AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Building a Test Environment for Android Anti-Malware Tests

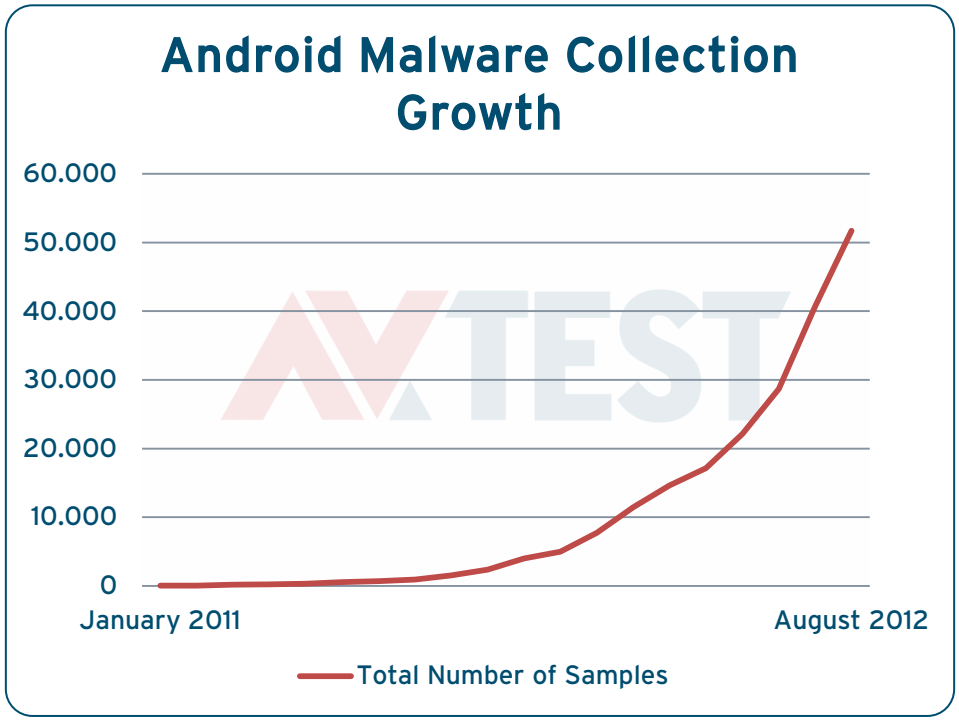
Hendrik Pilz
Director Technical Lab / Mobile Security
hpilz@av-test.de

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Agenda

- Android Malware Landscape
- Real Devices or Emulator?
- Preparation
- Test Scenarios
- Automation
- Problems

