AndroTotal

A Scalable Framework for Android Antivirus Testing

Joint work with Andrea Valdi (MSc) and Stefano Zanero (PhD)

Federico Maggi

federico@maggi.cc

Politecnico di Milano

Who I am

POLITECNICO
DI MILANO

Federico Maggi, PhD

Post-doctoral Researcher

NECST laboratory

Topics

Android malware, botnet detection, web measurements

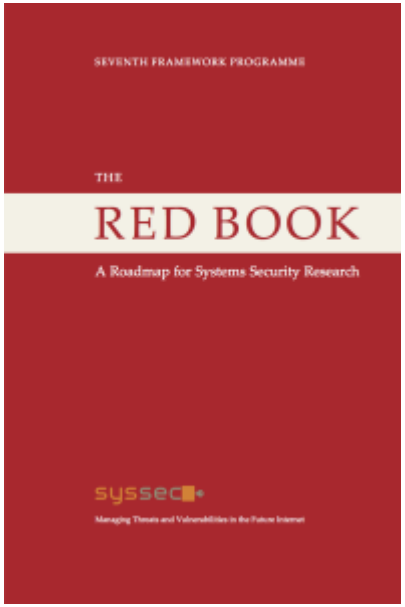
Background

Intrusion detection, anomaly detection

www.red-book.eu

The RED BOOK

A Roadmap for Systems Security Research



Free PDF

Audience

Policy makers

Researchers

Journalists

Content

Vulnerabilities

Social Networks

Critical Infrastructure

Mobile Devices

Malware

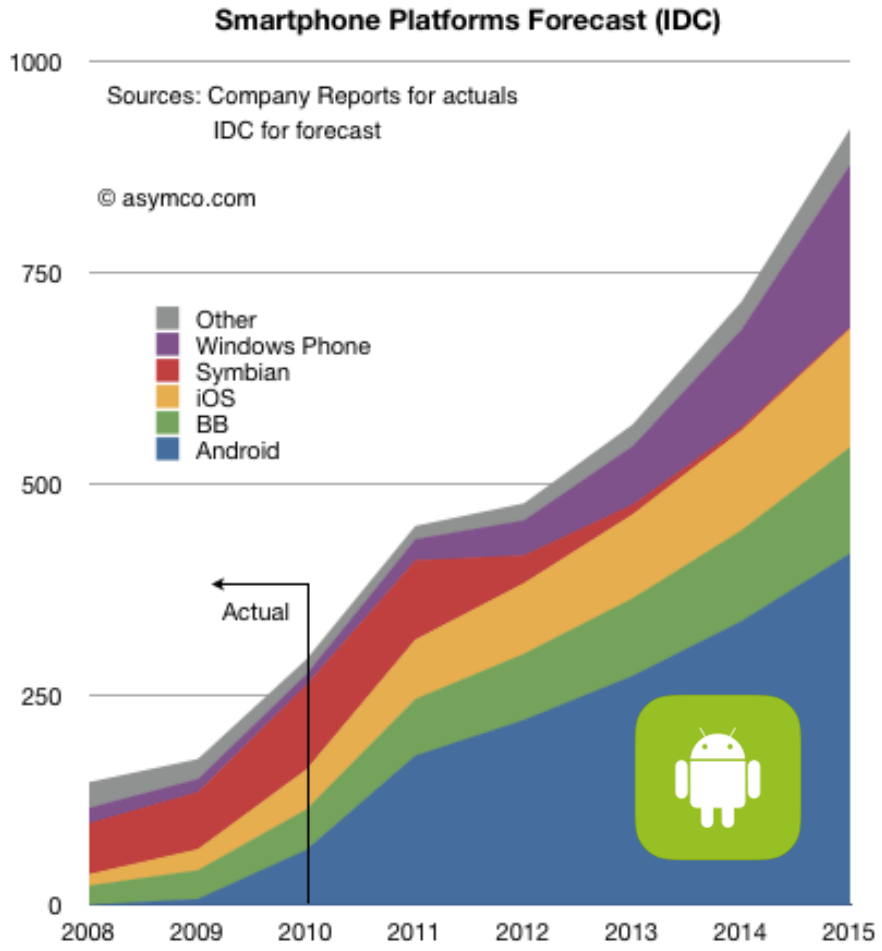
. . .

Roadmap

1. Android threats and protections
2. Limitations
3. Testing antivirus apps
4. AndroTotal
5. Status

1. **Android threats and protections**
2. Limitations
3. Testing antivirus apps
4. AndroTotal
5. Status

Android beats them all

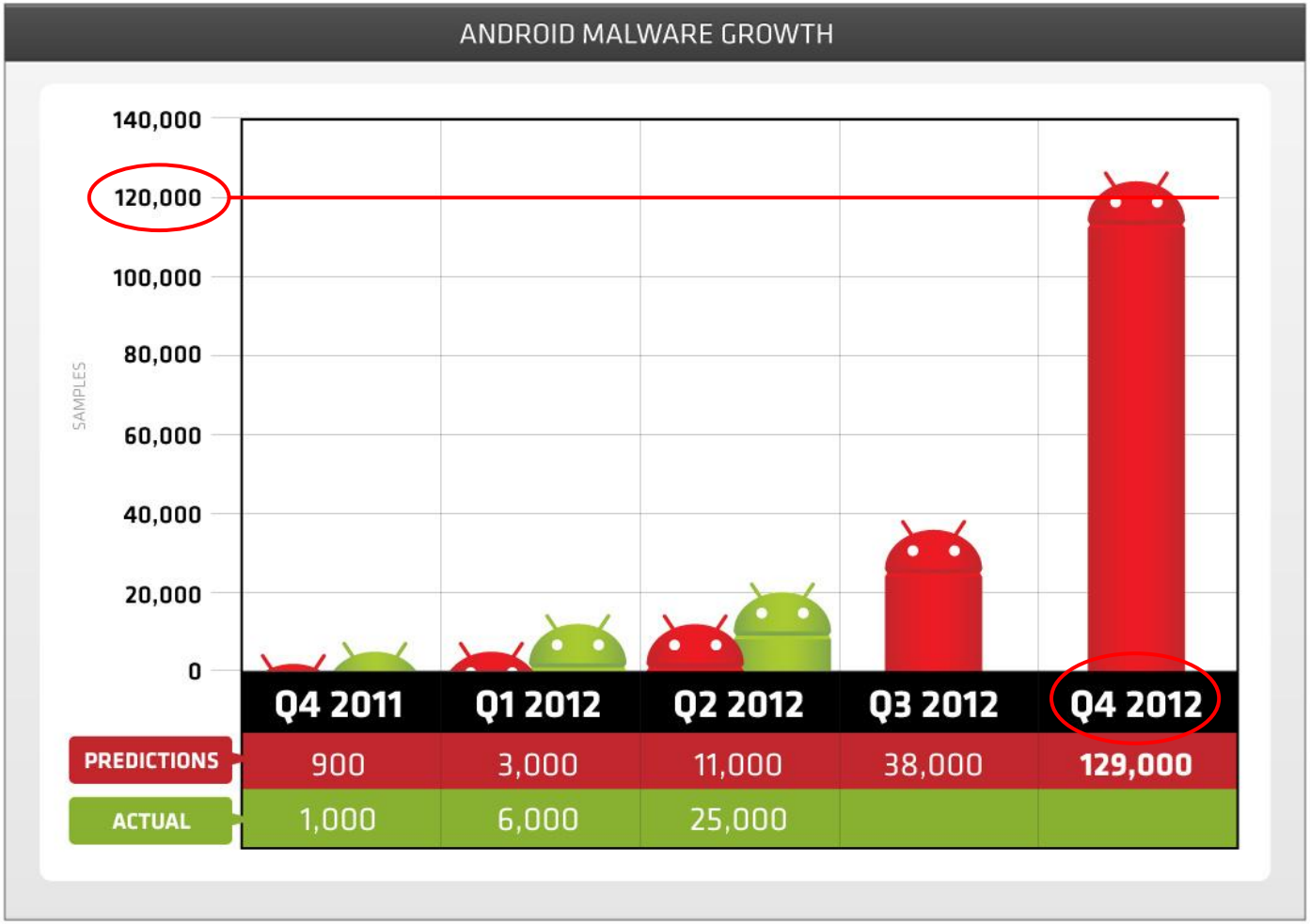


July 2013

- 79% market share
- 1,000,000 official apps
- ~90 alternative stores

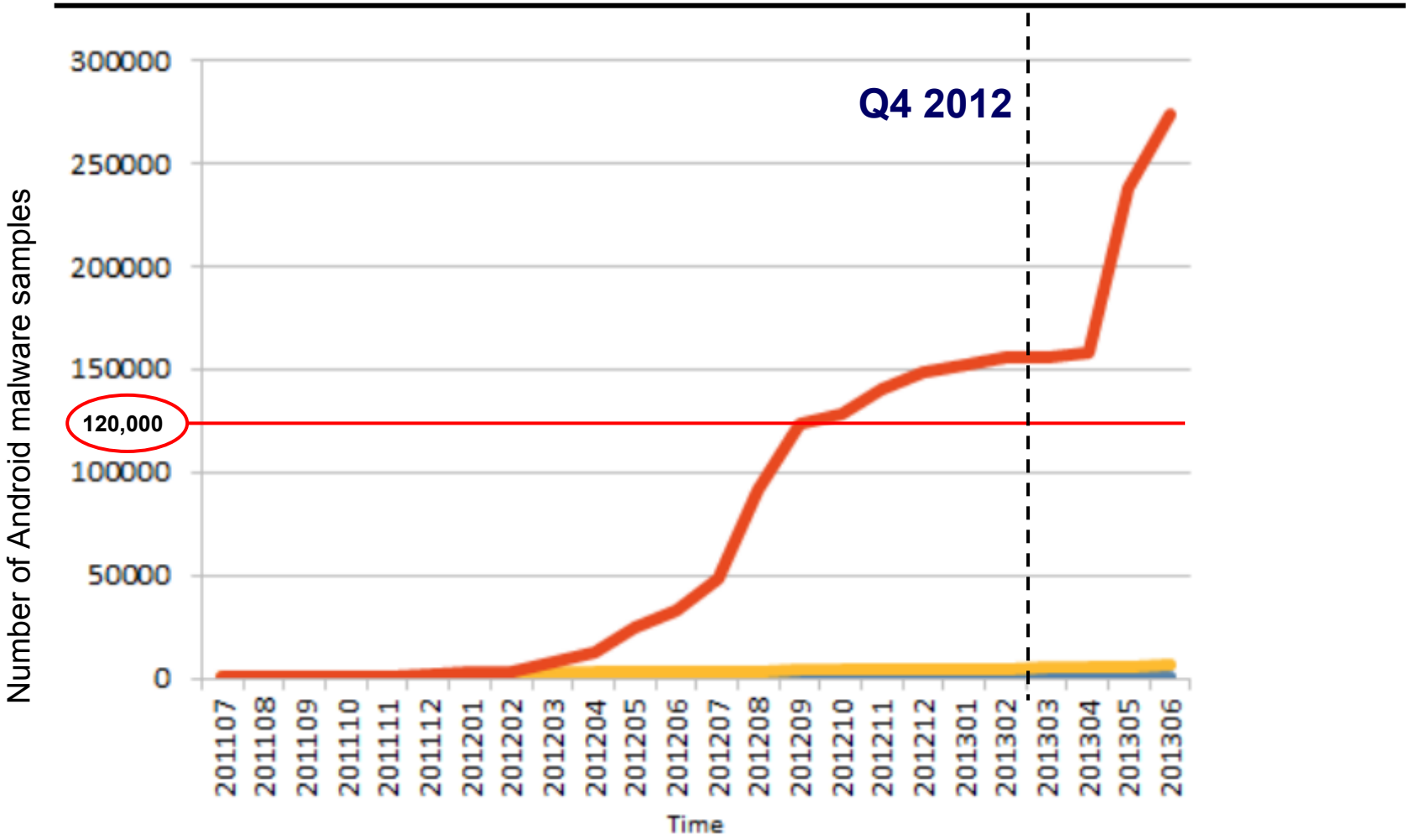
Popularity = Security Risks

Number of Android malware samples



Source (Trend Micro, Q2 2012)

Popularity = Security Risks



Source (Symantec, October 2013)

