RE Android

Základy reverzného inžinierstva

How to reverse Android malware ?

1 First glance matters
- Are they trying to hide something ?
- What's the name of the package?
- What does the certificate say?
- Where did I find it ?

2 Disassemble it

The code says it all !
Don't be lazy 

and read it in depth.

3 Still don't understand ?

Run it in an emulator, display logs and capture network traffic.

Never use your own phone.
Do not provide any personal data (name, IMEI, phone number...)

THE CODE DOES NOT MAKE SENSE ?

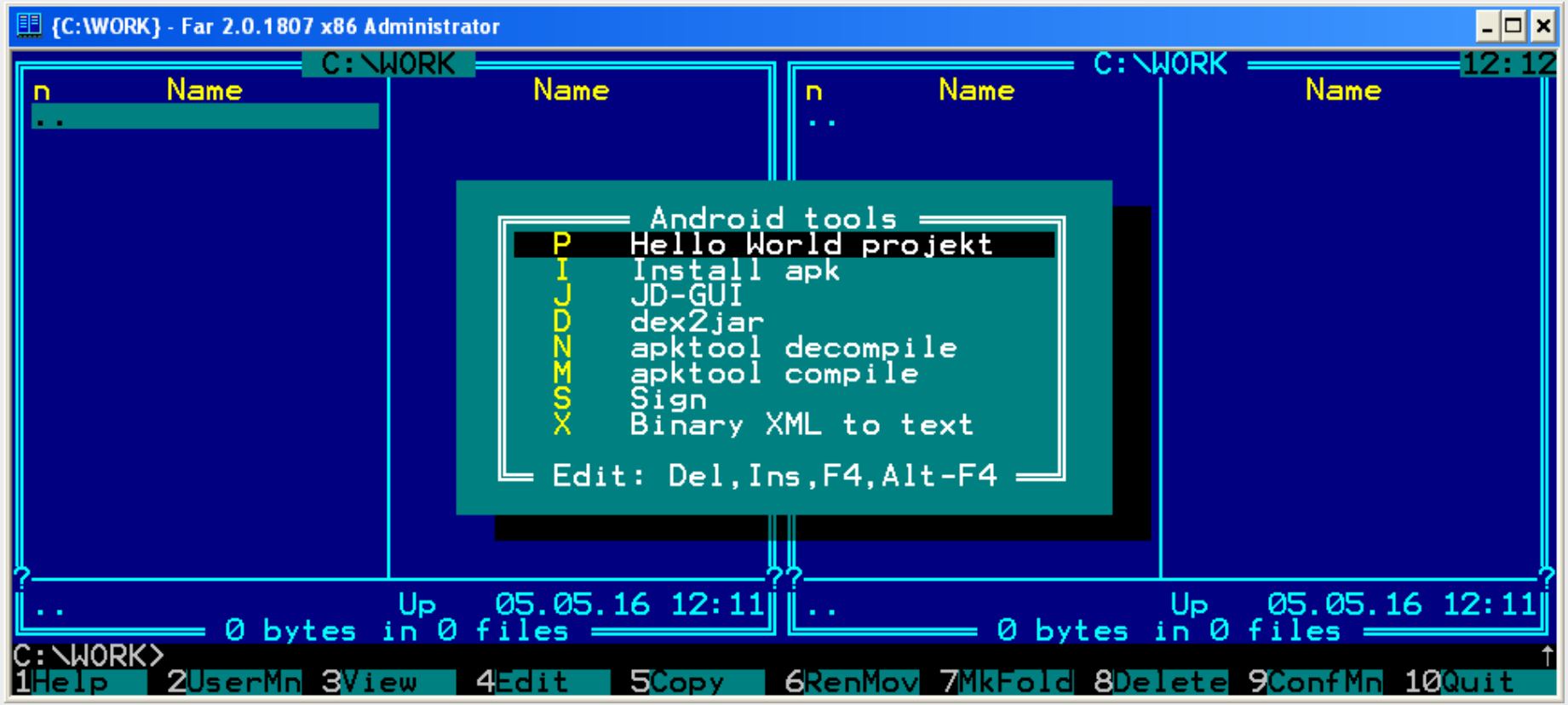
Maybe it's heavily obfuscated or packed.

THERE'S NOTHING SUSPICIOUS ?!

Good ☺ Check the assets and resources directory for Javascript or ARM executables.

@cryptax
2016

RE – nástroje



RE – nástroje

Android SDK

- adb
  - základný nástroj pre ladenie Android zariadenia
- android
  - Android SDK Manager
- monitor
  - Android Device Monitor
- zipalign
  - Optimalizačný nástroj na „zarovnanie“ archívneho súboru .apk
- Aapt
  - Android Asset Packaging Tool – výpis relevantných info z .apk
- logcat

RE – nástroje

Java JDK

- keytool

  Generovanie / spravovanie certifikátov, verejného / privátneho kľúča.

