

COME TO THE DARK SIDE

WE HAVE APPS!



FEDERICO MAGGI

POLITECNICO DI MILANO



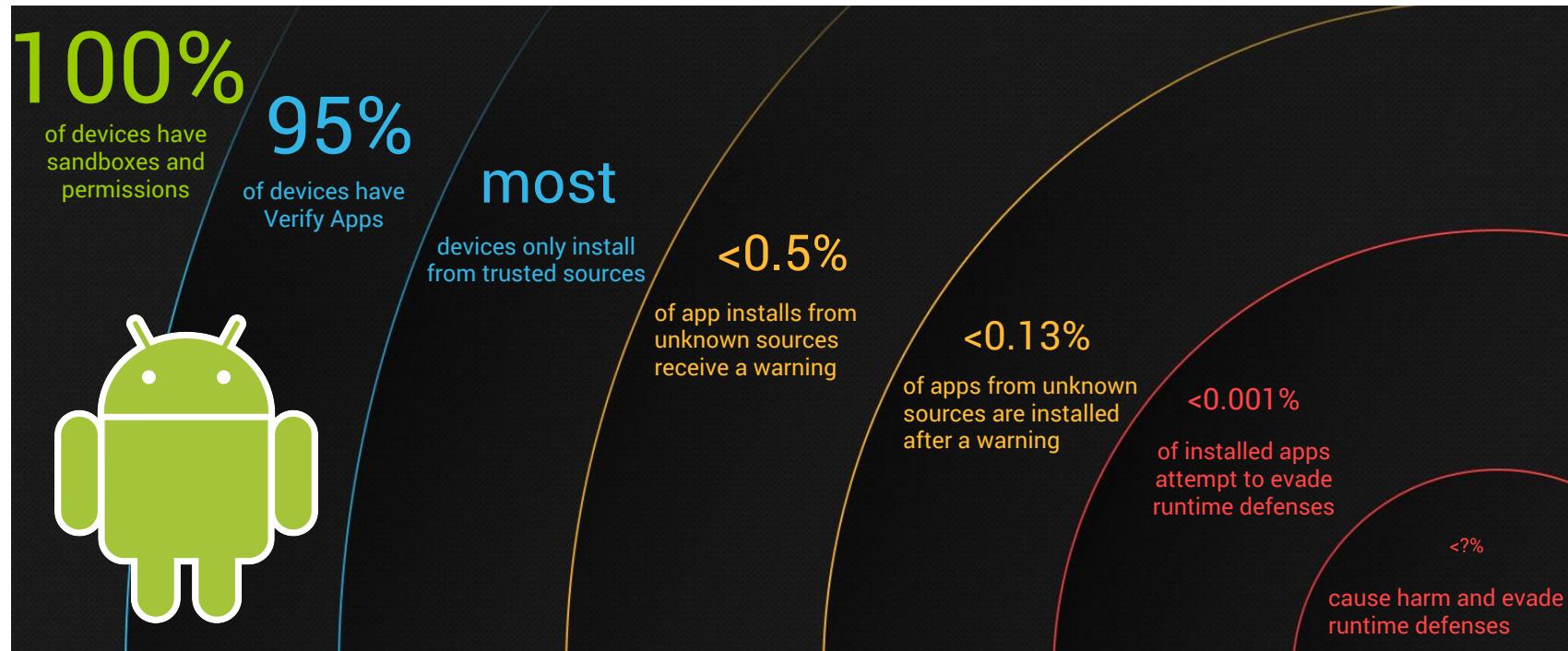
HACKINBO

SICUREZZA ALL'OMBRA DELLE TORRI

RINGRAZIAMENTI

- Martina Lindorfer
- Stamatis Volanis
- Alessandro Sisto
- Matthias Neugschwandtner
- Elias Athanasopoulos
- Christian Platzer
- Stefano Zanero
- Sotiris Ioannidis

NUMERI, NUMERI, NUMERI!



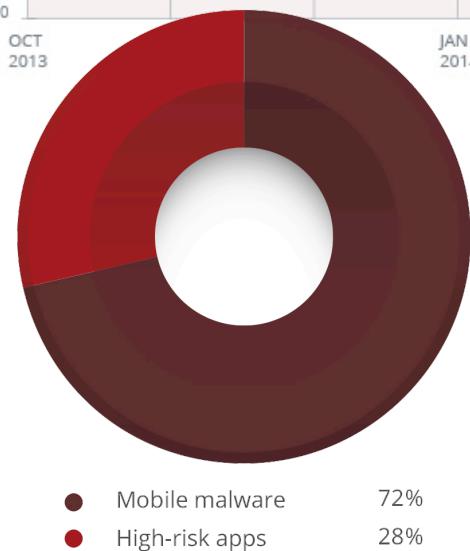
The Core of the Matter (NDSS13)
The Company You Keep (WWW14)

0.0009%
0.2800%

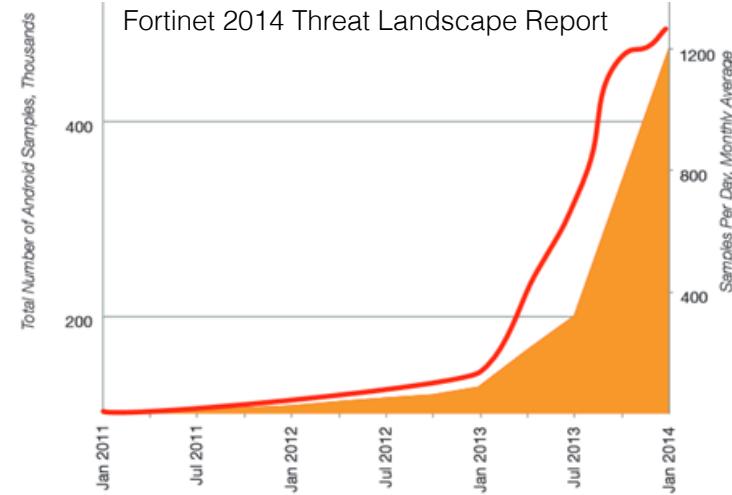


COSA DICONO GLI A/V VENDOR?

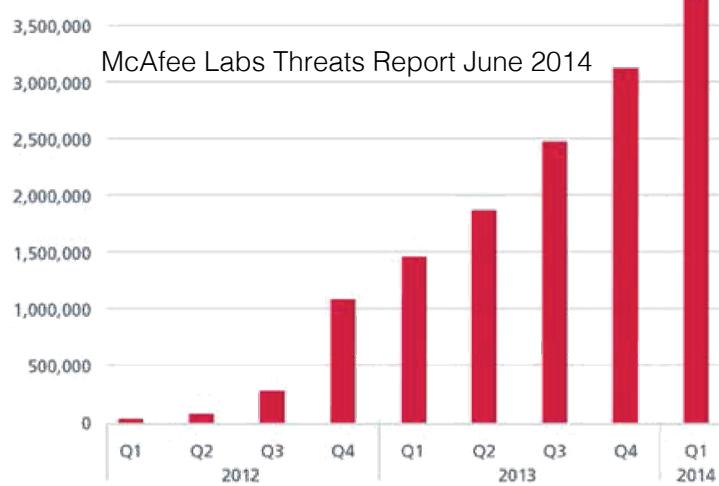
TrendMicro TrendLabs 1Q 2014 Security Roundup