Attackers goals

Steal sensitive data

- intercept texts or calls
- steal passwords

Turn devices into bots

- perform malicious actions

Financial gain

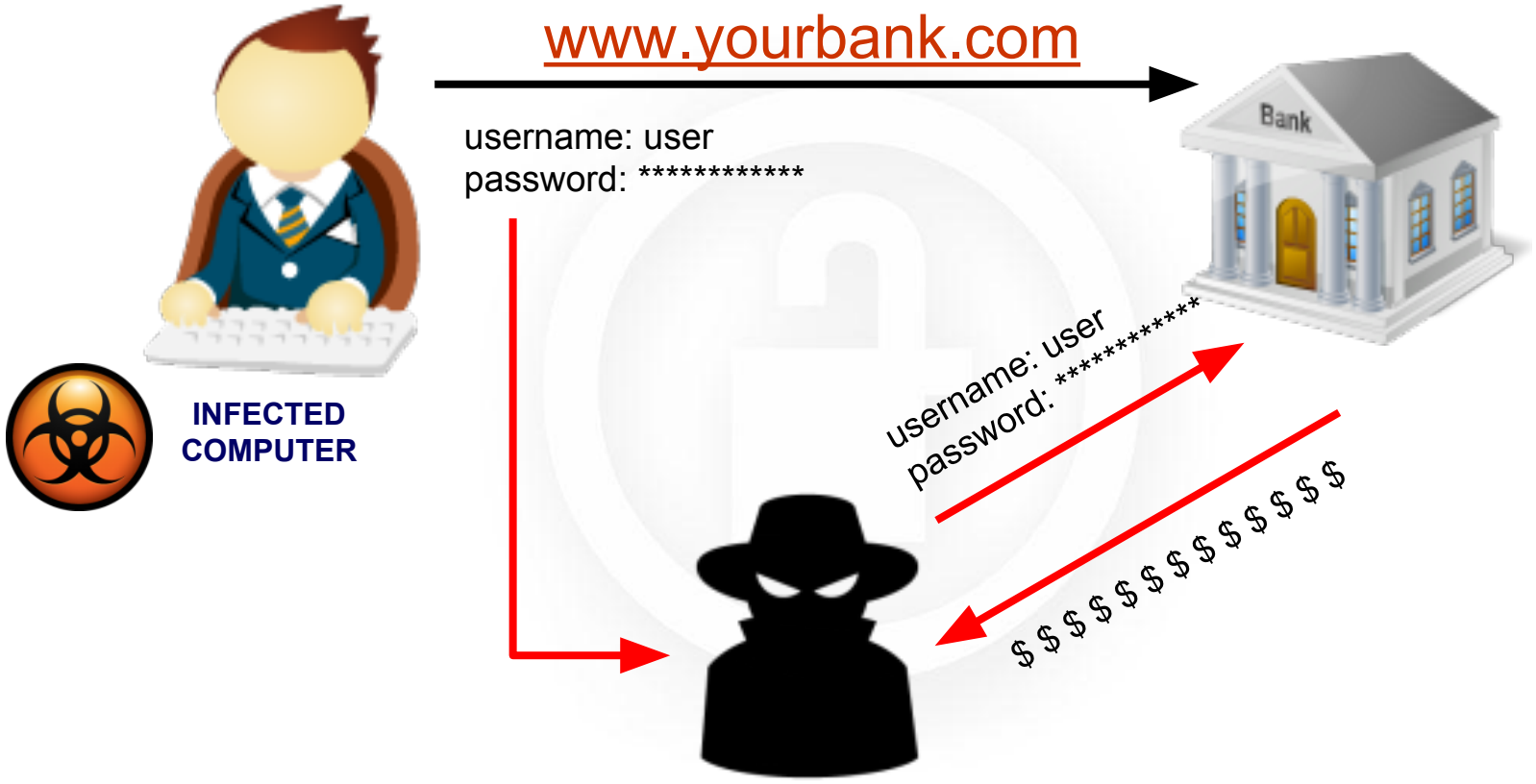
- call or text premium numbers
- steal online banking credentials

EXAMPLE

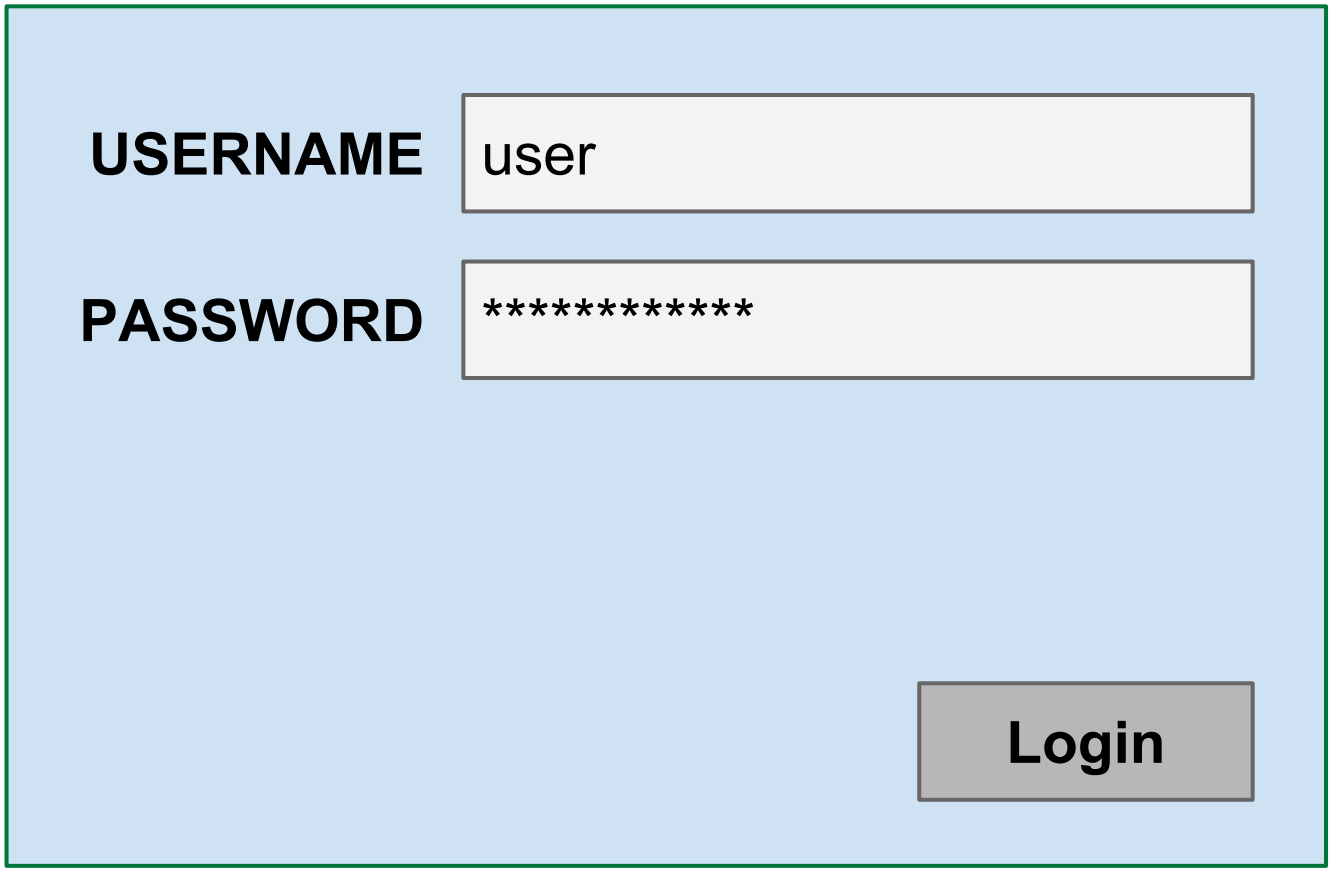
Perkele (Android malware kit)

- Sold for $1,000 on underground markets
- Dev kit for bypassing 2-factor authentication

The attack scheme (1)

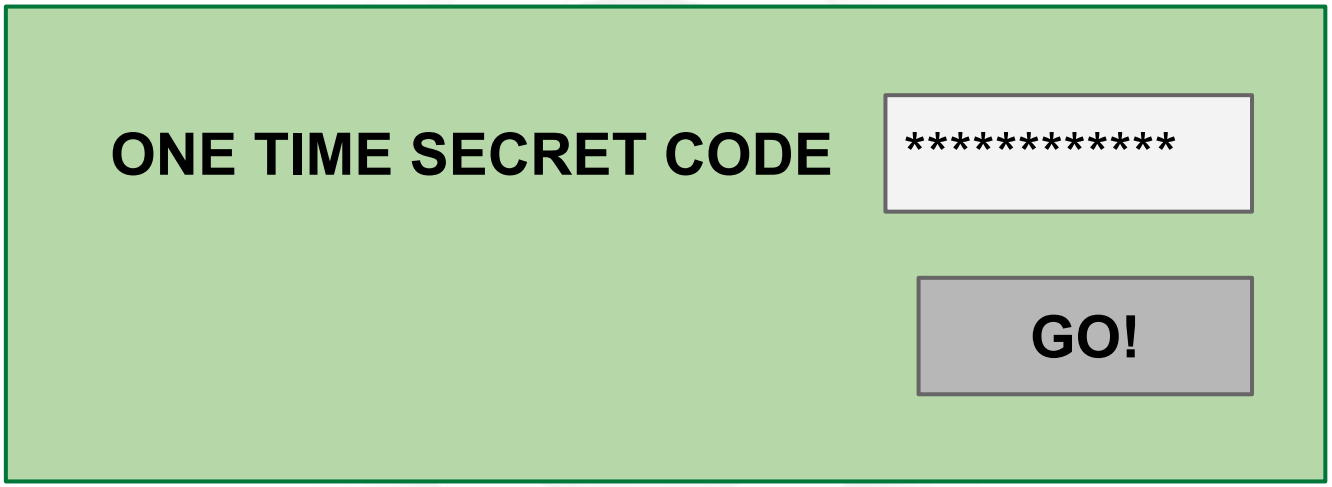


1-factor authentication (password)

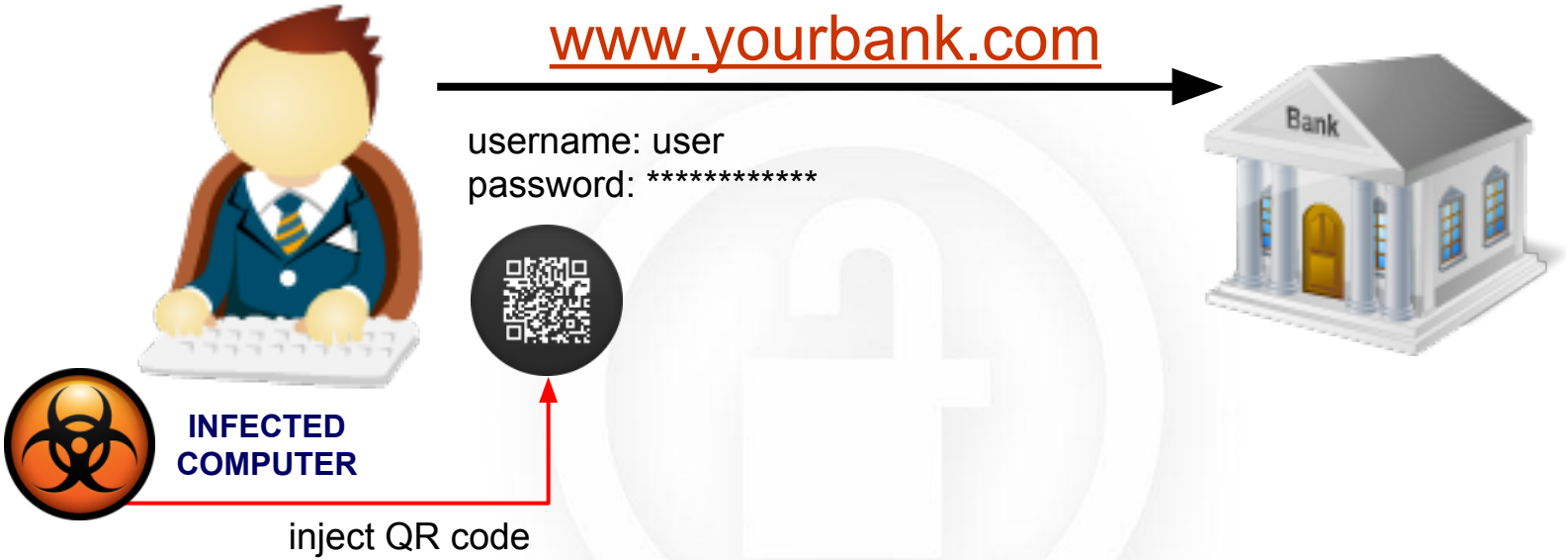


The attack scheme (2)

