COME TO THE DARK SIDE

WE HAVE APPS!

FEDERICO MAGGI

POLITECNICO DI MILANO

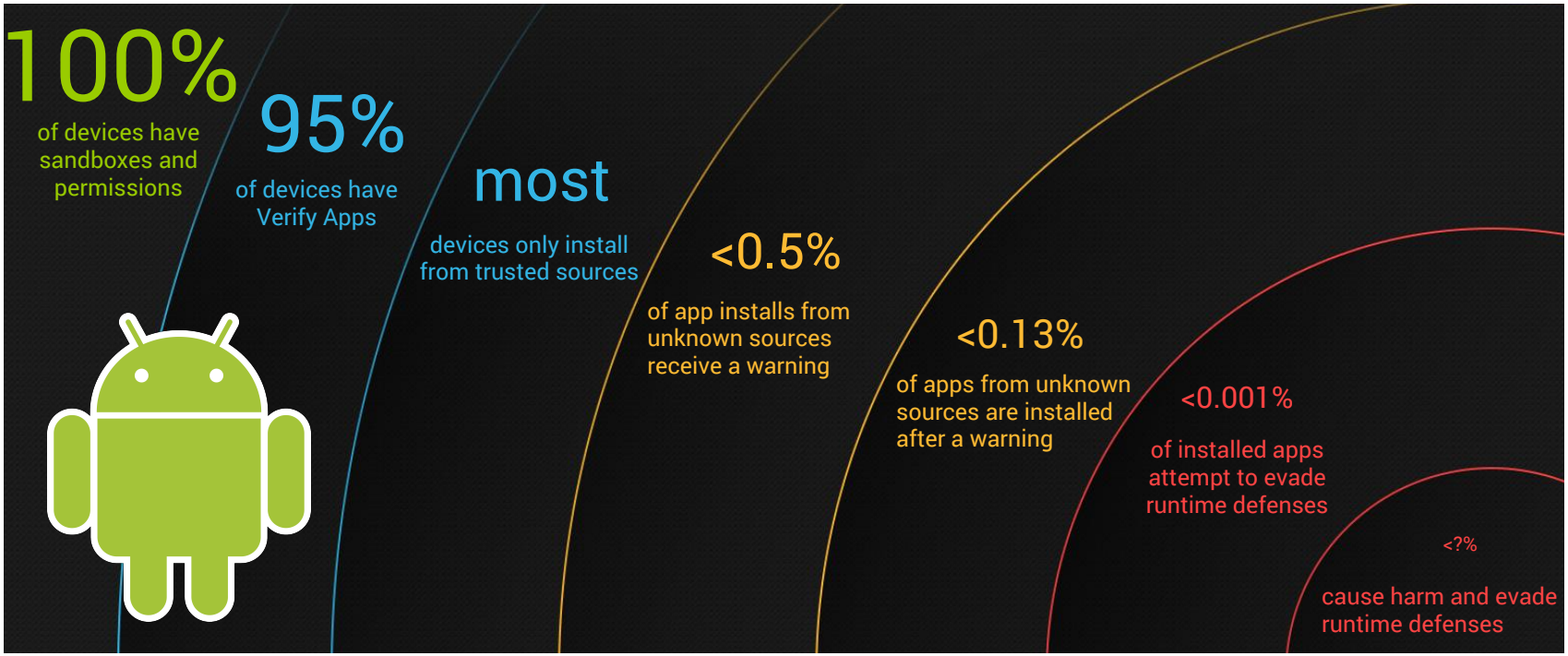
HACKINBO

SICUREZZA ALL'OMBRA DELLE TORRI

RINGRAZIAMENTI

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

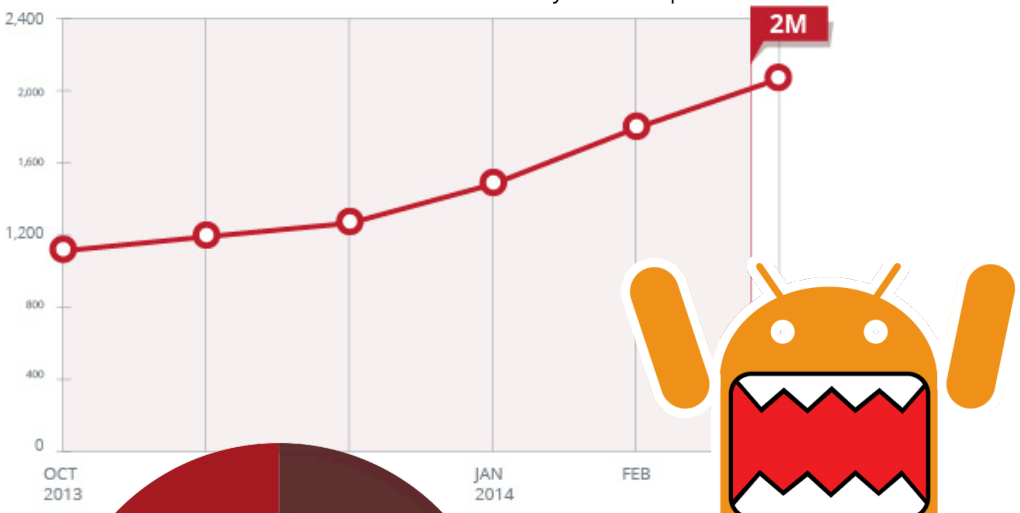
NUMERI, NUMERI, NUMERI!

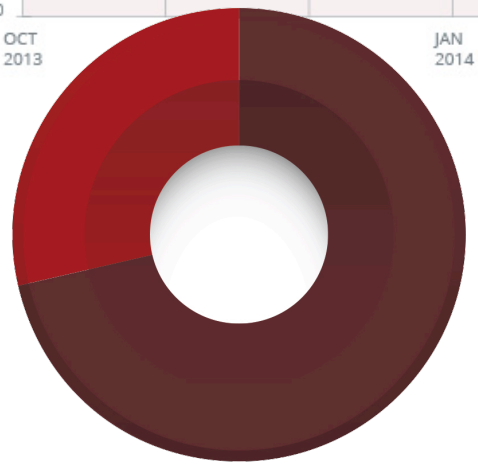


The Core of the Matter (NDSS13)	0.0009%
The Company You Keep (WWW14)	0.2800%

COSA DICONO GLI A/V VENDOR?

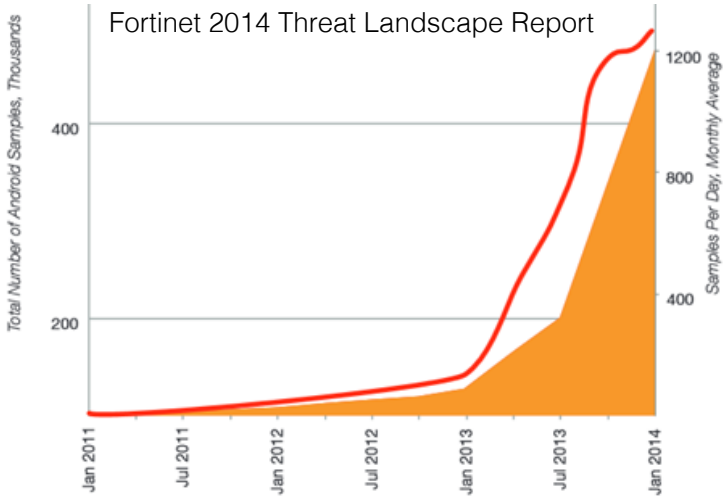
TrendMicro TrendLabs 1Q 2014 Security Roundup