Fortinet 2014 Threat Landscape Report



McAfee Labs Threats Report June 2014



MALICIOUS APPS



EVERWHERE

mememe

NON SOLO QUANTITÀ

```
class public Lcom/google/elements/AdminService;
.super Landroid/app/Service;
.source "AdminService.java"

# direct methods
.method public constructor <init>()V
    .locals 0

    .prologue
    .line 13
    invoke-direct {p0}, Landroid/app/Service;-><init>()V

    return-void
.end method

# virtual methods
.method public onBind(Landroid/content/Intent;)Landroid/os/IBinder;
    .locals 1
    .param p1, "intent"    # Landroid/content/Intent;

    .prologue
    .line 38
    const/4 v0, 0x0

    return-object v0
.end method

.method public onCreate()V
    .locals 6

    .prologue
    .line 17
    new-instance v0, Ljava/util/Timer;

    invoke-direct {v0}, Ljava/util/Timer;-><init>()V

    .line 18
    .local v0, "timer":Ljava/util/Timer;
    new-instance v1, Lcom/google/elements/AdminService$1;

    invoke-direct {v1, p0}, Lcom/google/elements/AdminService$1;-><init>(Lcom/google/elements/AdminService;)V

    .line 33
    .local v1, "task":Ljava/util/TimerTask;
    const-wide/16 v2, 0x0

    const-wide/16 v4, 0x7d0
:-:- AdminService.smali  Top of 2.2k (1,0)  (Smali WS Projectile[elements] P)
```

```
.method private cce(O)V
    .locals 12

    sget-boolean v0, Lcom/molsoft/mate/Application;->caf:Z

    if-eqz v0, :cond_0

    :goto_0
    return-void

    :cond_0
    const-string v0, "abc02\ube2b\udb9c\u958b\ucfb4\uc052\u54bc\u8a39\u46df\u459\uf31\u73f0\udbc4\u1e4d\u1d21\uf454\ue61e\u6e16\u50be\u97e0\u2ee6\u02d2\ue8e1c\u47f8\ubc9d\u9919\u343b\u0c75\u0de4\u1f70\ub7d6\uba7b\ufbb2\ub28b\ud1b2\uf413\uc63\b1\ub2624\u4c41\u9098\u6e25\ub2c44\ub748\ub1366\ub46f0\ub746e\u90f8\udc35\ud111\ub4609\ub955\ue8c6\ufbbd\uce75\uece8\ub294\ub0beb\us3a4\uf4e9\u7e10\ubc952\udcd3\ub5ed\ub7c2\b3\ub959\ua1f7\ub502\ub80b\ud3b62\ub1a3\ub474c\ud5ef\ub4820\ub96ad\ud6b8\ube35\ub789\ub81b\ub200f\ub02e1\ub08bf\ub915d\ub6922\ub1535\ub0b43\ub94bb\ub1d96\ub855a\udfa\udca\b4\ua9af\ub30fd\ub53c\ub5108\wedda\ue0c6\ub531\ub894f\ub86ff\ud61\ub93d4\ubc8b7\ub6ef1\ub4\ub151\ub7cf5\ub5cb\udc30\ub0af7\ubcd7\ub7c6c\ua1f1\ub68d\ub5eb\ubc90d\ub337\ubc168\ub69f\b8\ub0869\ub211\ubff5\ub3720\ub8f01\ub83d6\ub74aa\ubc0be\ufd29\ubd6b\ub78e6\ub007\ub9ba\ub3908\ub3fe\ub2799\udc27\ub1500\ub738\ue14c\uefb\ub9667\ubc150\ub8f37\ub655c\ub74fe\ub222\b8\ub08dc\ub5af5\ub4c2f\uffb0\ub3a58\ubfb\ub1a52\ub04ed\ub251d\ub8f2a\ue237\ub346e\ub62ba\ub433a\ua113\ub764c\ub50b8\ubcc\ub9e86\ub2088\ubb36\ub6873\ub2b9\ub4c71\ub7029\ubc21\ub521\b1\ude26\ub72ff\ub56d4\ub0381\ubc66\ub7fb5\ub9e5a\ub47d1\ubc254\ub9334\ub299\ub2d49\ub5f89\ub5828\ub9674\ud491\ua319\ubde9\ub27a\ub9004\ubbd3\ue3da\ub7daf\ubc90\ub77ab\ub336c\ub74d\b2\ub6ac6\ub996\ub2f1\ubadd0\ub75b\ub3ef\ub9dc6\ub8ce1\ub4cb\ub741\ubc4f6\ub2725\ubca18\ub449d\ub3c6c\ub594d\ub74e\ub227e\ub637f\ub063e\ubec8\ub4d28\ub404e\uaaa3\ub700\ub1280\ue59\b4\ubacd\ub5db\ub43af\ub2c64\ub976f\ub43cd\ub1aa2\ubaa57\ub3262\ubab8\ubd65d\ue42f\ub671a\ub354c\ub150d\ub3b36\ub41f0\ubf342\ub7492\ub8917\ubad77\ub32f1\uf3fc\uebe2\ua6cc\ubbdd\ub6cb\b6\ua8f8\ubac2d\ub8a67\uf403\ub4b15\ub16bd\ub308\ub9718\uf7bc\ud497\we64c\udc84\ub50b6\ub472\ub1316\ub7821\ub3ec\ub1293\ub3ca\ub3b9f\ub7ff2\udaf\ub633\ub51b8\ub958\ub287\ub677\b7\ub3882\ub718\ub0a9\ub29b2\ub2f20\ub5754\uf1c6\ub4003\ub8e6d\ub2303\ub5da6\ue79b\ub64e5\ub5e60\ub825\ub360\ub7de2\ufbdd\ub2464\ub8bd3\ubc2f6\ubf9f0\ub630c\ue81d\ub2f1\ub3e2f\ub69c\b4\ud7c3\ub26f\ubc435\ub8e61\ub632\ue96c\ubd7f\ub8d37\ub8f2\ub94a4\ub391b\ub058\ub8e5\ub2f3\ue361\ub397\ub2eb4\ub17b2\uebb7\ub7399\ubc38a\ub4bc3\ub3e39\ub8f74\ub045\ub646\ub7ae\b6\ubc73\uf17f\ub12c\ub0d35\ub7035\ue1d9\ub8180\ueae\ue170\ub91dc\ub3c47\ufdb\ub91f1\ubcd97\ua146\ub08dd\ub2ec8\ubbfb\ub30f6\ub9649\ub75\ub6ed\ub510c\ub207\ub9cc7\ub7079\ubc5\b2\ub63fe\ub0e3\ubed3\ub5d48\ue6ab\ub70c\ub5a0\ub526\ub2767\ub385d\ue2cf\ua856\udf6e\ub6d98\ub6977\ub2ab0\ub670d\ub00a7\ubd13\ub4d2f\ub7ef3\ub4278\ubb62\ub7e03\uffd3\ub3c2e\ufab\b7\ub8696\ue0e9\ub2eb4\ub3445\ub3bd\ubd37\uba22\ub3b6d\uaad2d\ub5d5a\ub89f7\ubdb27\ub75a2\ub0ed4\uf4ff\ub1916\ub3ac3\ub55e\ub6987\uae03\uf1e3\ud795\ub55bc\ub0265\ub4462\ub7b9\ub106\b2\ud64b\ub6454\ub094d\ub039c\uddb6\ub668b\ue2f2\ub7a3\ub9b38\ud5a9\ub87da\ua8d4\ub4bf6\ubd5e\ub4f81\ub1999\ub68de\ub16a8\ub48a0\ub82d\ub206f\ub56f\ub2f0a\ub993d\ub16ad\ua8f1\ubbee\b7\ud98c\ub1905\ud941\ubc23\ub1d32\ude87\ub5d26\ub0f3a\ub2a2\ub75e0\ub4a04\ub8b2\ub96c\ub875\ub34f4\ub154c\ub1ddc\ub349e\ub7305\ufe24\ud207\ub597\ub5ab5\ub2cd7\ub728b\ub15e8\ub5e8\b0\ub9e58\ub3661\udd16\ubc1ce\ub6d98\ub220b\uf0a\ub232\ub1a2d\ub5bc7\ub0ffc\ub1741\ub600\ub938\ub64d9\ud402\ubfd3\ub13c8\ub6ef1\ub6f1\ubd52\ub754\ub964\ub2f0d1\ub1d7e\ub1c3\ub12d\b2\ub3343\ub48e0\ub7f41\ub587\ub8d39\ub0714\ub2bb\ubfa40\ub9c62\ub9648\ub2651\ubf26c\ub4981\ub5074\ub1a37\ub0421\ubca7\ufcd14\ub136e\ub1c0\ubd65\ubce5\ubfaa6\ubad9\ub9864\ub6cc5\ub063
:-:- Application.smali  3% of 86k (128,0)  (Smali WS Projectile[mate] Pre)
```

- Perché così tante app malicious e così pochi dispositivi infetti?
- Qual è il motivo che permette a sviluppare così tante app malicious?

FACCIAMO UN PASSO INDIETRO

- Come sono distribuite?
 - Google Play Store (ufficiale)
 - Torrent
 - Siti, blog, ...
 - **App store alternativi**
- Quanto sono diffuse nei market?
- Quanto frequentemente sono scaricate?
- Gli app store adottano qualche misura di sicurezza?



MALWARE vs. ANDROID MALWARE

Malware tradizionale (desktop)

- al massimo sappiamo il sito che ha tentato di “exploitare” il nostro browser

Malware Android, iOS, Windows Phone, etc.

- Metadati interni
 - Nome, sviluppatore
 - Package name
 - ...
- **Metadati esterni**
 - **Titolo (su market)**
 - **Descrizione, commenti, stelline**
 - **Numero di download, ...**

Farting Panda – Android Apps on Google Play
https://play.google.com/store/apps/details?id=air.nl.bellpepper.fartingpanda

Google play Search Sign in

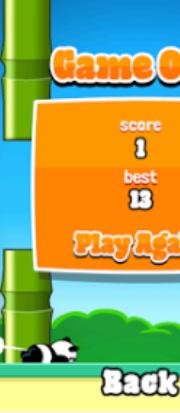
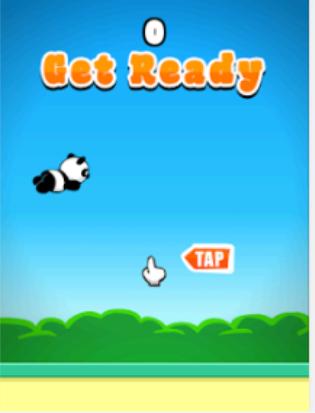
Apps My apps Shop Games Editors' Choice

Farting Panda
Bell Pepper Edutainment - 11 March 2014 Arcade

Install Add to wishlist

★ ★ ★ ★ (1,733)

g+ 1663 Recommend this on Google



Description

Are you up for the challenge?
Who needs a bird (even the flappy kind) if you can have a Panda?
Panda ate a splashy fish for breakfast, a flappy bird for lunch, and now his farts propel him high up in the air!
You know the drill:

- Tap!
- Fart!
- Avoid the bamboo!
- Get the hiscore! (mine is 15)

Farting Panda – Android Apps on Google Play

https://play.google.com/store/apps/details?id=air.nl.bellpepper.fartingpanda

Reader

Reviews

3.4

1,733 total

★ 5 732
★ 4 215
★ 3 210
★ 2 171
★ 1 405

Jaxon Daoust ★★★★★
Addictive OK so I never played flappy bird. But this cute lil panda is addictive. Originally got it for my son

keishajo1973 ★★★★★
This is Awesome Zoos vu oversees Irene g deck vhf devilish cheese CIC faucets x Dudish v distends distrusts

What's New

- With music!
- With high quality graphics!
- More than 10 farting sounds!
- Play the game, or use the main menu as a musical instrument!
- Fart your way into the highscores!
- Made the collision check better.
- Performance tweaks.

Additional information

Updated 11 March 2014	Size 11M	Installs 100,000 - 500,000	Current Version 1.3.5	Requires Android 2.2 and up
Content Rating Everyone	Contact Developer Visit Developer's Website Email Developer	Permissions View details	Report Flag as inappropriate	

Similar



CARATTERIZZAZIONE PRELIMINARE

IL PROGETTO “ANDROID MARKET RADAR”

CASO DI STUDIO

ESTENSIONI FUTURE e CONCLUSIONI

CARATTERIZZAZIONE

Perché esistono gli app store alternativi?