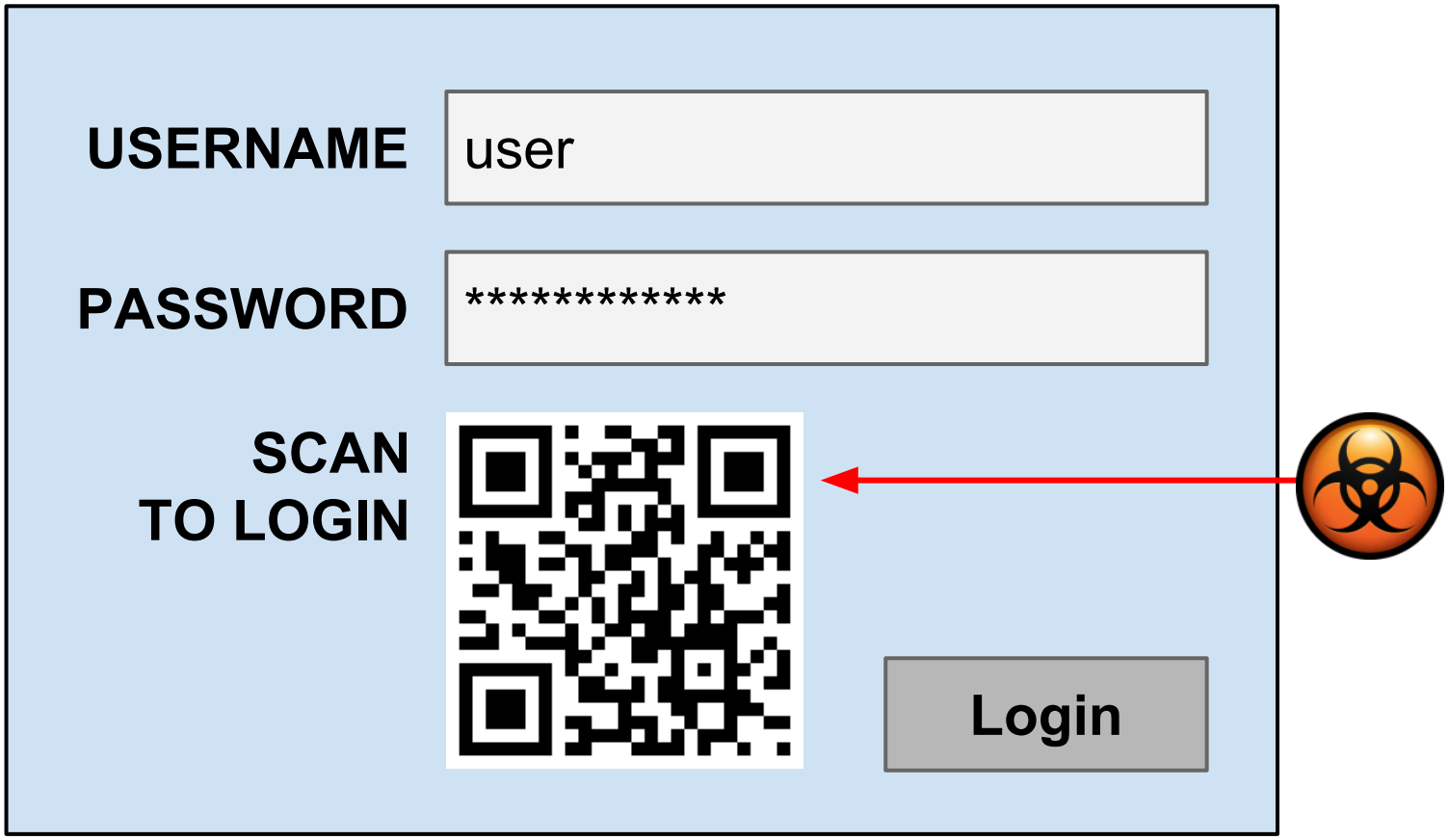
2-factors authentication (password + secret code)



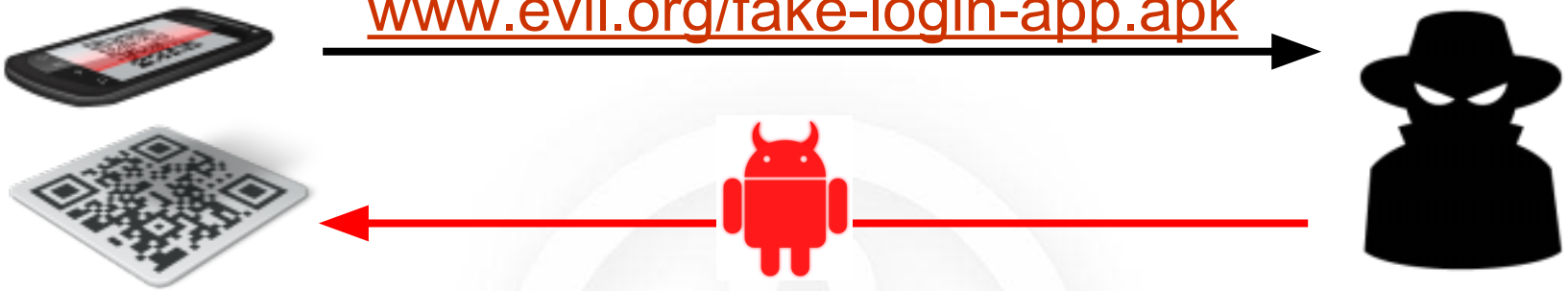
The attack scheme (2)



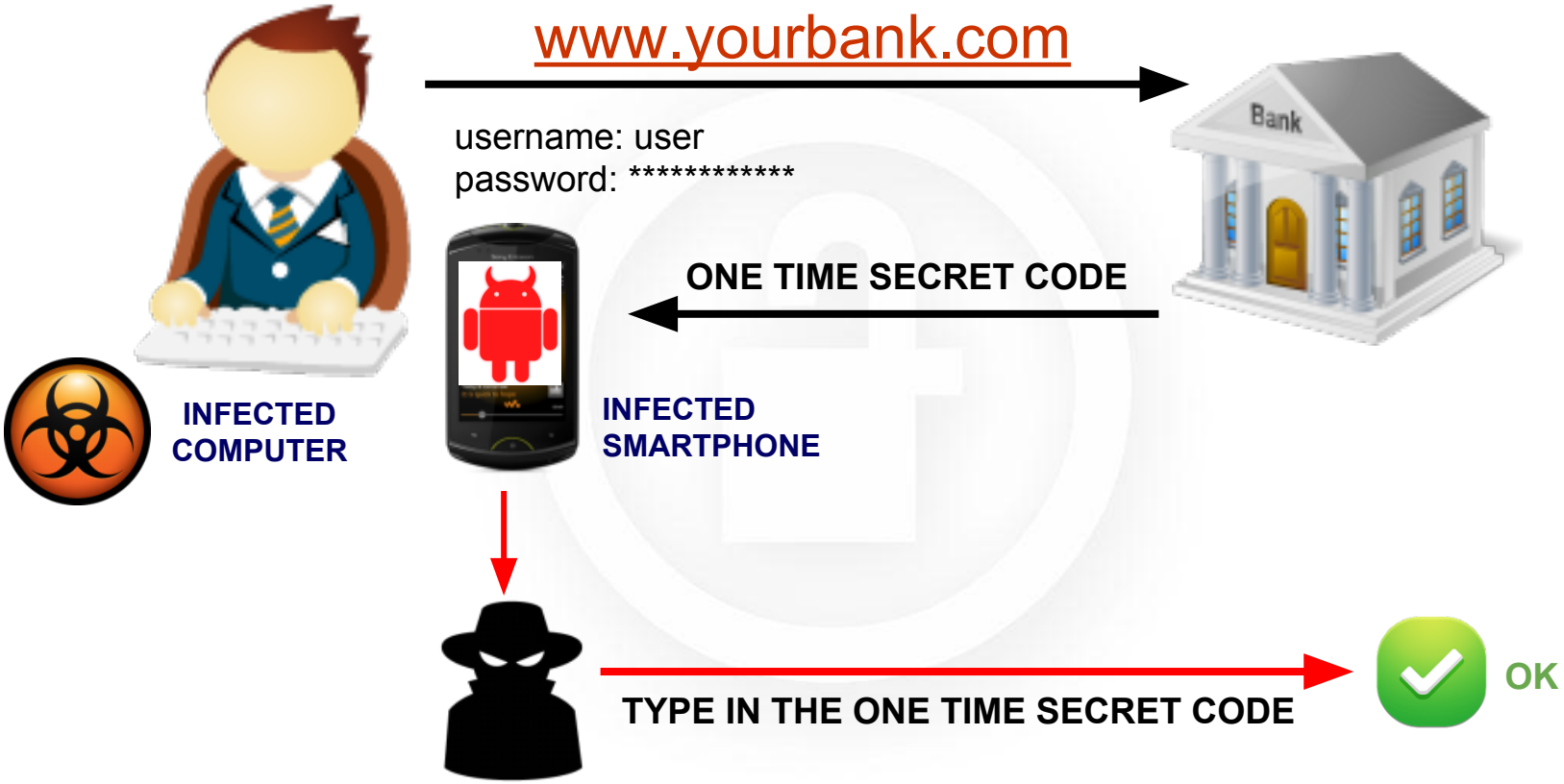
Luring QR code



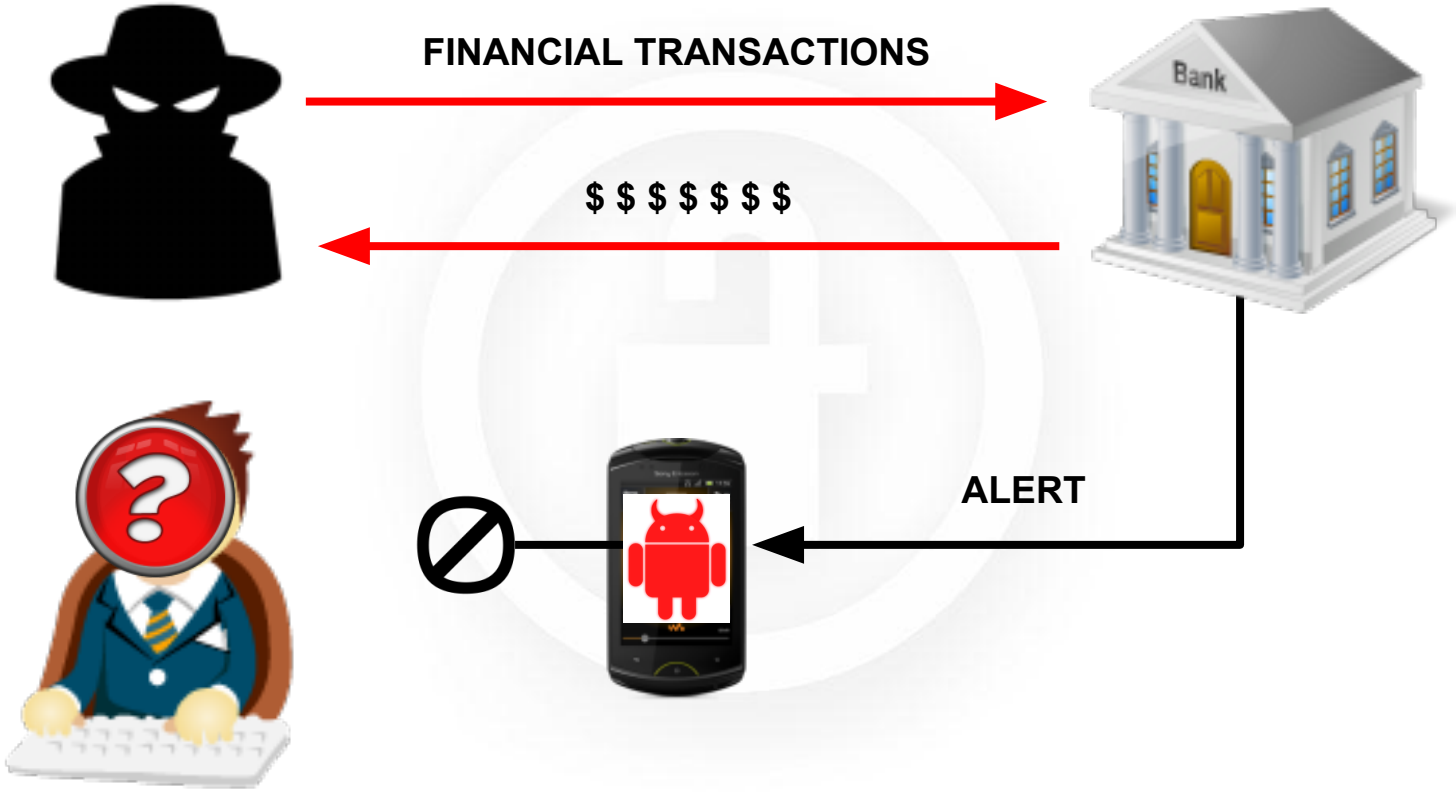
The attack scheme (3)