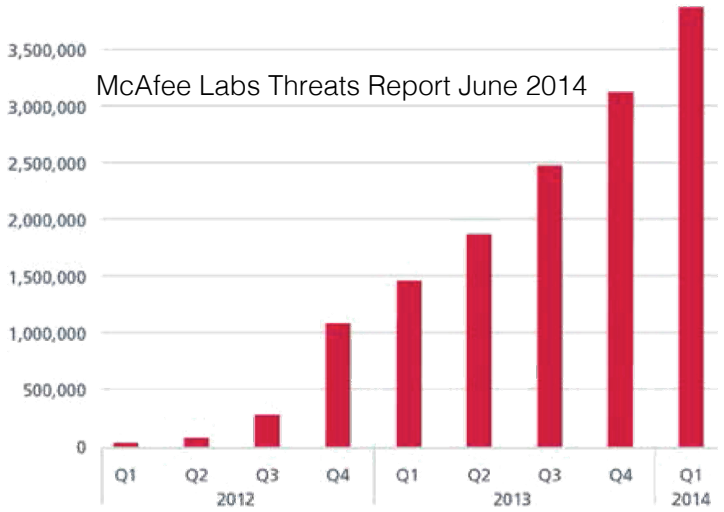


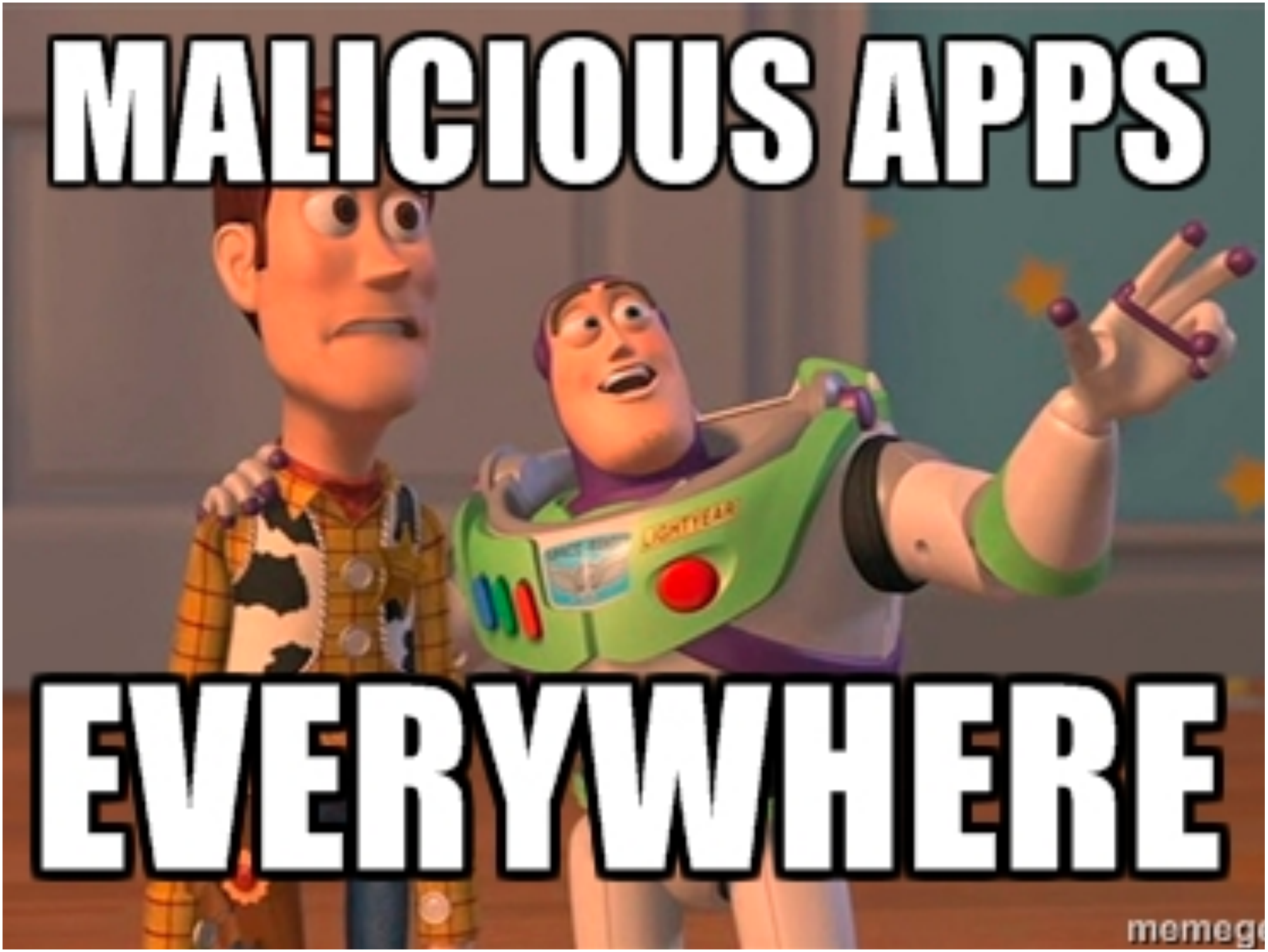
Mobile malware 72%
High-risk apps 28%

Fortinet 2014 Threat Landscape Report

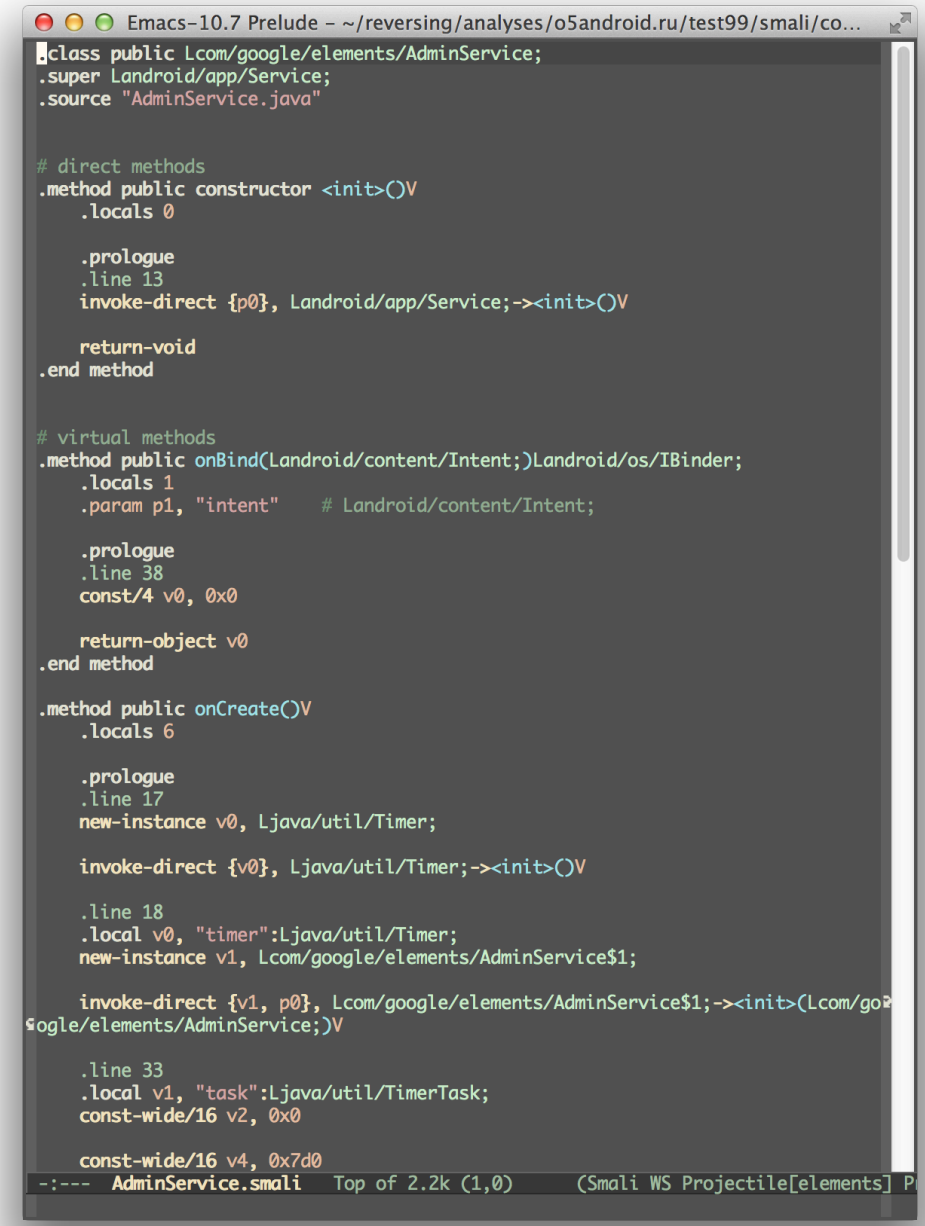


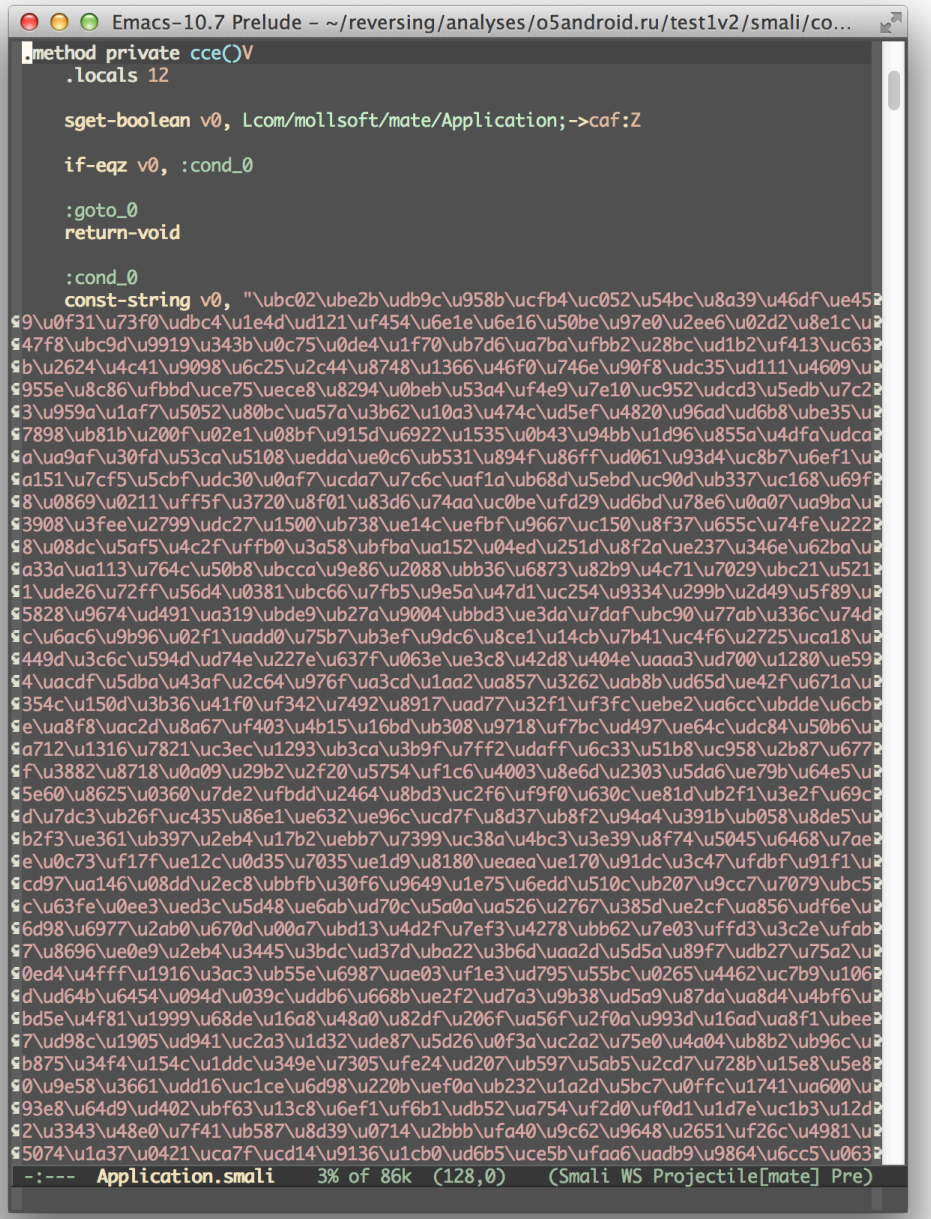
McAfee Labs Threats Report June 2014




MALICIOUS APPS
EVERYWHERE

NON SOLO QUANTITÀ





- Perché così tante app malicious e così pochi dispositivi infetti?

