

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

Federico Maggi, PhD

Post-doctoral Researcher



**POLITECNICO
DI MILANO**



Topics

Android malware, botnet detection, web measurements

Background

Intrusion detection, anomaly detection

The RED BOOK

A Roadmap for Systems Security Research

Audience

Policy makers

Researchers

Journalists

Content

Vulnerabilities

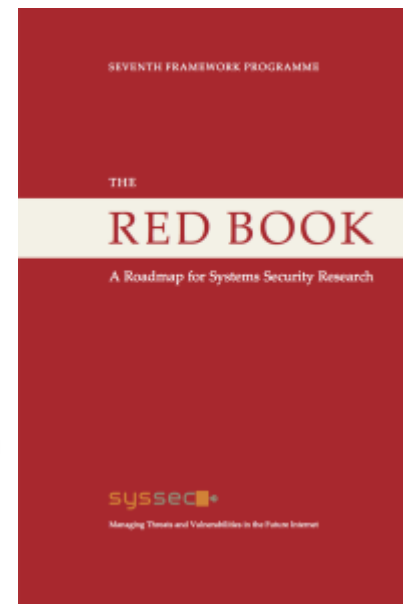
Social Networks

Critical Infrastructure

Mobile Devices

Malware

. . .



Free PDF

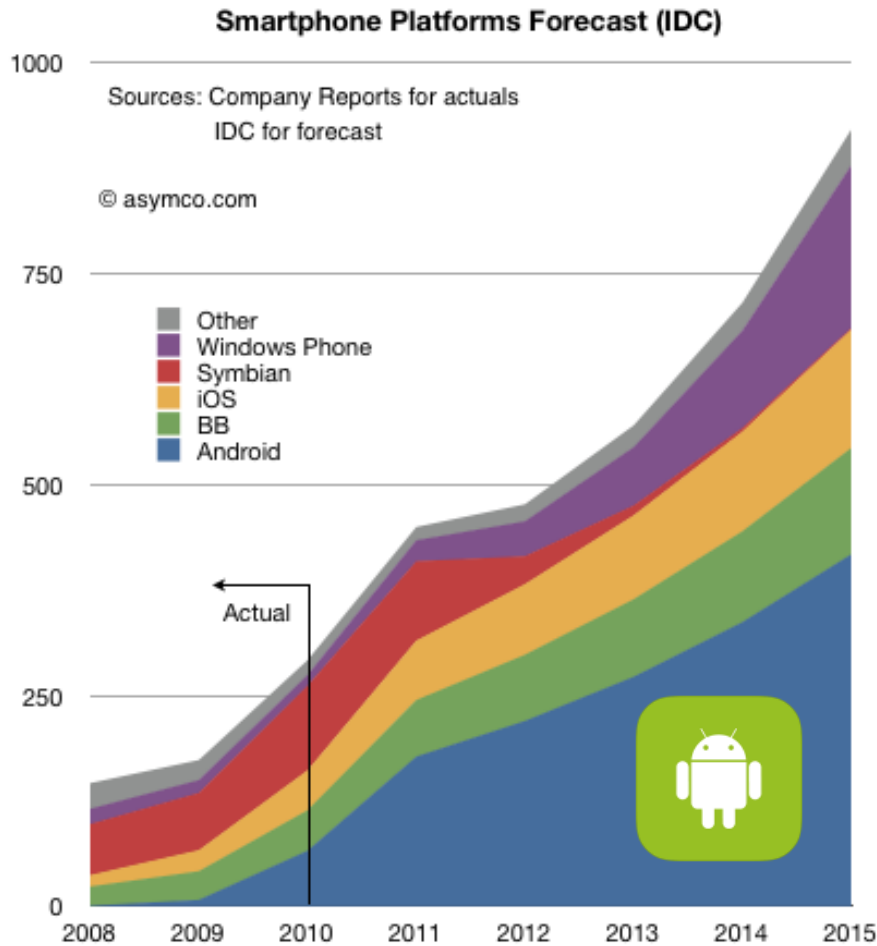
Roadmap

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

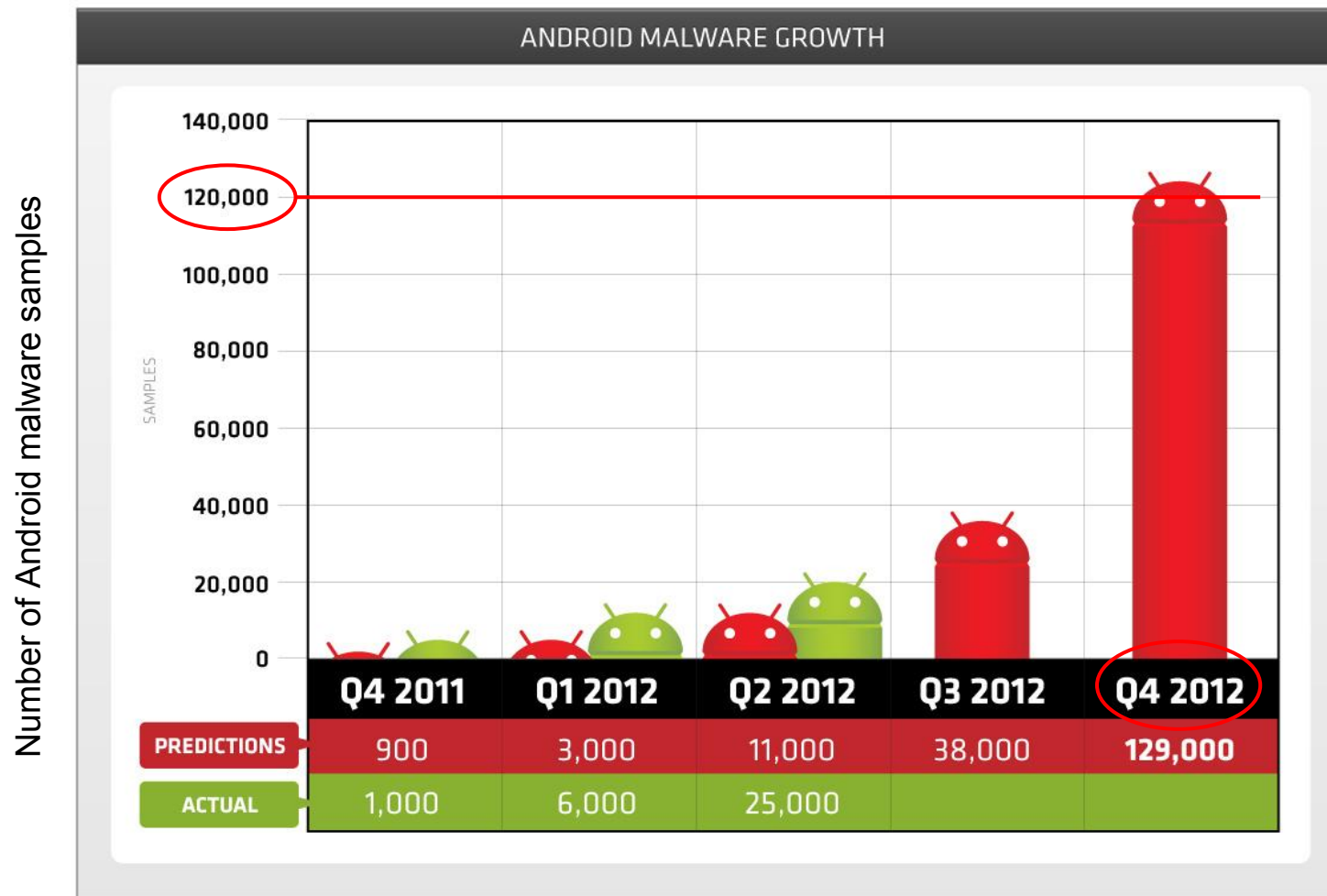
Android beats them all



July 2013

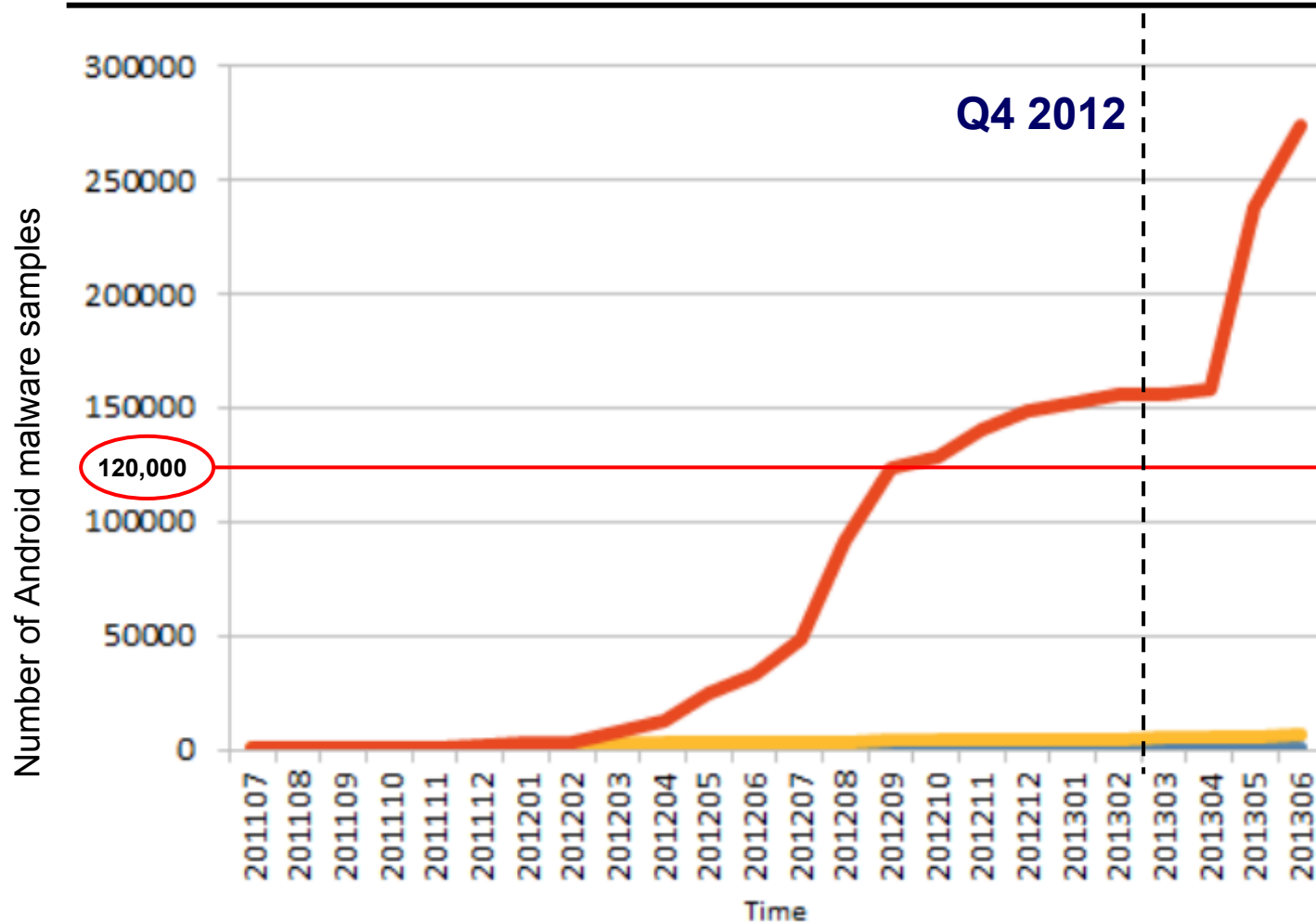
- 79% market share
- 1,000,000 official apps
- ~90 alternative stores