The attack scheme (4)



The attack scheme (5)



THE MALWARE HIDES SMSs FROM THE BANK

Android malware distribution

Alternative app stores with pirated apps

Social engineering

Email attachments

Example fake (malicious) app

Source (Symantec)

Some names

Perkele

- Crimeware kit

Backdoor.AndroidOS.Obad.a

- Most sophisticated trojan

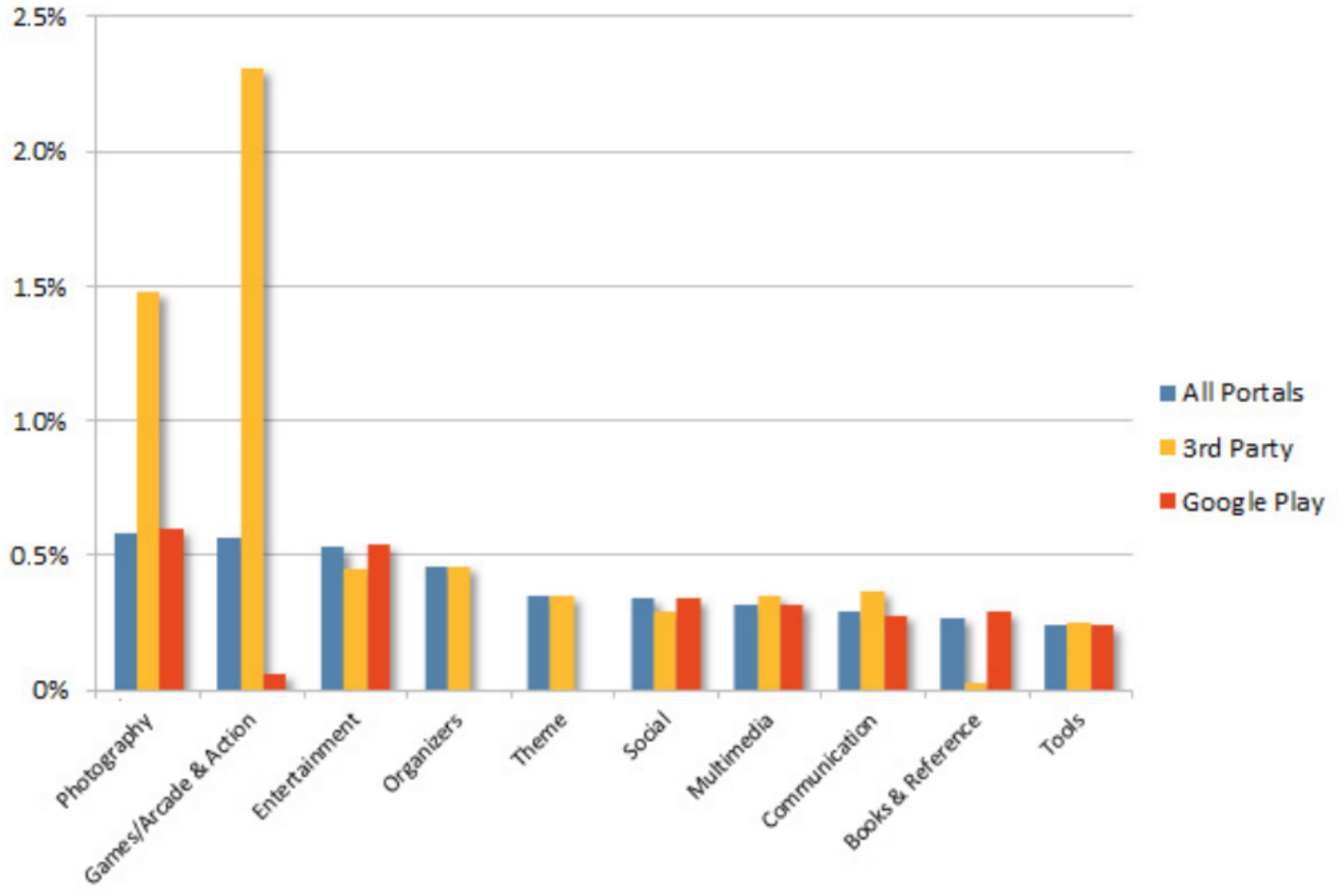
Android.Trojan.FakeMart

- Trojan, SMS stealer

Stells

- Multi-purpose trojan

Dangerous apps categories



Source (Symantec, October 2013)

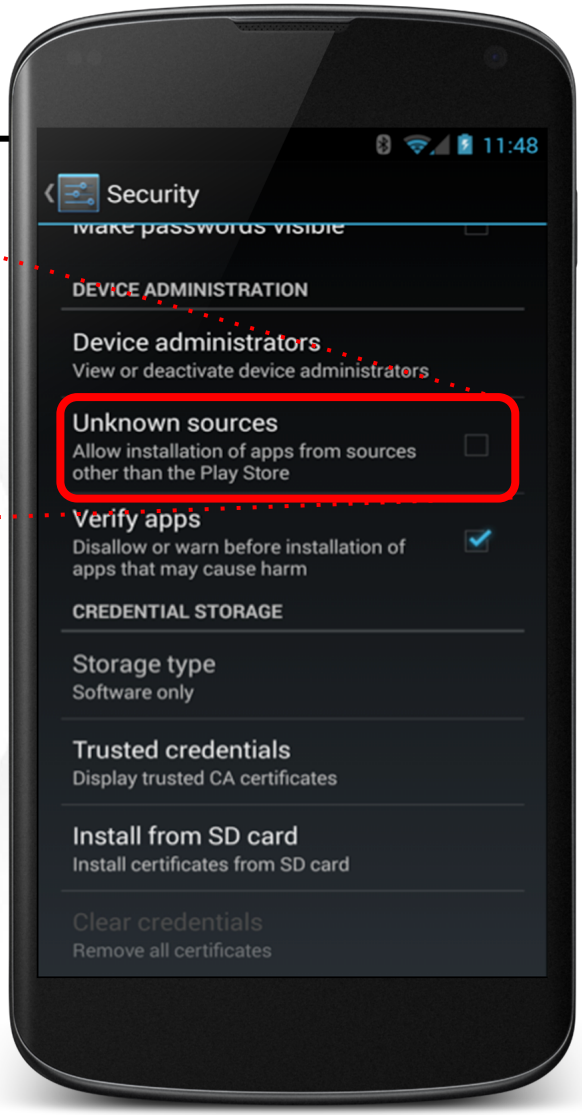
3rd party app marketplaces

Andapponline	Aptoide	Soc.io	92Apk	T Store	Cisco Market
SlideMe	Insydemarket	Android Downloadz	AppChina	Yandex App Store	Lenovo App Store
AndroidPit	PandaApp	MerkaMarket	CoolApk	Pdassi	Omnitel Apps
AppsZoom	AppsEgg	Good Ereader	Anzhi Market	iMedicalApps	TIM Store
ApkSuite	AppTown	Mobile9	EOE Market	Barnes & Noble	T-Store
Opera App Store	AppBrain	Phoload	HiApk	Nvidia TegraZone	T-Market
Brothersoft	AppsLib	Androidblip	Nduoa	AppCake	AT&T
Camangi	ESDN	1Mobile	Baidu App Store	Handmark	CNET
Blackmart Alpha	Mobilism	Brophone	D.cn	Appolicious	Android games room
F-Droid	Mob.org	LG World	Gfan	Appitalism	91mobiles
Amazon	Handango	Samsung App Store	Millet App Store	WhiteApp	mobiles24
AndroLib	Mikandi	Handster	Taobao	AppCity	Android Freeware
GetJar	Nexva market	AppsFire	Tencent App Gem	AlternativeTo	MplayIt
Tablified Market	Yet Another Android Market	Mobango	Hyper Market	Appzil	Hami
Fetch		AndroidTapp	No Crappy Apps	Naver NStore	Olleh Market

3rd party sources

Unknown sources

Allow installation of apps from sources other than the Play Store



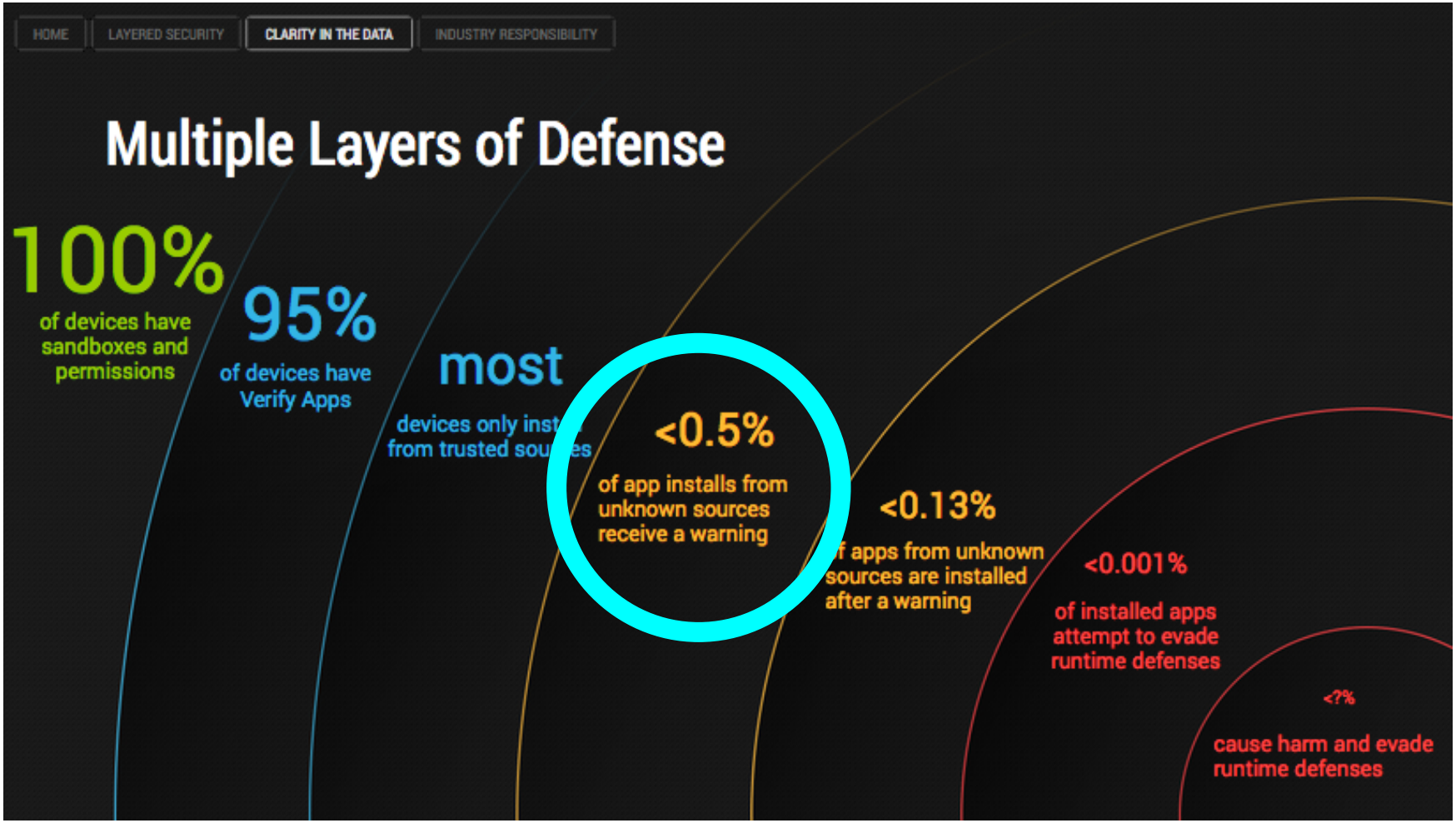
Do we have any clue on the size?