- Qual è il motivo che spinge 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

Reader

Google play

Search

Sign in

Apps

My apps

Shop

Games

Editors' Choice

Farting Panda

Bell Pepper Edutainment - 11 March 2014

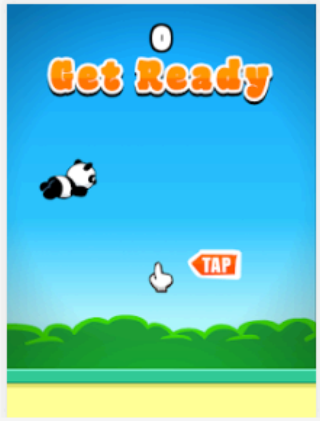
Arcade

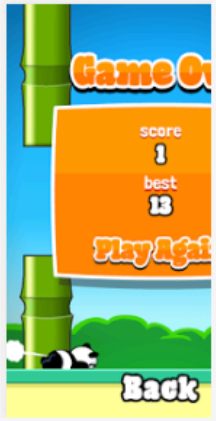
Install

Add to wishlist

★★★☆☆ (1,733)

+1 +1663 Recommend this on Google

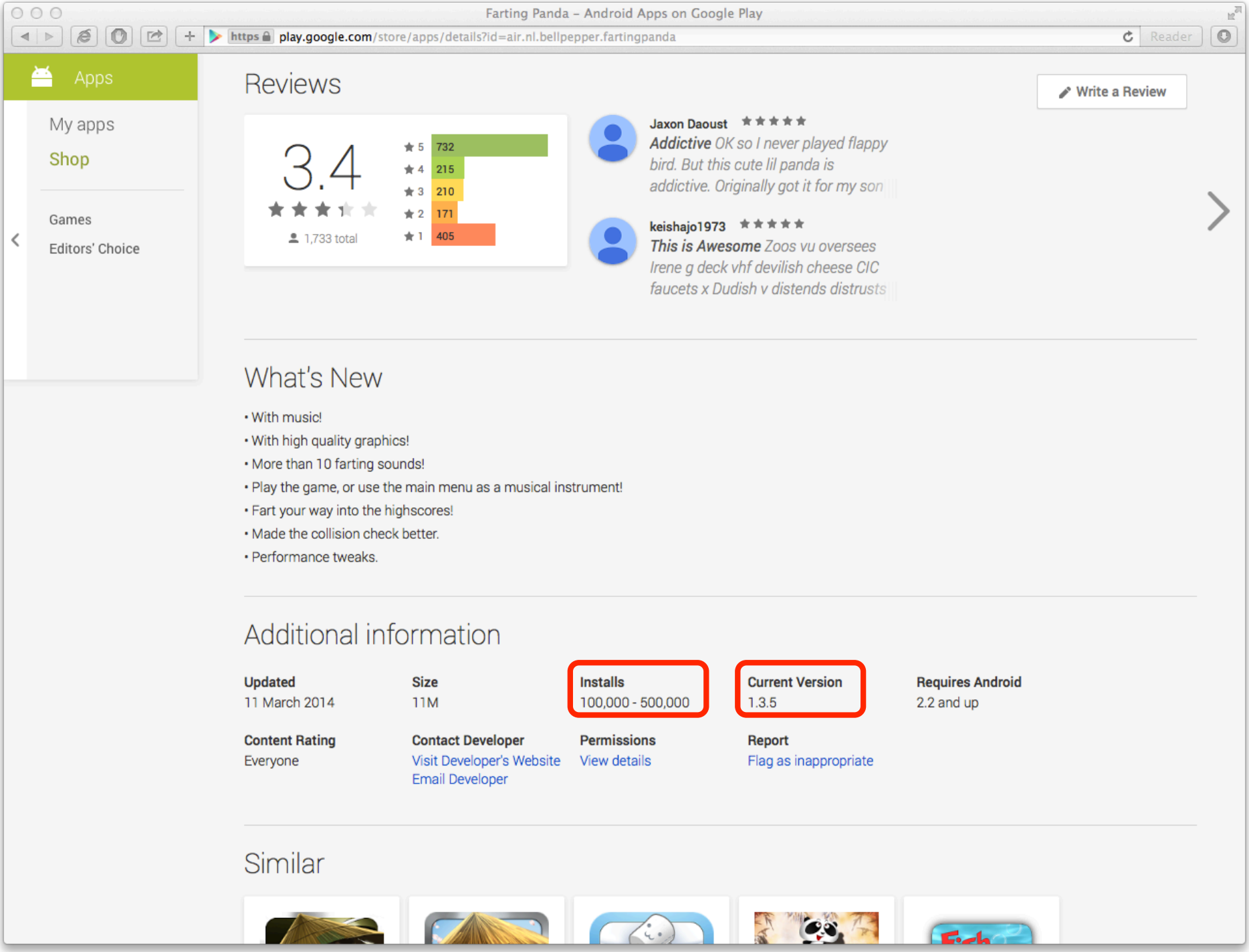




Description

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
Apps
My apps
Shop
Games
Editors' Choice
Reviews
Write a Review
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

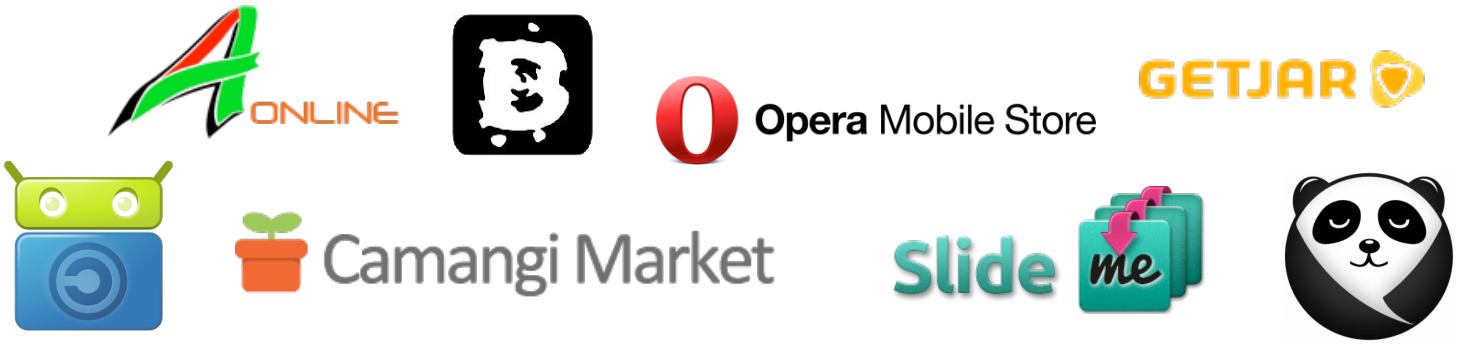
CARATTERIZZAZIONE

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

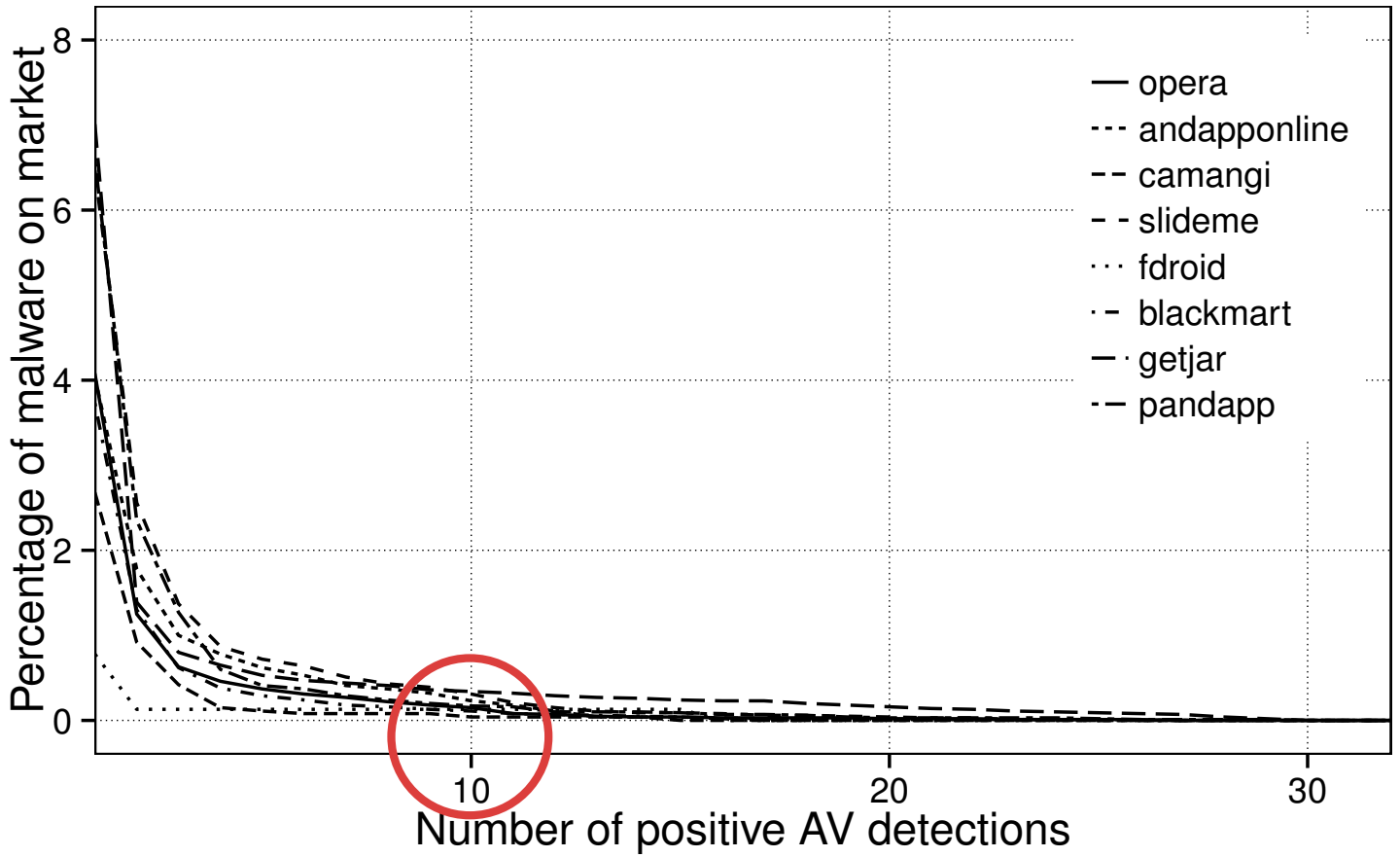
Studio preliminare su 8 app store alternativi