- jarsigner

  Podpisovanie a overovanie podpisu.

RE – nástroje

Nástroje tretích strán

- Apktool

  https://ibotpeaches.github.io/Apktool/
- BinXML to Text

  Konverzia
- backsmali / smali

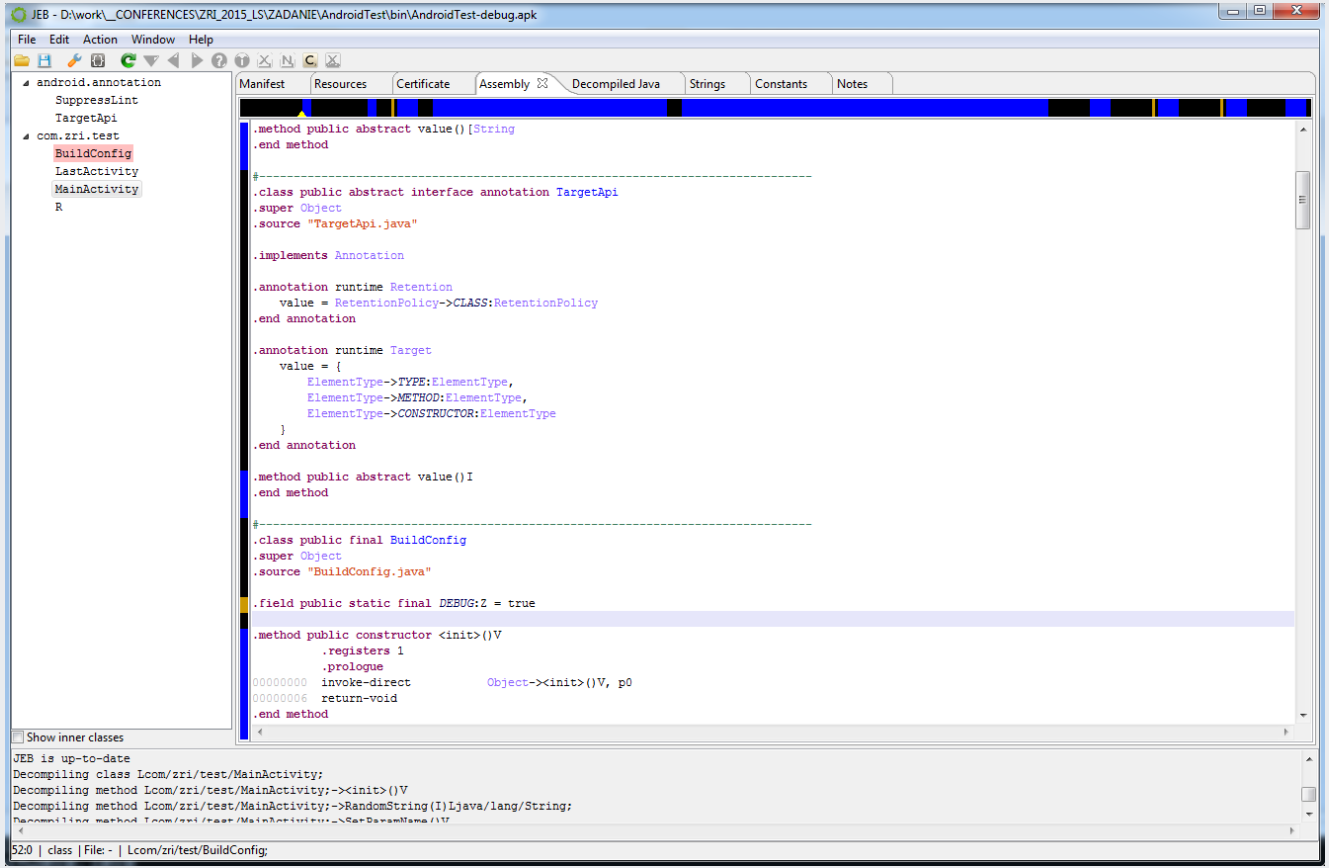
  Vytiahnutie smali kódu z dex súboru a naopak
- DexToJar

  Pomocný prepis do pseudo java zdrovojého kódu
- JD-GUI

  Java Decompiler
- Unzip

RE – advanced tools

- IDA
- JEB
- VTS



Android zadanie – Vypíš dekryptovaný text!

Android zadanie

- Vyhľadanie / stiahnutie apk do pc; na základe názvu package **2b**
- Rozbalenie, dekompilácia, zisti entry-point (Activity) **2b**
- Spustenie aplikácie cez adb, logcat s najdeným tagom **2b**
- Spustenie aplikacie so správnym názvom parametru + hodnota parametru = krsné meno **2b (3b)**
- Splniť podmienku na dekryptovanie textu (prebalenie apk) **2b (3b)**
- Vložiť výpis dekryptovaného textu (prebalenie apk) **3b**

Zadanie slúži aj ako praktická ukážka reverzovania Android aplikácií

Android zadanie – Vypíš dekryptovaný text!