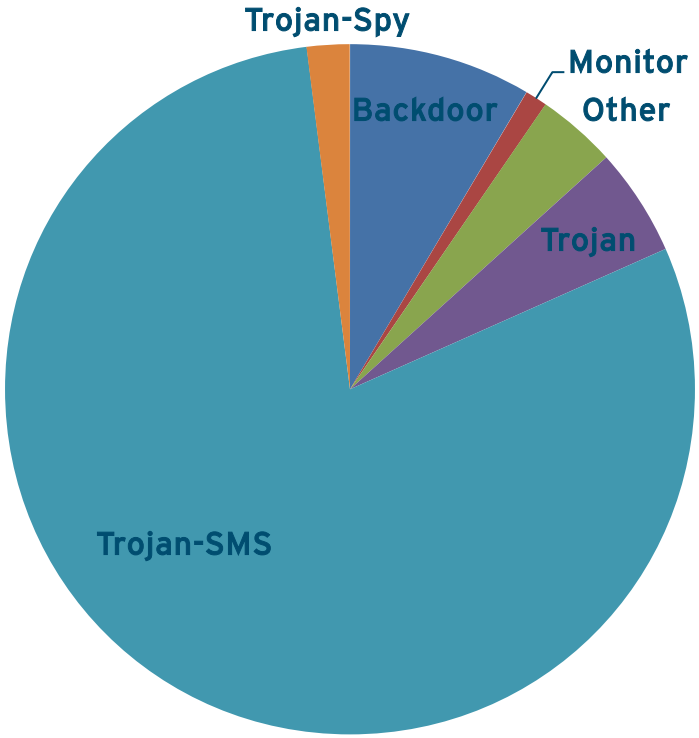
Android Malware Landscape



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Android Malware Landscape

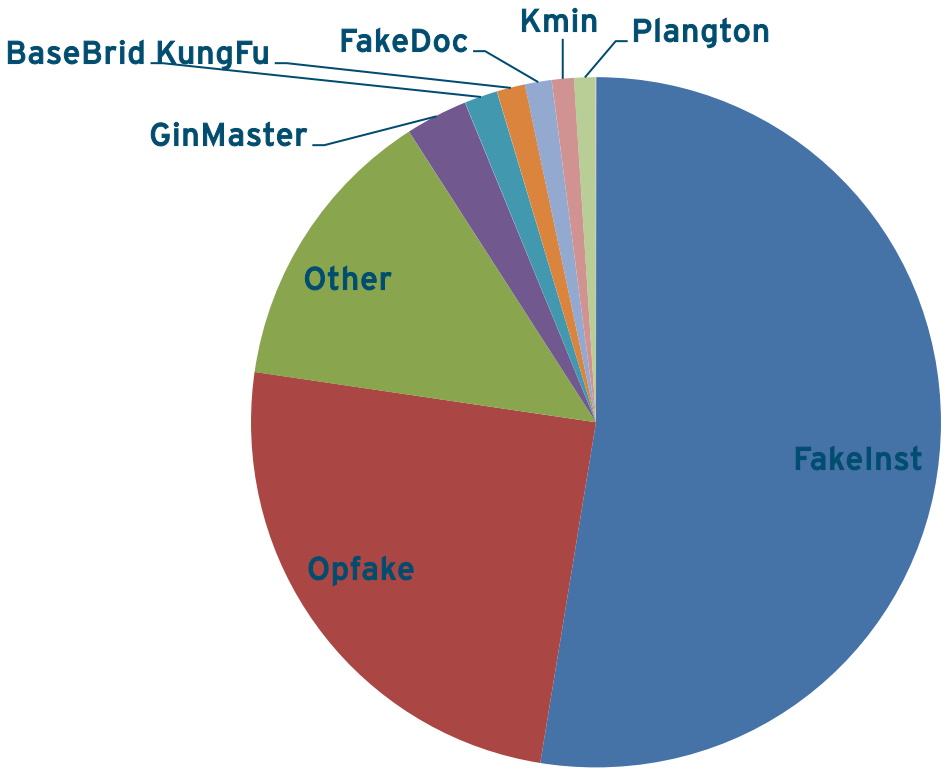
Malware Categories August 2012



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Android Malware Landscape

Malware Families August 2012



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Real Devices or Emulator

Device

- Real user experience
- App activation via SMS
- Real life environment

Emulator

- Cost efficient, scalable
- Root privileges
- Multiple API versions and hardware configurations
- Snapshots

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Preparation

System Requirements:

- PC which is capable to run the Android SDK
- Android device, prepaid SIM
- USB cable
- WiFi-Internet for Android device

Preparation

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Preparation

- Install Android SDK from developer.android.com/sdk
- Choose Malware Samples according to AMTSO Guidelines
- Install Anti-Malware on test device, update signatures

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Preparation

- **Connect device to PC**
- **Create device backup**

```
$: adb backup -f <file> -apk -shared -all -system
$: adb restore <file>
```

- **Take Screenshots**

```
$: android-sdk/tools/ddms
```

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Demand Scan

- **Copy samples to device**
  `$: adb push <source> /sdcard/samples`
- **Perform on-demand scan, delete all malicious files**
- **Save remaining files**
  `$: adb pull /sdcard/samples <dest>`
- **Save scan reports, if possible**

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Demand Scan

Alternative to `adb push/pull`:

Copy files over WiFi from/to network share (e.g. with Astro File Manager)

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Demand Scan

Some Anti-Malware apps scan installed apps only!

An On-Access Test is always required to determine accurate detection rates!

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Access

- Install each sample one-by-one
  `$: adb install <apk-file>`
- Check warnings and messages of Mobile Security
- Remove or uninstall sample
  `$: adb uninstall <package-name>`

Test Scenarios – On-Access

on-access.sh

```
#!/bin/bash

c=1
# traverse sample directory
for i in `ls $1`
do
        sample="${1}/${i}"
        echo "${c}: Installing ${i}"
        # get android package name
        package=`aapt dump badging ${sample} |\
        grep package: | sed "s/package: name='//" |\
        sed "s/' versionCode.*$//"`
        echo "Package: ${package}"
        # install, enter result, uninstall
        adb install ${sample}
        echo "Was the sample detected? (1 - yes / 0 - no)"
        read result
        echo -e "${sample}\t${result}" >> "on_access_report.txt"
        adb uninstall $package
        let c=c+1
done
```