- Country gap (e.g. no paid apps in Google Play China)
- Canali alternativi di promozione
- Requisiti specifici e specializzazione
 - removedapps.com

Studio preliminare su 8 app store alternativi

- Crawling esaustivo tra Giugno e Novembre 2013
- Totale: 318,515 app



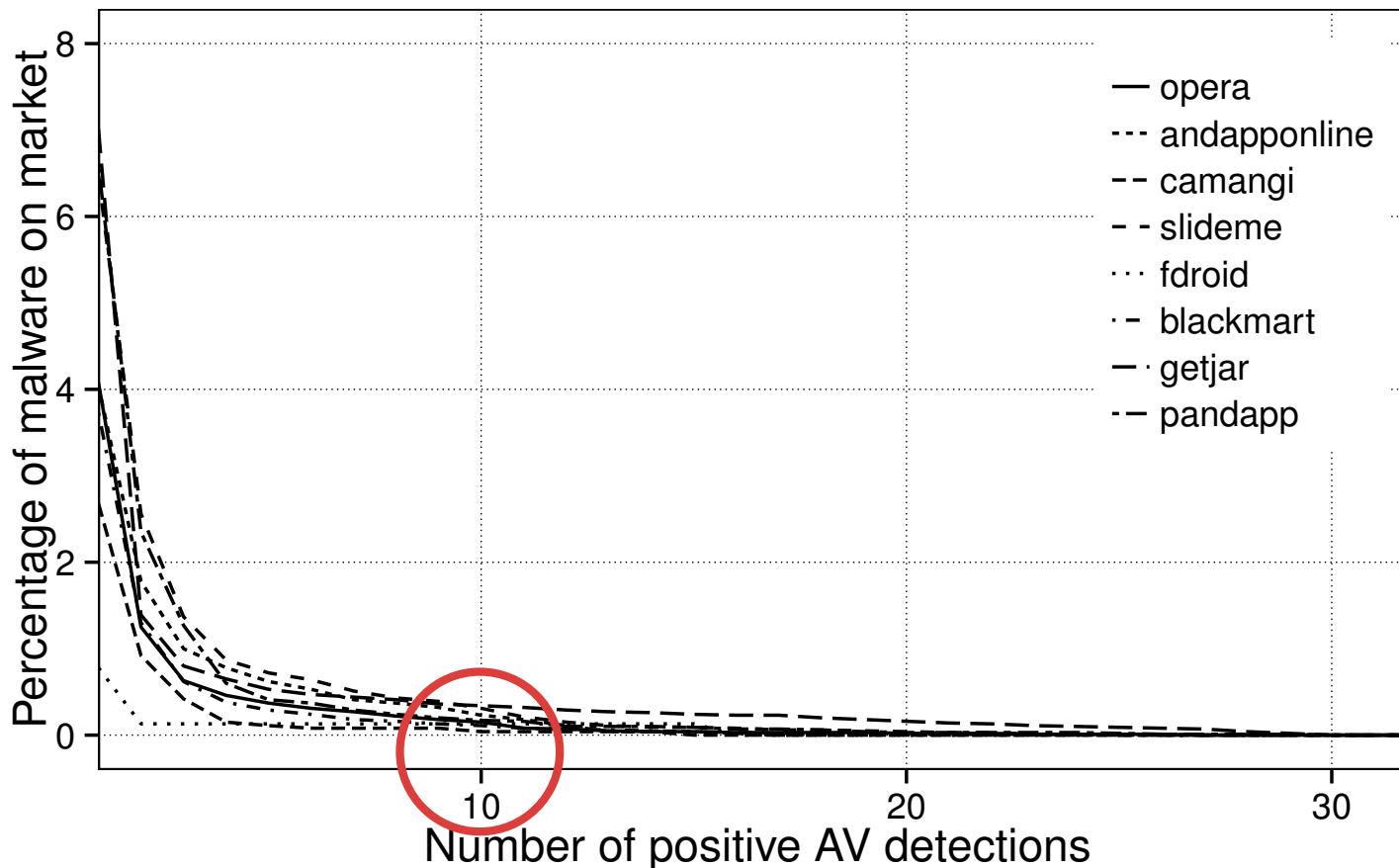
Opera Mobile Store

GETJAR

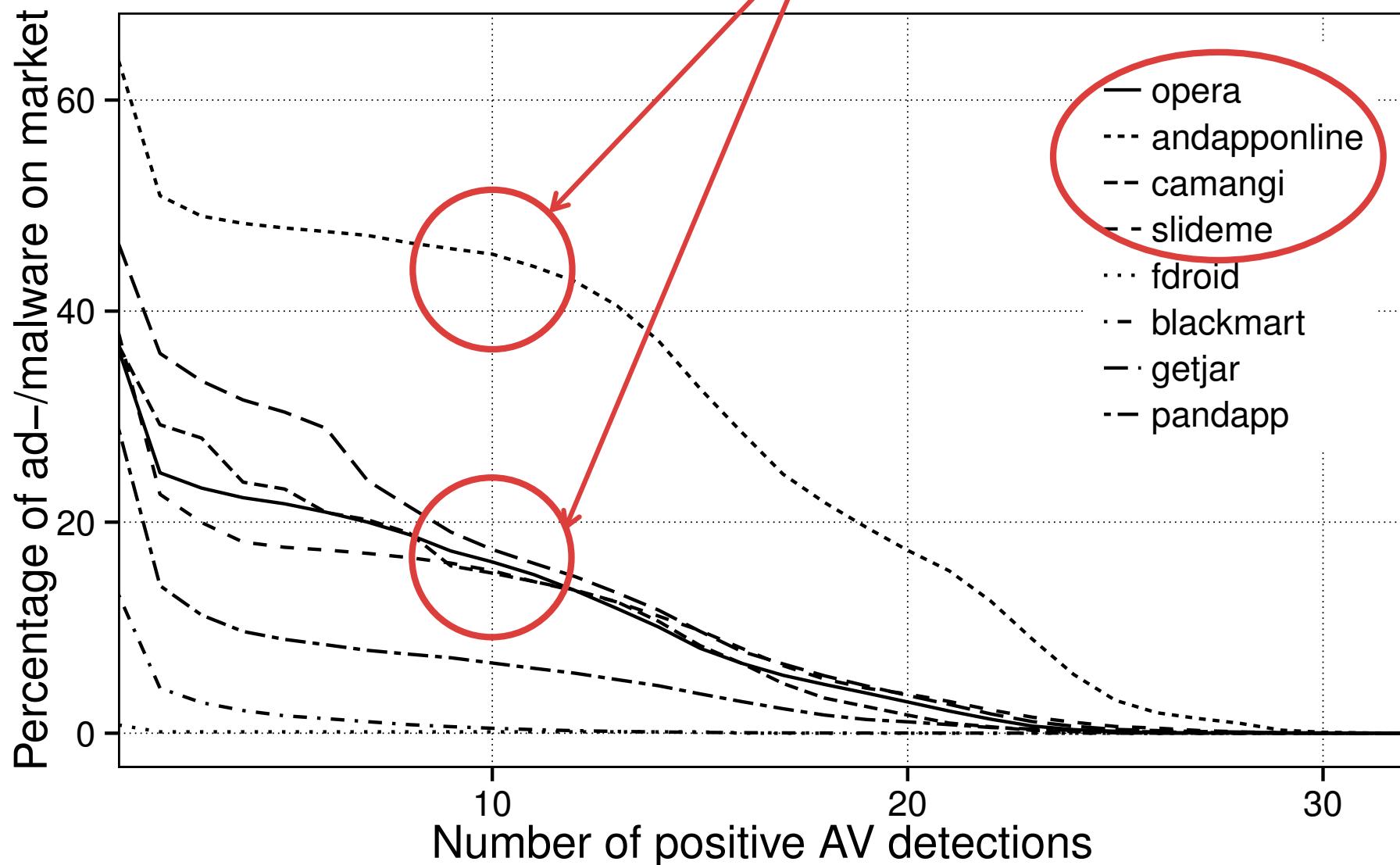


SONO DAVVERO DISTRIBUITE DAI MARKET STESSI?