How many malicious "Android threats"? (Q1 2013)

- Symantec: ~3,900
- McAfee: ~60,000
- TrendMicro: ~509,000

Goolge says that this is vastly exaggerated

This is vastly exaggerated

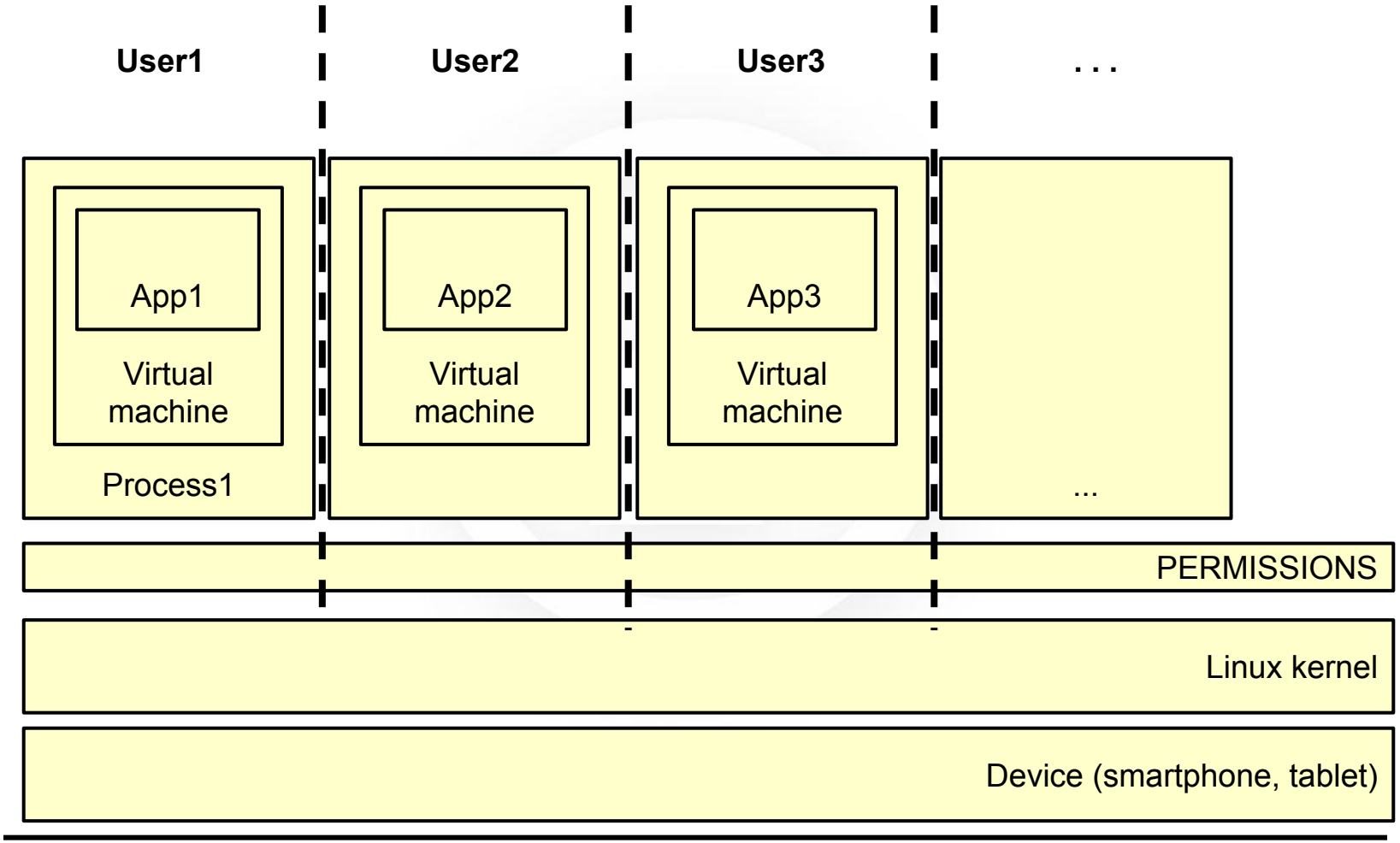


Source (Google, VB2013)

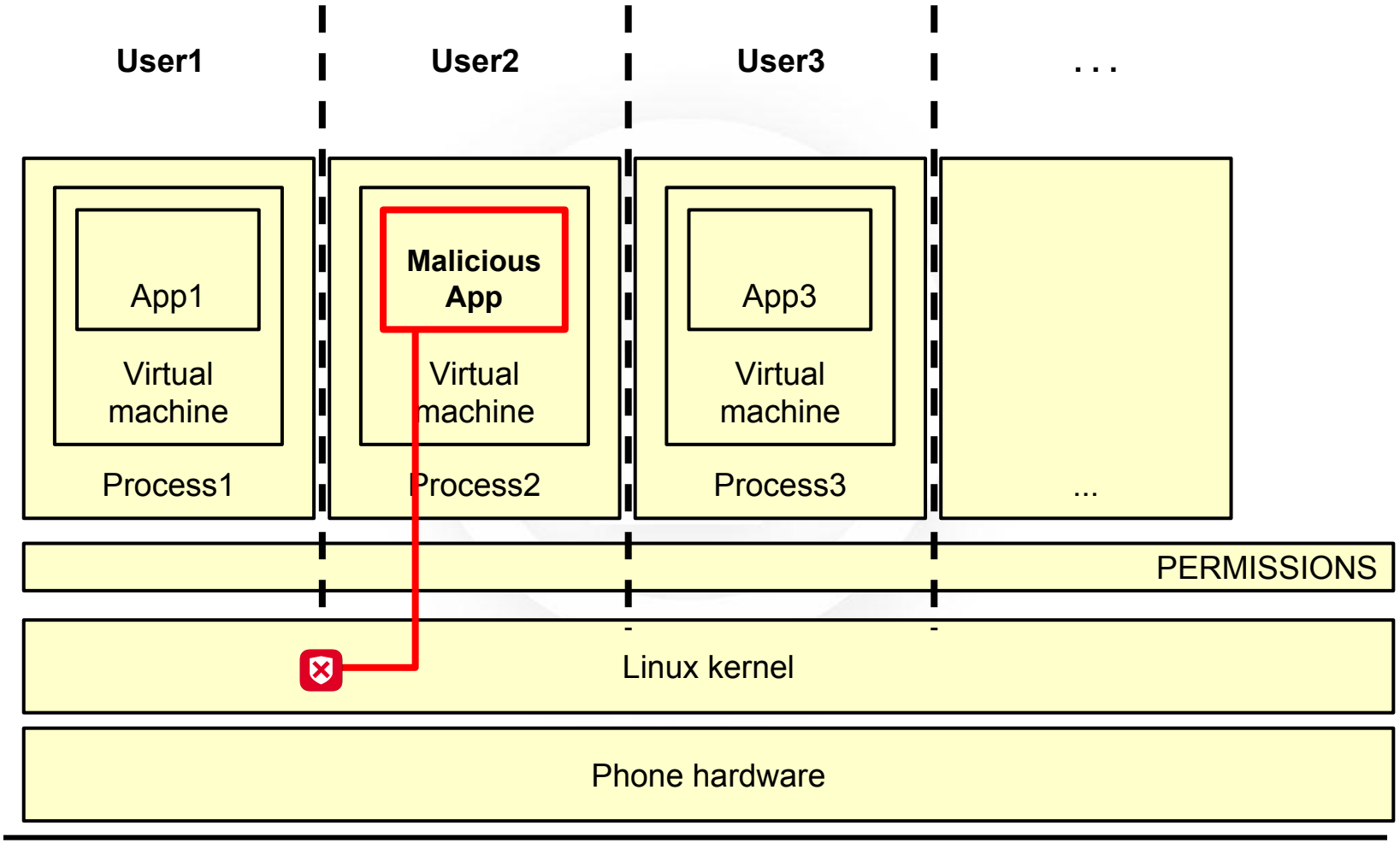
Protections

- Google Play app vetting
- Install and permission confirmation
- SMS/call blacklisting and quota (Android 4.3)
- Runtime checks
- App sandboxing
- SELinux policies (Android 4.4)

App sandboxing



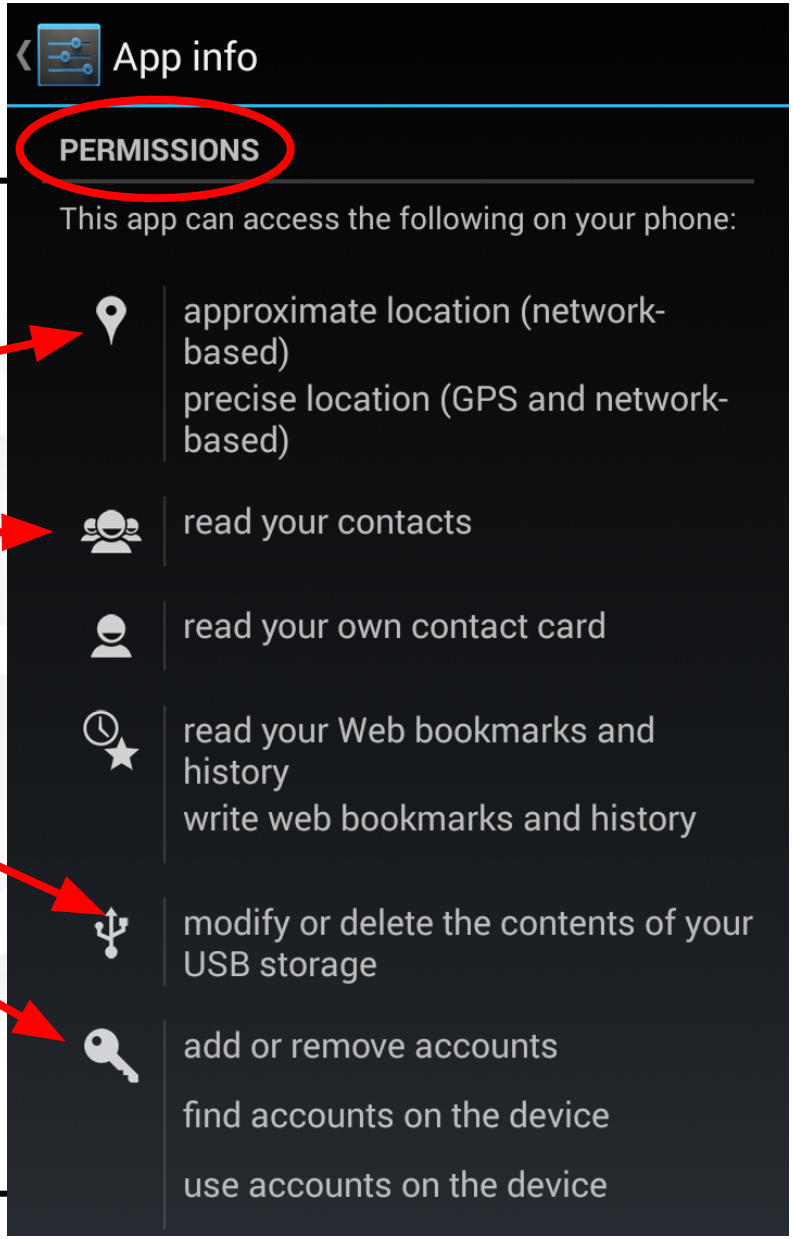
Linux-based process isolation



Permissions

Sensitive resources

- Location
- Contacts
- Storage
- Accounts



How about anti-virus apps (AVs) for Android?