Popularity = Security Risks



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





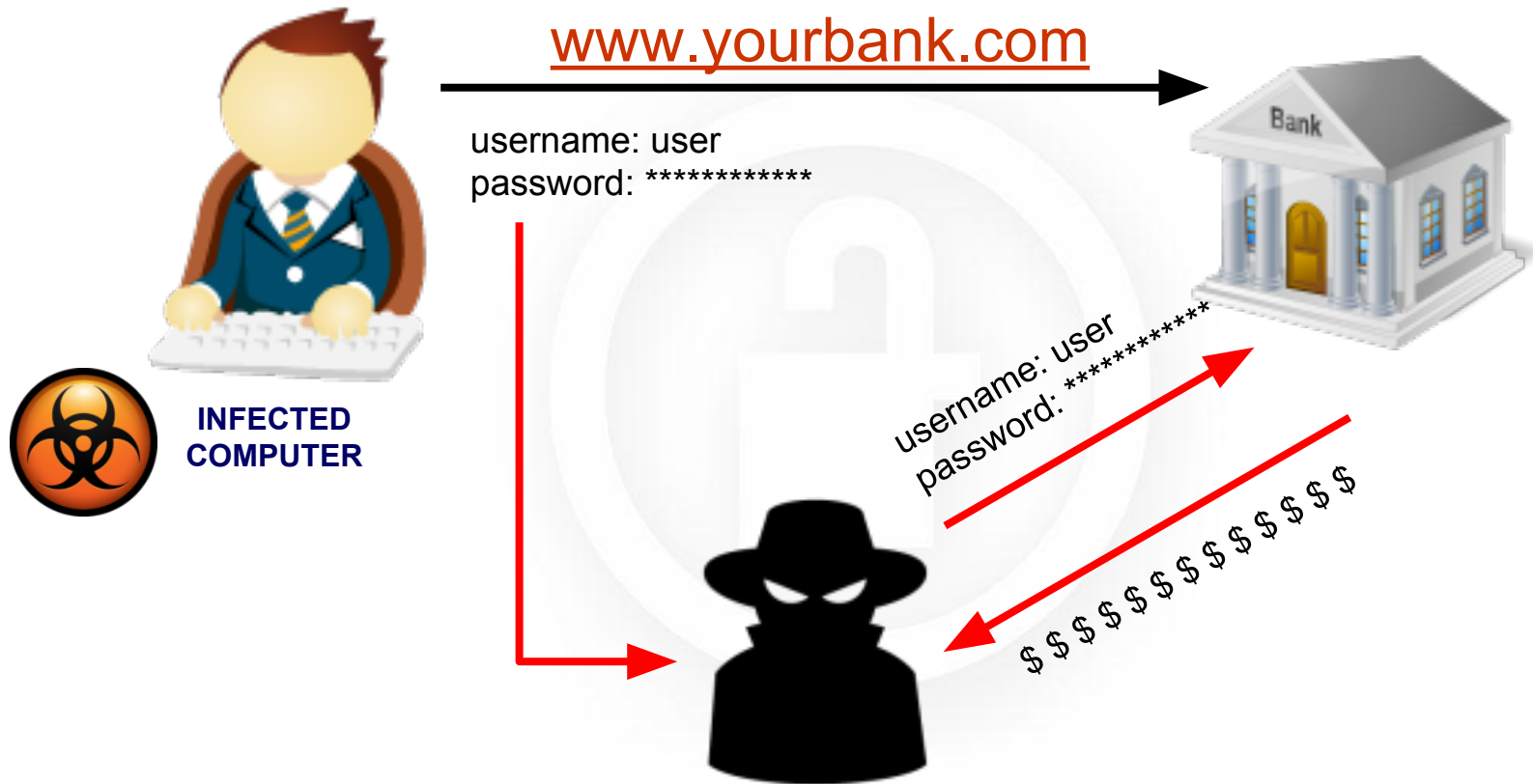
EXAMPLE

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)

A login form with a light blue background and a green border. It contains two input fields and a button. The first field is labeled 'USERNAME' and contains the text 'user'. The second field is labeled 'PASSWORD' and contains ten asterisks '*****'. A grey button labeled 'Login' is positioned at the bottom right of the form.

USERNAME	user
PASSWORD	*****

The attack scheme (2)

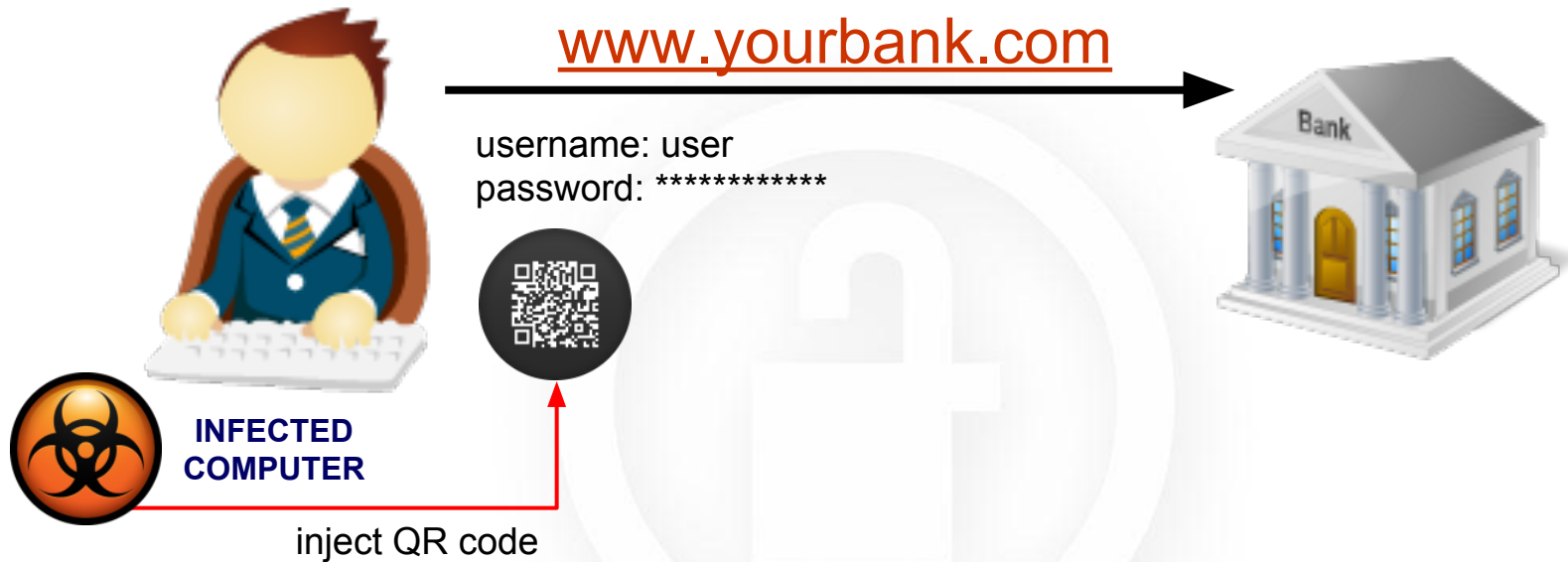


2-factors authentication (password + secret code)

ONE TIME SECRET CODE

GO!

The attack scheme (2)