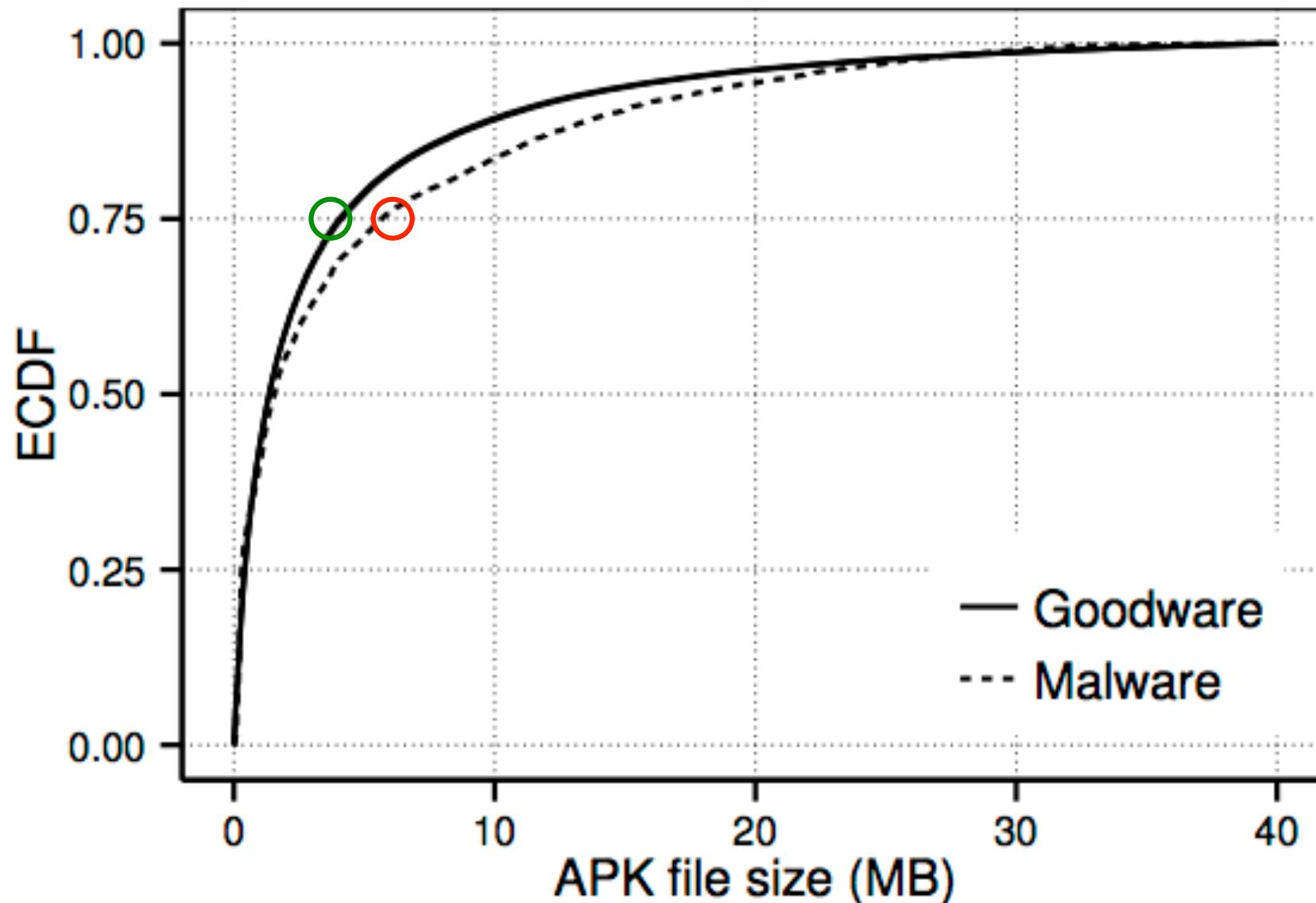
- Ebbene sì :-)
 - 5–8% delle 318,515 app nel nostro dataset sono ben note a 10+ antivirus come “malicious” (esclusi gli “adware”)



alcuni market sono
"specializzati" in adware

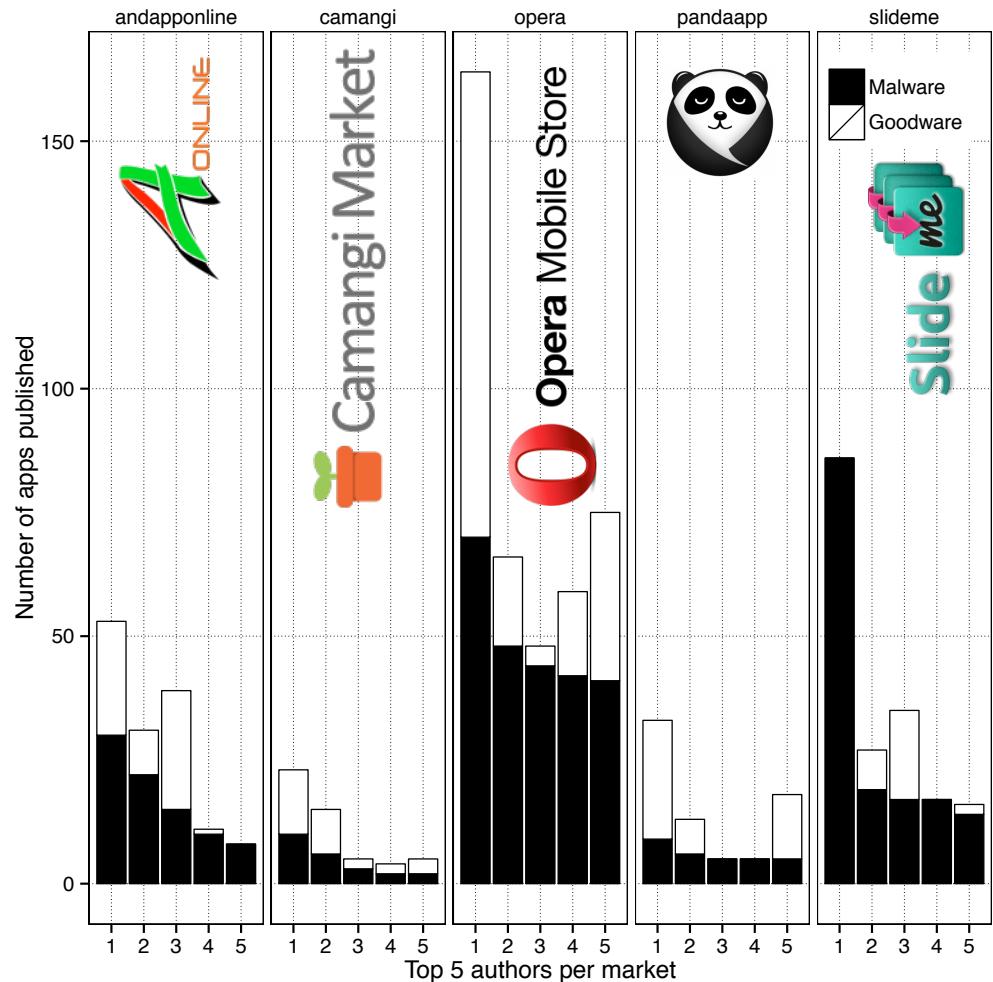


LE DIMENSIONI FANNO LA DIFFERENZA



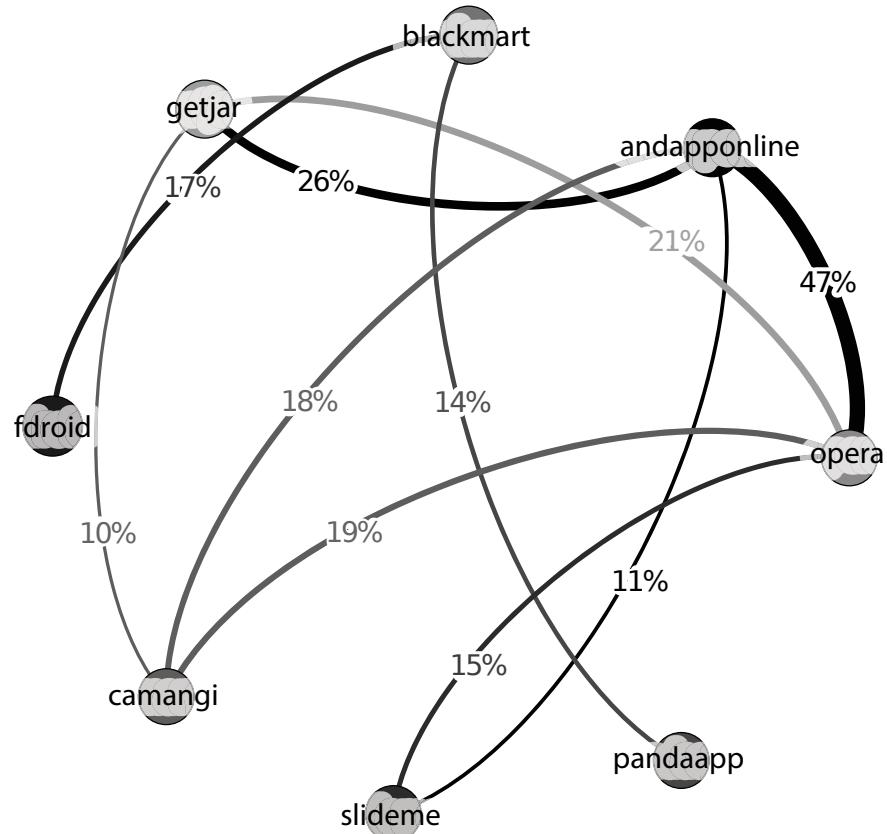
QUANTO È FACILE CASCARCI?

- Abbastanza facile...
- Lista degli sviluppatori in ordine decrescente di “numero di app”
- Malicious app ben visibili e note agli operatori del market
- Nella “top five” ci sono sviluppatori che pubblicano sia malware che goodware

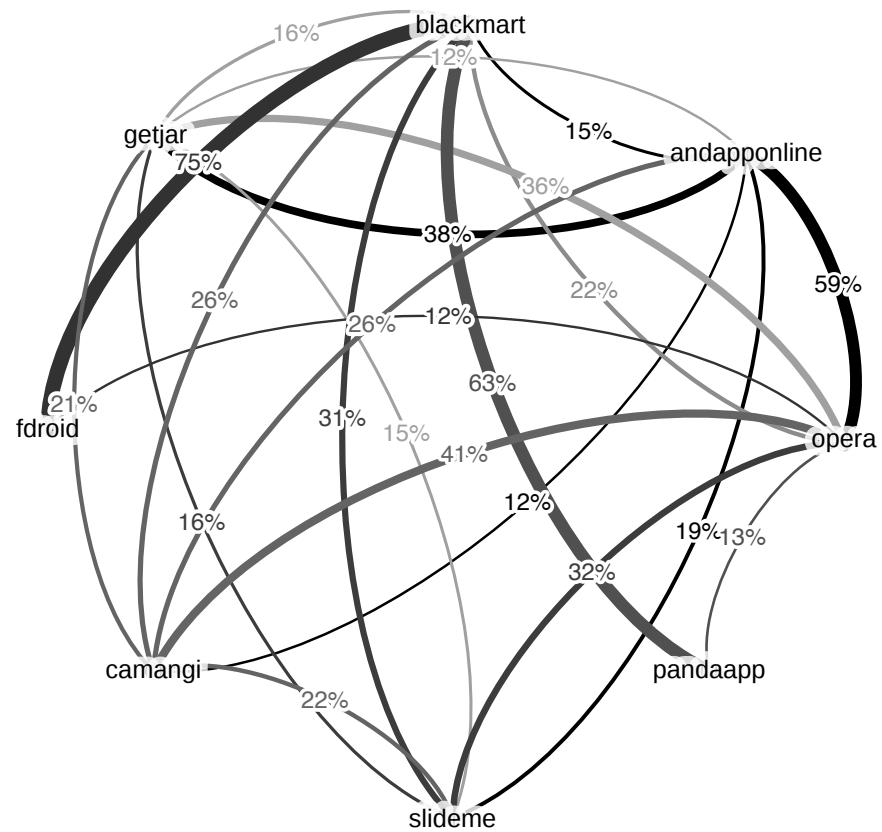


UNO ALLA VOLTA, PER CARITÀ!