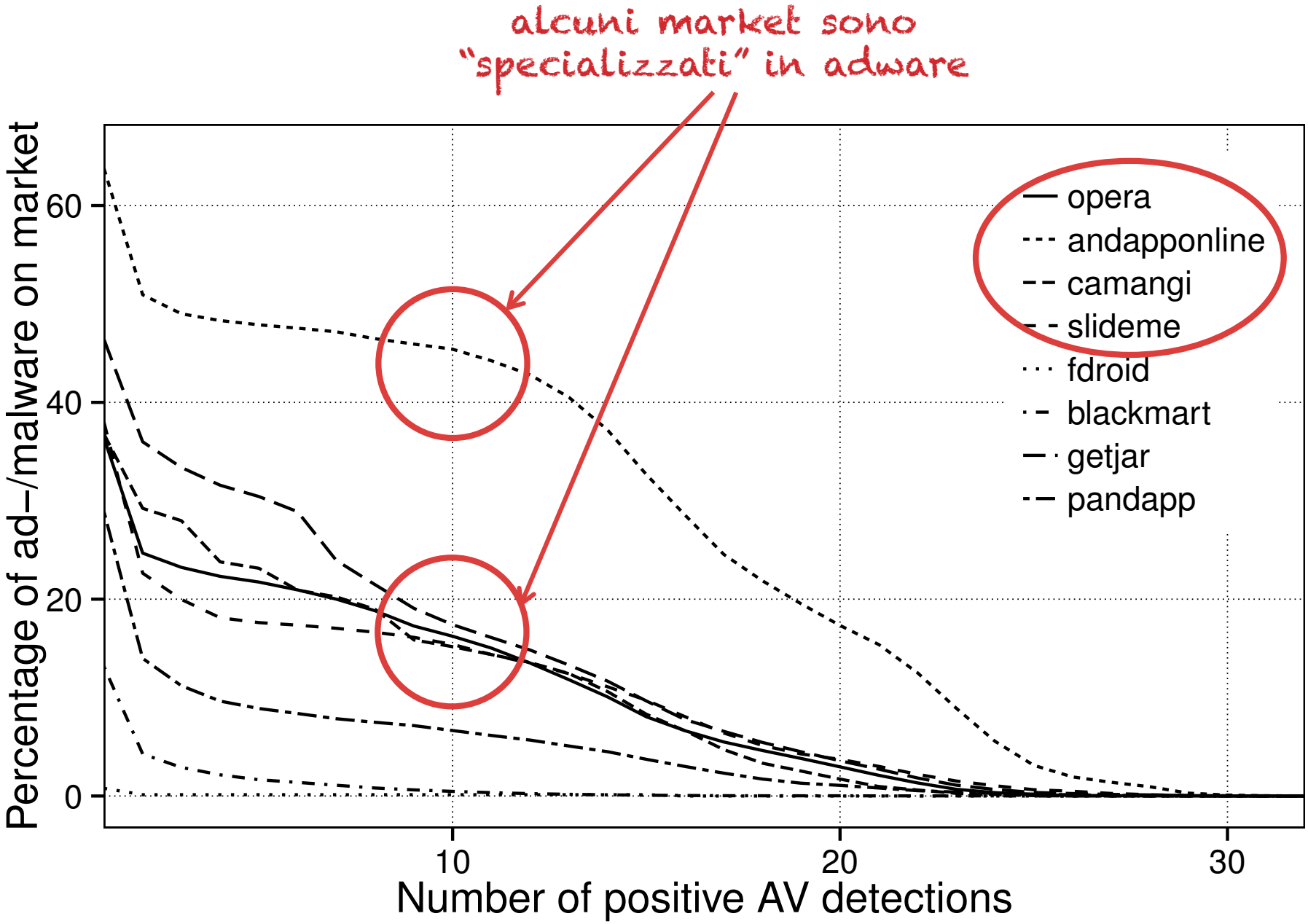
- Crawling esaustivo tra Giugno e Novembre 2013
- Totale: 318,515 app



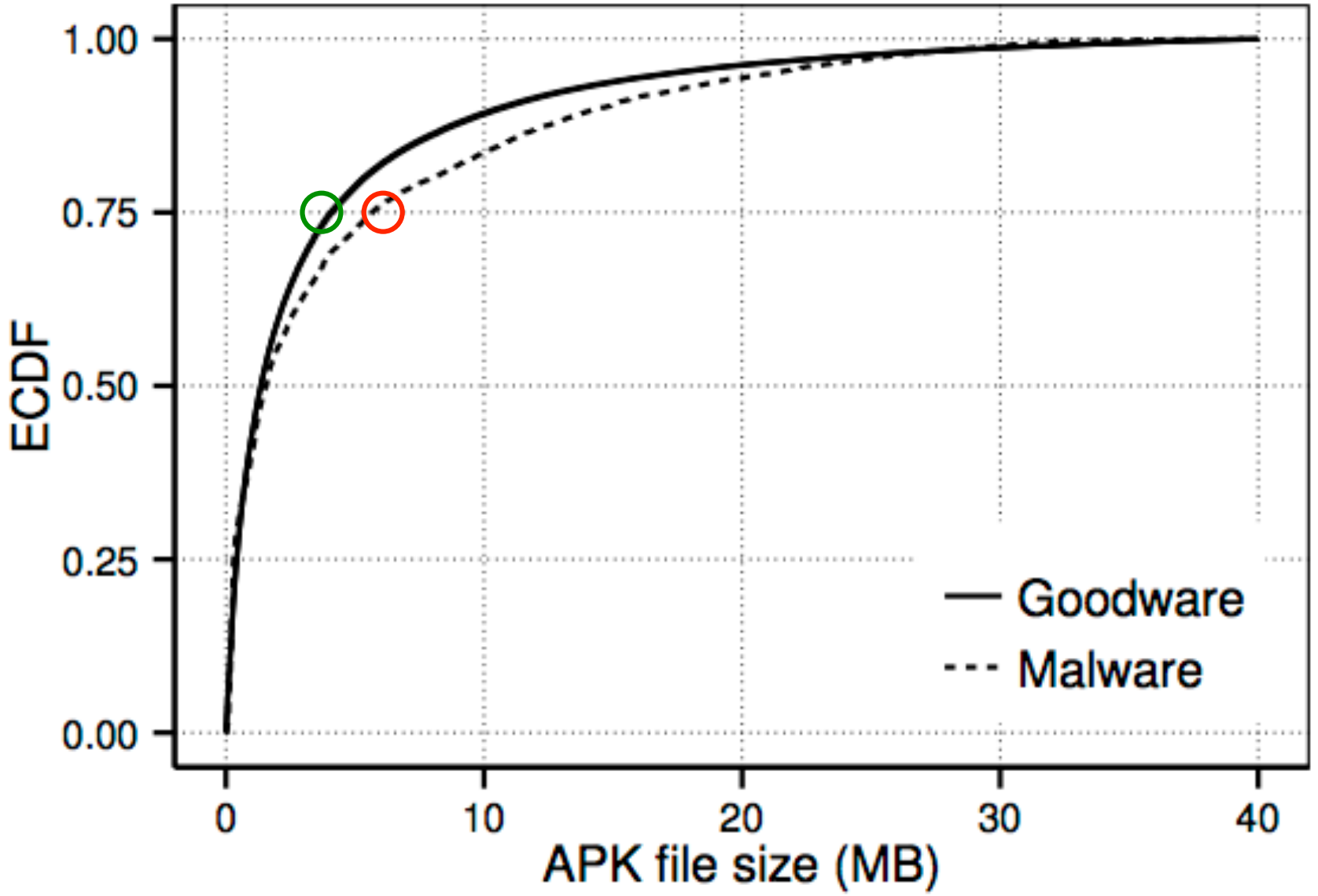
SONO DAVVERO DISTRIBUITE DAI MARKET STESSI?

