Android apps in sheep's clothing

April 1st, 2015

Tobias Ospelt, modzero AG

SIGS Special Event –

"It's not a joke - it can happen"

modzero

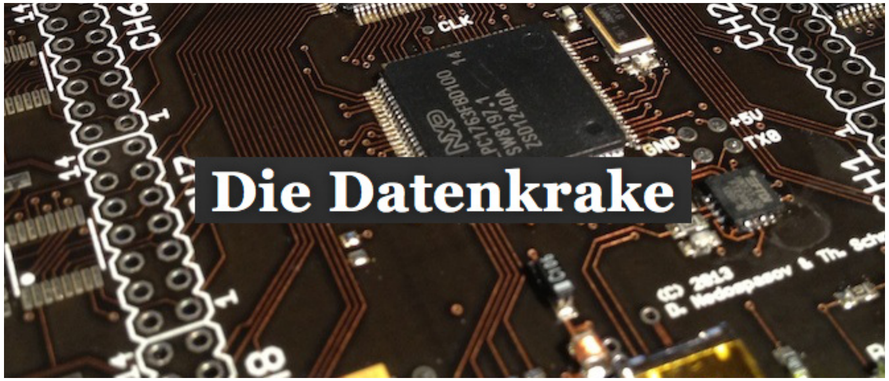
- 6 IT security experts
- We do all areas of technical HW & SW security analysis
  - Penetration Testing, Crypto, Web, embedded devices, etc.

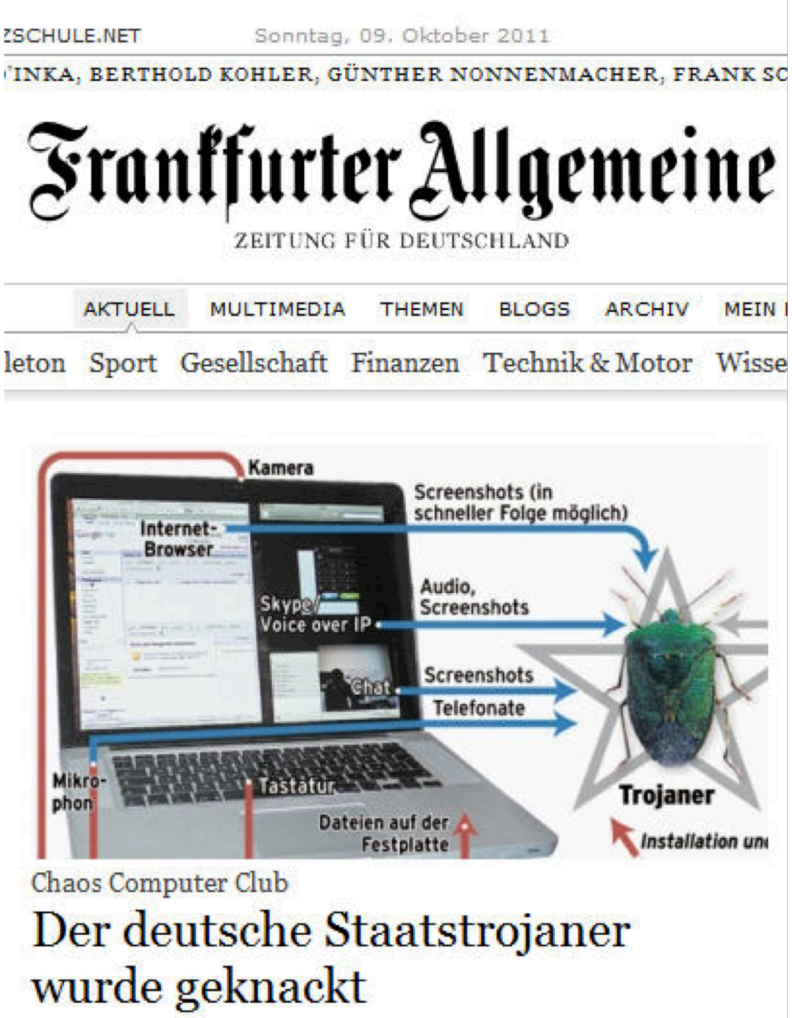
KeyKeriki v2 - Keyboards Are Not Enough - KeyKeriki v2