Per MD5



Per package name



PROBING

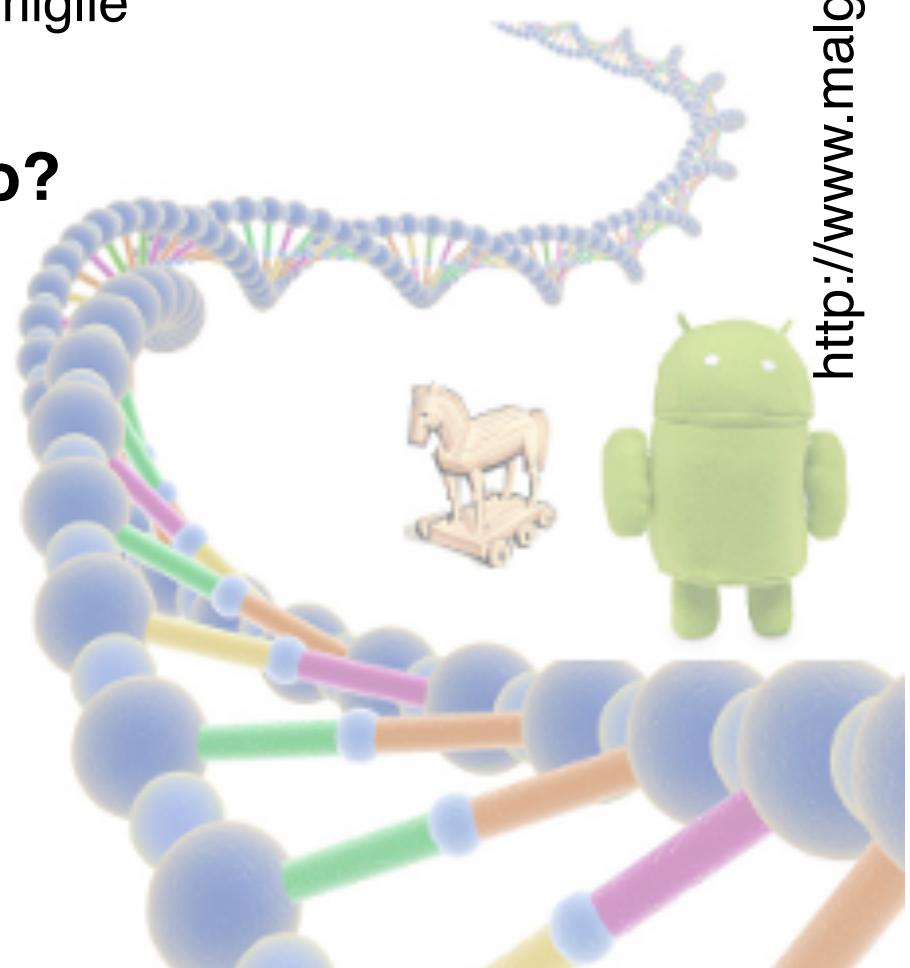
Android Malware Genome Project

- dataset pubblico di malicious app (2012!)
- ~1,300 applicazioni per ~50 famiglie

Gli app store se ne accorgono?

- alcuni sì
 - reazione immediata
 - rimozione differita
- gli altri...ahem...

...probabilmente le app in
questione sono ancora lì
dove le avevamo lasciate :-)



CARATTERIZZAZIONE PRELIMINARE

IL PROGETTO “ANDROID MARKET RADAR”

CASO DI STUDIO

ESTENSIONI FUTURE e CONCLUSIONI

OBIETTIVI vs. OSTACOLI

OBIETTIVI

- Cercare app, goodware o malware, in tempo reale
- Monitorare la distribuzione di app su tutti i market

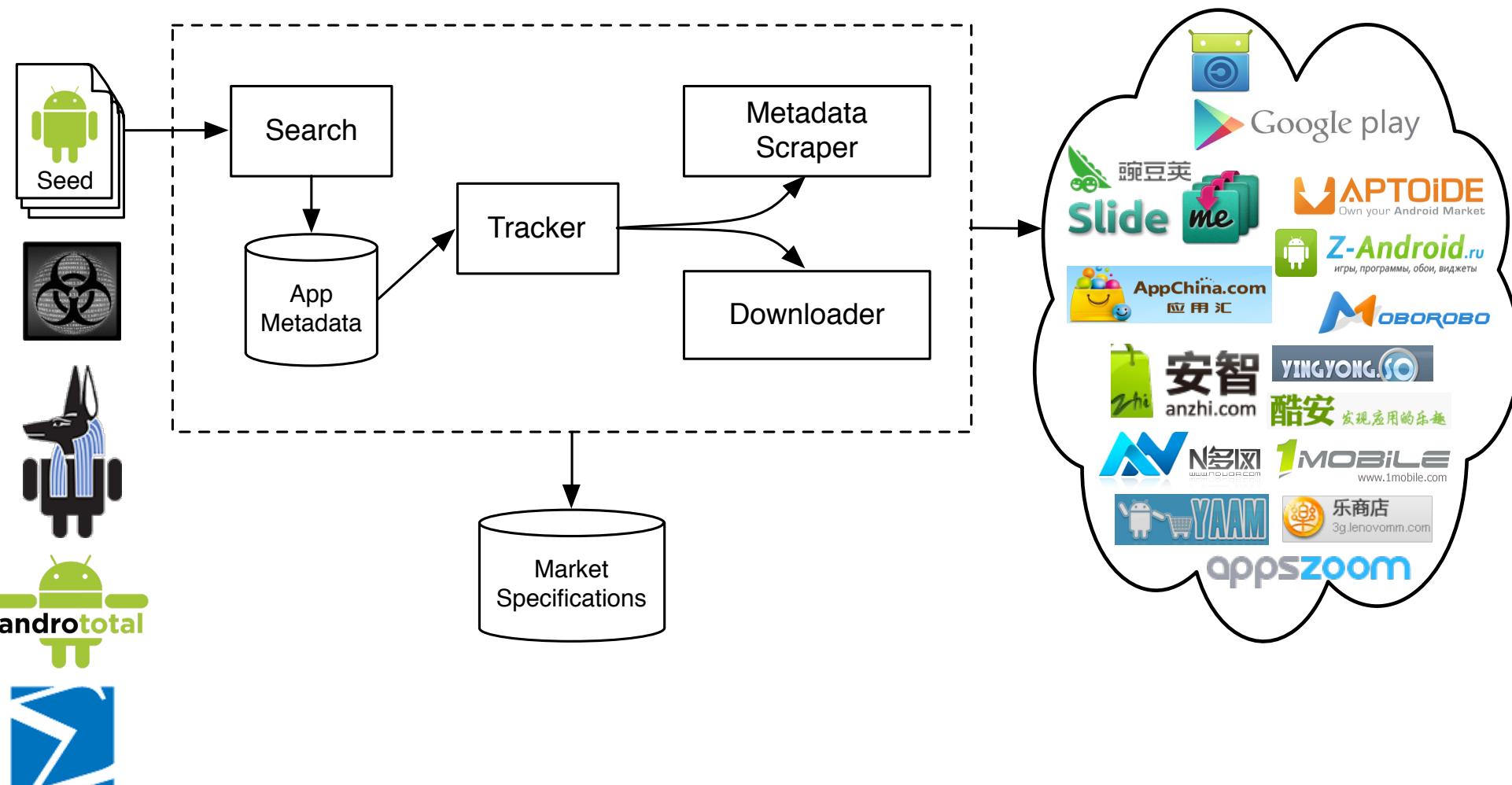
OSTACOLI

- Lo spazio di stoccaggio richiesto cresce indefinitamente
- I metadati cambiano → una “fotografia” non basta

Crawling esaustivo di tutti i market: infattibile!