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



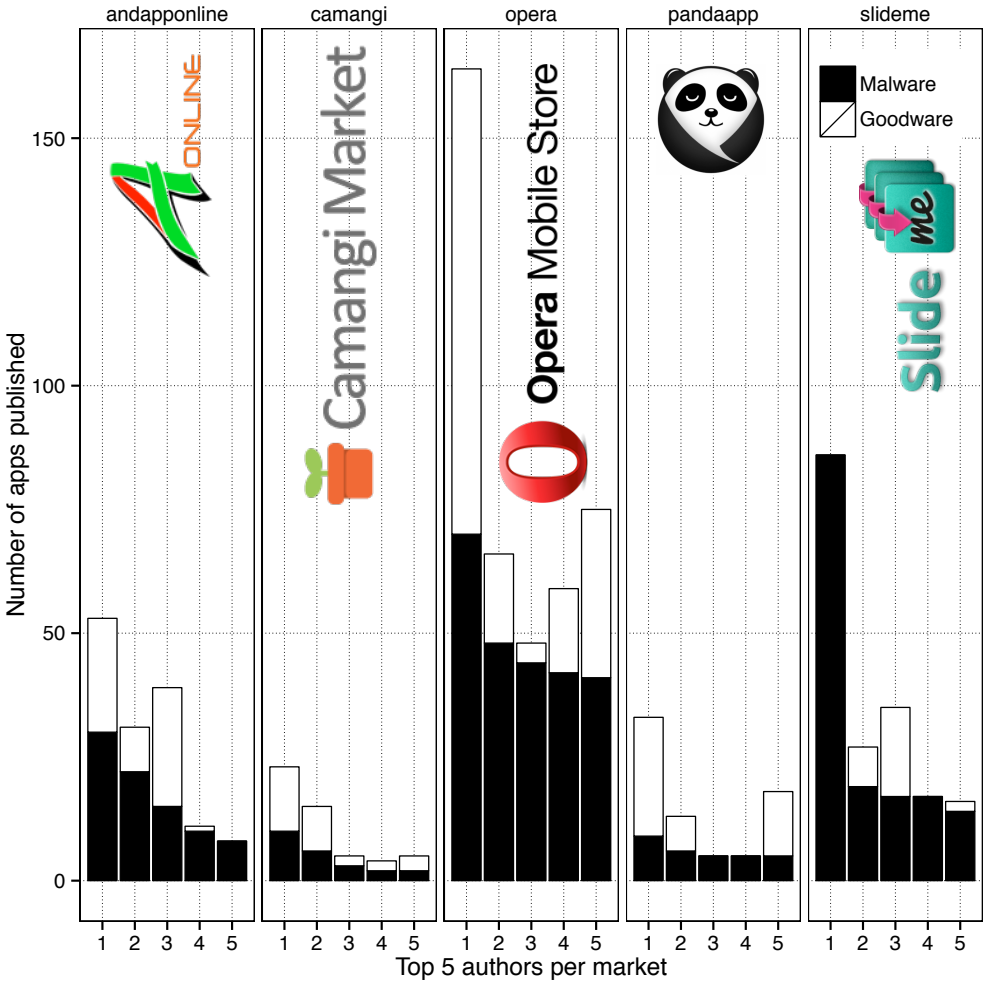

alcuni market sono
"specializzati" in adware
Percentage of ad−/malware on market
0
20
40
60
10
20
30
Number of positive AV detections
opera
andapponline
camangi
slideme
fdroid
blackmart
getjar
pandapp

LE DIMENSIONI FANNO LA DIFFERENZA



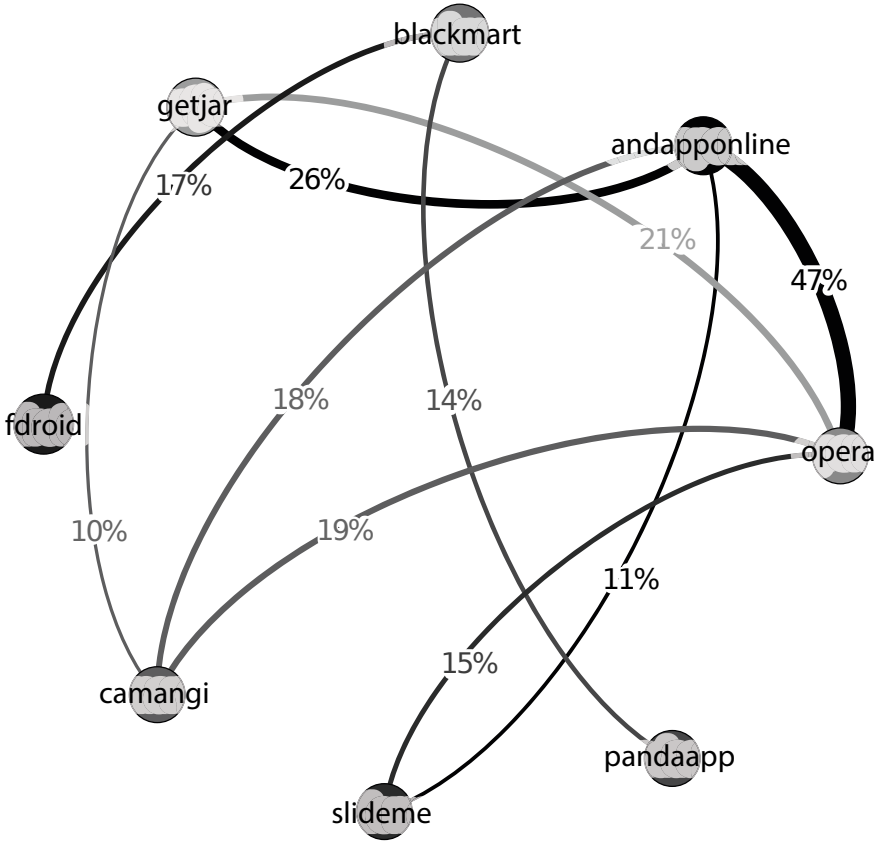
QUANTO È FACILE CASCARCI?

- 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

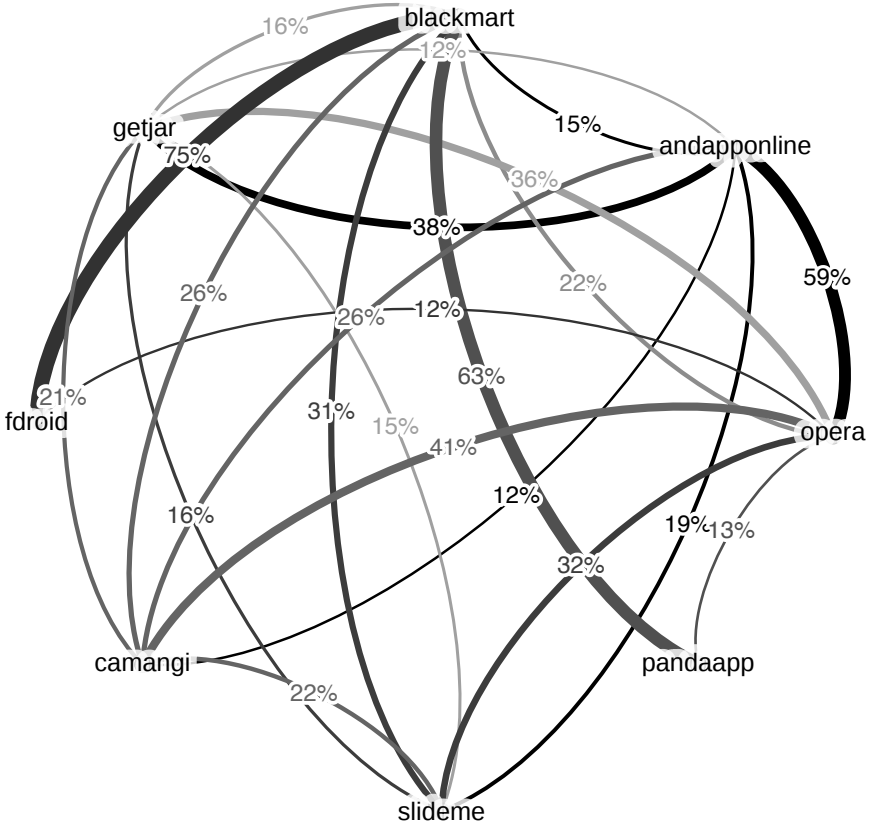


UNO ALLA VOLTA, PER CARITÀ!

Per MD5



Per package name



PROBING

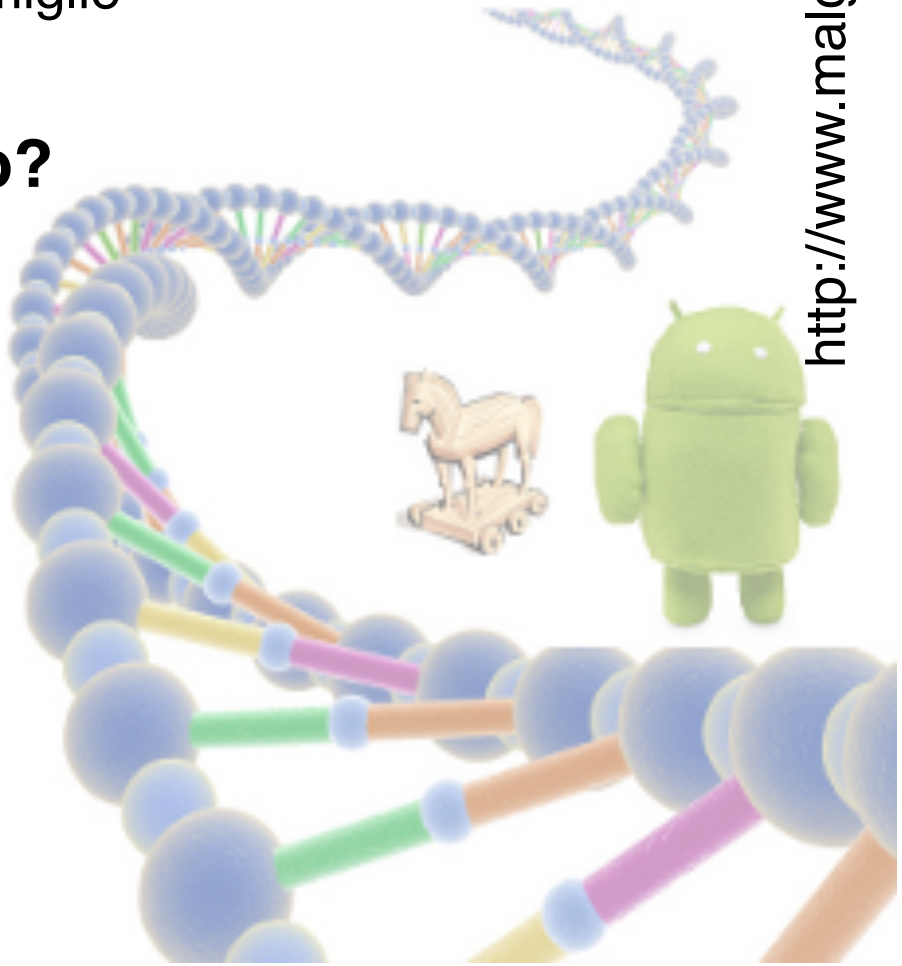
Android Malware Genome Project

- 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 :-)