remote
exploit
.org

<<back|track

degate


Die Datenkrake


ZSCHULE.NET Sonntag, 09. Oktober 2011

'INKA, BERTHOLD KOHLER, GÜNTHER NONNENMACHER, FRANK SC

Frankfurter Allgemeine

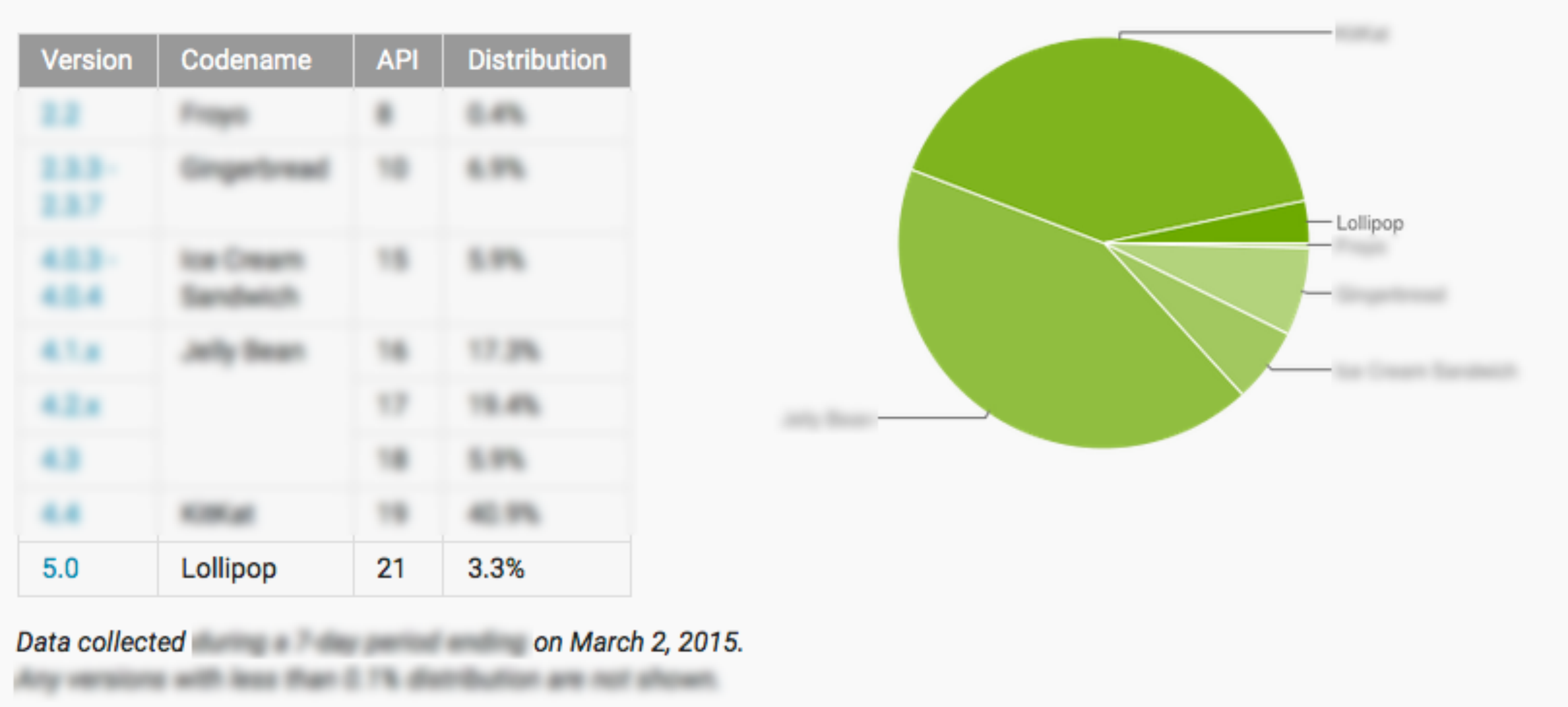
ZEITUNG FÜR DEUTSCHLAND

Chaos Computer Club

Der deutsche Staatstrojaner wurde geknackt

Android