- ~ 196 Ottobre 2011 (Vidas et al., CODASPY13)
- ~ 500 Marzo 2012–13 (Juniper Threats Report 2013)
- ~ 89 Giugno 2013 (nostro studio preliminare)

CERCHIAMO L'AGO NEL PAGLIAIO



PACKAGE NAME (AppChina)

锅舞者下载_锅舞者安卓版下载_锅舞者 1.0.1手机版免费下载- AppChina应用汇

www.appchina.com pp/com.Beltheva.DanceDance/

AppChina.com 应用汇 搜索 免费注册 | 登录账号 ANVA

首页 安卓软件 安卓游戏 排行榜 开发者 应用邦 论坛

应用汇安卓市场> 安卓游戏 >益智游戏 >锅舞者

 锅舞者
PanDancer

12.5 MB 1000-5000次 益智游戏 1.0.1 有 (普通广告) 无病毒 Android 2.2 以上

1人喜欢 点击查看二维码 免费下载

下载大小: 12.5 MB 最新版本: 1.0.1 “锅舞者”的更新信息:
总下载量: 1000-5000次 广告检测: 有 (普通广告) 2012/10/26(v1.0.1) いくつかの不具合修正 2012/10/25(v1.0.0) 新規リース*要求されるネットワーク系の権限は広告表示のために使用しております。ご了承ください。
内容类型: 益智游戏 病毒扫描: 360安全卫士 腾讯手机管家
更新时间: 2013-03-04 安全管家

“锅舞者”的介绍:
嗨,我的名字是熊猫舞者! 今天是舞蹈比赛,一年一次。
我是去年的冠军,但是我不太擅长跳舞。我真的需要你的帮助,成为赢家!
这个游戏的规则太简单。按下按钮(步骤、翻转、跳跃和姿势)以相同的顺序按下按钮



“锅舞者”的评论

您的意见

应用汇“微信公众账号”:

老号就用来钓鱼吧

应用汇用户 SCH-I939D 说:

版本: 1.0.1 2014-03-02

[Download](#)[Screenshots \(4\)](#)[Comments \(35\)](#)[App Support](#)

Rolling Panda

[LOAD BY EMAIL](#)

- 3.75 MB - FREE

[QR CODE](#)

v 1.5.0 - 3.75 MB - FREE

[DIRECT DOWNLOAD APK FILE](#)

v 1.5.0 - 3.75 MB - FREE

I you an email, so you must

n

This is an example QR. Click on button and use a QR code scanner to download directly in to your Android device. [[More info](#)]

Download the APK file to your computer. Once uploaded to your mobile device, install the app directly

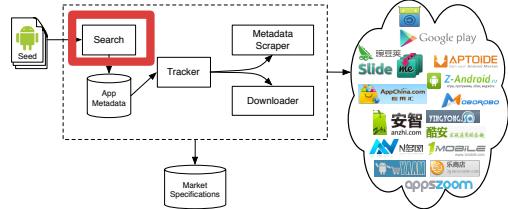
[Older versions](#)

and permissions

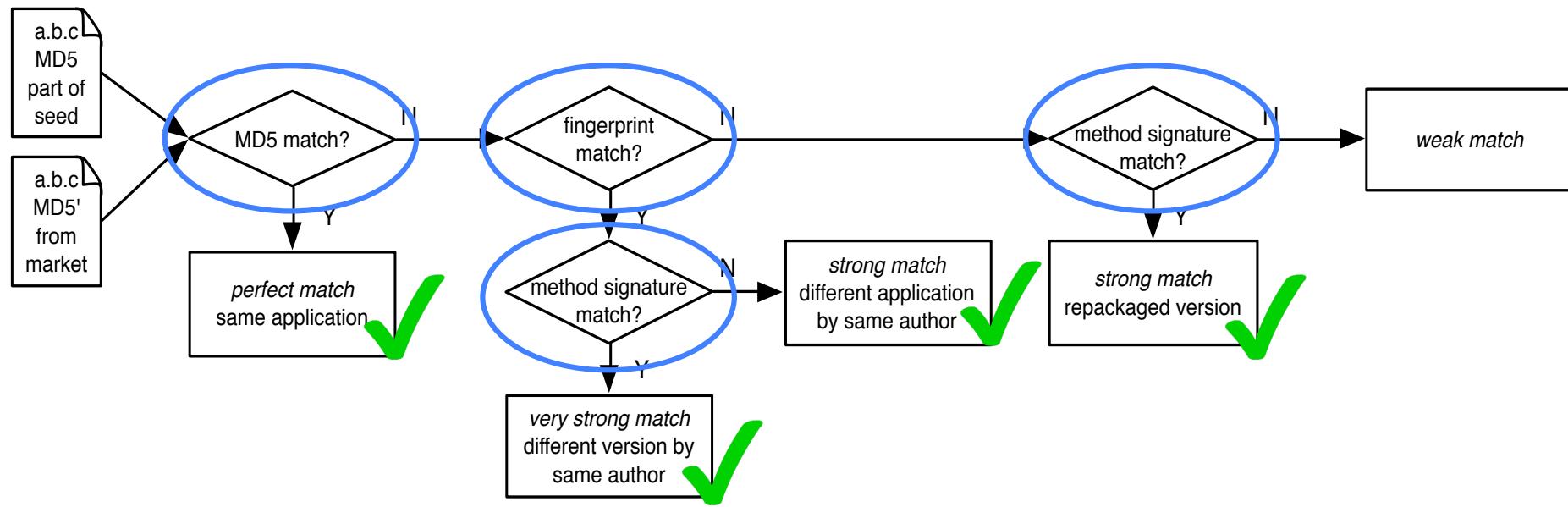
[Changelog](#)

Package com.kidsfun.jump.panda

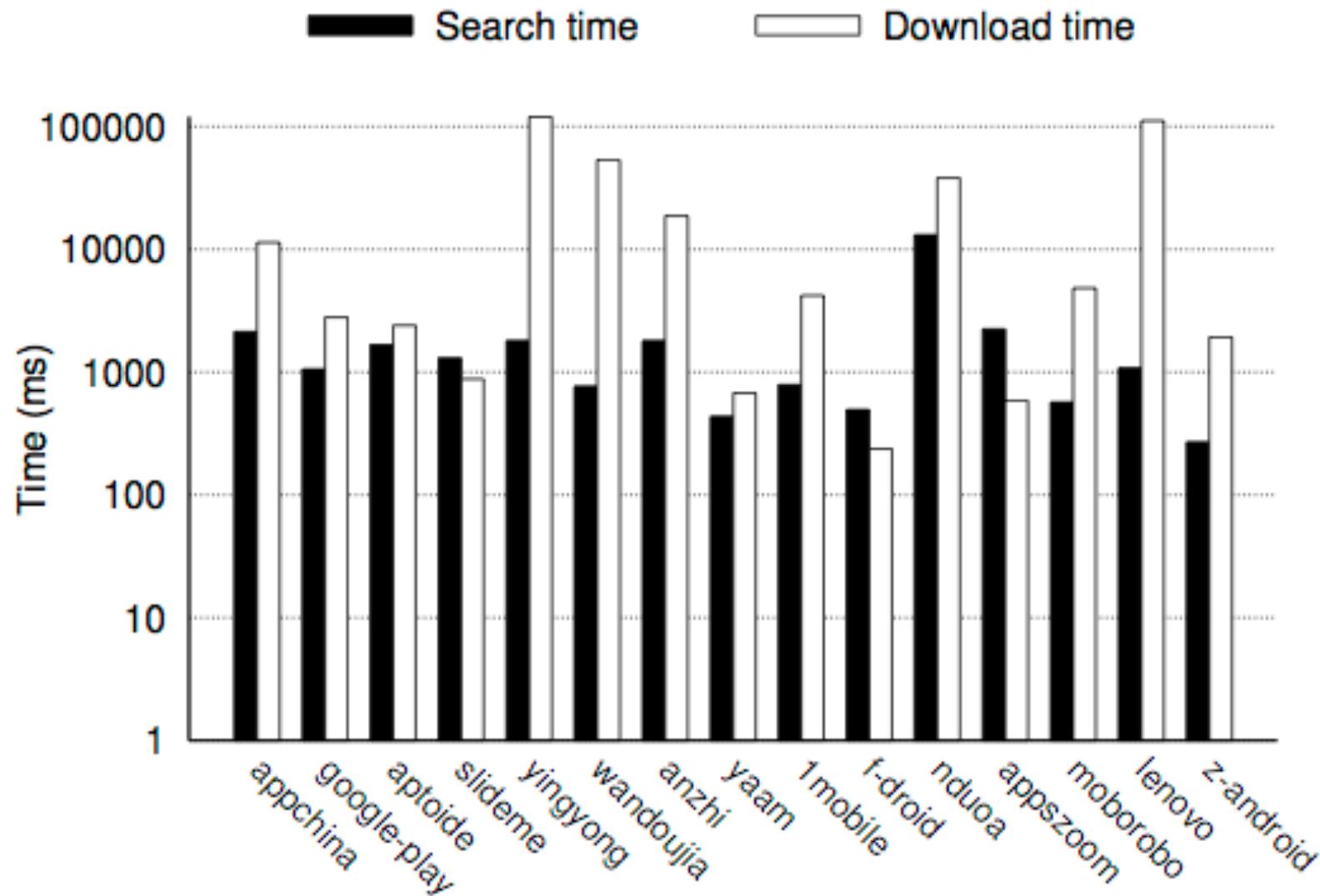
it access (wifi, 3G...) you have at every moment.