http://www.malgenomeproject.org/

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

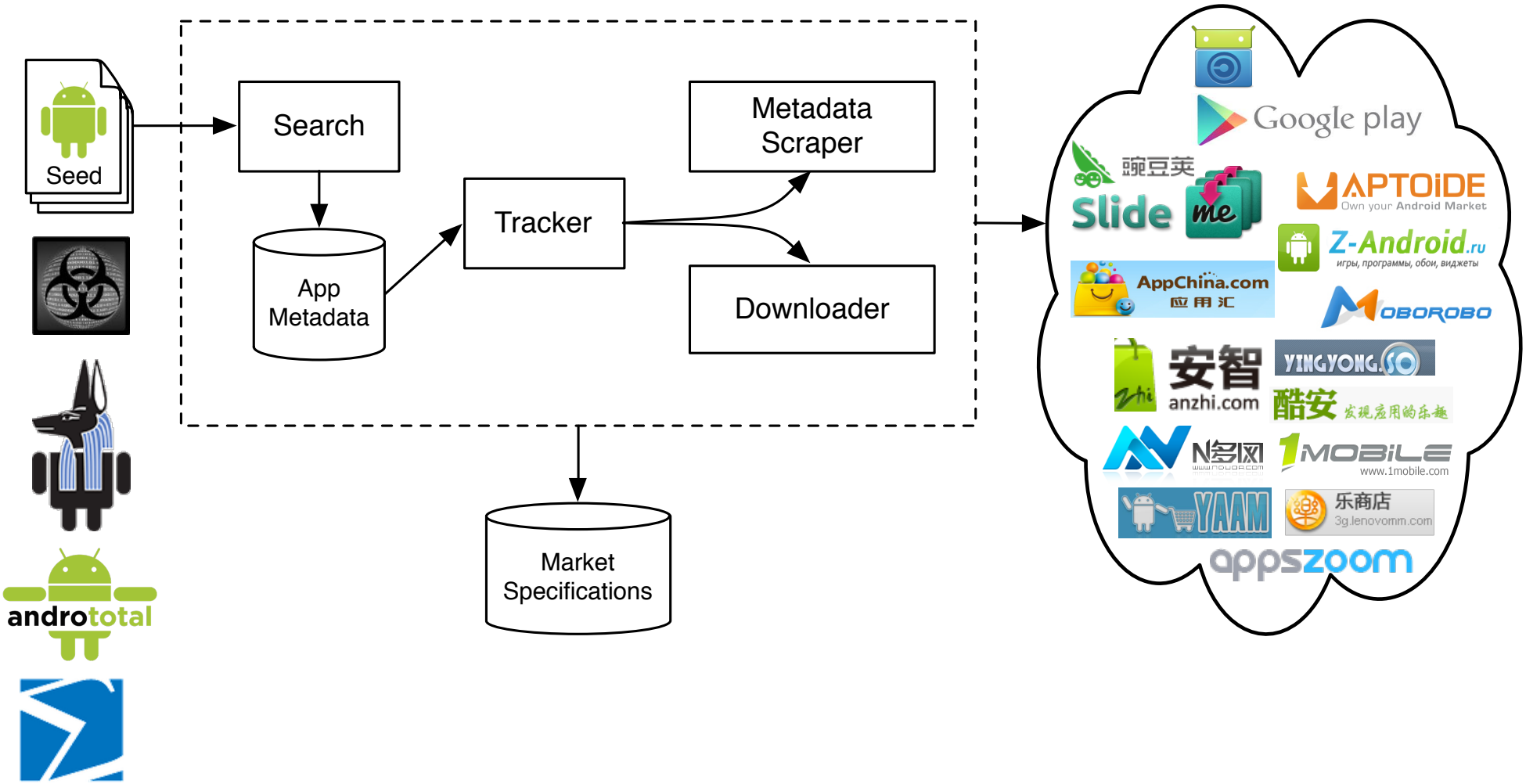
OSTACOLI

- 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)