Luring QR code

USERNAME

PASSWORD

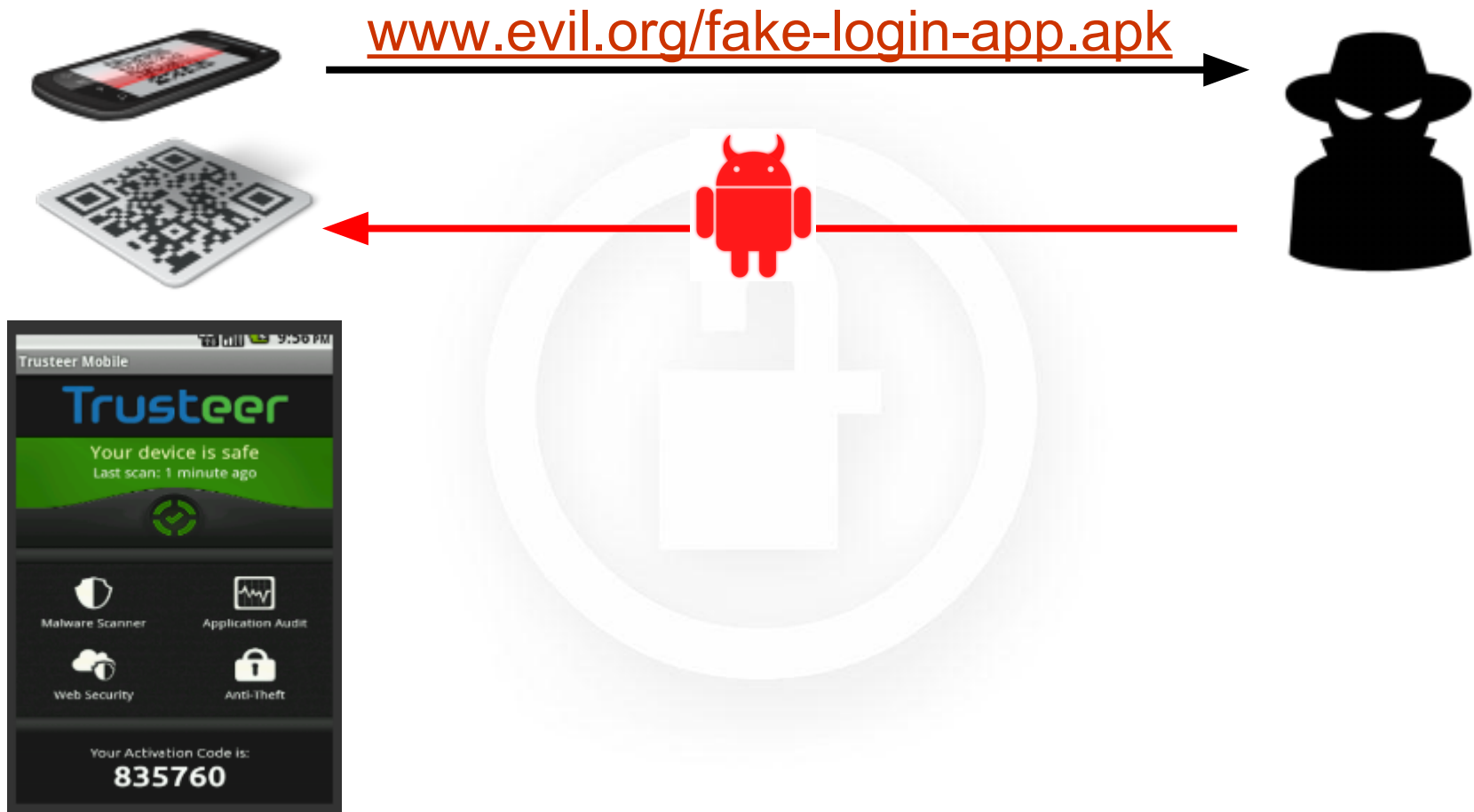
SCAN TO LOGIN



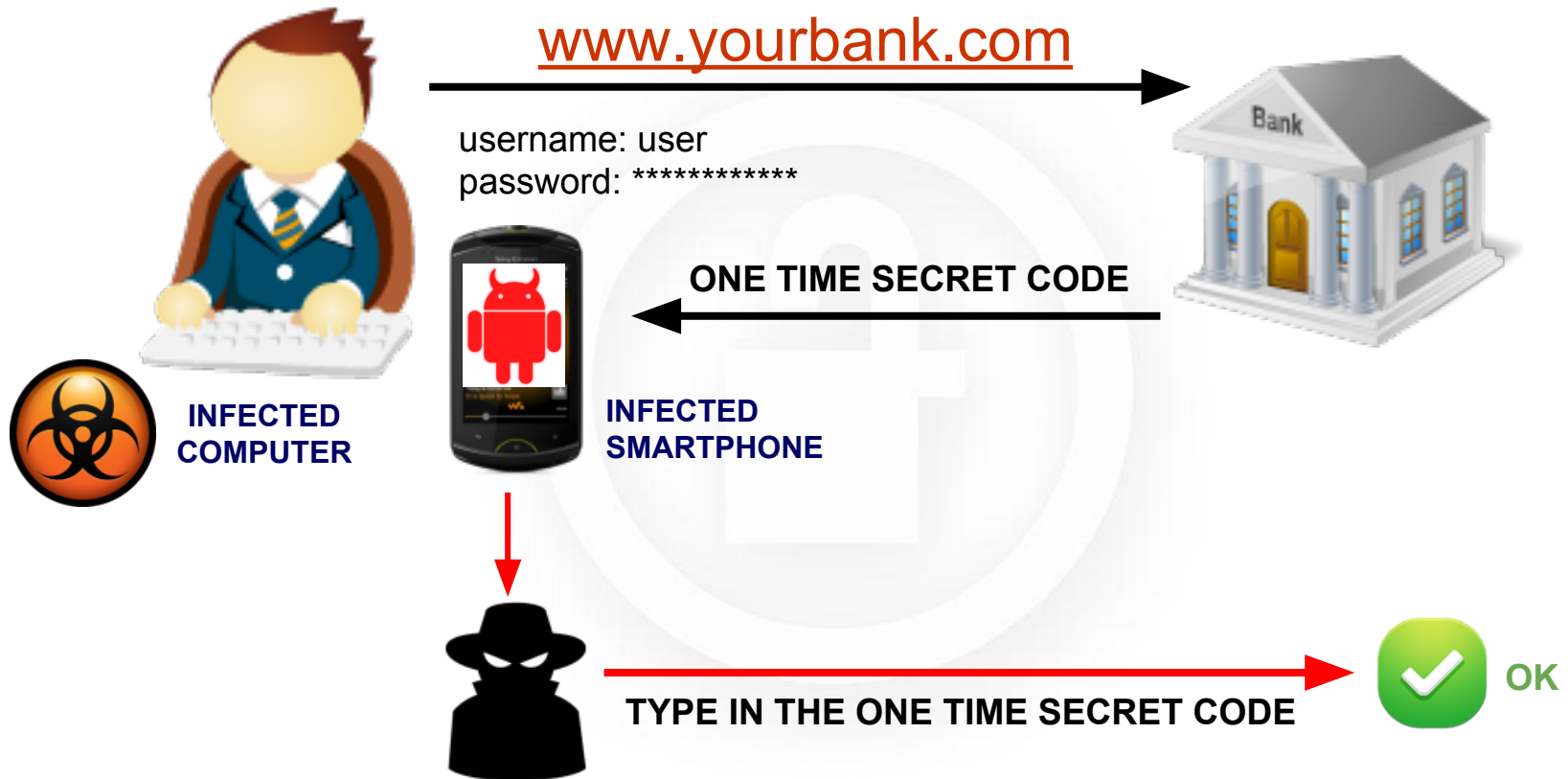
Login



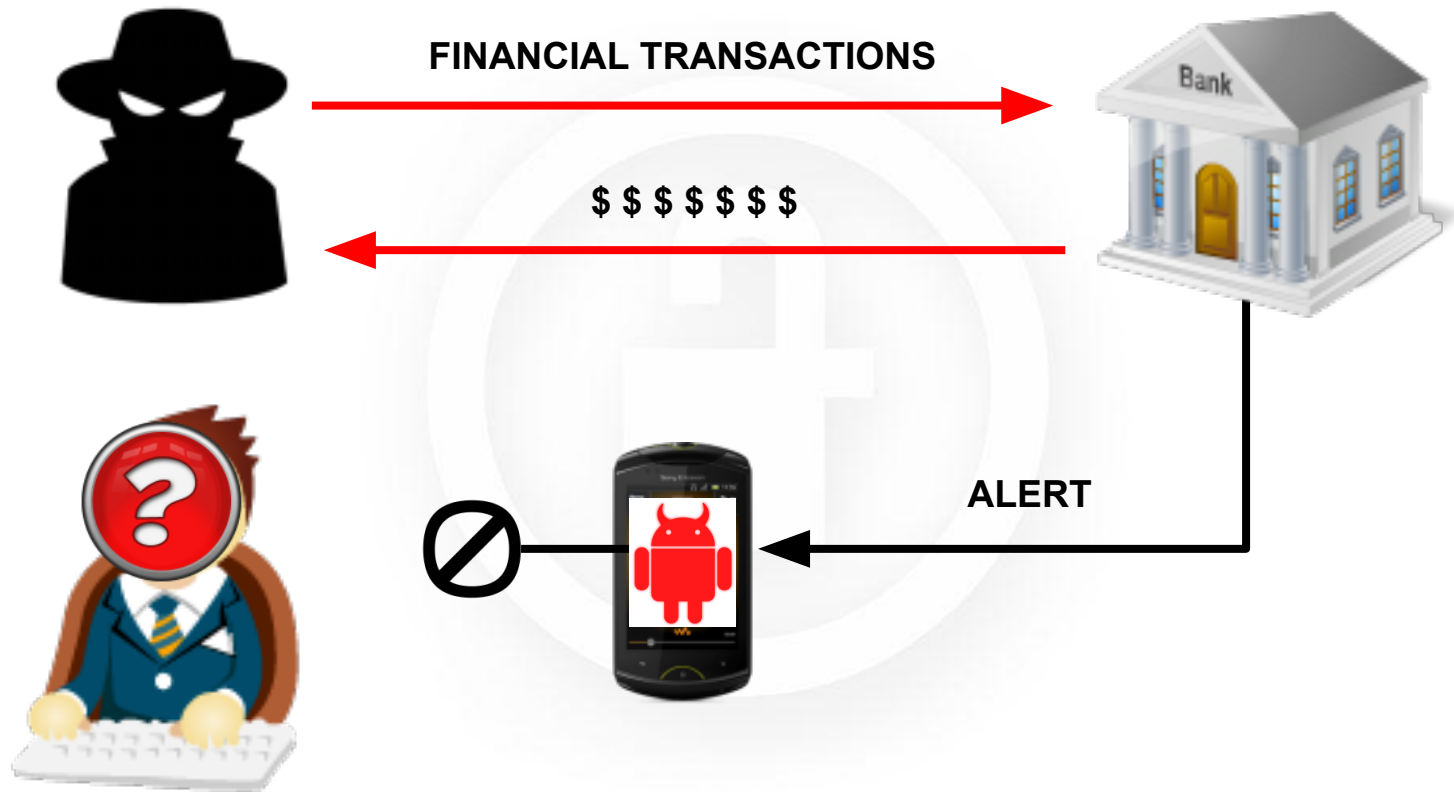
The attack scheme (3)