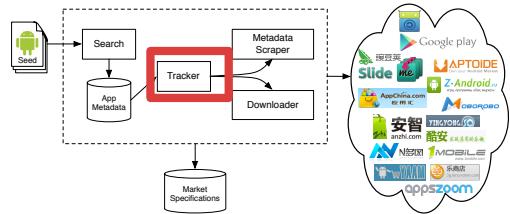
ORA ABBIAMO L'APK



VELOCITA`



v.s. quasi tre mesi per scaricare tutti gli APK da 8 market



TRACKING

- Monitoraggio continuo di ogni nuova app trovata
- Estraie informazioni dalle pagine di ogni app
 - Data di upload
 - Descrizione
 - Screenshot
 - Numero di download
 - Valutazioni (stelline)
 - Commenti degli utenti
 - Altre app dello stesso autore
 - Data di cancellazione
- Un modulo di “scraping” dedicato per ogni market
 - LUA

CARATTERIZZAZIONE PRELIMINARE

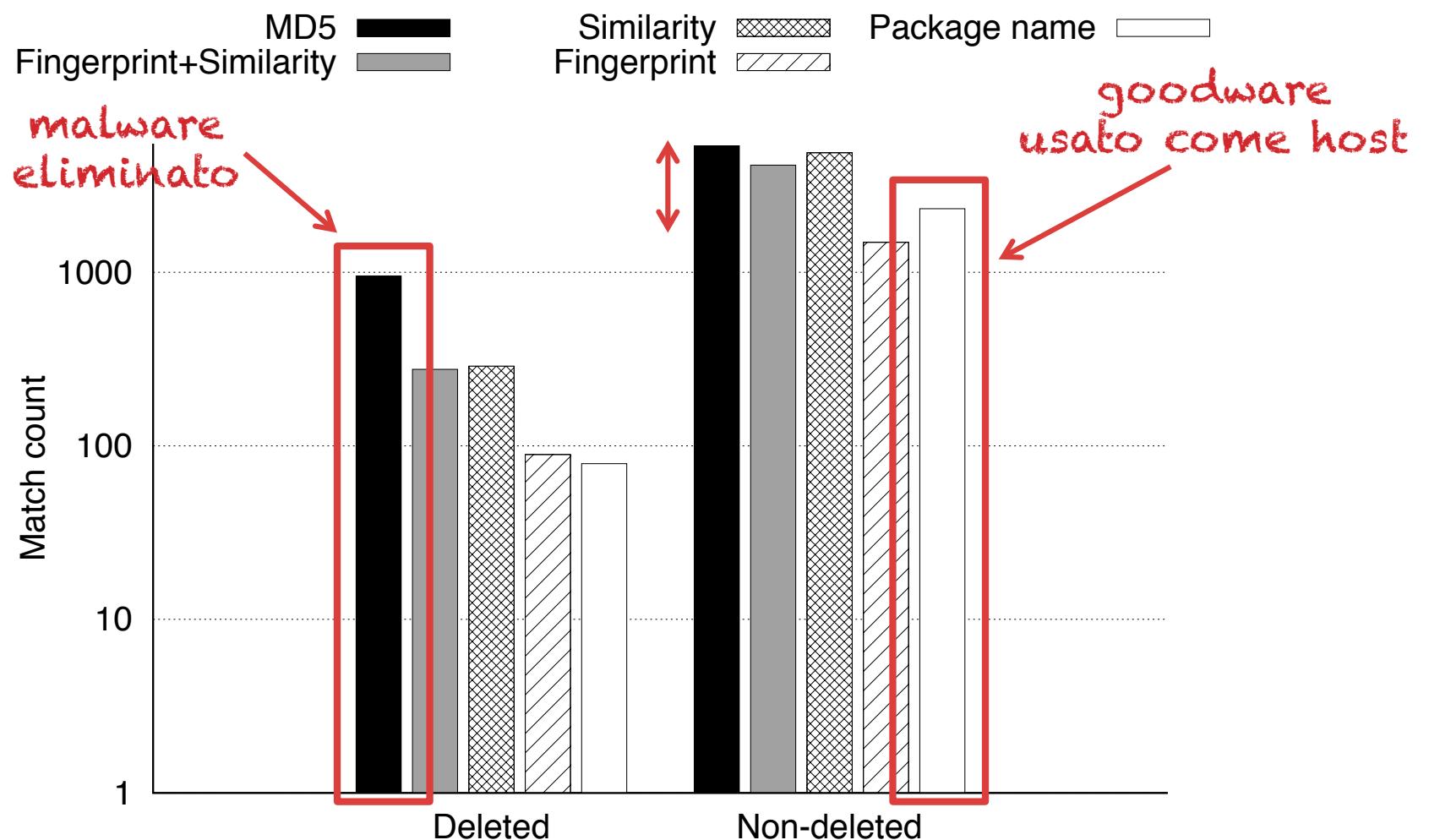
IL PROGETTO “ANDROID MARKET RADAR”

CASO DI STUDIO

ESTENSIONI FUTURE e CONCLUSIONI

CASO DI STUDIO (AGO–DIC ‘13)

20,000 malicious app (circa 1,500 cancellazioni)



CICLI DI VITA DI UN APP MALICIOUS

NORMALE (90.57%)

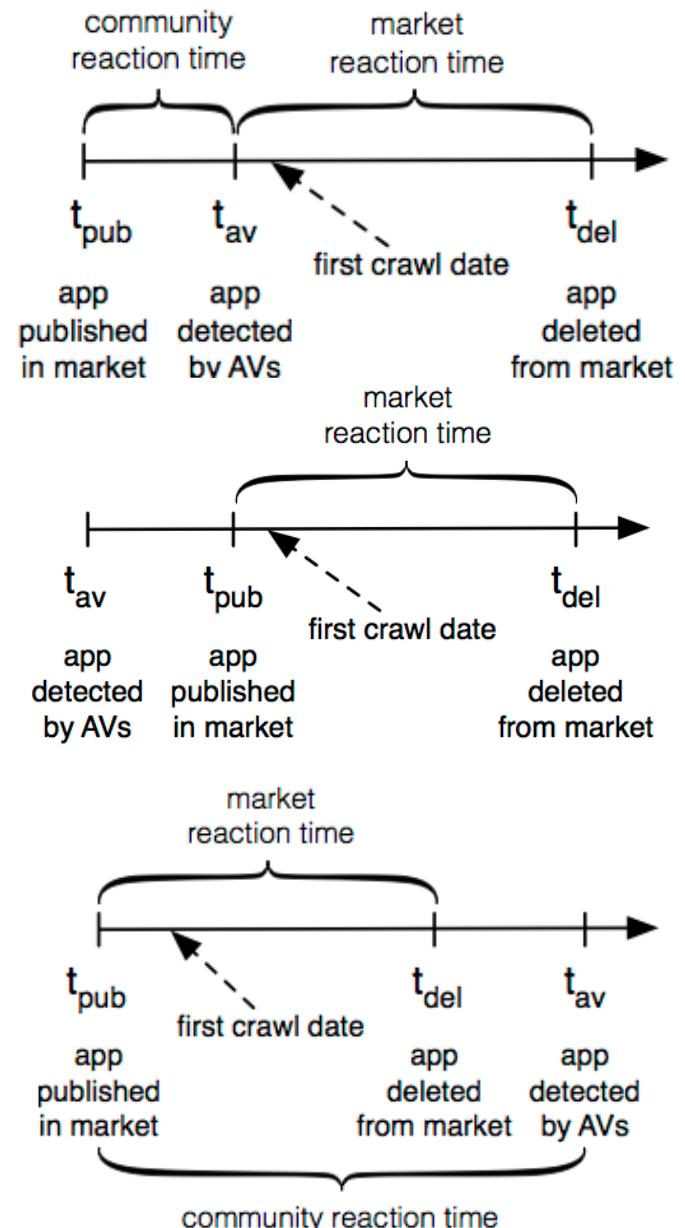
Rimozione dopo notifica da AV

HOPPING (7.89%)

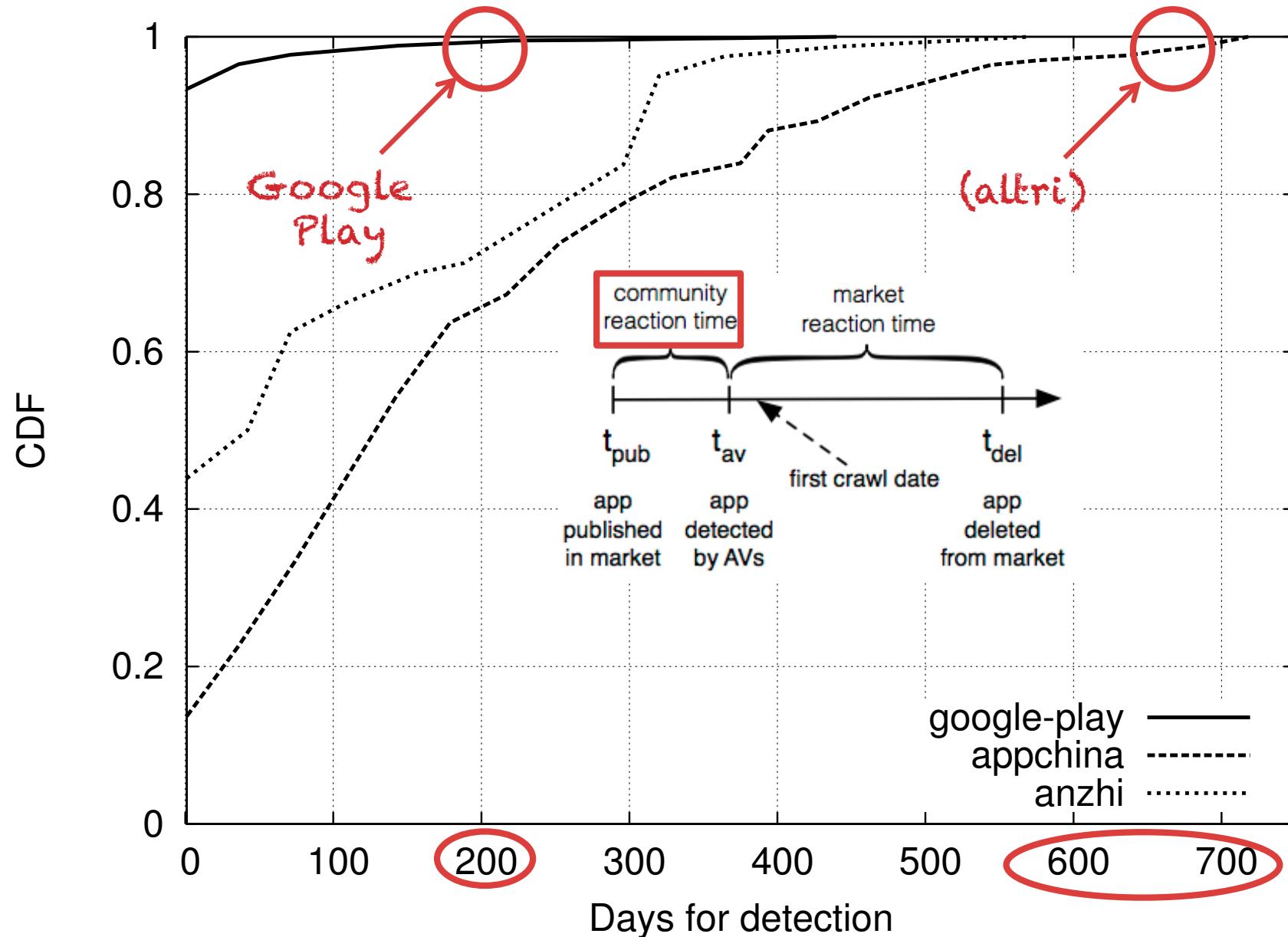
A volte ritornano...