- Android has about 62% market share



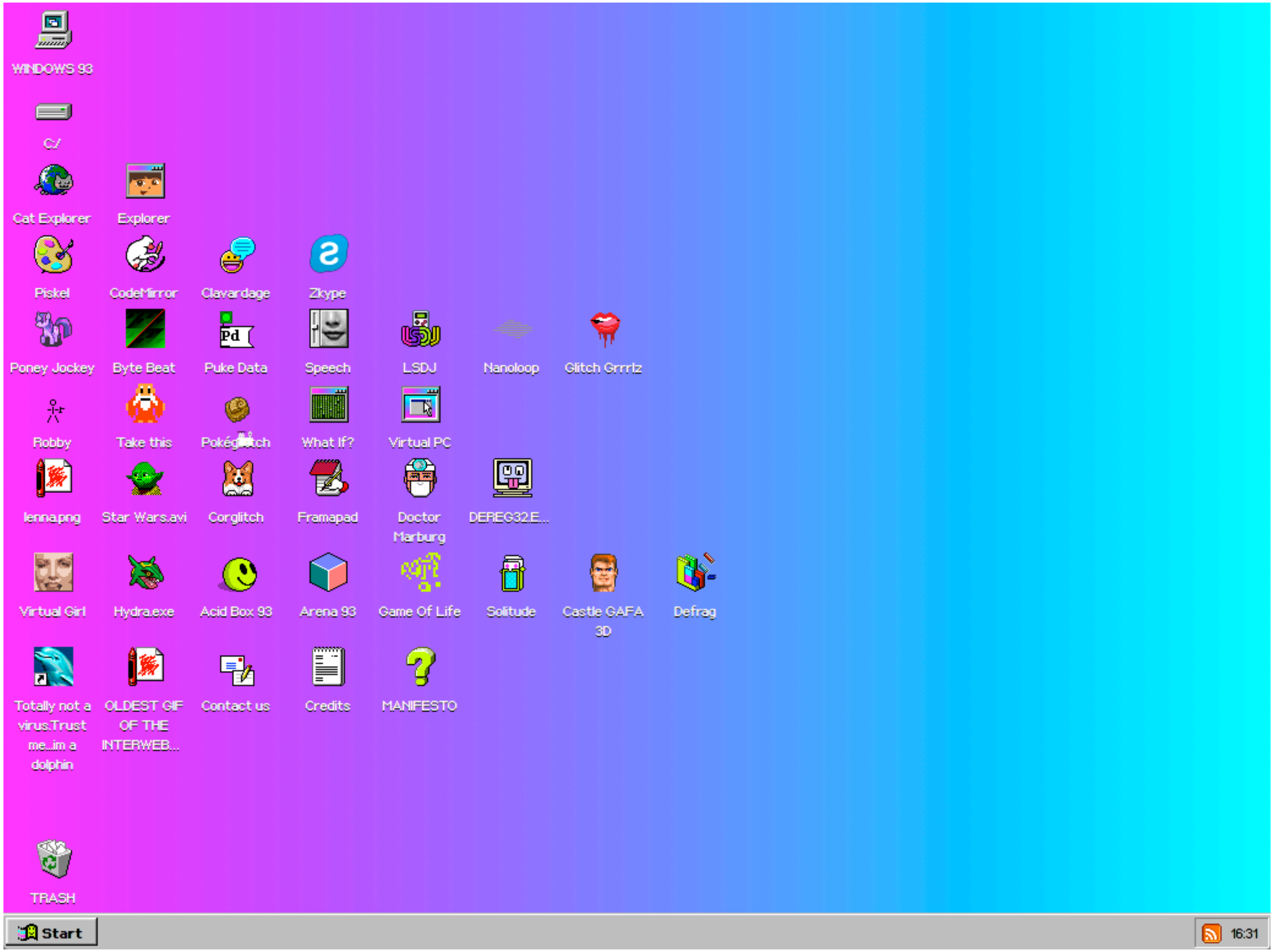
Version	Codename	API	Distribution
2.2	Froyo	8	0.4%
2.3.3 - 2.3.7	Gingerbread	10	6.9%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.9%
4.1.x	Jelly Bean	16	17.3%
4.2.x		17	19.4%
4.3		18	5.9%
4.4	KitKat	19	40.9%
5.0	Lollipop	21	3.3%