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

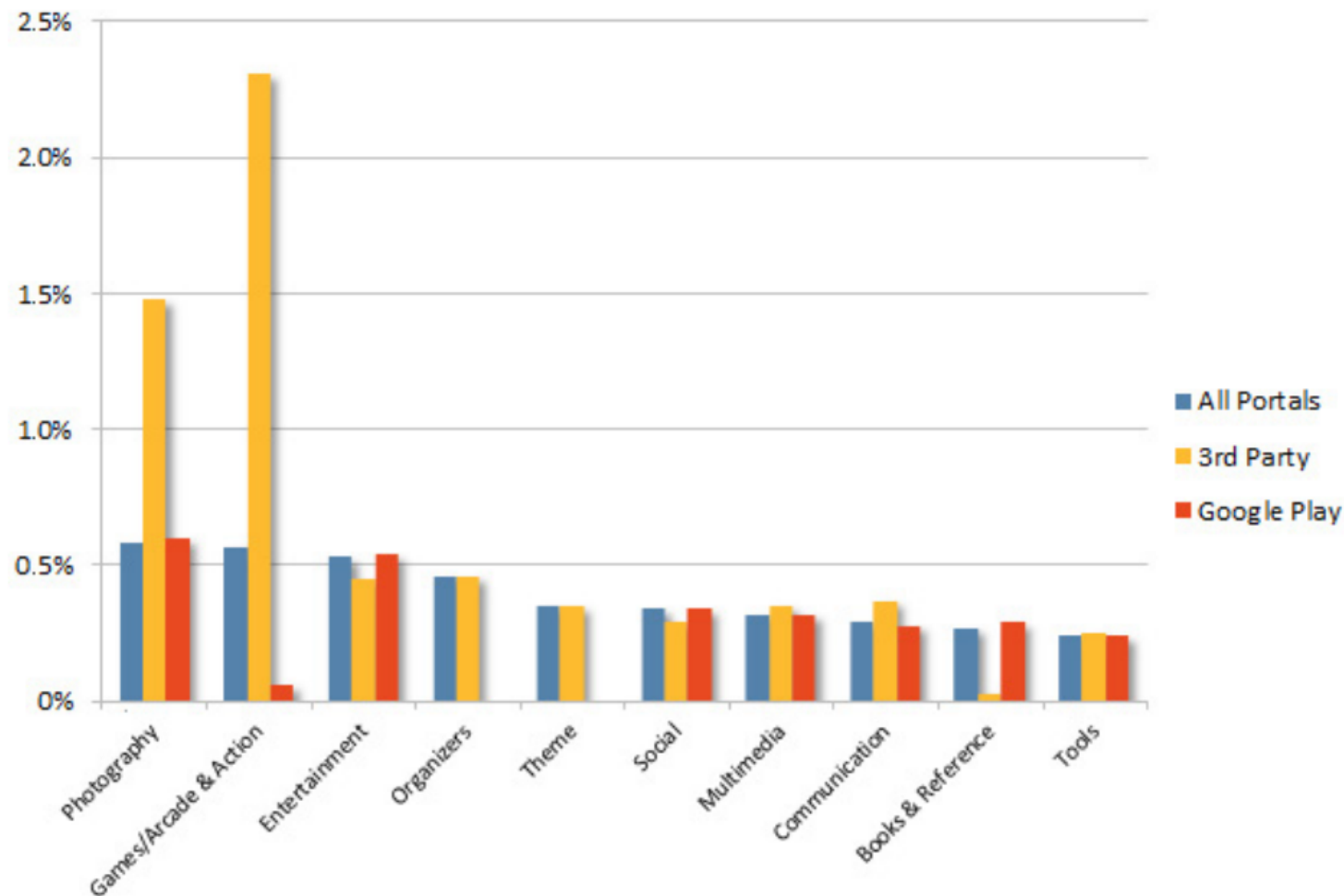
Android.Trojan.FakeMart

- Trojan, SMS stealer

Stells

- Multi-purpose trojan
-

Dangerous apps categories



Source ([Symantec, October 2013](#))

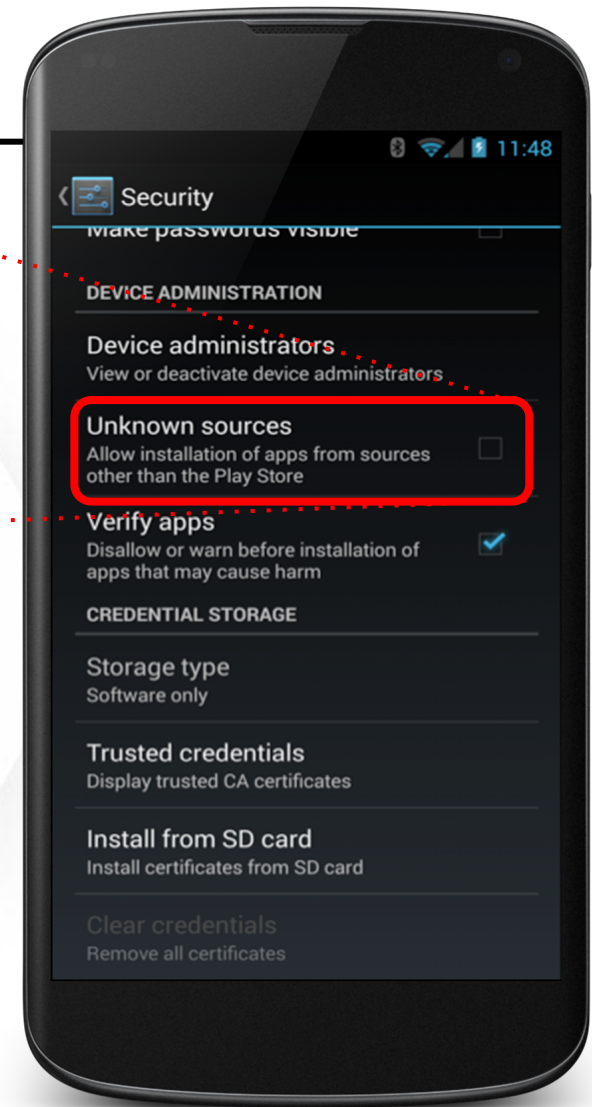
3rd party app marketplaces

Andapponline	Aptoid	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	Applicious	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



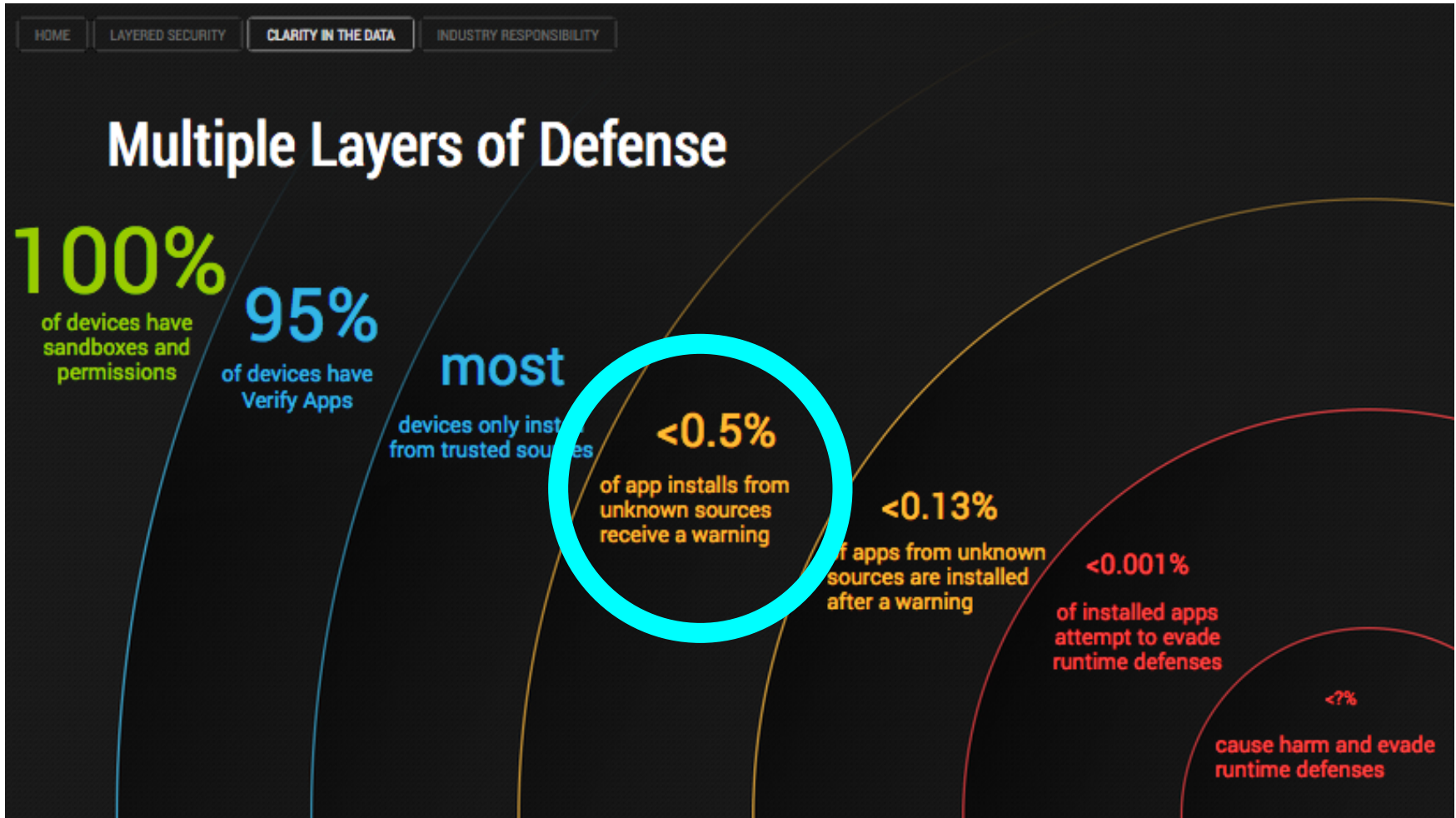
Do we have any clue on the size?