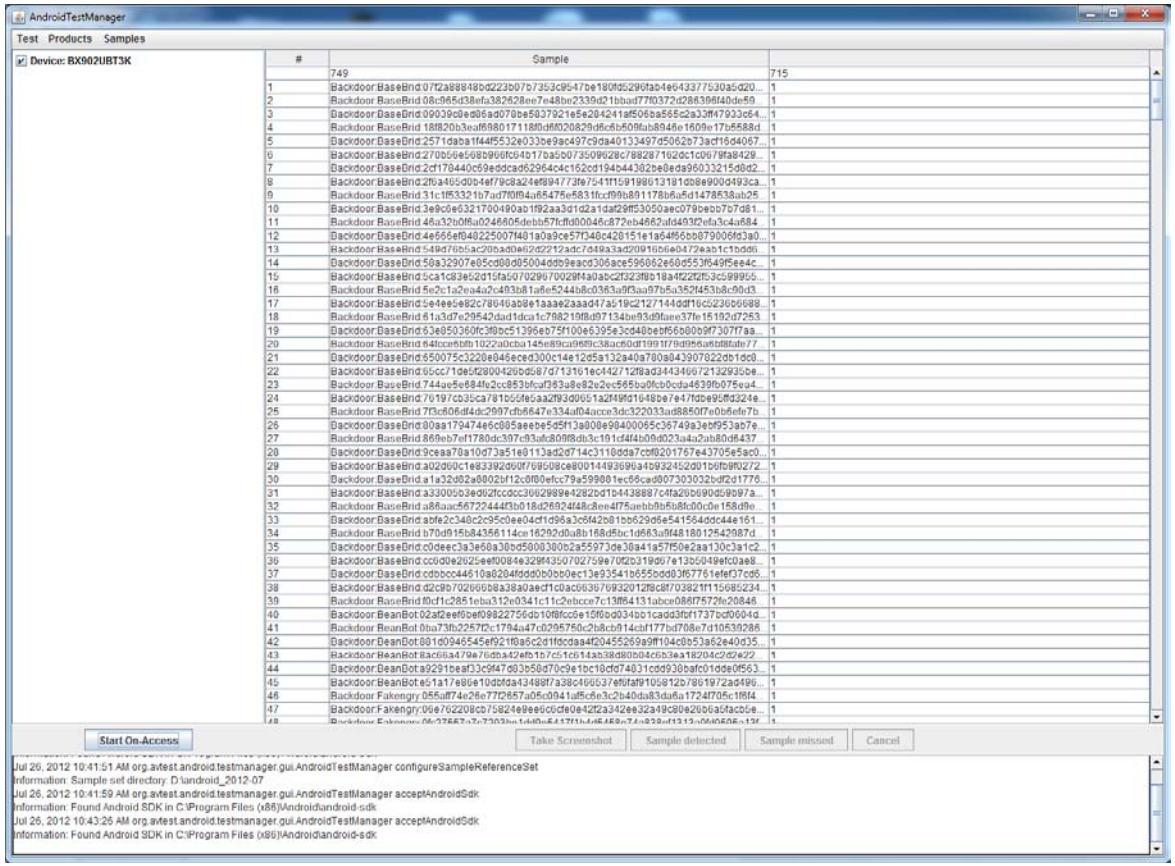
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Access

```
android@android-VirtualBox:~$ on-access.sh /media/android/
1: Installing 00a9677cd438dd8b3b3320ad45562d409b929e33587ed7211356d40477725dfc.apk
Package: com.keji.danti34
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
415 KB/s (923684 bytes in 2.168s)
        pkg: /data/local/tmp/00a9677cd438dd8b3b3320ad45562d409b929e33587ed7211356d40477
725dfc.apk
Success
Was the sample detected? (1 - yes / 0 - no)
1
Success
2: Installing 0153e70bb3573e3fa701e307ae8a5b1b5d2ad72e2339b75acf5770cfda0c9a60.apk
Package: com.keji.Graphisa
422 KB/s (10997244 bytes in 25.399s)
        pkg: /data/local/tmp/0153e70bb3573e3fa701e307ae8a5b1b5d2ad72e2339b75acf5770cfda
0c9a60.apk
Success
Was the sample detected? (1 - yes / 0 - no)
1
```

The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – On-Access



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – False Positives

- Combination of OA & OD
- Install clean apps via ADB
- Run an OD-scan afterwards
- Note all warnings and detections