Antivirus/antimalware for Android

Great market opportunity

- More than 100 AV-like apps only on Google Play
- About 71% of them are mobile only

New companies created solely to produces Android AVs


AntiVirus Security
AVG Mobile
Mobile Security &
AVAST Software
Antivirus Free
Creative Apps
AntiVirus & Security
Lookout Mobile Security
Dr.Web v.7 Anti-viru
Doctor Web, Ltd
Norton Security ant
NortonMobile
FREE Tablet AntiVir
AVG Mobile
Android Antivirus
Android Antivirus
NQ Mobile Security
NQ Mobile Security (NYS
LINE Antivirus
LINE Corporation
Antivirus & Mobile S
TrustGo Inc.
Zoner AntiVirus Fre
ZONER, Inc.
McAfee Antivirus &
McAfee Mobile Security
Dr.Web v.8 Anti-viru
Doctor Web, Ltd
Bitdefender Antiviru
Bitdefender
Android Antivirus
Android Antivirus
Mobile AntiVirus Se
AVG Mobile
€10,99
Free Antivirus 2014
Android Antivirus Resea
360 Mobile Security
Qihu 360 Software Co., L
Android Antivirus
Android Antivirus Pro
Mobile Security & A
Teebik Apps
Mobile Security & A
ESET
Antivirus for Androi
Mobilla Corporation
Antivirus for Androi
Dala Apps
best antivirus
inventor
Mobile Security & A
Bitdefender
Antivirus Free
Comodo Security Solutic
Mobile Security & A
Trend Micro
Zoner AntiVirus Fre
ZONER, Inc.
VIRUSfighter Antivi
SPAMfighter aps
GuardX Antivirus
QStar
Webroot Security &
Webroot Inc.
Hornet AntiVirus Fr
Hornet Mobile Security
Bkav Security - Anti
Bkav Corporation
G-Protector Anti Vir
Gpc
G Data AntiVirus Fre
G Data Software AG
SAFE antivirus and
MSP Inc.
MYAndroid Protecti
MYMobile Security
AegisLab Antivirus F
AegisLab
Antivirus TESTVIRU
P.Defender Antivirus
Best Antivirus Andr
MSP Inc.
Free Antivirus and S
Sophos Limited
Fastscan free Anti-V
K-TEC Inc.
Antivirus & Anti-Adv
SeCore Lab
Tablet AntiVirus Sec
AVG Mobile
€10,99
EICAR Anti-virus Te
eXtorian
Video antivirus revie
PashaYakushev
BluePoint Antivirus
BluePoint Security, Inc.
Dr.Web v.8 Anti-viru
Doctor Web, Ltd
€58,13
Armor for Android™
Armor for Android™
€23,02
Mobile Security & A
Panda Security
Secure AntiVirus for
Demand Apps
White-Gate Antiviru
White Gate
My Antivirus
Mobile Cloud Labs Plc.
Test Virus - Android
Android Antivirus Pro
AntiVirus
Playerum
Android Antivirus Pr
Android Antivirus
€3,99
MyAntiVirus Pro - A
P.Defender Antivirus
€7,15
BlackBelt AntiVirus
BlackBelt SmartPhone D
Security & Antivirus
Webroot Inc.
€7,49
Mobile Security Ant
Wolfguard
Zoner AntiVirus Tes
ZONER, Inc.
Fastscan Anti-Virus
K-TEC Inc.
€1,53
FREE Android Antiv
Cat Apps
LabMSF Antivirus b
LabMSF
VG 기업용 Web SDK
인프라웨어 테크놀러지
AegisLab Antivirus
AegisLab
Free Android Antivi
Meetio
AntiVirus Laser
MyNikko
TWTR Antivirus And
SToX.biz
xCore Antivirus
xCore LLC
Privateer Antivirus &
Privateer Labs

PALSIT

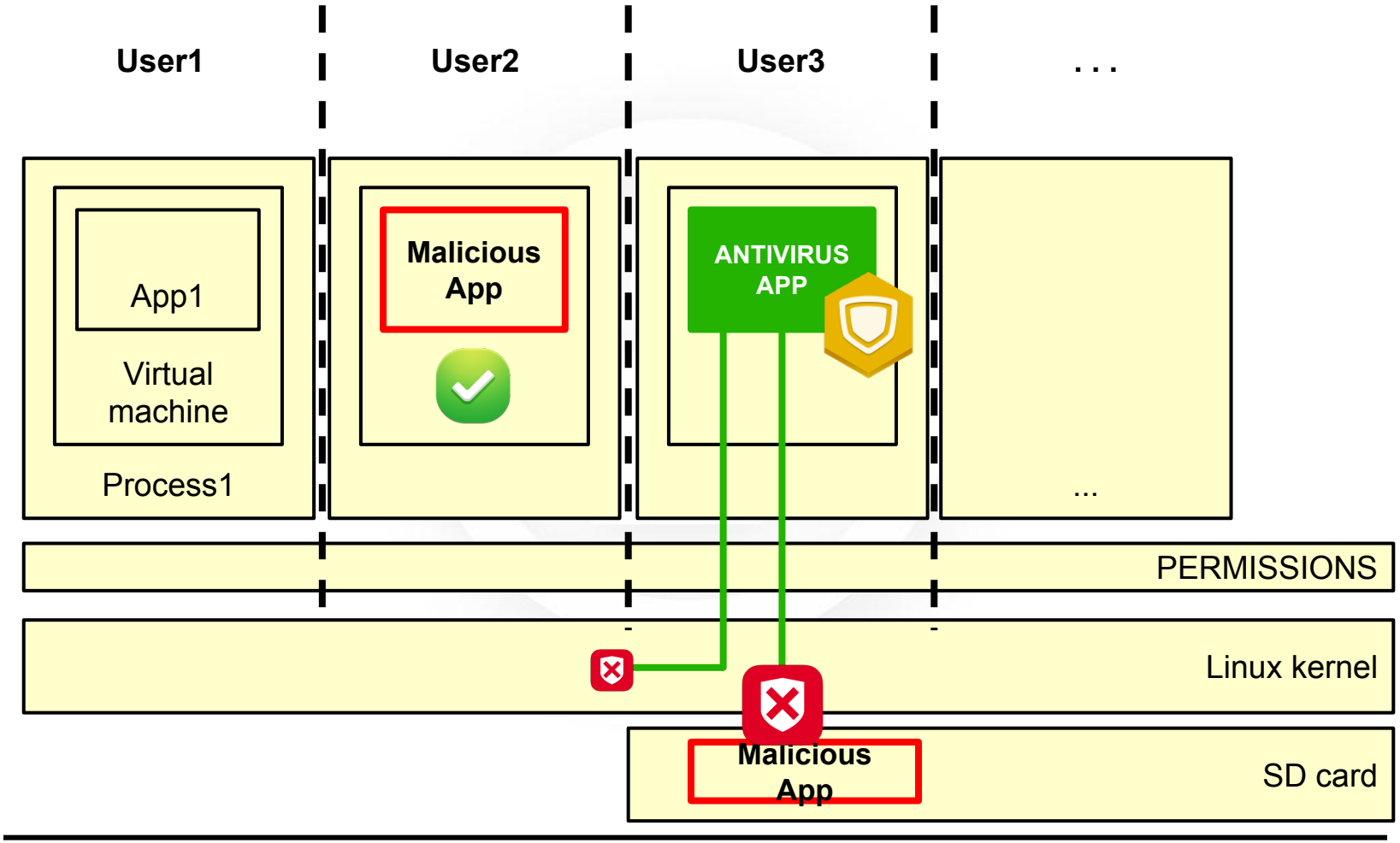
1. Android threats and protections
2. **Limitations**
3. Testing antivirus apps
4. AndroTotal
5. Status

Antivirus apps are constrained

No primitives for auditing running processes

- ✗ advanced heuristics
- ✗ runtime checks

No primitives for process auditing



Antivirus apps are constrained

Workarounds

- Signature-based matching
- Scan limited portion of the storage
- Send sample to cloud service
- Custom kernel (not market proof)
- Require root privileges (drawbacks)