loaded Community Blog DEVELOPERS EN

Download | Screenshots (4) | Comments (35) | App Support

Rolling Panda

LOAD BY EMAIL
- 3.75 MB - FREE

I you an email, so you must
n

QR CODE
v 1.5.0 - 3.75 MB - FREE

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

DIRECT DOWNLOAD APK FILE
v 1.5.0 - 3.75 MB - FREE

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

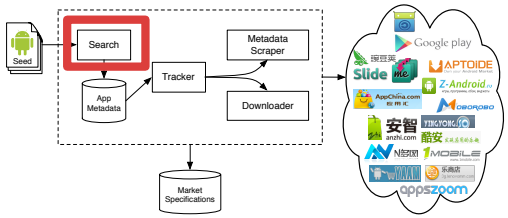
Older versions

and permissions

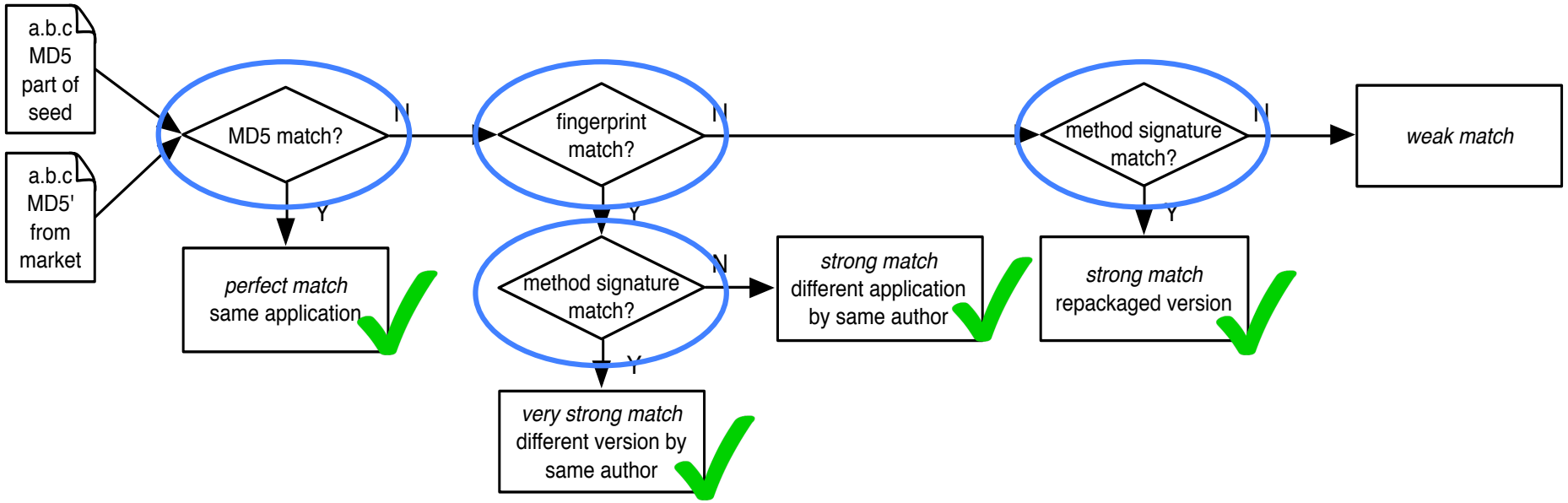
Changelog

Package com.kidsfun.jump.panda

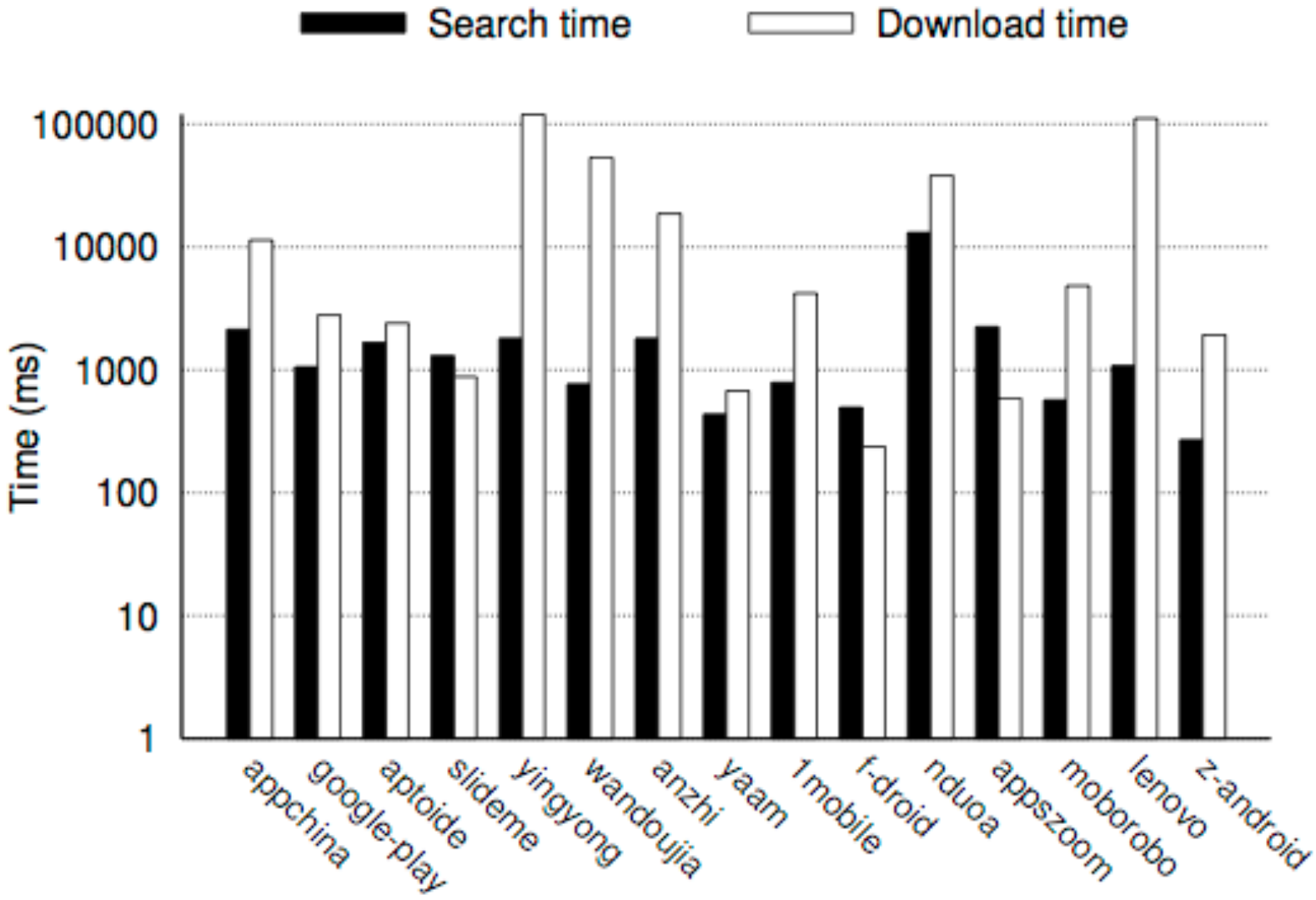
t access (wifi, 3G…) you have at every moment.



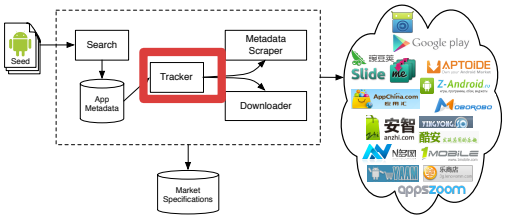
ORA ABBIAMO L'APK



VELOCITA`



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



TRACKING

- Monitoraggio continuo di ogni nuova app trovata
- Estrae 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

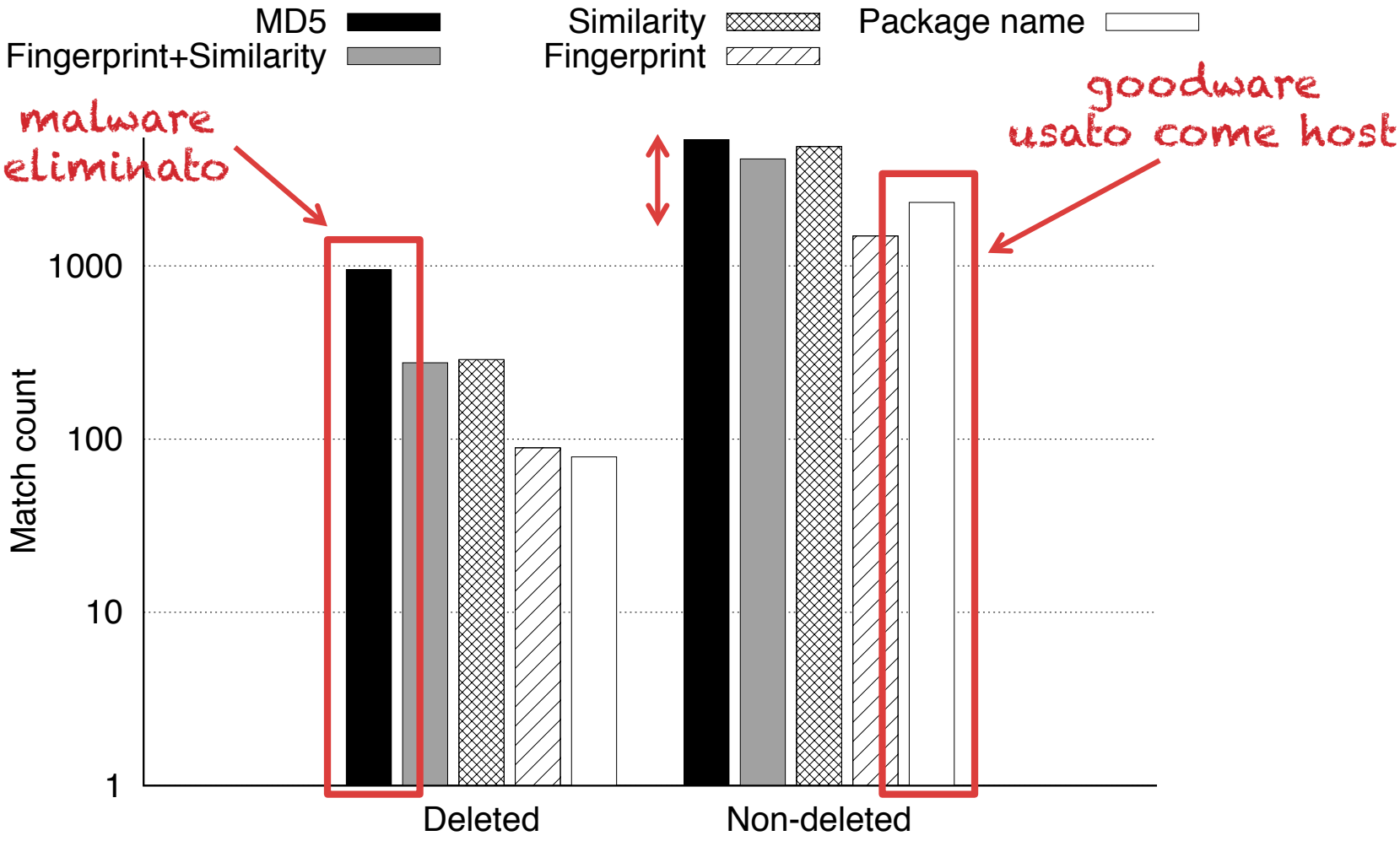
IL PROGETTO “ANDROID MARKET RADAR”

CASO DI STUDIO

ESTENSIONI FUTURE e CONCLUSIONI

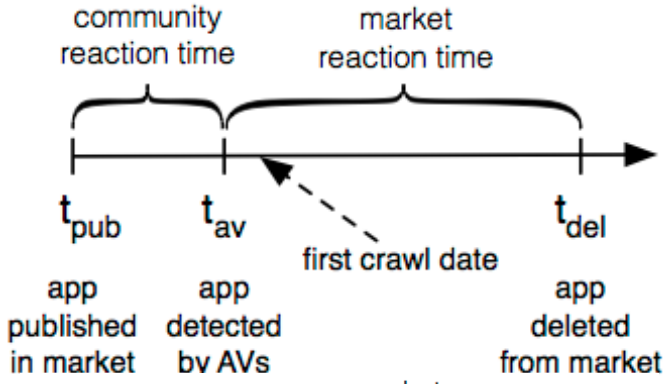
CASO DI STUDIO (AGO–DIC ‘13)

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

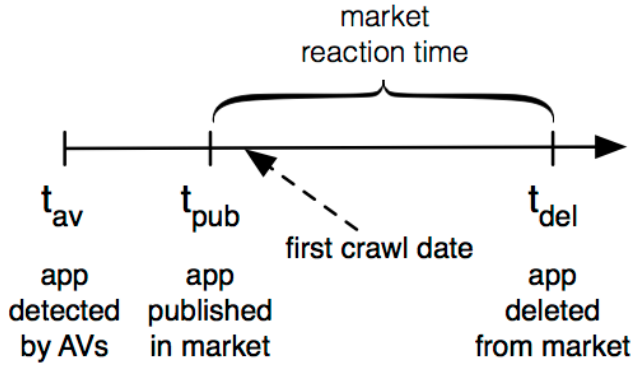


CICLI DI VITA DI UN APP MALICIOUS

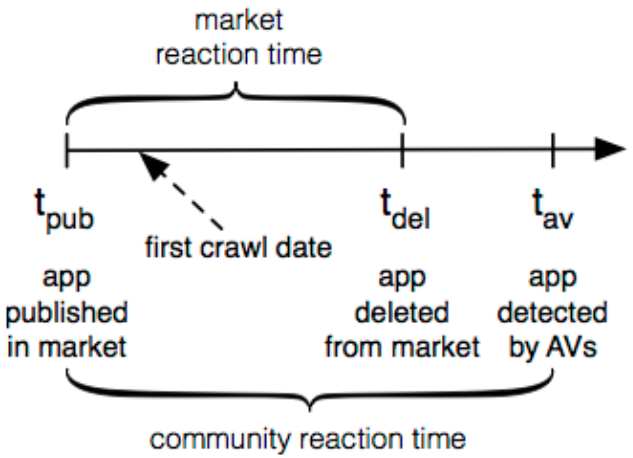
NORMALE (90.57%)
Rimozione dopo notifica da AV