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – False Positives

- Be aware of greyware:
  - Ad supported apps
  - Privacy risks

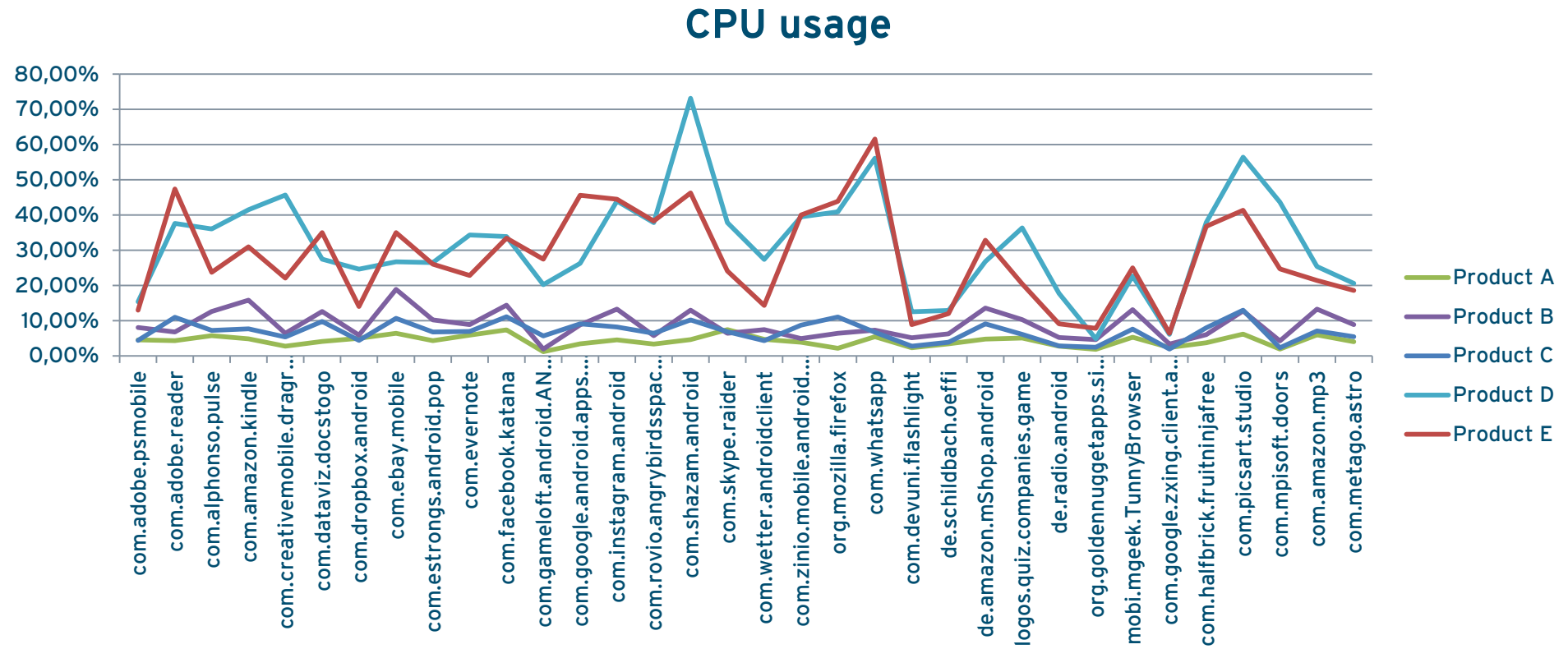
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – Performance

- Install clean apps from Google Play
  - We can‘t use ADB here, because we can‘t disable USB charging
- Monitor CPU-usage and battery discharge
- Repeat several times