Malware apps are constrained, too

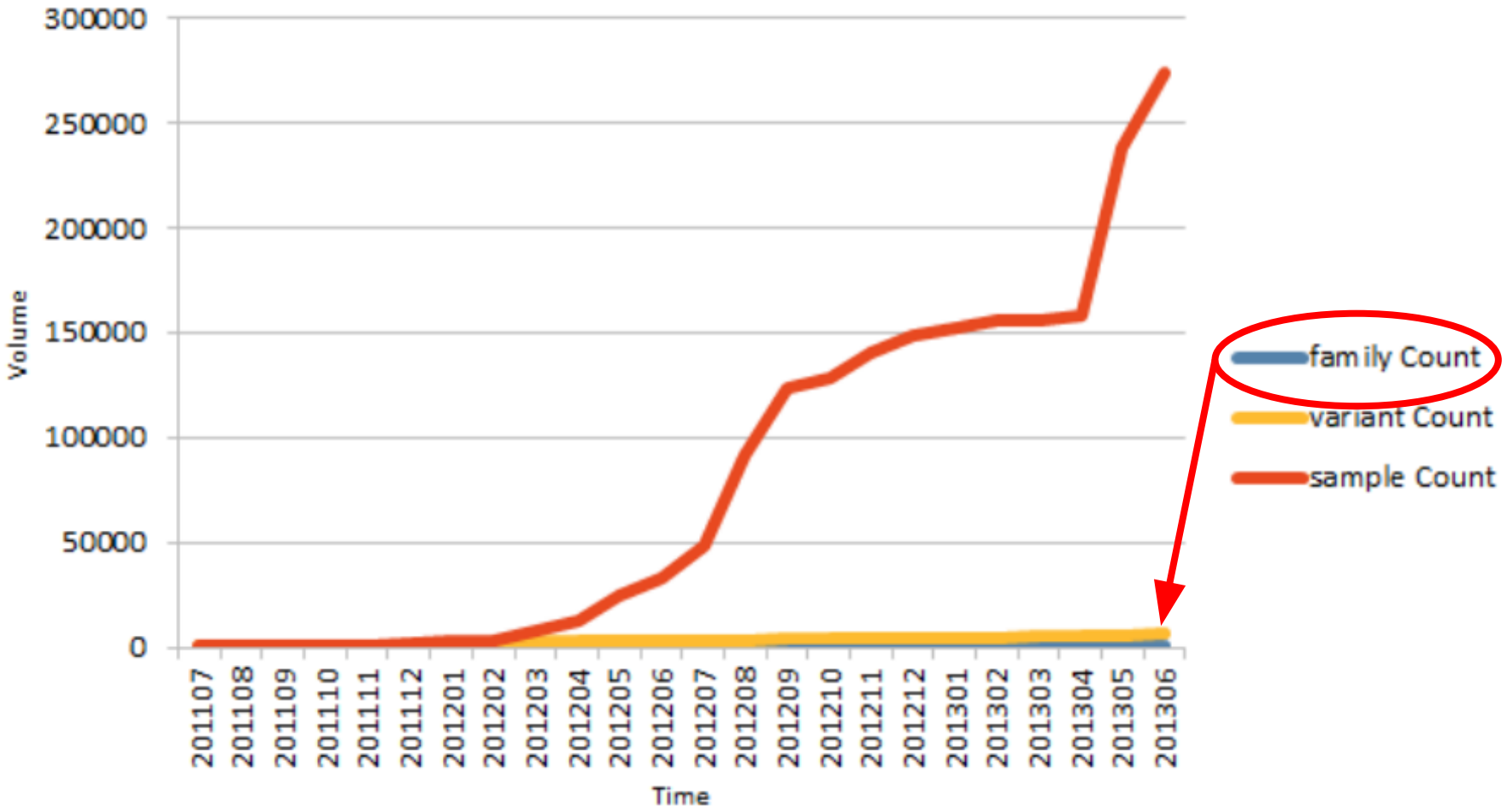
Less freedom

- A malware is an isolated app itself

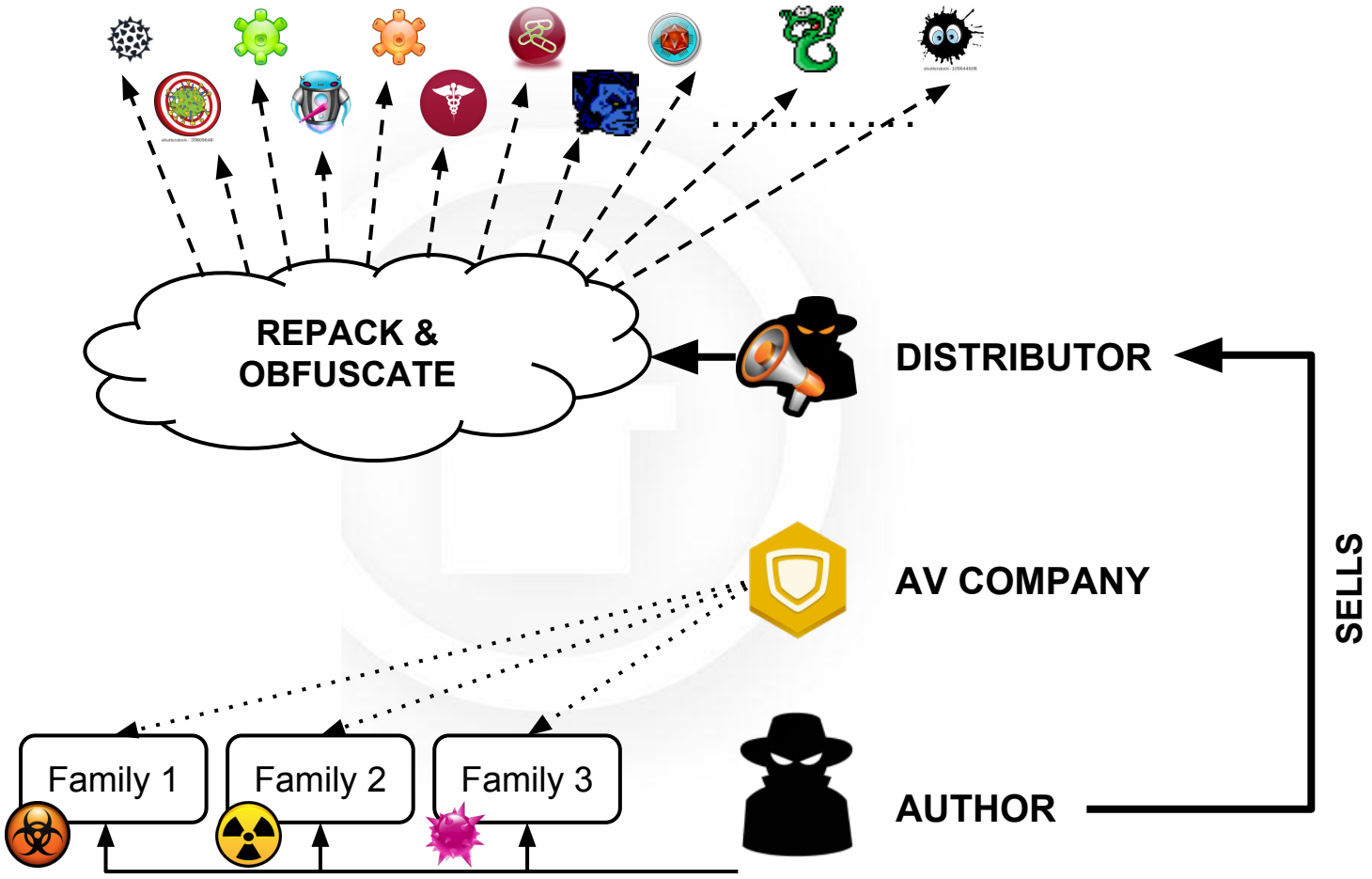
Workarounds

- Social engineering (users must install the malware)
- **Signature evasion**

Signature evasion



Few families, thousands of samples



1. Android threats and protections
2. Limitations
3. **Testing antivirus apps**
4. AndroTotal
5. Status

Are these AV apps any good?

Simple checks (easily evaded)

- Package name
- Class names

Signatures (easily evaded)

- Static signatures

Cloud based (network intensive or easily evaded)

- Send each installed APK (network intensive)
- Send the hash of the APK (easily evaded)

How to test Android AV apps?

1. Obtain ***M*** samples of known malware

2. Apply ***T*** code transformation to each sample

3. Produce ***M*** × ***T*** variants

4. Analyze the variants with ***P*** antimalware apps

5. Repeat for each of the ***A*** Android versions

Let's do the math

- Samples = **1,000** (very conservative)
- Code Transformations = **10**
- AV Products = **100**
- Android versions = **3** (e.g., 2.3, 4.1, 4.2)

1,000 × 11 × 100 × 3 = 3,300,000 tests

Lack of tools

- **VirusTotal.**com covers ~29% of Android AVs
- H. Pilz, *"Building a test environment for Android anti-malware tests,"* Virus Bulletin Conference '12
  - human oracle needed
- M. Zheng, P. P. C. Lee, and J. C. S. Lui, *"ADAM: An Automatic and Extensible Platform to Stress Test Android Anti-Virus Systems,"* DIMVA'12
  - Focus on code transformation
- V. Rastogi, Y. Chen, and X. Jiang, *"DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks,"* AsiaCCS'13
  - Focus on code transformation

1. Android threats and protections
2. Limitations
3. Testing antivirus apps
4. **AndroTotal**
5. Status

AndroTotal www.andrototal.org

SDK for writing UI tests/scrapers

Pluggable adapters for each antimalware

Parametric tests (e.g., version, platform)

Web frontend for humans

REST/JSON API for machines

Scan application (advanced)

Sample File [ ] Browse

Is this sample a malware?
- ( ) Yes
- ( ) No
- ( ) I do not know

Force sample reanalysis [ ]

Are you human?

Antivirus name	Antivirus version	Android platform	Detection method	
Trend Micro, Mobile Security & Antivi	2.6.2	Android 4.1.2	On install	+
AVAST Software, avast! Mobile Security	2.0.3380	Android 4.1.2	On install	✖
AVAST Software, avast! Mobile Security	2.0.3380	Android 4.1.2	On demand	✖
AVAST Software, avast! Mobile Security	2.0.3917	Android 4.1.2	On install	✖

andrototal (beta)

Scan | Results | Admin | Logout

Sample MD5	cbdf63b2e5666799c4b74a8cd15565dd
Sample SHA-1	d9c2bc199769f8e1c817ccd23f1860f5125bdaf6
Sample SHA-256	d11de9bb4d7451ffe7e4b6bd6bab529e7411e3dbe90d468243ef87a5ed98941e
File size	959488 Bytes
First seen on	08 May 2013
Malicious labels	(Android:FakeInst-EO [PUP]). AndroidOS_FakeInst.VTD not a virus Adware.Startapp.origin.5
Package name	com.issghai.thattere
File names	com.issghai.thattere.apk
External analysis	[VirusTotal] [SandDroid]

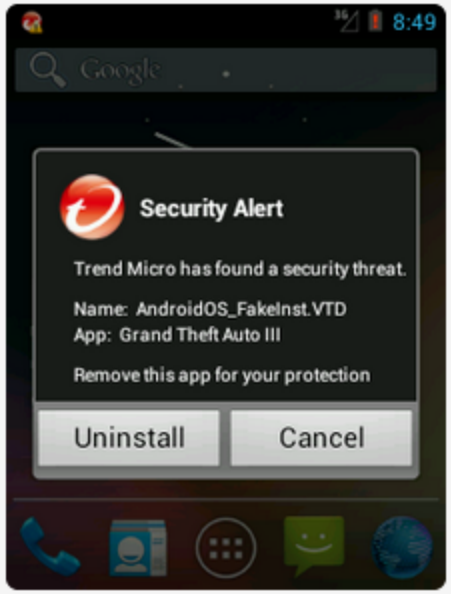
Last 10 scans performed on this sample View all »

Platform	Antivirus Name	Detected name	Date	Results
Android 4.1.2	Doctor Web, Ltd, Dr.Web Anti-virus Light (free) 7.00.3	not a virus Adware.Startapp.origin.5	08/05/13	Full report »
Android 4.1.2	Trend Micro, Mobile Security & Antivirus 2.6.2	AndroidOS_FakeInst.VTD	08/05/13	Full report »
Android 4.1.2	AVAST Software, avast! Mobile Security 2.0.3917	(Android:FakeInst-EO [PUP]).	08/05/13	Full report »
Android 4.1.2	Kaspersky Lab, Kaspersky Mobile Security Lite 9.36.28	No threat detected	08/05/13	Full report »
Android 4.1.2	NortonMobile, Norton Security & Antivirus 3.3.4.970	No threat detected	08/05/13	Full report »

Trend Micro / Mobile Security & Antivirus / 2.6.2 / 2013-05-08 17:07:23 - cbdf63b2e5666799c4b74a8cd15565dd

Mobile Security & Antivirus 2.6.2 scan for cbdf63b2e5666799c4b74a8cd15565dd

Task id	131bd4fe-3bcd-4a72-a207-683ed8eb79f1
Vendor name	Trend Micro
Antivirus name	Mobile Security & Antivirus
Engine version	2.6.2
Analysis started on	08/05/2013 at 17:05
Analysis completed on	08/05/2013 at 17:07 (took *91* seconds)
Detection method	On install
Analysis result	AndroidOS_FakeInst.VTD
Sample md5	cbdf63b2e5666799c4b74a8cd15565dd



Logcat dump (download)

```
I/tmms-vsapi-jni(  674): VSReadVirusPattern OK. Action successful.
I/tmms-vsapi-jni(  674): OK. VSSetProcessAllFileInArcFlag. oldValue = ret = 0.
I/tmms-vsapi-jni(  674): OK. VSSetExpandLiteFlag. oldValue = ret = 1.
I/tmms-vsapi-jni(  674): OK. VSSetProcessAllFileFlag. oldValue = ret = 0.
I/tmms-vsapi-jni(  674): OK. VSSetCleanZipFlag. oldValue = ret = 0.
I/tmms-vsapi-jni(  674): OK. VSSetCleanBackupFlag. oldValue = ret = 0.
I/tmms-vsapi-jni(  674): VSGetDetectableVirusNumber virus in patter num = 3283
I/tmms-vsapi-jni(  674): filename = /data/data/com.trendmicro.tmmspersonal/Library/pattern/msvpnaos.457
I/tmms-vsapi-jni(  674): InternalVer = 145700, PtnVer = 457.
D/PrepareVSAPI4RTScan(  674): before tmmsAntiMalwareJni4RTScan.init()!
I/tmms-vsapi-jni(  674): VSInit OK!
D/PrepareVSAPI4RTScan(  674): after tmmsAntiMalwareJni4RTScan.init()!
I/tmms-vsapi-jni(  674): in vsSetPatternPath, vc = 711579352
I/tmms-vsapi-jni(  674): Current pattern path is : /etc/iscan
I/tmms-vsapi-jni(  674): Pattern path is set to : /data/data/com.trendmicro.tmmspersonal/Library/pattern
I/tmms-vsapi-jni(  674): Pattern file(s) successfully deleted.
I/tmms-vsapi-jni(  674): in vsLoadPattern, vc = 711579352, sharedVC = 708085592, scanType =
I/tmms-vsapi-jni(  674): vsLoadPattern patternPath = /data/data/com.trendmicro.tmmspersonal/Library/pattern,
```

andrototal (beta)

Search | Scan | Results | Admin | Logout

Sample File | Browse

Is this sample a malware?
- Yes
- No
- I do not know

Force sample reanalysis

Obfuscate sample

Antivirus name	Antivirus version	Android platform	Detection method	
AVAST Software, avast! Mobile Secur	2.0.3917	Android 4.1.2	On install	+

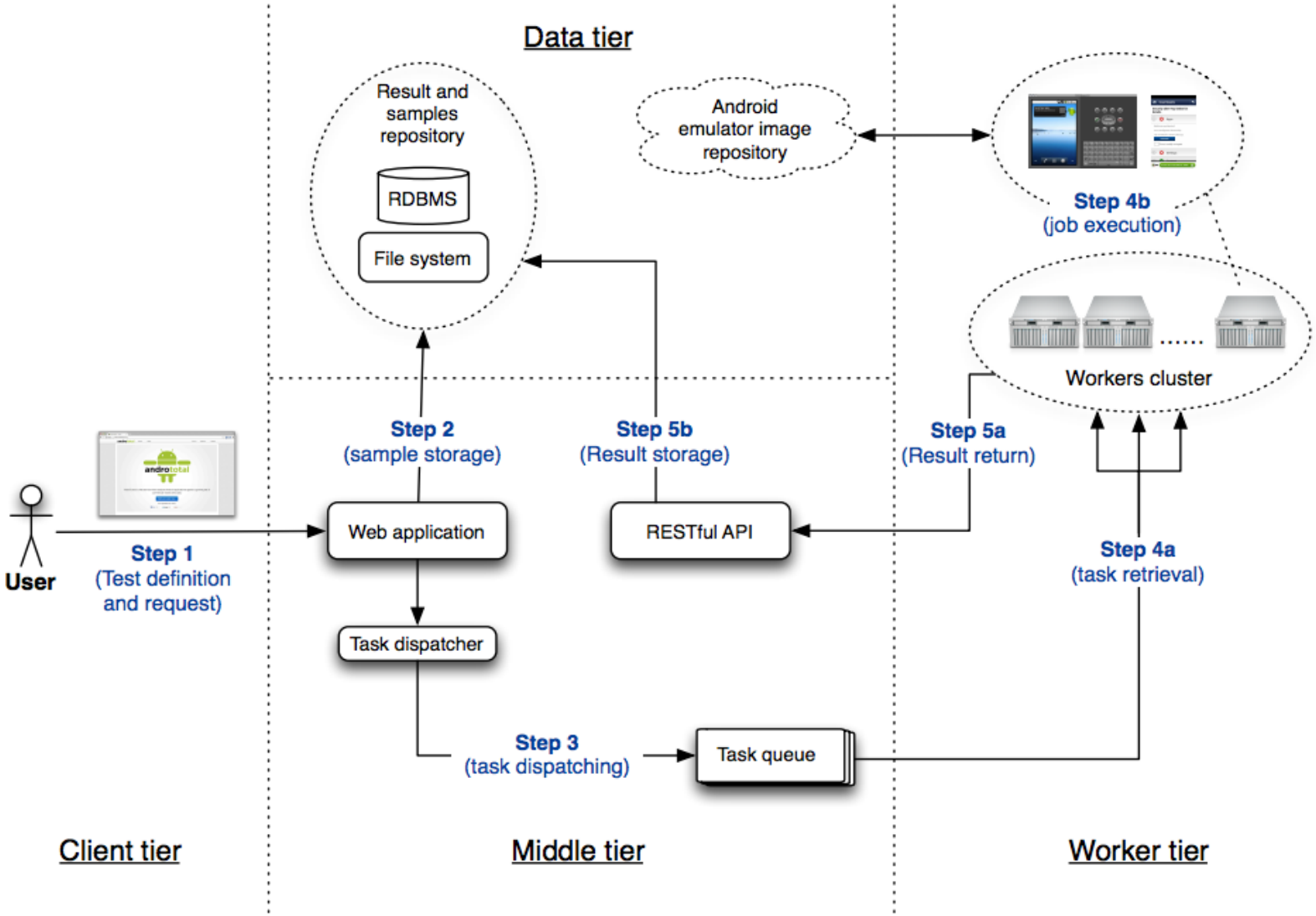
- ✓ Alignment
- ArithmeticBranch
- Debug
- Defunct
- Goto
- Indirections
- Nop
- Rebuild
- Reflection
- Renaming
- Reordering
- Repacking
- Resigned
- StringEncrypt