Data collected during a 7-day period ending on March 2, 2015.
Any versions with less than 0.1% distribution are not shown.

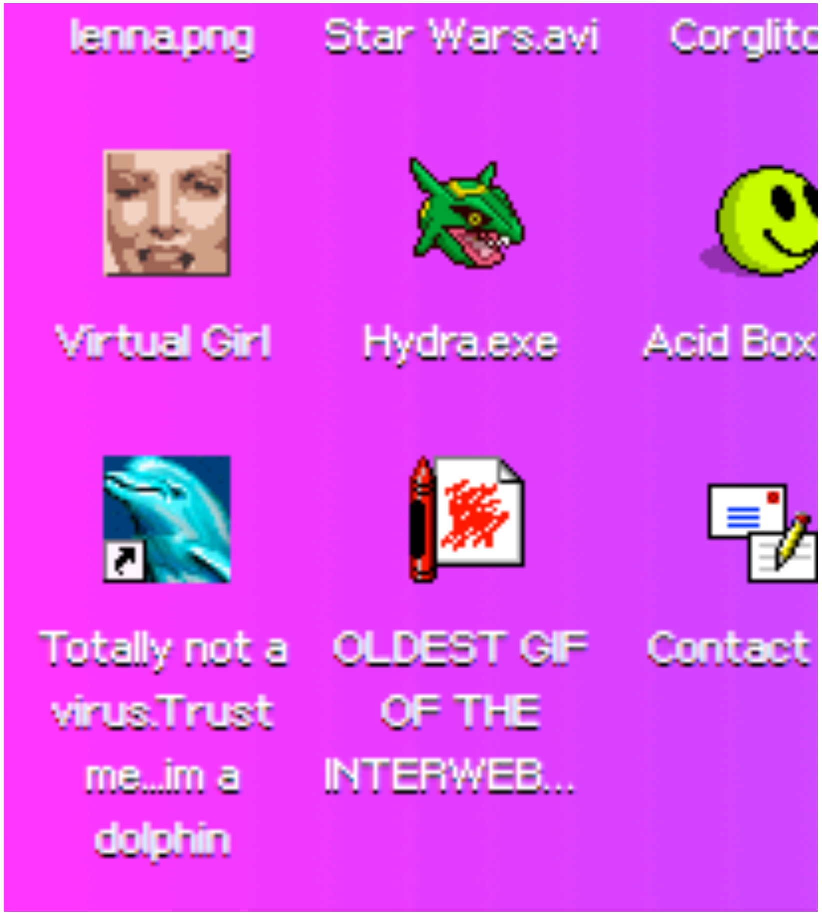
We are going to see a User Interface (UI) attack today

