
this.listView = ((ListView)findViewById(2131099653));
```

# Ransomware – Fake Avast! #2

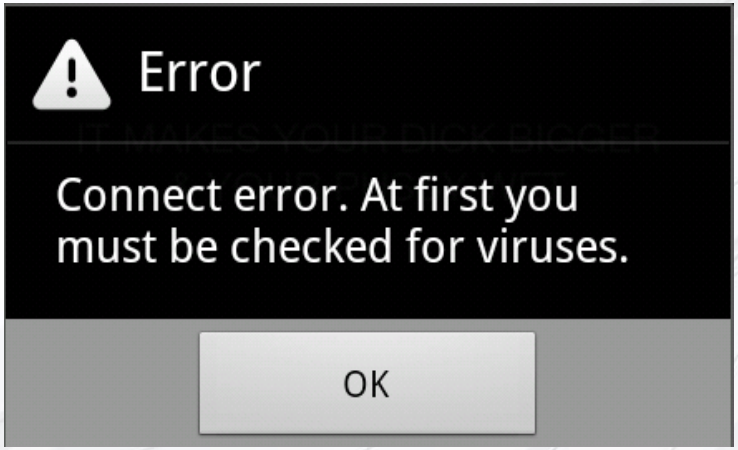
- Dekompilujeme

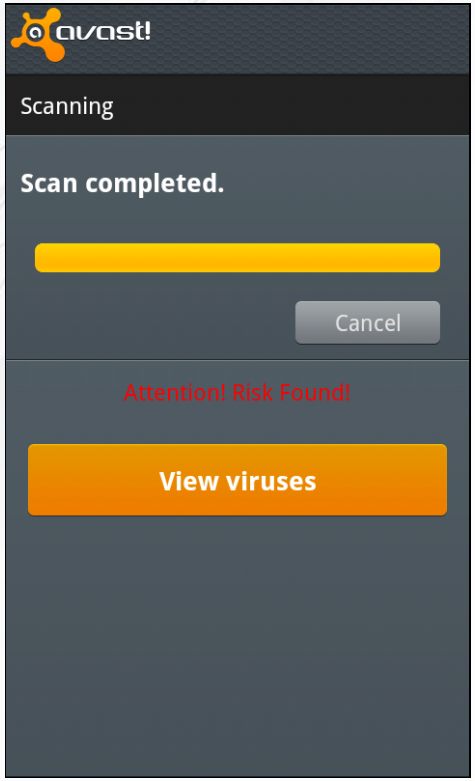
```
ArrayList localArrayList = new ArrayList();
localArrayList.add("Android/TrojanSMS.Agent.NB.Gen");
localArrayList.add("Android-Trojan/Agent");
localArrayList.add("Android:Agent-AHS [Trj]");
localArrayList.add("Android.Lijo.A");
localArrayList.add("AndroidOS/GenBl.147C189D!Olympus");
localArrayList.add("UnclassifiedMalware");
localArrayList.add("Android.SmsSend.730.origin");
localArrayList.add("a variant of Android/TrojanSMS.Agent.NB");
localArrayList.add("Trojan:Android/SmsSend.AE");
localArrayList.add("Android/SMSSend.AZ");
this.listView = ((ListView)findViewById(2131099653));
```

# Ransomware – Fake Avast! #3

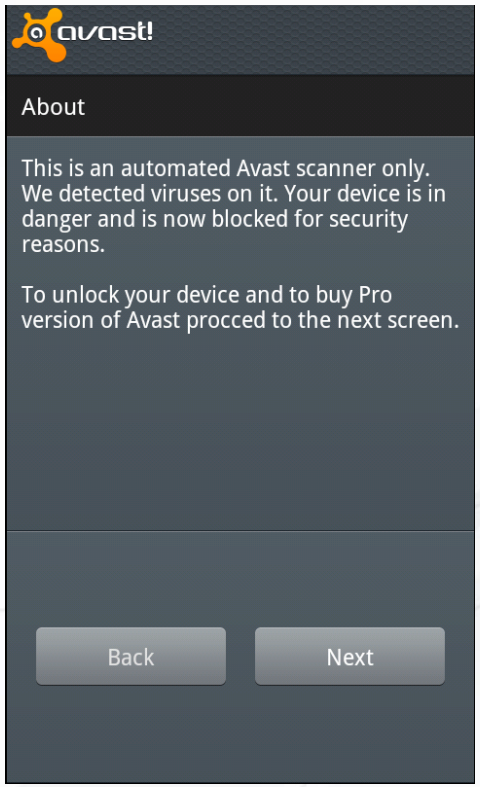
- Ukládá název a ID zařízení
- Vše odesílá informace na
  - tube8androidapp.net (184.75.254.73)
- Skrývá se za PornHub
- Mutace AndroidDefenderu
  - Pravděpodobně první FakeAv na Android

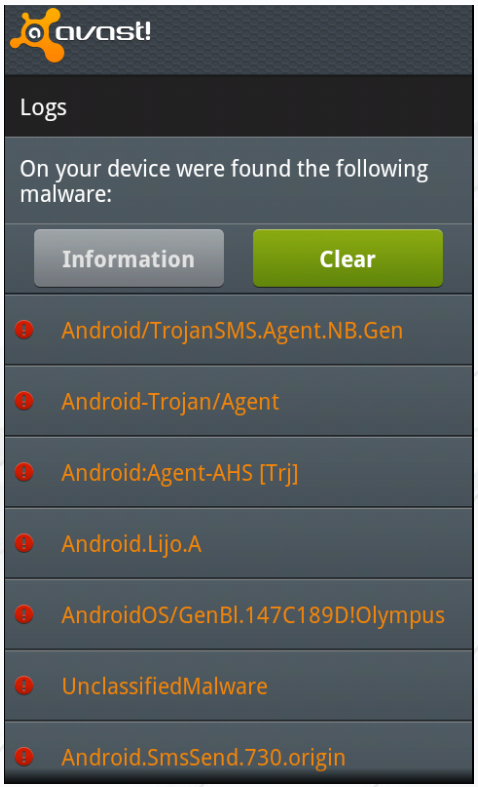
# Ransomware – Fake Avast! #4 screenshoty

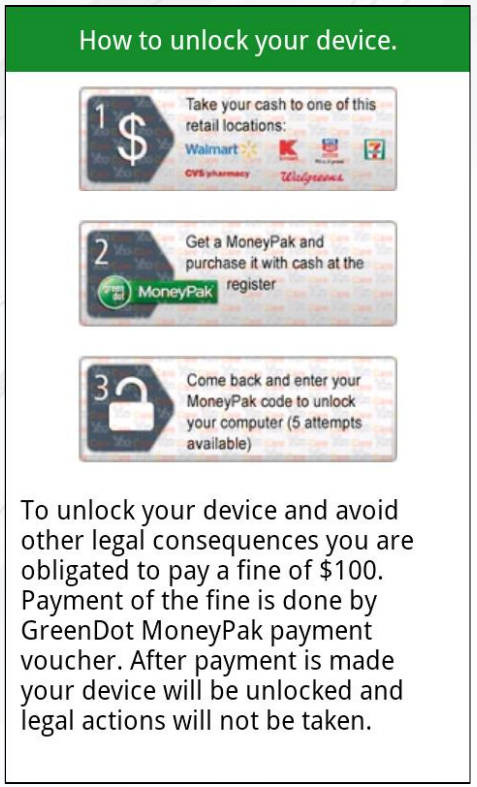



# Ransomware – Fake Avast! #5 screenshoty

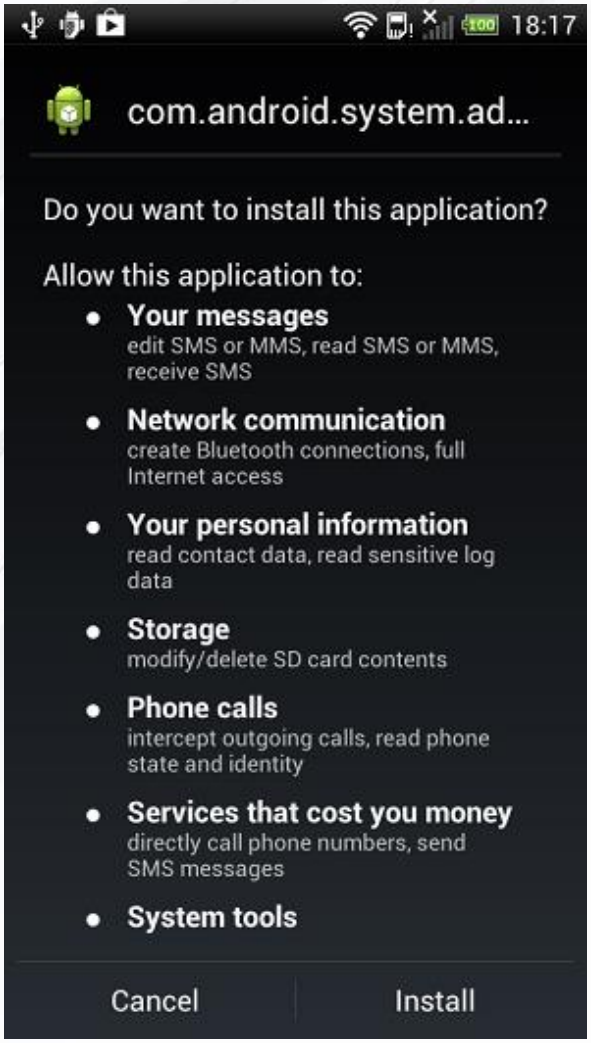


# Android:Obad #1

- Android:Obad
  - Objeven v polovině června 2013
  - Multifunkční Trojan
  - Device administrator
    - Dříve nebyla nikdy zneužita
  - Celý proces běží na pozadí
  - Skoro nemožné smazat



# Android:Obad #2

- Kompletně kryptovaný kód
- Malwarové chování
  - Zasílání placených SMS
  - Stahování a instalace dalších balíků