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

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

Google says that this is vastly exaggerated

This is vastly exaggerated

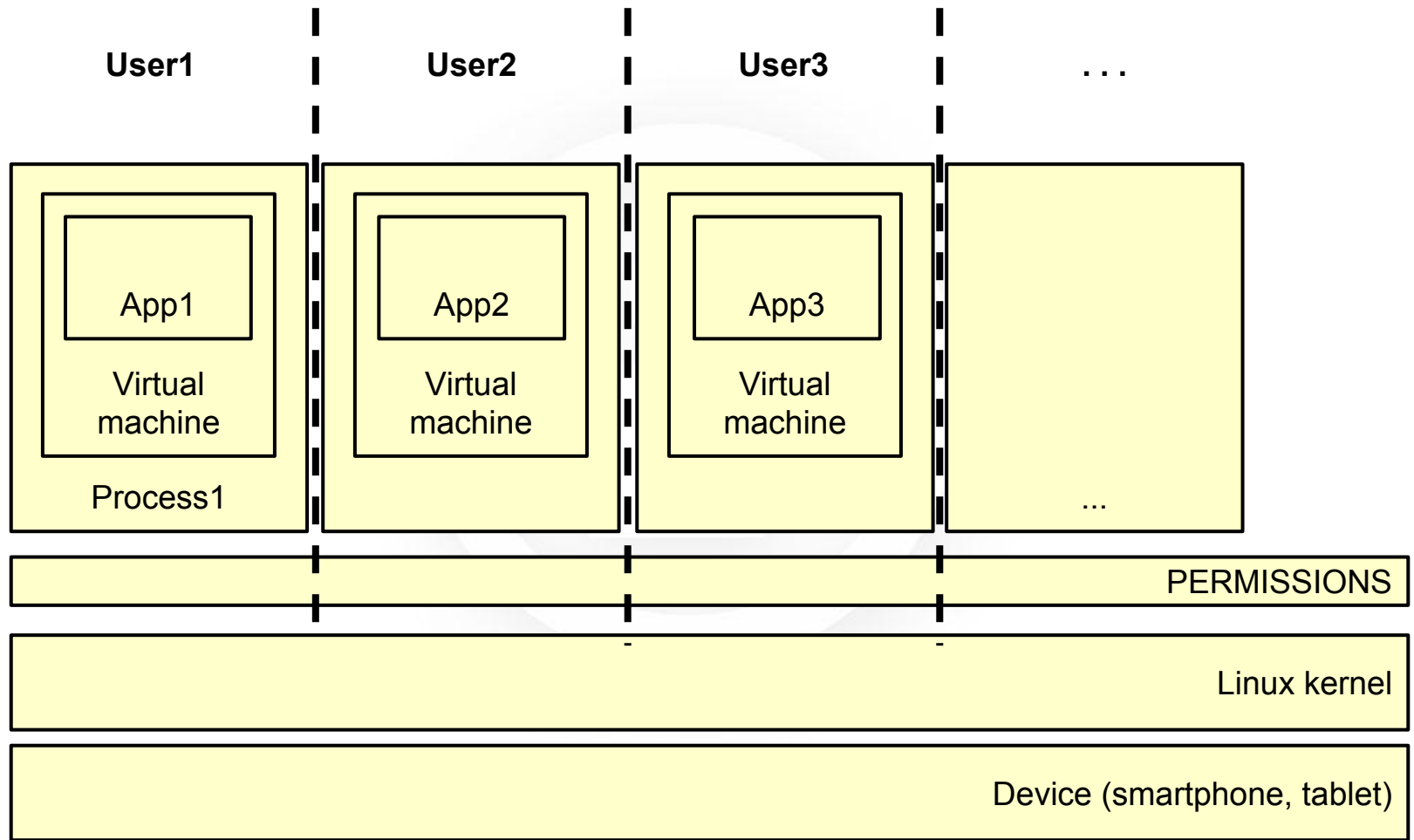


Source (Google, VB2013)