1. adb shell dumpsys package
2. adb pull
3. FAR; Shift+F2 (unzip)
4. FAR; F2+A+X(BinXML2Text)
5. Nájdem “entry-point” Activity
6. FAR; F2+A+D (dexToJar)
7. FAR; F2+A+J (JD-GUI)
8. Statická analýza + vyhľadanie Log tagu
9. adb shell am start –n
10. adb logcat –s

Android zadanie – Vypíš dekryptovaný text!

11. adb shell am start –n ... –e
12. apktool d XXX.apk
13. Upraviť LastActivity.smali
14. apktool b XXX
15. jarsigner (heslo:android)
16. adb uninstall com.zri.test
17. FAR; F2+A+I (install apk)
18. adb shell am start –n
19. adb shell am start –n …–e

Android zadanie – Vypíš dekryptovaný text!

Živá ukážka

Modularita

Hlavná časť

- Obsahuje všetky potrebné permissions
- Má prístup na internet
- Dokáže spúšťať program z externého zdroja (DexClassLoader) / modul

Prídavné moduly

- Vopred neznámy zdroj
- Obsahuje škodlivý kód (bez permissions)

Modularita

Živá ukážka

Obfuskácia

- Zmena názvu tried a metód

  Vo večšine prípadov sú názvy tvorené jedným písmenom
- Nadbytočné prázdne triedy a metódy

  Zreťazenie vzájomného volania „prázdnych“ metód.
- Parametrické volanie tied

  Metóda invoke prijíma ako parameter názov volanej metódy a jej parametre

Obfuskácia

Živá ukážka

DexProtector

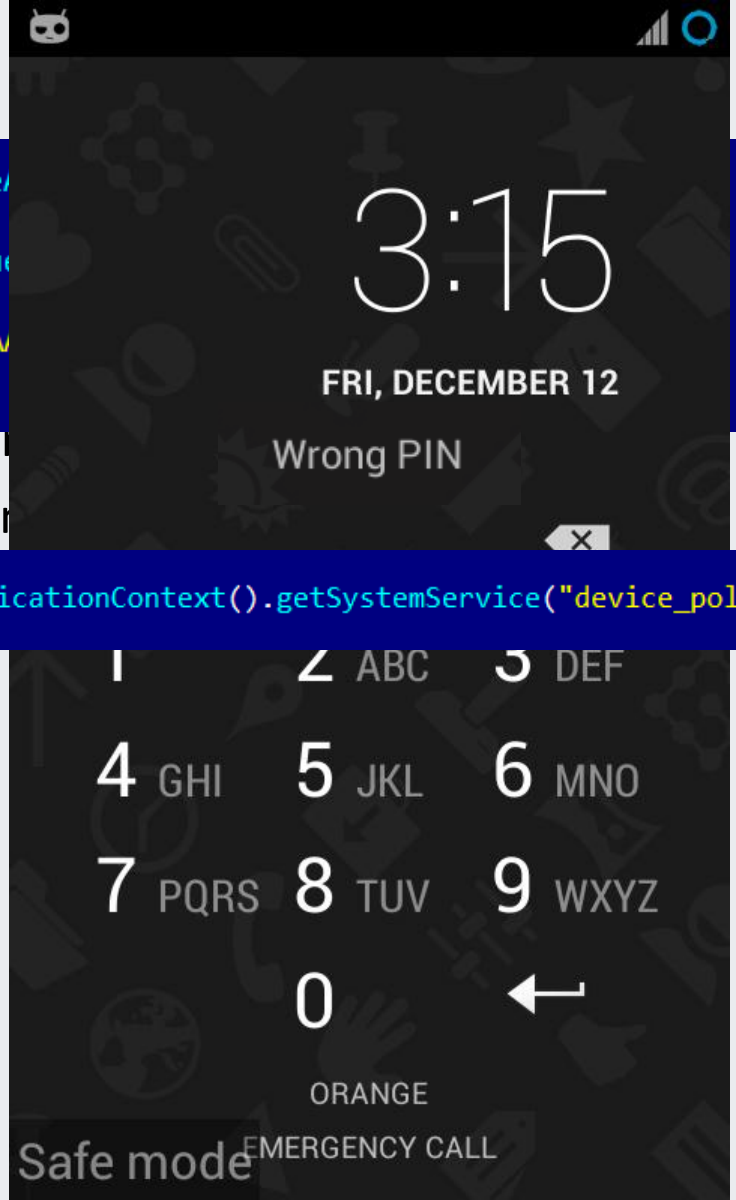
DexProtector 672,60 €

Hard

```
public class Device
    public CharSequ
    {
        return "WHA
    }
```

```
Intent intent)
```

1. A
2. N
3. Nastavit PIN kód
4. Vypnutý debuggi




```
((DevicePolicyManager)this.getApplicationContext().getSystemService("device_policy")).resetPassword("1234", 0);
```

EOF