  - Možnost proxy serveru
  - Sběr dat o uživateli
- http://bit.ly/17TYxB9

# Android:Obad #3

- Požadavek na 24 oprávnění

```
xmlns:android="http://schemas.android.com/apk/res/android">
  <uses-sdk ="1" ="17" />
  <uses-permission ="android.permission.RECEIVE_BOOT_COMPLETED" />
  <uses-permission ="android.permission.READ_LOGS" />
  <uses-permission ="android.permission.WAKE_LOCK" />
  <uses-permission ="android.permission.READ_PHONE_STATE" />
  <uses-permission ="android.permission.PROCESS_OUTGOING_CALLS" />
  <uses-permission ="android.permission.READ_EXTERNAL_STORAGE" />
  <uses-permission ="android.permission.WRITE_EXTERNAL_STORAGE" />
  <uses-permission ="android.permission.ACCESS_WIFI_STATE" />
  <uses-permission ="android.permission.CHANGE_WIFI_STATE" />
  <uses-permission ="android.permission.ACCESS_NETWORK_STATE" />
  <uses-permission ="android.permission.CHANGE_NETWORK_STATE" />
  <uses-permission ="android.permission.MODIFY_PHONE_STATE" />
  <uses-permission ="android.permission.WRITE_SECURE_SETTINGS" />
  <uses-permission ="android.permission.WRITE_SETTINGS" />
  <uses-permission ="android.permission.INTERNET" />
  <uses-permission ="android.permission.BLUETOOTH" />
  <uses-permission ="android.permission.BLUETOOTH_ADMIN" />
  <uses-permission ="android.permission.ACCESS_BLUETOOTH_SHARE" />
  <uses-permission ="android.permission.RECEIVE_SMS" />
  <uses-permission ="android.permission.SEND_SMS" />
  <uses-permission ="android.permission.READ_SMS" />
  <uses-permission ="android.permission.WRITE_SMS" />
  <uses-permission ="android.permission.READ_CONTACTS" />