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

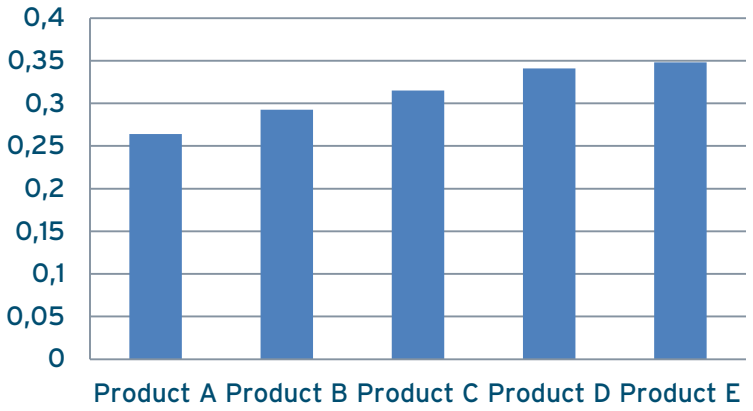
Test Scenarios – Performance



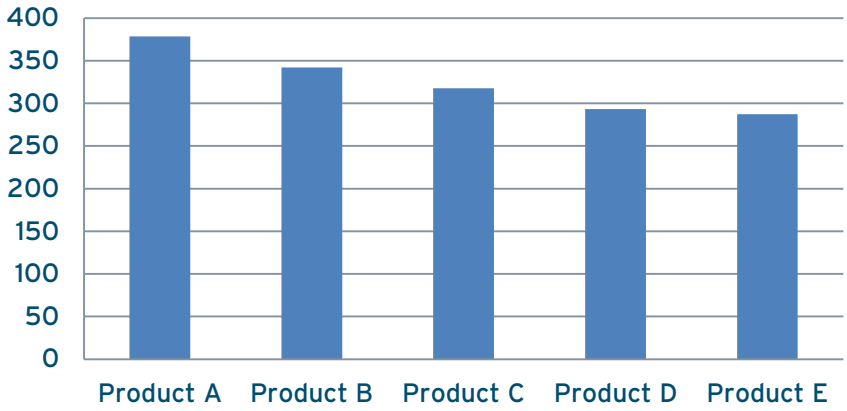
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – Performance

Discharge rate in % per minute



Estimated battery life in minutes



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – Performance

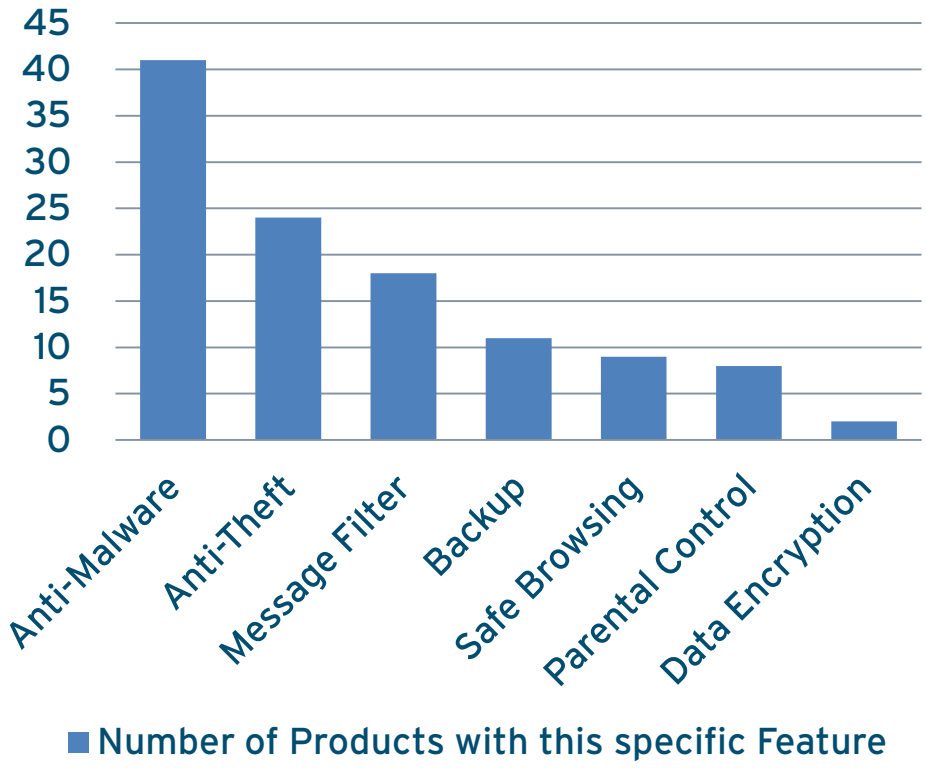
- Measure impact on real-world usage
  - Loading websites
  - Sending/receiving messages
  - Opening apps
  - Playing media files
  - …

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Test Scenarios – Others?

- Other functions are not common among all AV/mobile security products:
  - Anti-Theft
  - Backup, Encryption
  - Spam, Phishing
  - …

Test Scenarios – Others?



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Automation

- ADB-CLI
- ddmlib.jar (included in SDK)
  - High Level API to control ADB
- Robotium <http://code.google.com/p/robotium/>
  - GUI automation of Android apps

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Problems

- Not all apps support SD card scan
- No proper reporting
- No export of report files

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Thank You!

Questions?