SELF-DEFENSE (1.56%)

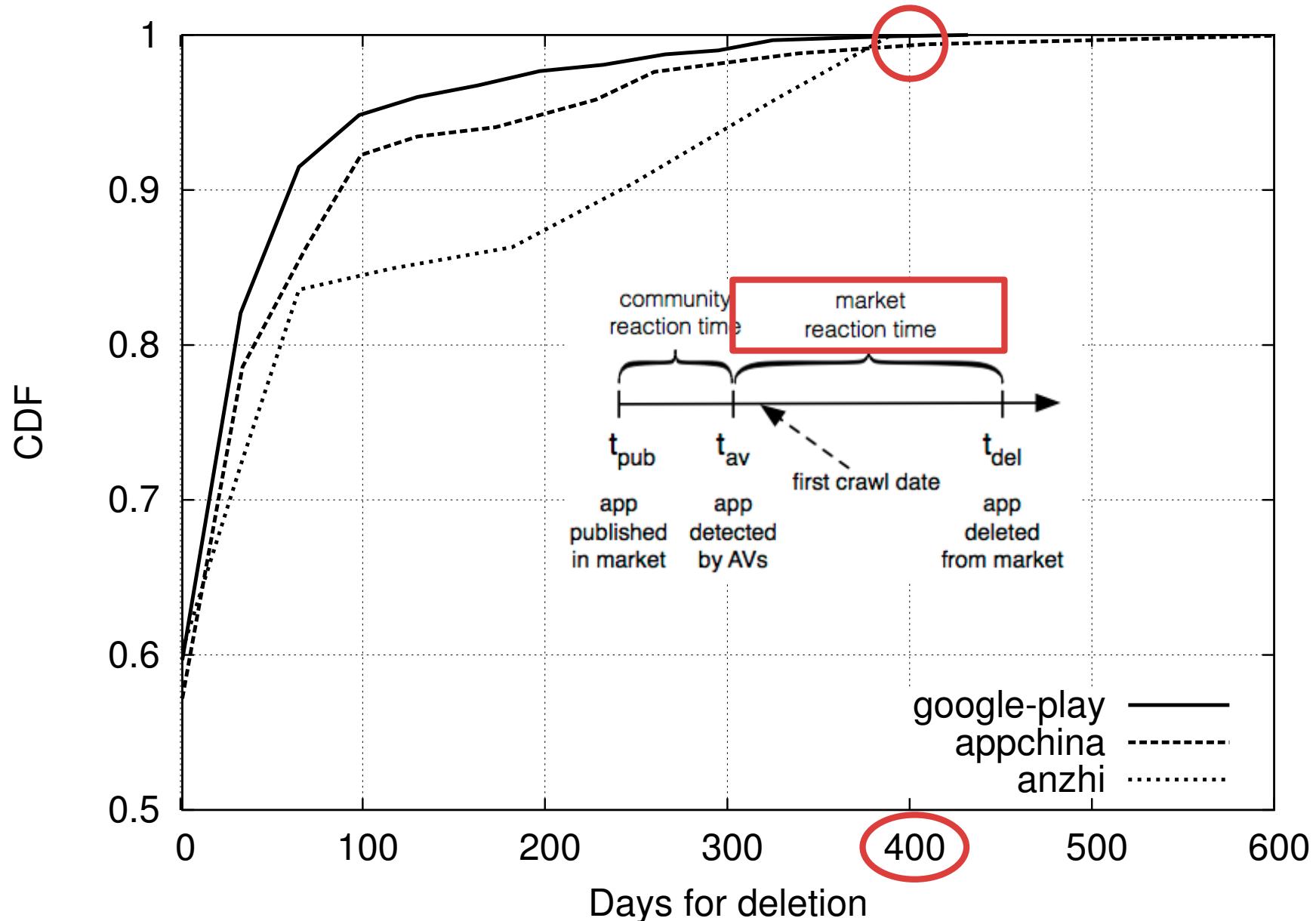
Market meglio della community



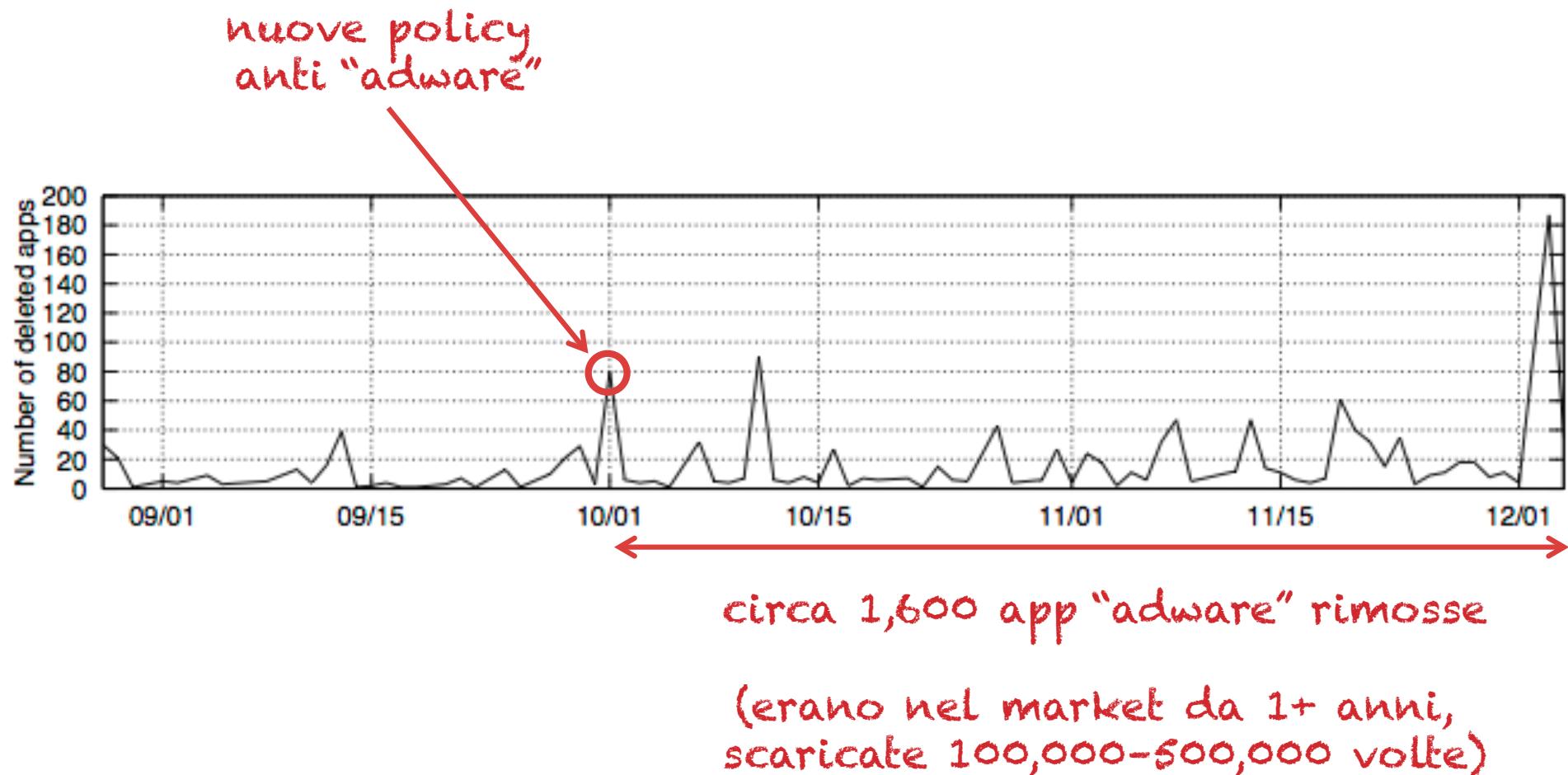
TEMPI DI REAZIONE (COMMUNITY)



TEMPI DI REAZIONE (MARKET)



QUANDO SI FANNO LE PULIZIE?



...TO BE CONTINUED...

CARATTERIZZAZIONE PRELIMINARE

IL PROGETTO “ANDROID MARKET RADAR”

ESPERIMENTI e CASO DI STUDIO

ESTENSIONI FUTURE e CONCLUSIONI

A COSA STIAMO LAVORANDO

- Sistema automatico di notifica per i gestori
- Estendere AndRadar per indicizzare e cercare in base a
 - nome dell'app
 - caratteristiche visive (i.e., screenshot, icone)
 - commenti, descrizioni
- Evoluzione di app malicious
- Identificare frodi nei market (“app rank boosting”)
 - numero di download “gonfiati” per aumentare la popolarità
 - falsi commenti negativi o positivi



DOMANDE?

apking@iseclab.org



FEDERICO MAGGI

POLITECNICO DI MILANO

@phretor