  <uses-permission ="android.permission.CALL_PHONE" />
  <application =".COcCccl">
      <activity ="System" =".CCOIoll">
```

# Android:Obad #4

- Administrátor zařízení
  - Novinka na poli Androidího Malware
  - Zajištění nemožnosti snadné odinstalace

```
<receiver ="System" =".OCllCoO" ="android.permission.BIND_DEVICE_ADMIN">
    <meta-data ="android.app.device_admin" ="@xml/ccclocc" />
    <intent-filter>
        <action android:name="com.strain.admin.DEVICE_ADMIN_ENABLED" />
    </intent-filter>
```

# Android:Obad #5

- Rozbalení .APK do Java Archive (JAR)
- Dex2Jar nejčastěji používaný decompiler
  - Využití chyby
  - Dalvik bytecode vs. Java bytecode http://bit.ly/PKmykf
  - Nemožnost použití
- Antiemulační triky

# Android:Obad #6

- Šifrování retězců
- Odkazy přes několik polí
  - Rozbalení
  - Rozdělení do několika dalších tříd
  - Znovurozbalení pomocí MD5
  - Rozbalení URL adresy
    - Androfox.com/load.php

```
{
  byte[] arrayOfByte1 = oCIlCll;
  int i = paramInt2 + 40;
  int j = paramInt1 + 75;
  byte[] arrayOfByte2 = new byte[i];
  int k = 0;
  int m;
  if (arrayOfByte1 == null)
    m = i;
  for (int n = paramInt3; ; n = arrayOfByte1[paramInt3])
  {
    paramInt3++;
    j = -4 + (m + n);
    arrayOfByte2[k] = (byte)j;
    k++;
    if (k >= i)
      return new String(arrayOfByte2, 0);
    m = j;
  }
```

# Android:Obad #7

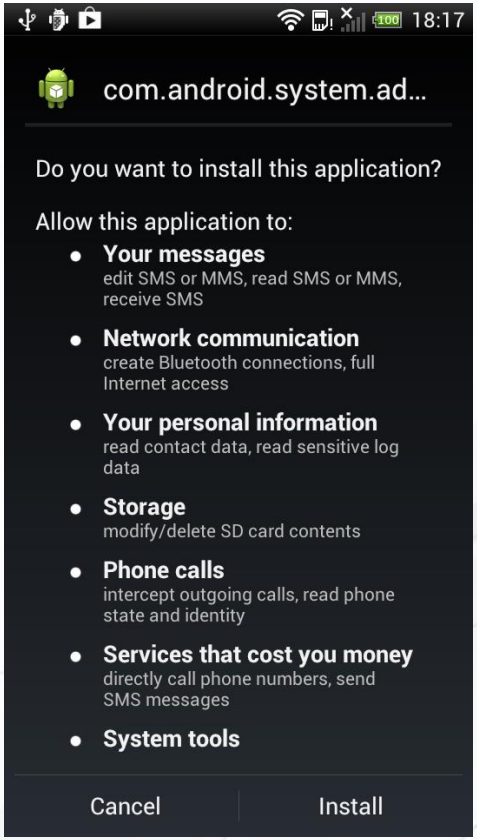
- Komunikace s tvůrci
  - IMEI, telefonní číslo, zůstatek u předplacené karty, oprávnění správce zařízení atd.
- Stažení infekčního balíku
  - Dešifrování
    - Využívá jako klíč část kódu ze stránek facebook.com