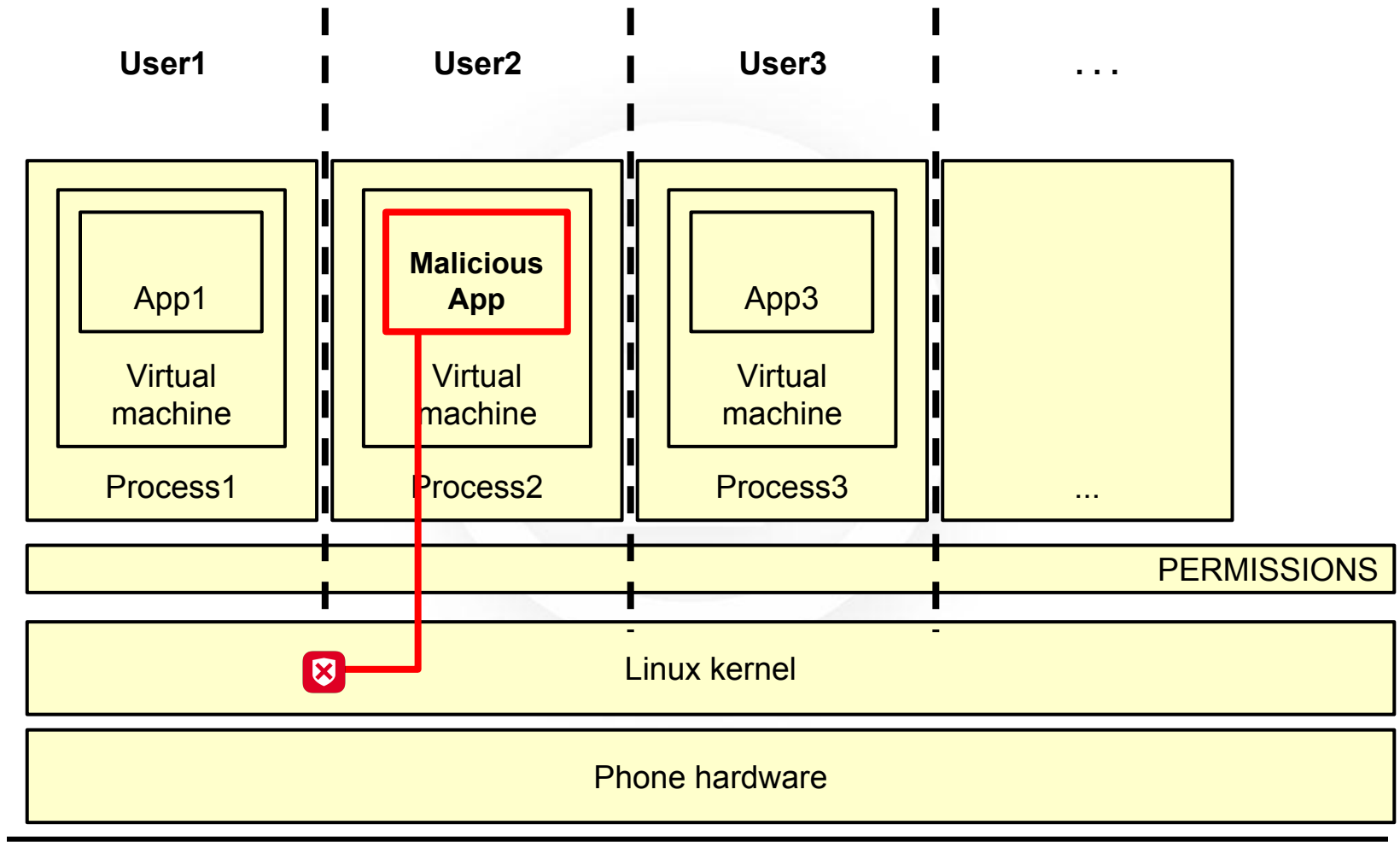
Protections

- 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



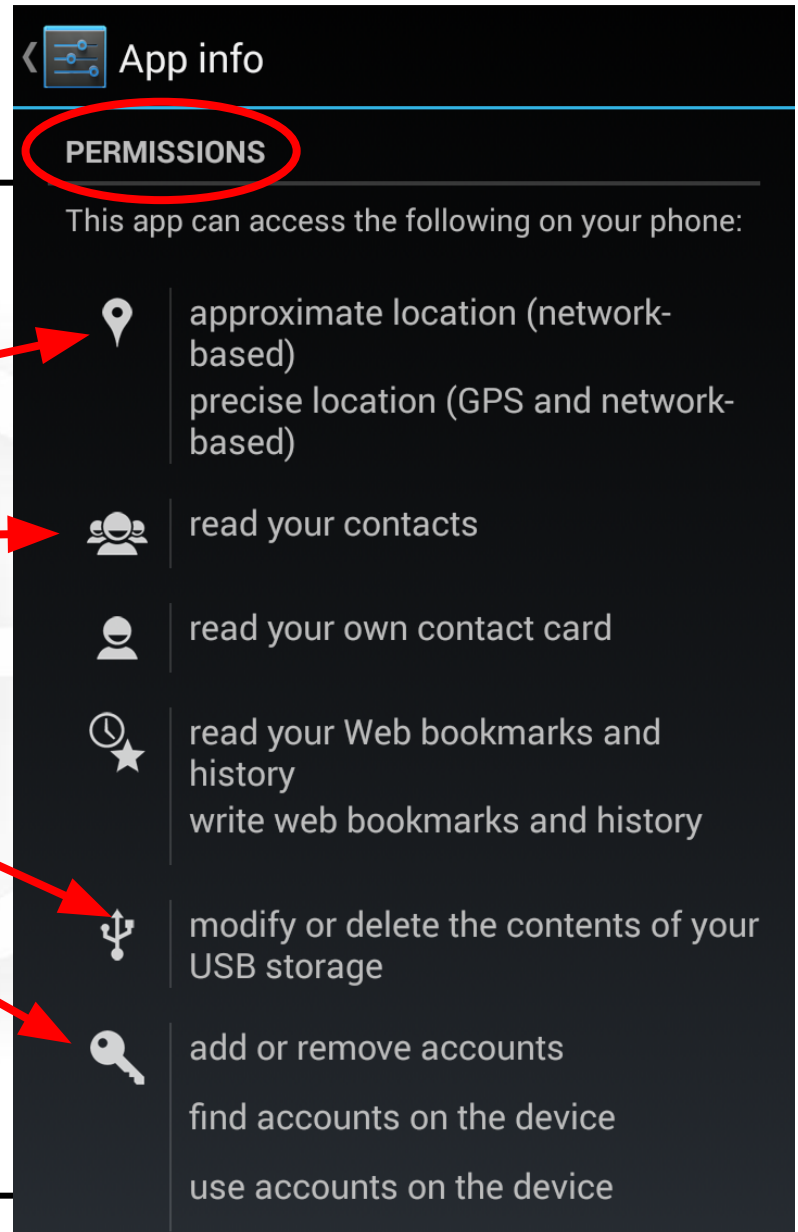
Linux-based process isolation



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 ★★★★★ FREE	 Mobile Security & A AVAST Software ★★★★★ FREE	 Antivirus Free Creative Apps ★★★★★ FREE	 Antivirus & Security Lookout Mobile Security ★★★★★ FREE	 Dr.Web v7 Anti-virus Doctor Web, Ltd ★★★★★ FREE	 Norton Security anti NortonMobile ★★★★★ FREE	 FREE Tablet AntiVir AVG Mobile ★★★★★ FREE	 Android Antivirus Android Antivirus ★★★★★ FREE	 NQ Mobile Security NQ Mobile Security (NYSE ★★★★★ FREE	 LINE Antivirus LINE Corporation ★★★★★ FREE	 Antivirus & Mobile S TrustGo Inc. ★★★★★ FREE	 Zoner AntiVirus Free ZONER, Inc. ★★★★★ FREE
 McAfee Antivirus & McAfee Mobile Security ★★★★★ FREE	 Dr.Web v8 Anti-virus Doctor Web, Ltd ★★★★★ FREE	 Bitdefender Antivirus Bitdefender ★★★★★ FREE	 Android Antivirus Android Antivirus ★★★★★ FREE	 Mobile AntiVirus Sec AVG Mobile ★★★★★ €10,99	 Free Antivirus 2014 Android Antivirus Resea ★★★★★ FREE	 360 Mobile Security Qihu 360 Software Co., L ★★★★★ FREE	 Android Antivirus Android Antivirus Pro ★★★★★ FREE	 Mobile Security & A Teebik Apps ★★★★★ FREE	 Mobile Security & A ESET ★★★★★ FREE	 Antivirus for Androi Mobla Corporation ★★★★★ FREE	 Antivirus for Androi Data Apps ★★★★★ FREE
 best antivirus inventor ★★★★★ FREE	 Mobile Security & A Bitdefender ★★★★★ FREE	 Antivirus Free Comodo Security Solutic ★★★★★ FREE	 Mobile Security & A Trend Micro ★★★★★ FREE	 Zoner AntiVirus Free ZONER, Inc. ★★★★★ FREE	 VIRUSfighter Antivi SPAMfighter aps ★★★★★ FREE	 GuardX Antivirus QStar ★★★★★ FREE	 Webroot Security & Webroot Inc. ★★★★★ FREE	 Hornet AntiVirus Fr Hornet Mobile Security ★★★★★ FREE	 Bkav Security - Anti Bkav Corporation ★★★★★ FREE	 G-Protector Anti Vin Gpc ★★★★★ FREE	 G Data AntiVirus Fr G Data Software AG ★★★★★ FREE
 SAFE antivirus and MSP Inc. ★★★★★ FREE	 MYAndroid Protecti MYMobile Security ★★★★★ FREE	 AegisLab Antivirus AegisLab ★★★★★ FREE	 Antivirus TESTVIRU PDefender Antivirus ★★★★★ FREE	 Best Antivirus Andri MSP Inc. ★★★★★ FREE	 Free Antivirus and S Sophos Limited ★★★★★ FREE	 Fastscan free AntiV K-TEC Inc. ★★★★★ FREE	 Antivirus & Anti-Adv SeCore Lab ★★★★★ FREE	 Tablet AntiVirus Sec AVG Mobile ★★★★★ €10,99	 EICAR Anti-virus Te xTorian ★★★★★ FREE	 Video antivirus revie PashaYakushev ★★★★★ FREE	 BluePoint Antivirus BluePoint Security, Inc. ★★★★★ FREE
 Dr.Web v8 Anti-virus Doctor Web, Ltd ★★★★★ €58,13	 Armor for Android™ Armor for Android™ ★★★★★ €23,02	 Mobile Security & A Panda Security ★★★★★ FREE	 Secure AntiVirus for Demand Apps ★★★★★ FREE	 White-Gate Antivirus White Gate ★★★★★ FREE	 My Antivirus Mobile Cloud Labs Plc. ★★★★★ FREE	 Test Virus - Android Android Antivirus Pro ★★★★★ FREE	 AntiVirus Playerum ★★★★★ FREE	 Android Antivirus P Android Antivirus ★★★★★ €3,99	 MyAntiVirus Pro - A PDefender Antivirus ★★★★★ €7,15	 BlackBelt AntiVirus BlackBelt SmartPhone C ★★★★★ FREE	 Security & Antivirus Webroot Inc. ★★★★★ €7,49
 Mobile Security Anti Wolfguard ★★★★★ FREE	 Zoner AntiVirus Test ZONER, Inc. ★★★★★ FREE	 Fastscan Anti-Virus K-TEC Inc. ★★★★★ €1,53	 FREE Android Antivi Cat Apps ★★★★★ FREE	 LabMSF Antivirus b LabMSF ★★★★★ FREE	 VG 기업용 Web SDK 인프라웨어 테크놀로지 ★★★★★ FREE	 AegisLab Antivirus AegisLab ★★★★★ FREE	 Free Android Antivi Meetio ★★★★★ FREE	 AntiVirus Laser MyNiko ★★★★★ FREE	 TWTR Antivirus An Stox.biz ★★★★★ FREE	 xCore Antivirus xCore LLC ★★★★★ FREE	 Privateer Antivirus Privateer Labs ★★★★★ FREE

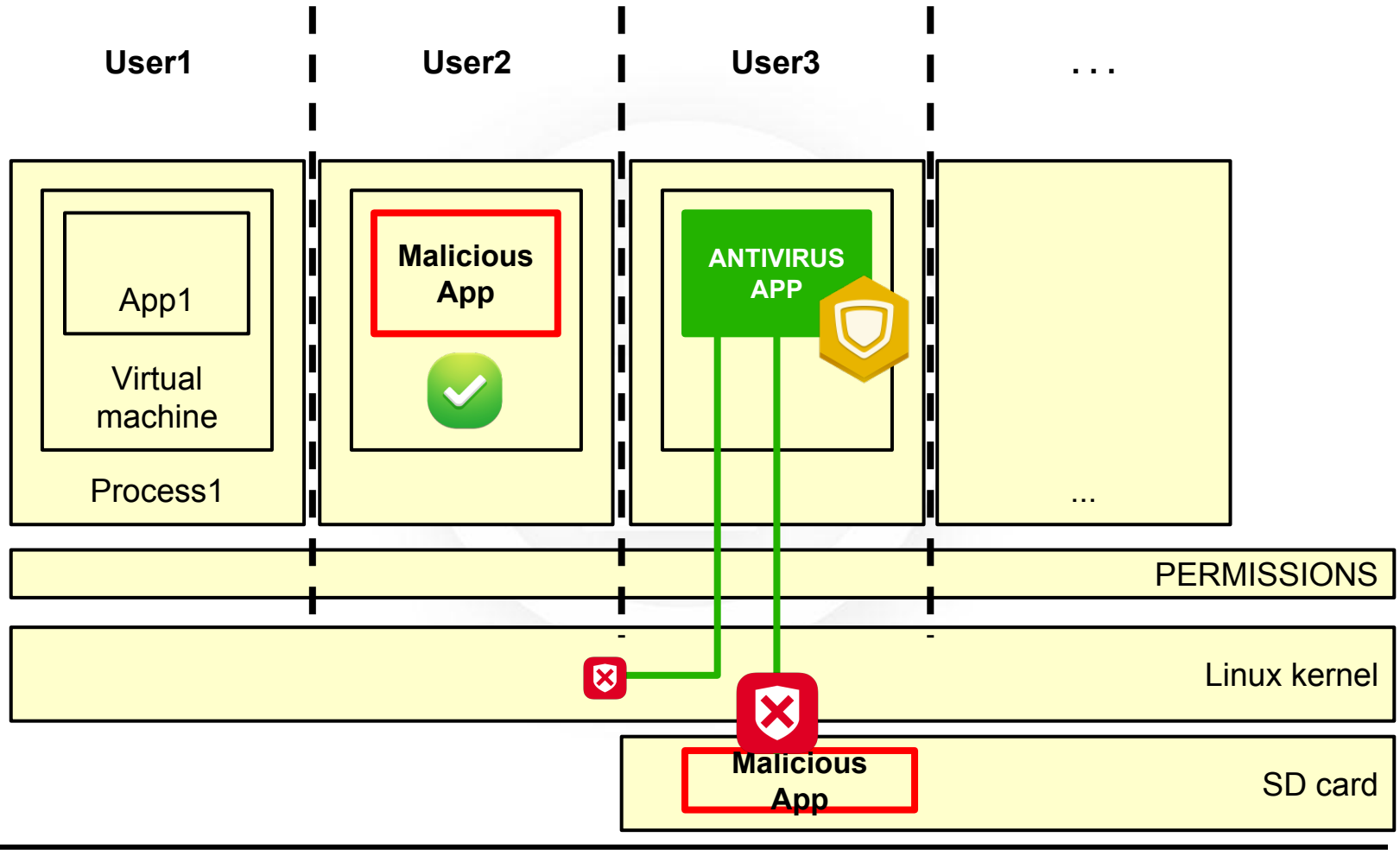
-
1. Android threats and protections
 2. **Limitations**
 3. Testing antivirus apps
 4. AndroTotal
 5. Status