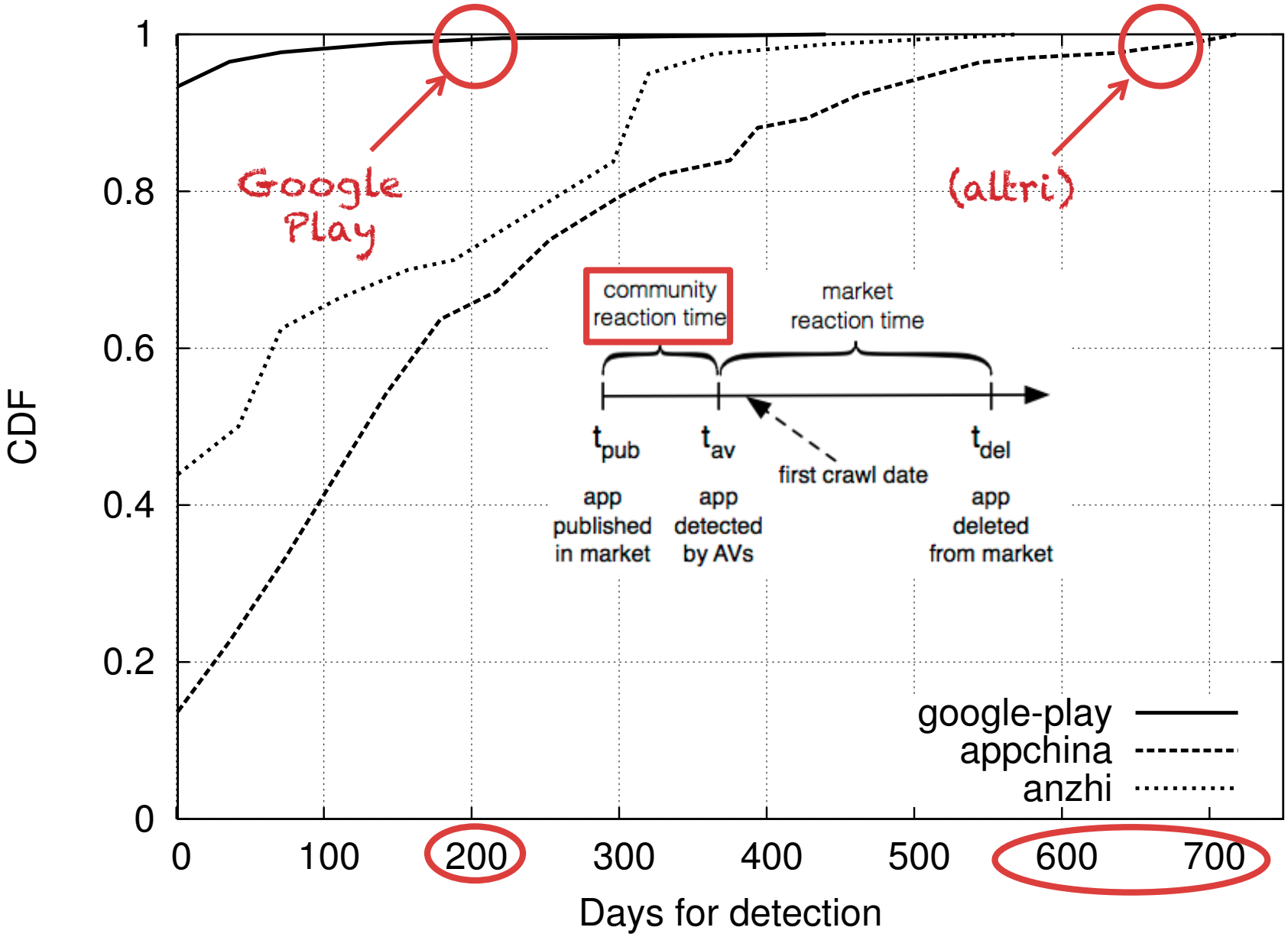
HOPPING (7.89%)
A volte ritornano…



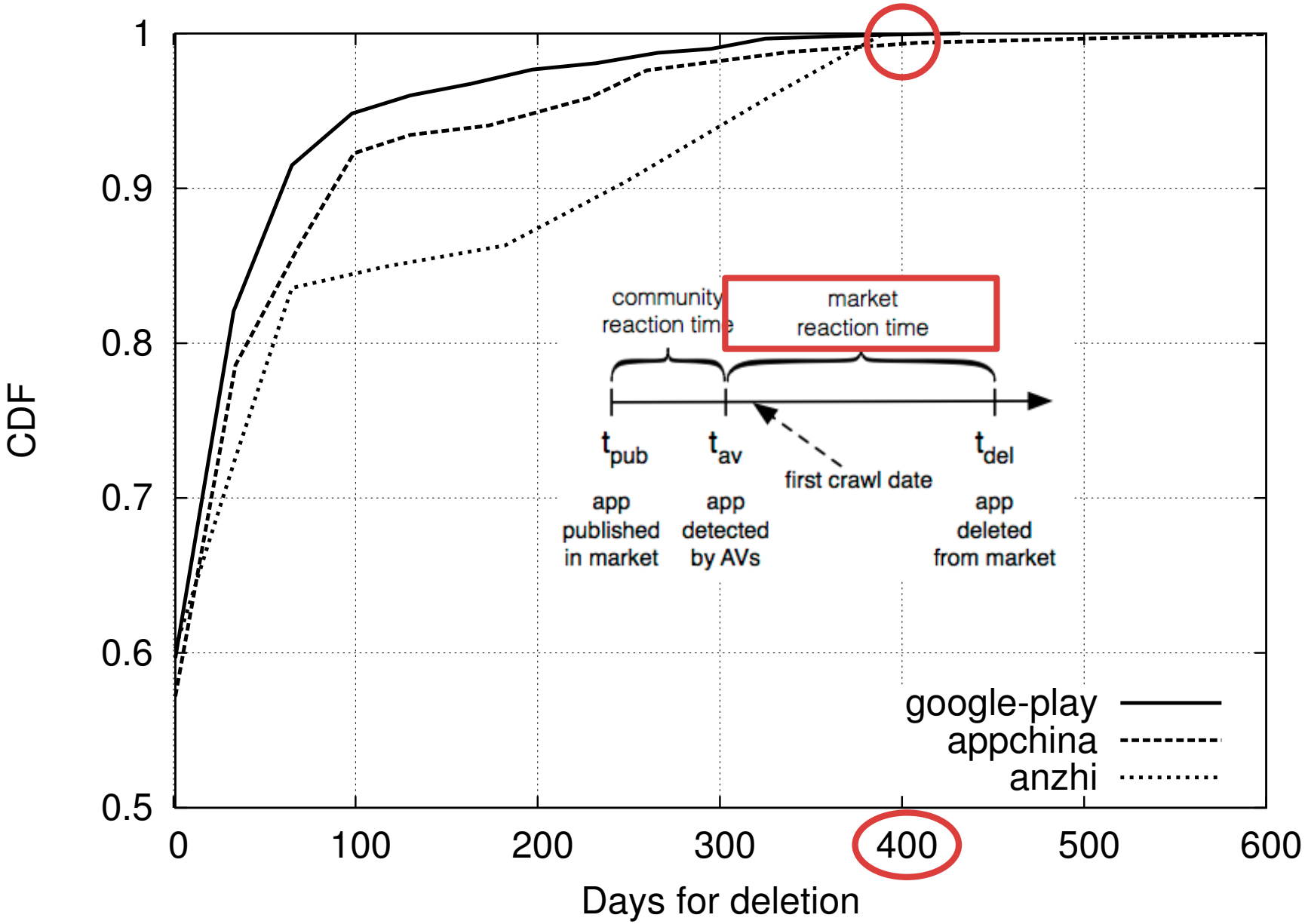
SELF-DEFENSE (1.56%)
Market meglio della community



TEMPI DI REAZIONE (COMMUNITY)

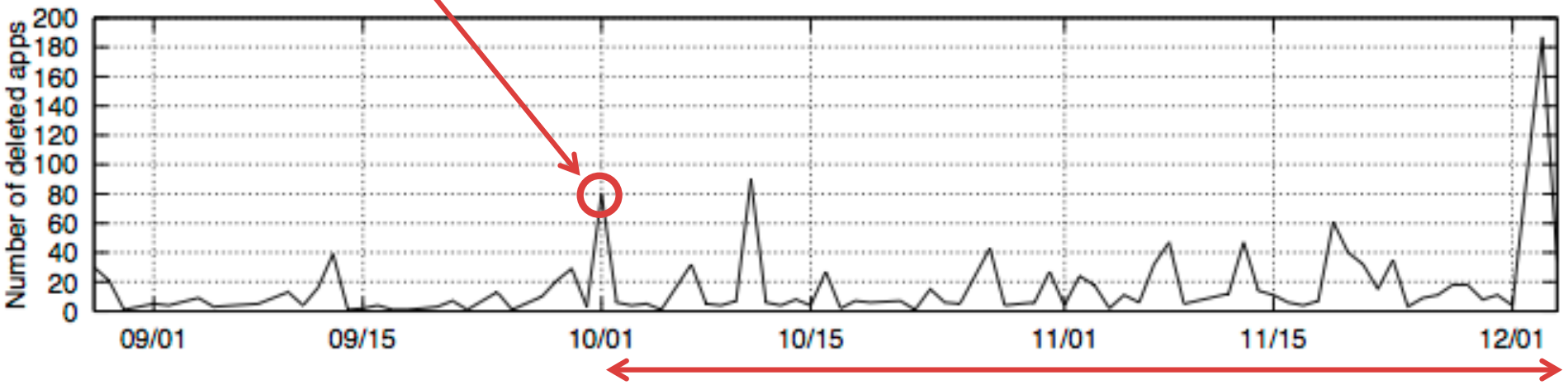


TEMPI DI REAZIONE (MARKET)



QUANDO SI FANNO LE PULIZIE?

nuove policy
anti "adware"



circa 1,600 app "adware" rimosse

(erano nel market da 1+ anni,
scaricate 100,000-500,000 volte)

…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

HackInBo

Sicurezza all'ombra delle Torri

FEDERICO MAGGI

POLITECNICO DI MILANO

@phretor