```
app":2,"bt_mac":0,"simOpName":"Beeline","numb":"********","task":{},"imei":"***************"
  "simCo":"Beeline","conf":{  "key_die":"",   "key_con":"",   "key_url":"",   "aoc_time":"30",
  "key_cip":"2585c63679df4994d58668f25f18f5de", "url":["http:\/\/www.androfox.com\/load.php",
  "http:\/\/www.androfox.tk\/load.php"]   }, "aoc":[], "balanceTime":1368813098158, "balance":"1200"
  "system":"no",  "time":1368813098158, "simOp":"Beeline", "netOp":"Beeline", "rooted":"no",
```

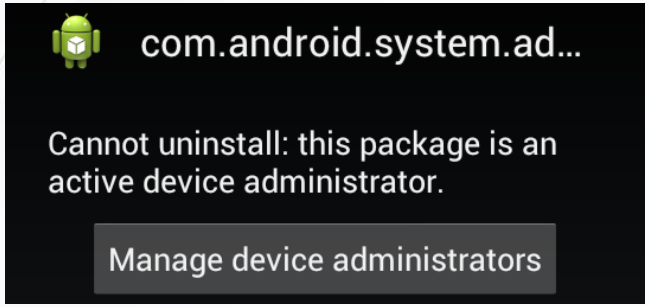
# Android:Obad #8

- Pravidelné navazování spojení se serverem a kontrola:
  - Odesílání textových zpráv
  - Kontrola zůstatku na účtu
  - Proxy
  - Otevírání adres
  - Stažení a instalace
  - Odesílání informací o telefonu
  - Vzdálené ovládání
  - Odeslání souborů přes BT

# Android:Obad #9 Screenshoty

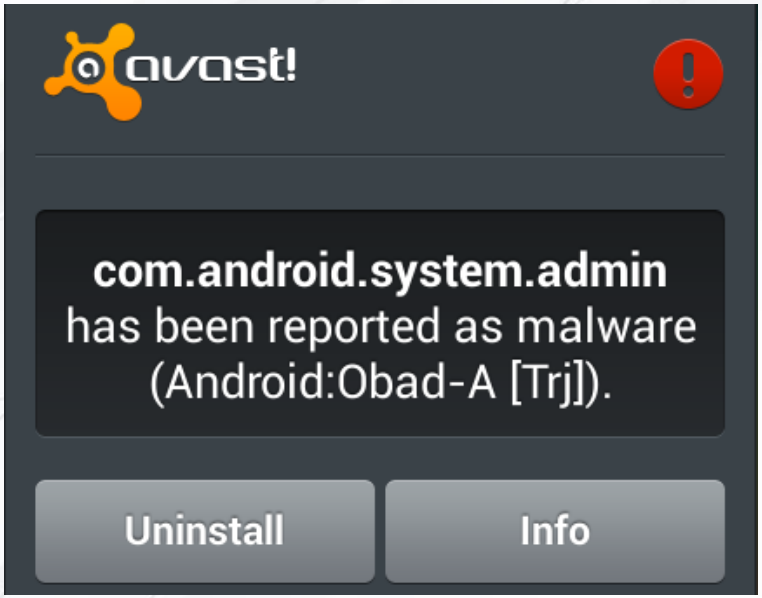






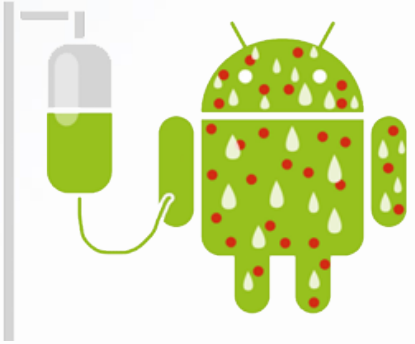
# Android:Obad #10 Jak se ho zbavit?

- **Jak se ho zbavit?**
  - Avast mobile security
  - Tovární nastavení
  - Další tooly



# CVE-2013-4787

- Android „Master key Vulnerability“
  - zneužití ověřovacího mechanismu
- Možnost zneužití od verze Androidu 1.6 a výše
  - Přibližně 1 miliarda zařízení
- Infekce jakýmkoliv kódem
- Google informován v únoru 2013



# CVE-2013-4787 – jak funguje ověření?

- Kde aplikace získává podpisy?
  Poskytuje je PackageManager
- Kde je získá PackageManager?
  Jako kopie podepsaného certifikátu
- Odkud pocházejí?
  Načteny po úspěšném ověření a instalaci aplikace
- Jak funguje ověřování?
  Všechny záznamy v APK jsou ověřeny podle Hashe