+

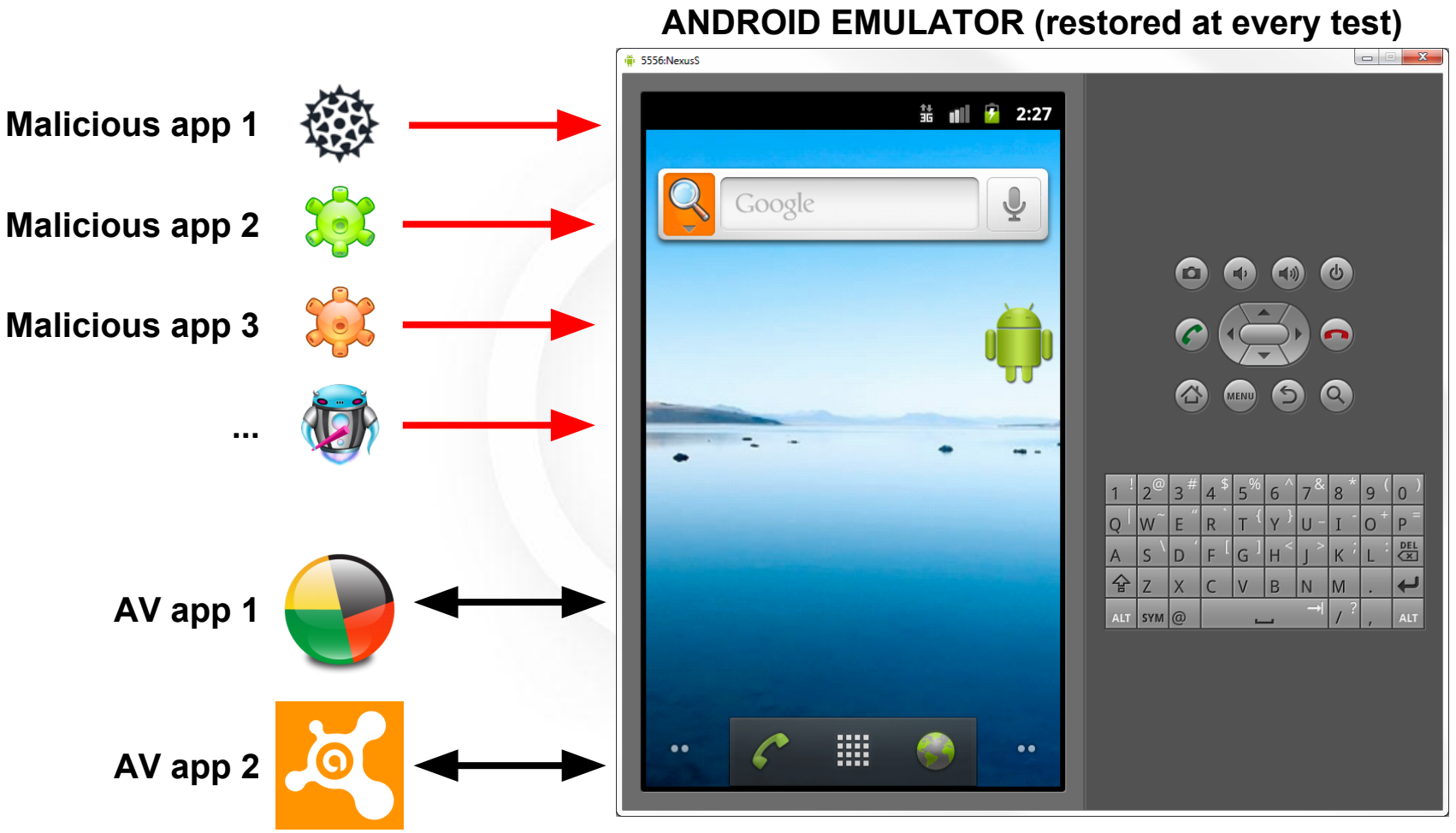
Start scan!

By clicking "Start scan!", you agree to our Terms of Service and our Privacy Policy.

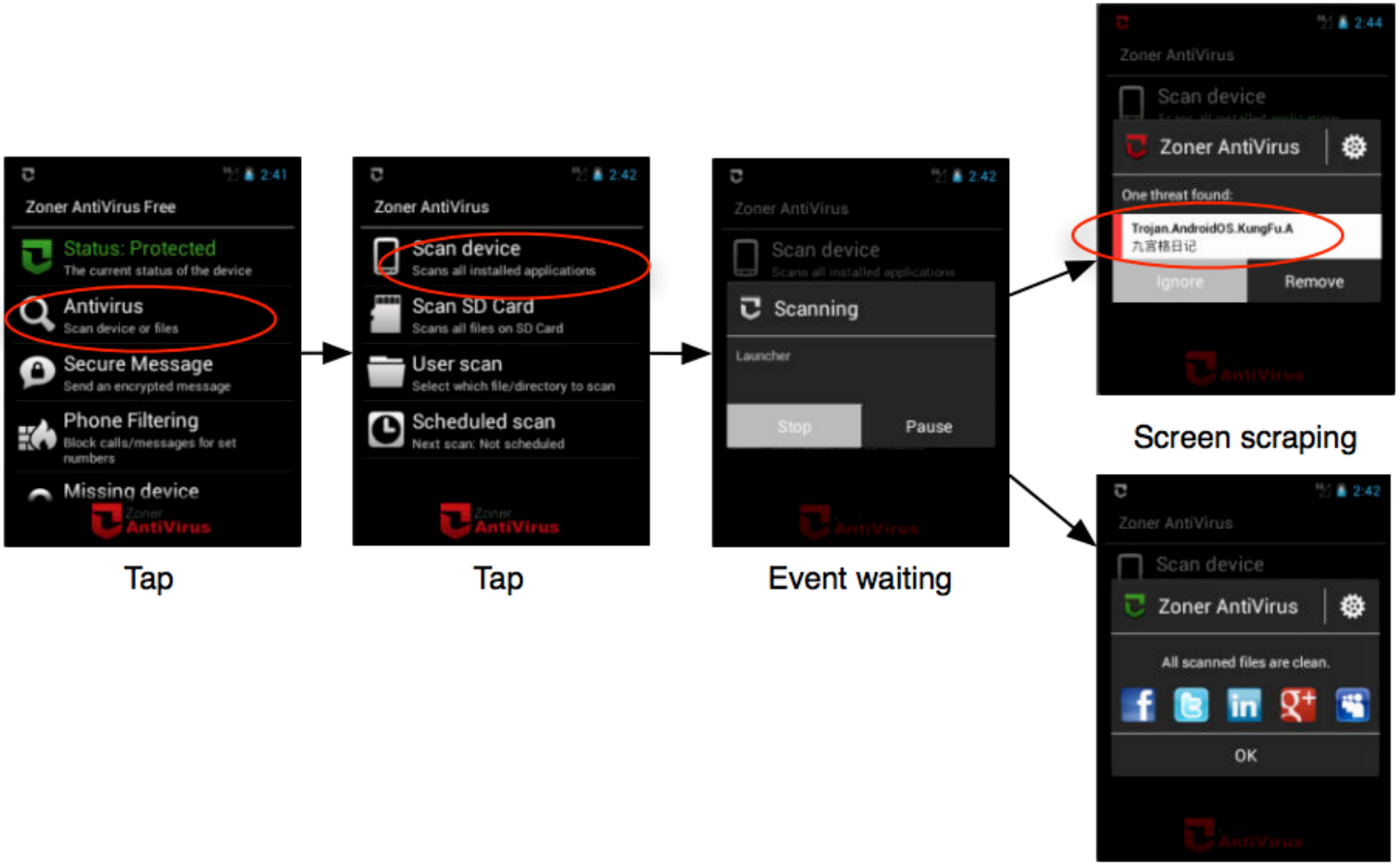
Architecture



The basics


ANDROID EMULATOR (restored at every test)
Malicious app 1
Malicious app 2
Malicious app 3
...
AV app 1
AV app 2
5556:NexusS
2:27
Google
MENU

User interface automation



Under the hood (1)

```
#andrototal-adapters/ComZonerAndroidAntivirus.py
class TestSuite(base.BaseTestSuite):
  def on_install_detection(self, sample_path):
    self.pilot.install_package(sample_path)

    if self.pilot.wait_for_activity(
        "com.zoner.android.antivirus_common.ActScanResults", 10):

      result = self.pilot.get_view_by_id("scaninfected_row_virus")
    else:
      result = False
```

Under the hood (2)

```
#...
def on_demand_detection(self, sample_path):
  self.pilot.install_package(sample_path)
  self.pilot.start_activity("com.zoner.android.antivirus", ".ActMain")
  self.pilot.wait_for_activity("com.zoner.android.antivirus.ActMain")

  self.pilot.tap_on_coordinates(120, 130)
  self.pilot.wait_for_activity("com.zoner.android.antivirus.ActMalware")

  # start scan
  self.pilot.tap_on_coordinates(120, 80)
  self.pilot.wait_for_activity(
    "com.zoner.android.antivirus_common.ActScanResults")

  self.pilot.refresh()
# ...
```

REST/JSON API and client

- http://code.andrototal.org/tool

```
$ python andrototal_cli.py -l DEBUG scan -at-key <...> -ms-key <...> pat

Running command: scan
Uploading file sample.apk
Scan response: {"resource": "10a6f3efc8bc40c1922facde7d055208"}
Uploading file sample2.apk
Scan response: {"resource": "e870c6748ca3409f84c9c9e1a91daf3f"}
Uploading file 40156a176bb4554853f767bb6647fd0ac1925eac.apk
Scan response: {"resource": "21d6c7234a184db6b8e52f2bab523787"}
Uploading file samples-3.apk
Scan response: {"resource": "ec5b3c94ed624d6993b52a50d63153fa"}
```

1. Android threats and protections
2. Limitations
3. Testing antivirus apps
4. AndroTotal
5. **Status**

Status

- **13** antivirus vendors supported (not all public)
- **16** products overall (not all public)
- **1,451** users subscribed
- **29,791+** distinct APKs submitted and analyzed

Notable consumer/producers

- **Symantec**
- **Kaspersky**
- **Sophos**
- **ESET**
- **Andrubis** (sandbox)
- **CopperDroid** (VM introspection)
- **ForeSafe** (sandbox)
- **SandDroid** (sandbox)
- **VisualThreat** (sandbox + static analysis)
- **AndroidObservatory** (data collection)

Most popular malware names

Label	Samples
UDS:DangerousObject.Multi.Generic	4820
not a virus Adware.Airpush.origin.7	1942
Trojan-SMS.AndroidOS.Opfake.bo	1542
AndroidOS_Opfake.CTD	795
Adware.AndroidOS.Airpush-Gen	789
Trojan-SMS.AndroidOS.Opfake.a	763
Android.SmsSend.origin.281	640
Android.SmsSend.origin.629	639
Android:FakeNotify-A [Trj]	631
Trojan-SMS.AndroidOS.FakeInst.a	616

Future work

- Add more cores and scale
- Add more antivirus apps
- Make it an open malware repository for research

We're always looking for good, motivated students to work on projects like this one!

http://andrototal.org

@andrototal_org

Questions?

Grab a sticker!

PALSIT

Federico Maggi

federico@maggi.cc

Politecnico di Milano