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

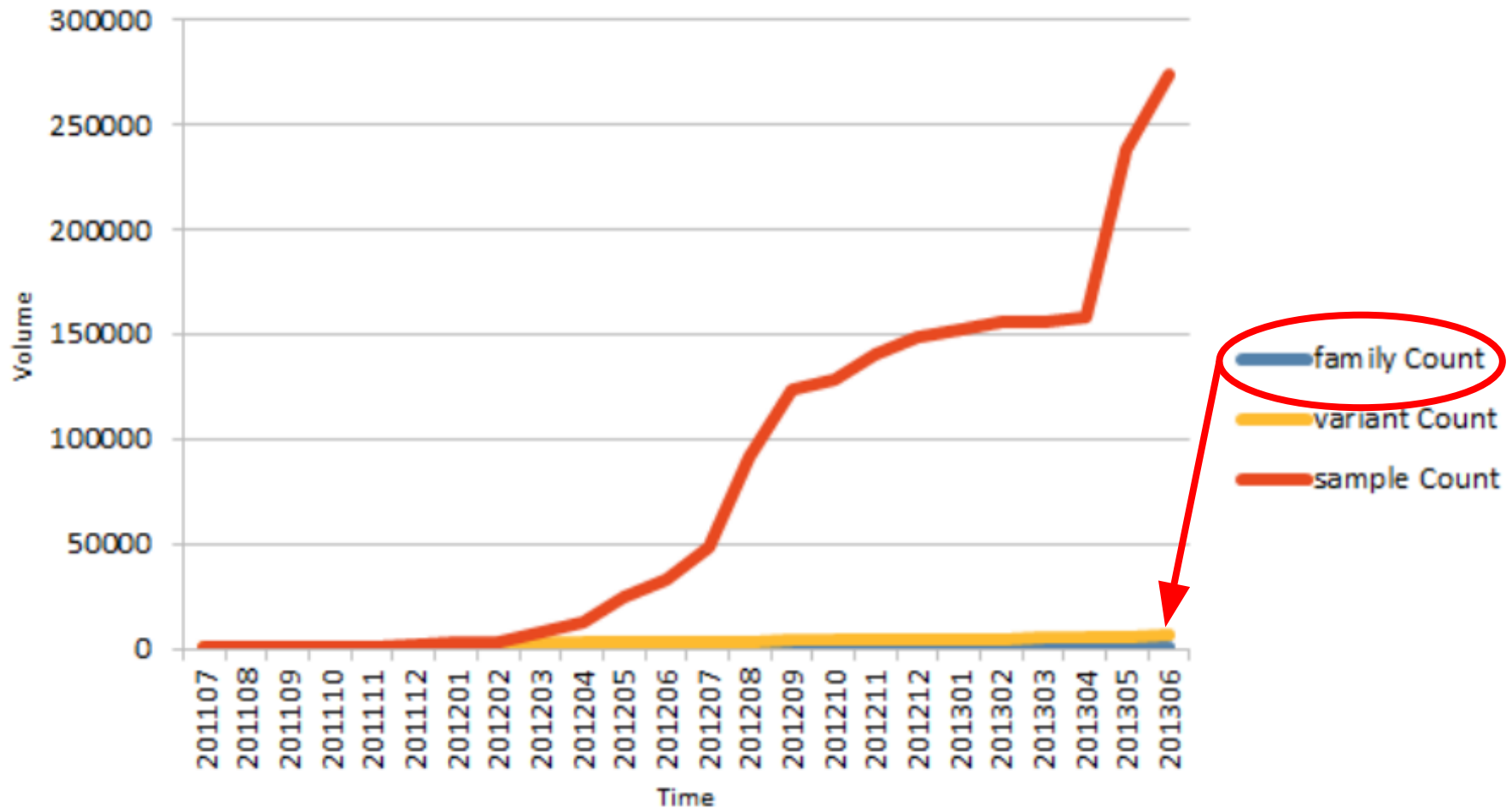
Less freedom

- A malware is an isolated app itself

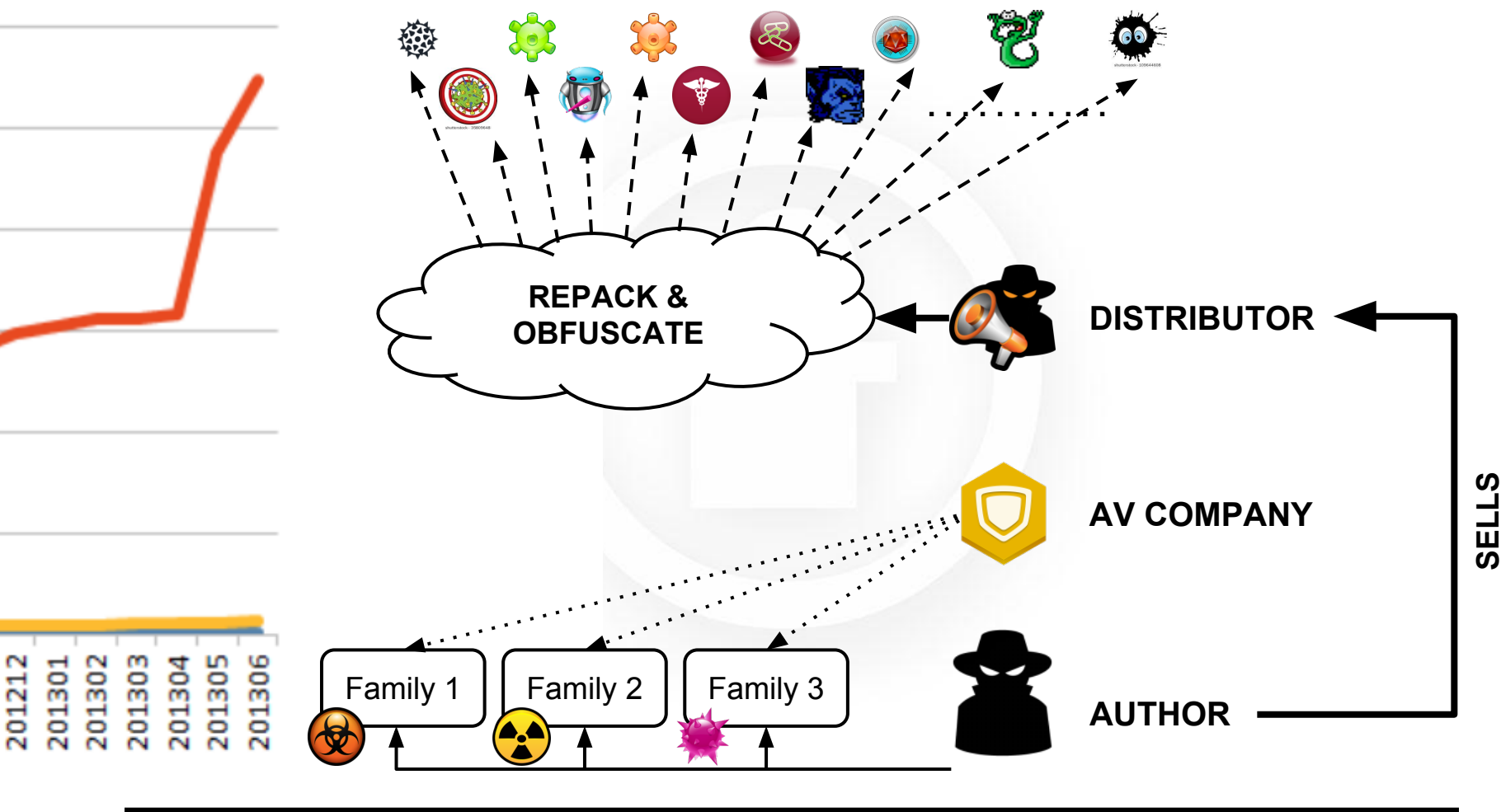
Workarounds

- 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)

$$1,000 \times 11 \times 100 \times 3 = 3,300,000 \text{ tests}$$

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.](http://www.andrototal.org)

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?

FISK

eaquito

Type the two words

reCAPTCHA™
stop spam.
read books.

Antivirus name	Antivirus version	Android platform	Detection method ⓘ	
Trend Micro, Mobile Security & Antivir	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	×

Sample MD5	cdbf63b2e5666799c4b74a8cd15565dd ⬇
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]

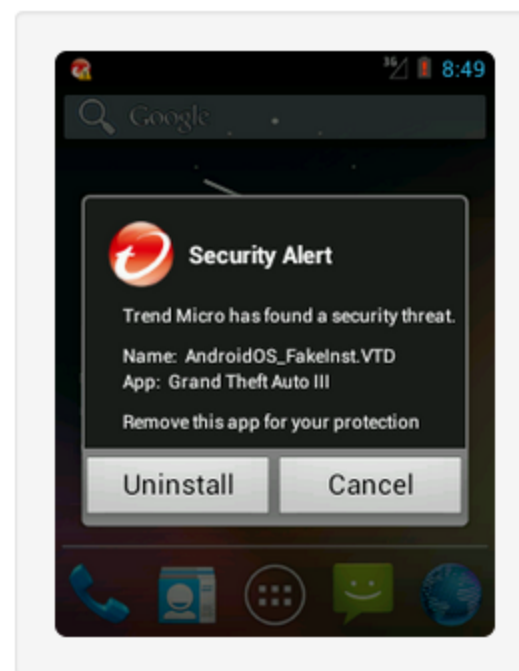
Last 10 scans performed on this sample

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 »

Mobile Security & Antivirus 2.6.2 scan for cddf63b2e5666799c4b74a8cd15565dd

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	cddf63b2e5666799c4b74a8cd15565dd 



Logcat dump [\(download\)](#)