- http://bit.ly/16BZjUb

# CVE-2013-4787 – jak to funguje?

- Ověření a instalace krok po kroku
  - .APK balík
    - Dva soubory stejný název balíku a tříd, ale jiný „infikovaný“ zdrojový kód
    - Rozbalit .APK
    - Extrahovat soubory .dex
    - Vložit „infikovaný“ .dex soubor
    - Zabalit
    - THATS IT!

# CVE-2013-4787 – rizika?

- Šíření přes oficiální markety Google Play
- Infikování aplikace s vysokými právy
  - Například Cisco AnyConnect
  - Ztráta a krádež dat
  - Zasílání placených SMS
  - Kompromitace firemních dat

# Hesperbot #1

- Objeven v září 2013
- Multiplatformní bankovní Trojan
- Hlavní výskyt Turecko, Česká republika
- Spy, Phishing, Spam
- cpost@ceskaposta.net
- zasilka.pdf.exe
- http://bit.ly/15DI25P

# Hesperbot #2

- Sledování zásilky
- Kontrola OS zařízení
- SMS obsahující URL na .APK
- Transaction authentication number - TAN
- Čekání na SMS
- Vzdálené řízení
- VNC

# BYOD – „Bring Your Own Device“

- Kompromitování firemní sítě
  - Zaměstnanci dostávají a nebo si nosí vlastní zařízení
    - Skoro nemožné hlídat bezpečnost
- Náhodné ztráty dat
- Cílené útoky
  - Nahrávání
  - Krádeže dat
  - Krádeže přístupových údajů

# BYOD – krok za krokem

- Co chceme bránit a proč?
- Kdy a kde se může útok stát?
- Máme dostatečnou ochranu?
- Jaká jsou rizika?

# BYOD - Co chceme bránit a proč?

- Jaké data/majetek stojí za to chránit?
- Jaký bude dopad?
  - Data, peníze, soukromí, hesla
  - Transakce a procesy
  - Inovace, algoritmy
  - Pověst, důvěra zákazníků
  - Zdroje

# Kdy a kde se může útok stát?

- Na co se nejčastěji cíli?