History of UI attacks

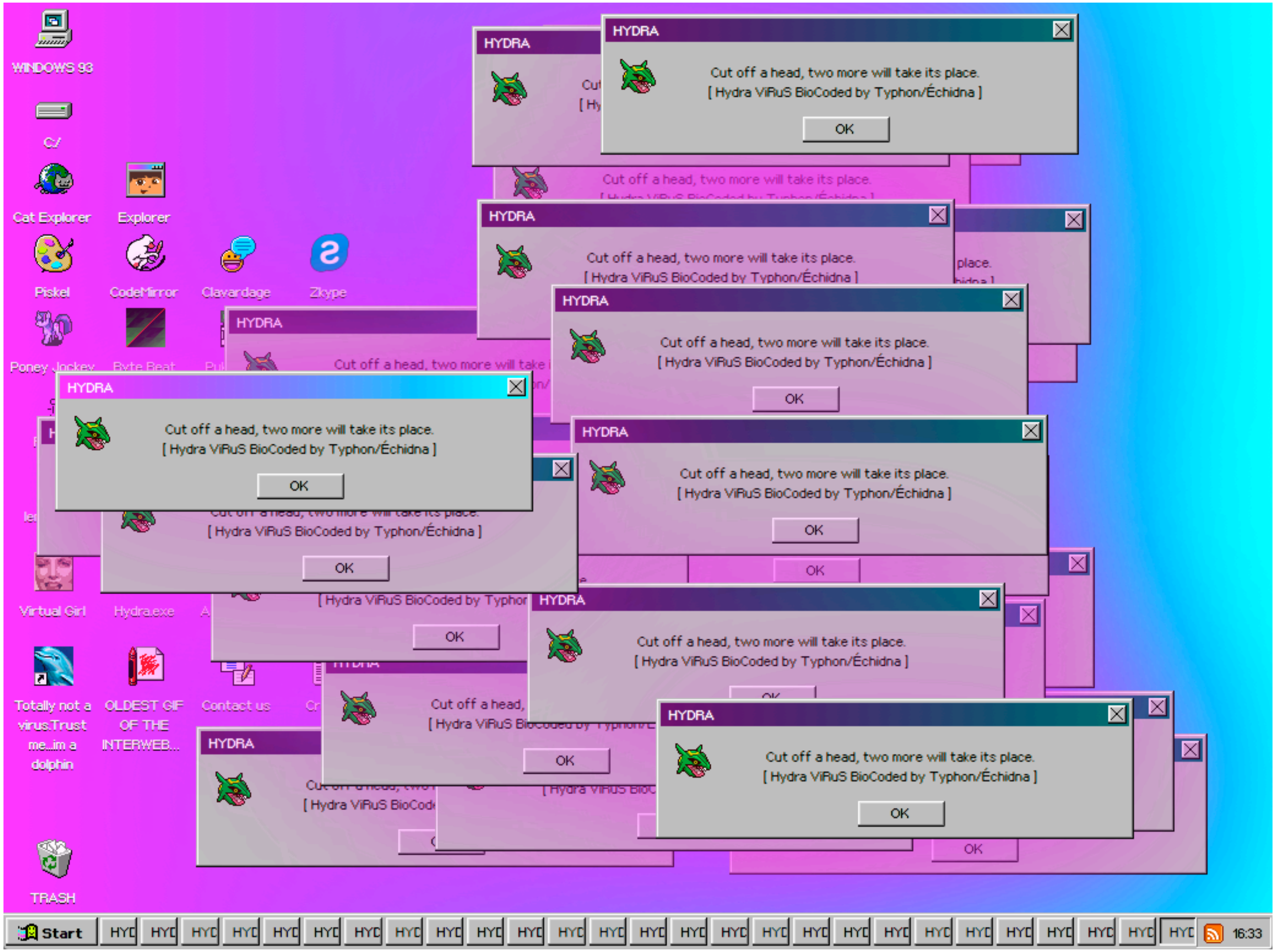
Microsoft Windows 90ies overlay



Microsoft Windows 90ies overlay

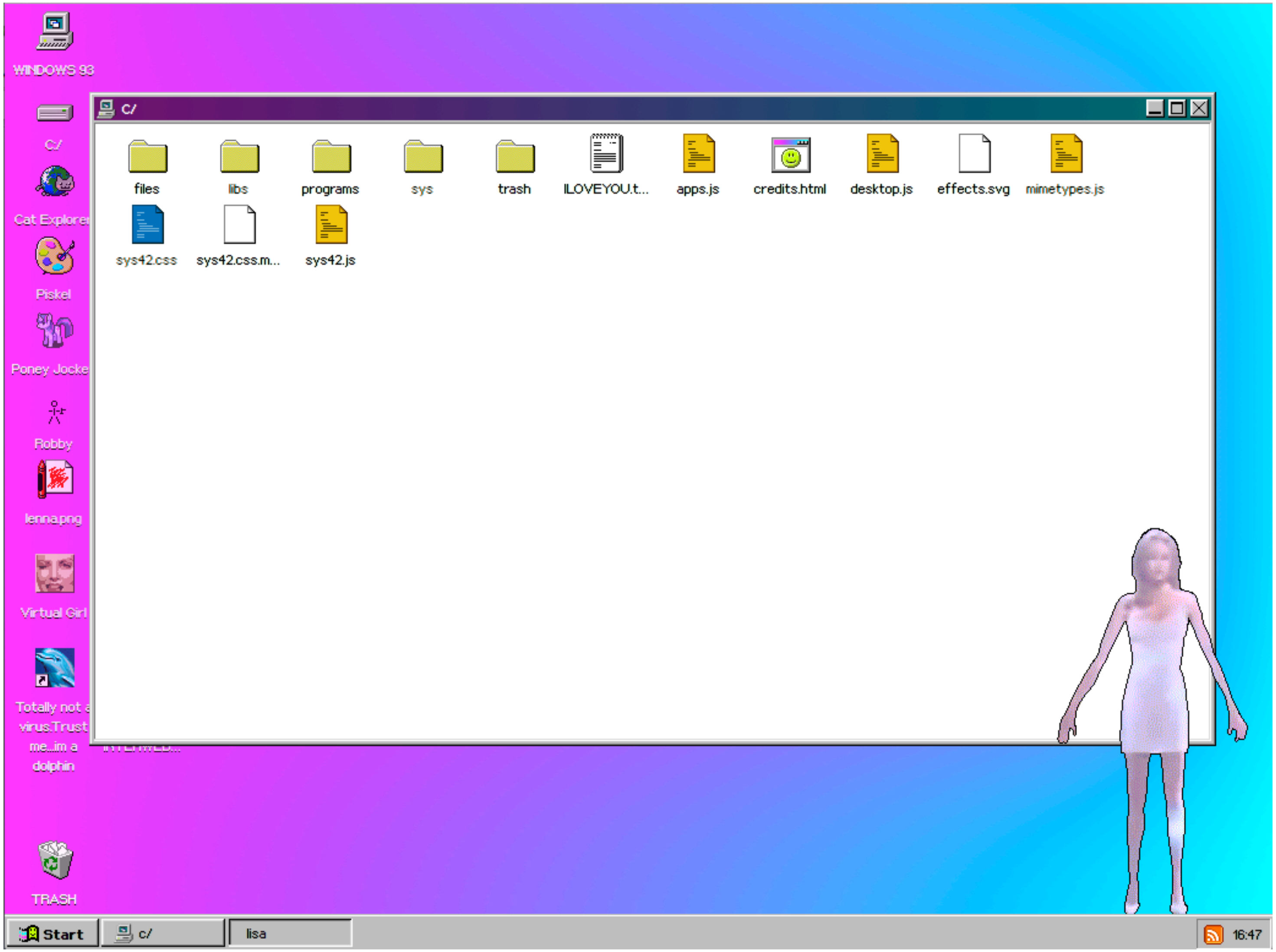

lenna.png
Star Wars.avi
Corglito
Virtual Girl
Hydra.exe
Acid Box
Totally not a virus.Trust me...im a dolphin
OLDEST GIF OF THE INTERWEB...
Contact