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

Sample File

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

Force sample reanalysis ☐

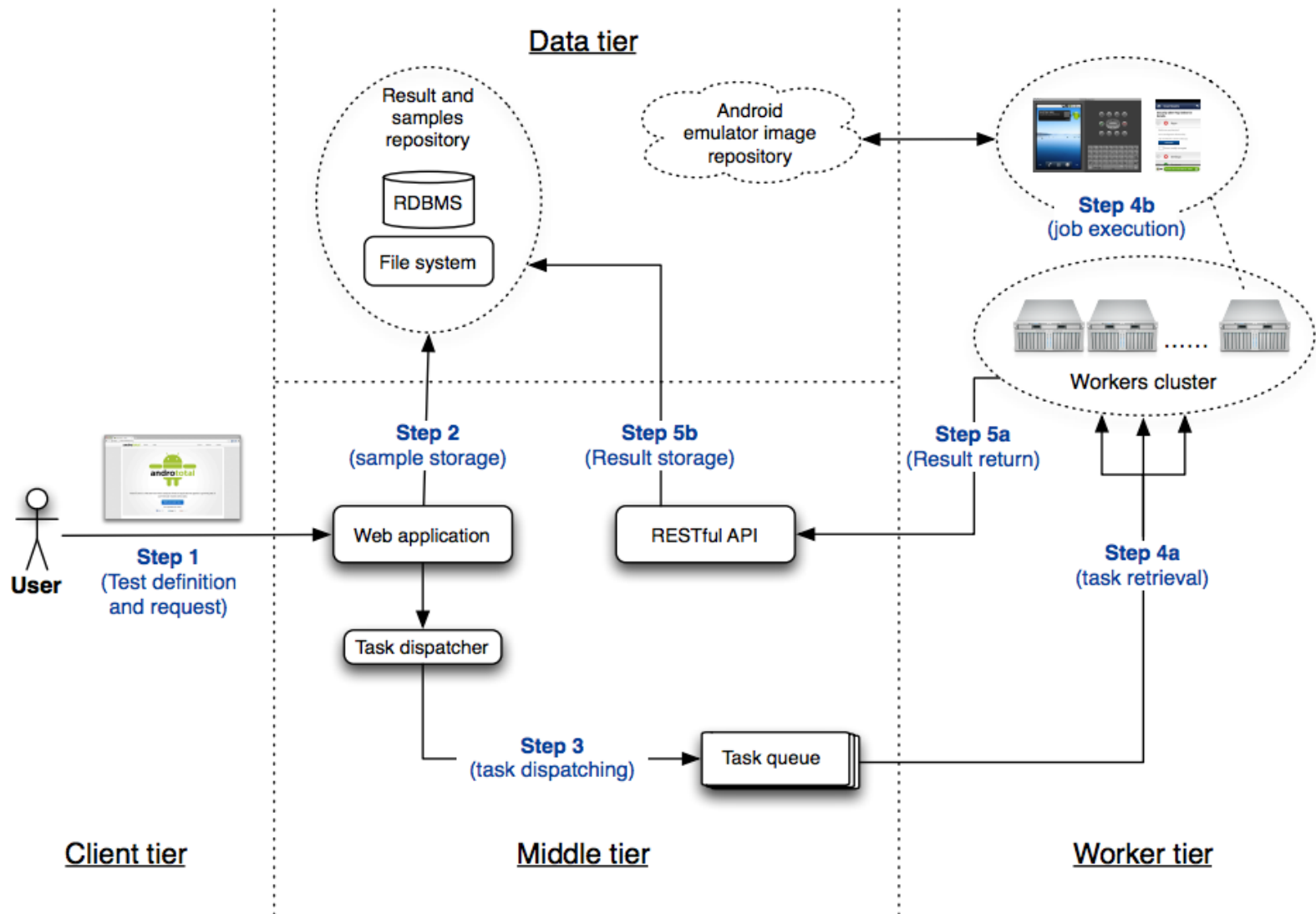
Obfuscate sample ☒

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

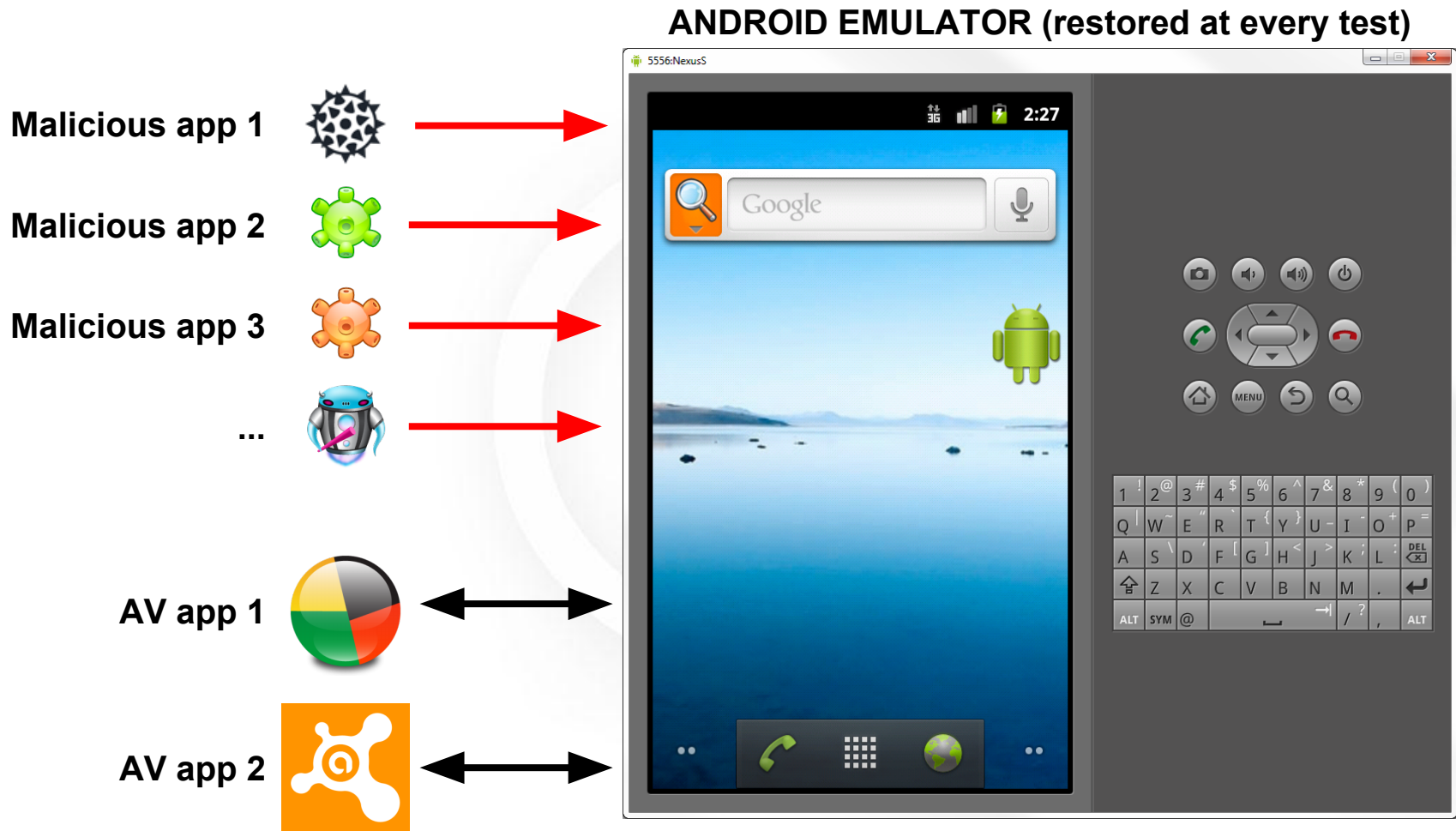
- ✓ Alignment
- ArithmeticBranch
- Debug
- Defunct
- Goto
- Indirections
- Nop
- Rebuild
- Reflection
- Renaming
- Reordering
- Repacking
- Resigned
- StringEncrypt

By clicking "Start scan!", you agree to our [Terms of Service](#) and our [Privacy Policy](#).

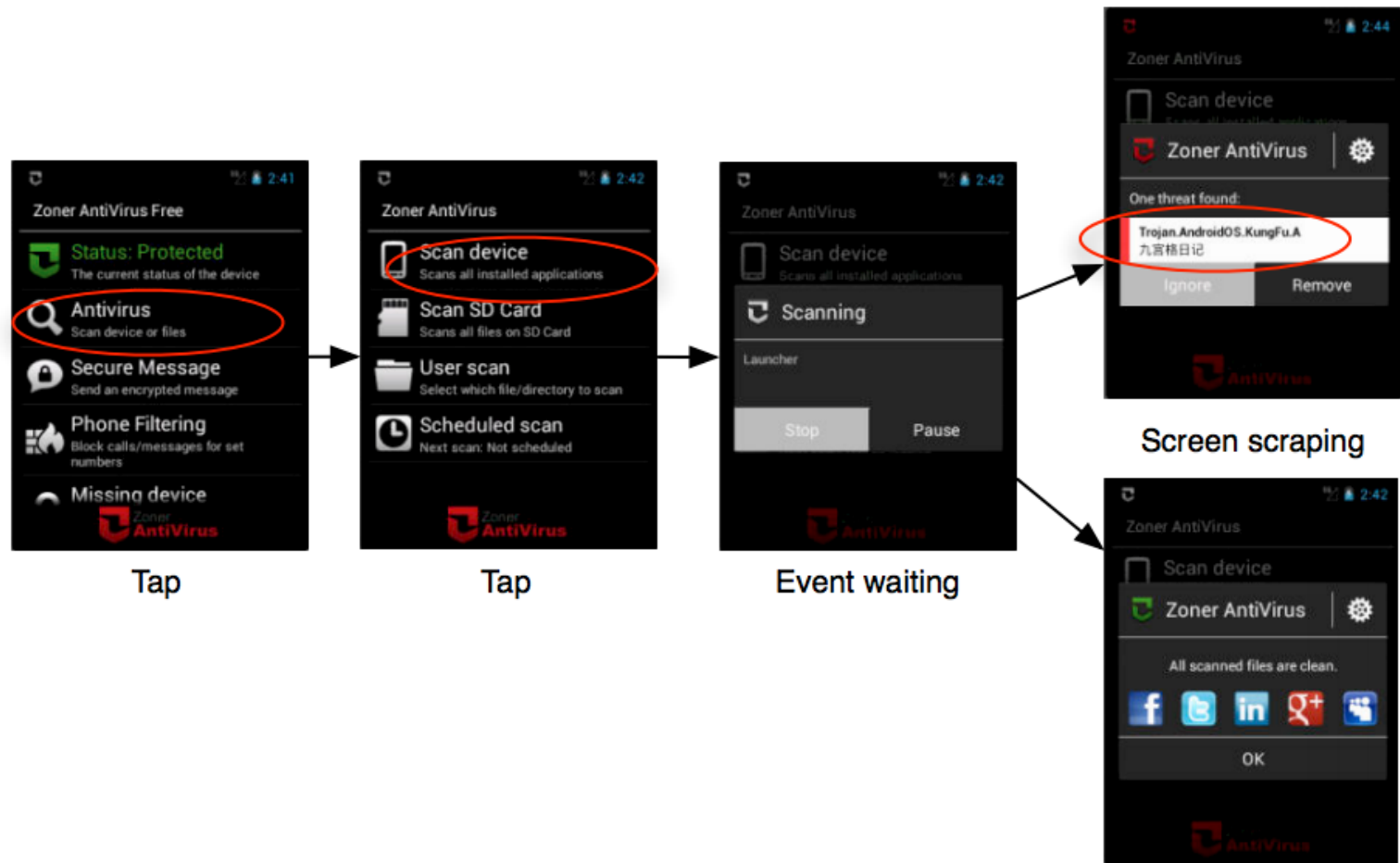
Architecture



The basics



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