  - Datová uložiště
  - Připojení k back-end serverům
  - Připojení ke službám třetích stran
  - Infikovaný uživatel
  - Web browsery a exploity
  - Komponenty třetích stran

# Máme dostatečnou ochranu?

- Hlavní útoky na mobilní zařízení
  - Únik dat vyplývající ze ztráty nebo krádeže zařízení
  - Neúmyslné zpřístupnění údajů
  - Zneužití vyřazených smartphonů
  - Phishing útoky
  - Spyware útoky
  - Finanční útoky škodlivého softwaru

* http://bit.ly/Rk8mhg
zdroj: European Network and information Security Agency (ENISA)

# BYOD – modelový příklad

- Nezodpovědný zaměstnanec
- Mobilní přístroj neustále sebou
- Obsahuje firemní data
- Trvale online
- Občas stáhne aplikace z neověřených zdrojů
- Ztratí telefon jednou ročně
- Heslo: 123456789

# Kdo mi ukradl telefon?

# BYOD - jak bránit firemní data?

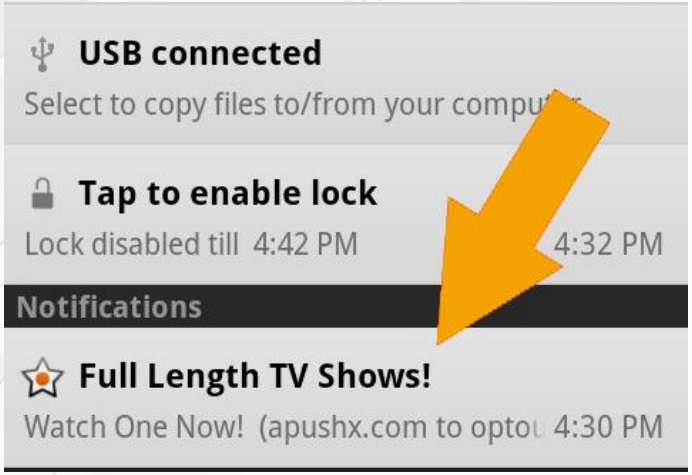
- Mobile-device-management
  - Červenec 2013 – Google management
  - Možnost vzdálené správy telefonu
  - Mazání dat
  - Vzdálená správa
  - Avast AntiTheft!
    - I pro soukromé účely

# Avast AntiTheft 3.0

- BackUp vašich dat
- Geofence
- Zamknout/Odemknout
- Získat data
- Vyfotit zloděje
- Spustit Alarm
- Zjistit polohu

# ADS – reklamní aplikace

- Reklamní aplikace
  - Většina z nich je legální
  - Add-ons doplněk legitimních aplikací
  - Mohou být pěkně otravné
    - In app reklamy
    - Out app reklamy
  - Většinou v bezplatných aplikacích



# NFC – potencionální hrozba? #1

- Prudce se rozšiřující „novinka“ posledních let
- Google wallet
- Komerční banka, ČSOB a jiné...
- Potencionální rizika
  - Stažení nežádoucího balíčku
  - Zachycení přenosu
  - Manipulace s daty

# NFC #2

- Tag ID (hex): f5 cc e1 cf
- Tag ID (dec): 5873256342
- ID (reversed): 908458166
- Technologies: IsoDep, MifareClassic, NfcA, NdefFormatable
- Mifare Classic type: Classic
- Mifare size: 1024 bytes
- Mifare sectors: 16
- Mifare blocks: 64

# NFC – zneužití v praxi? #3

- Vzdálenost v řádu centimetrů
- Odeslání krátkého tagu
- Využití zranitelnosti
- Při větším balíčku spojení přes BlueTooth
- Vzdálené ovládání

# Jak se bránit infekci?

- Používat jen originální markety!
  - Ani to ovšem není 100% řešení.
- Kontrolovat práva aplikací
- Nastavení BYOD politiky
- Používat Antivirus

# Avast! mobile security #1

- Jeden z nejvíce používaných AV na světě
- Nejlepší skóre na Google Play ze všech AV
- Jeden z nejlepších podle nezávislých AV testerů - http://bit.ly/14k9Zkh
- Obsahuje Avast Anti-Theft zdarma
  - Vzdálené řízení telefonu My Avast! Account
  - Sledovat, blokovat, vymazat telefon

# Q&Mailwk

Questions & Maybe answers if I will know

Otázky & možná odpovědi

Filip Chytrý
chytry@avast.com
Malware Analyst
http://blog.avast.com/author/chytry/