Microsoft Windows 90ies overlay

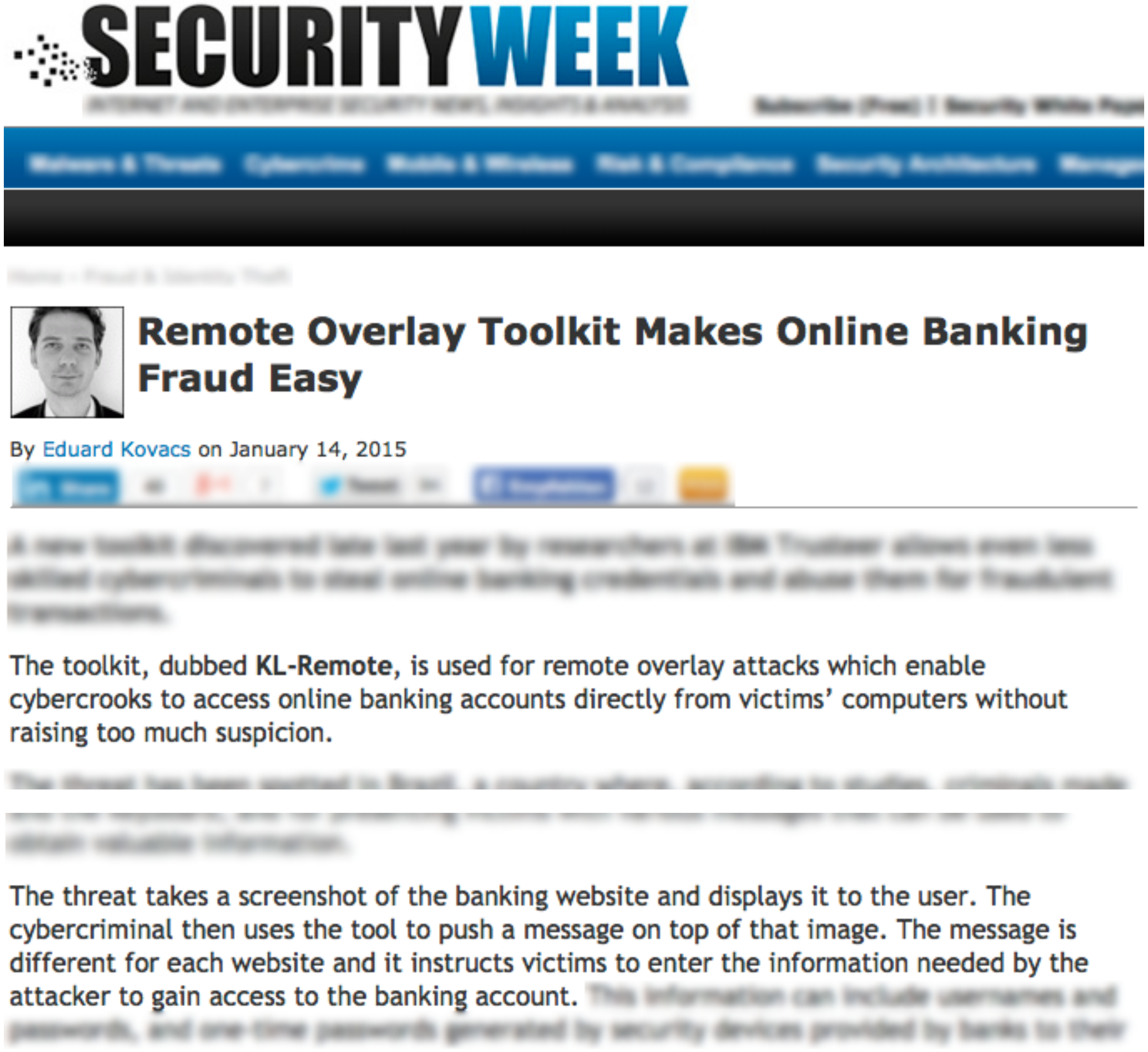

HYDRA

Cut off a head, two more will take its place.
[Hydra ViRuS BioCoded by Typhon/Échidna]

Microsoft Windows 90ies overlay



Modern Windows Overlays


SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | Security White Pape
Malware & Threats
Cybercrime
Mobile & Wireless
Risk & Compliance
Security Architecture
Managem
Home › Fraud & Identity Theft

Remote Overlay Toolkit Makes Online Banking Fraud Easy

By Eduard Kovacs on January 14, 2015

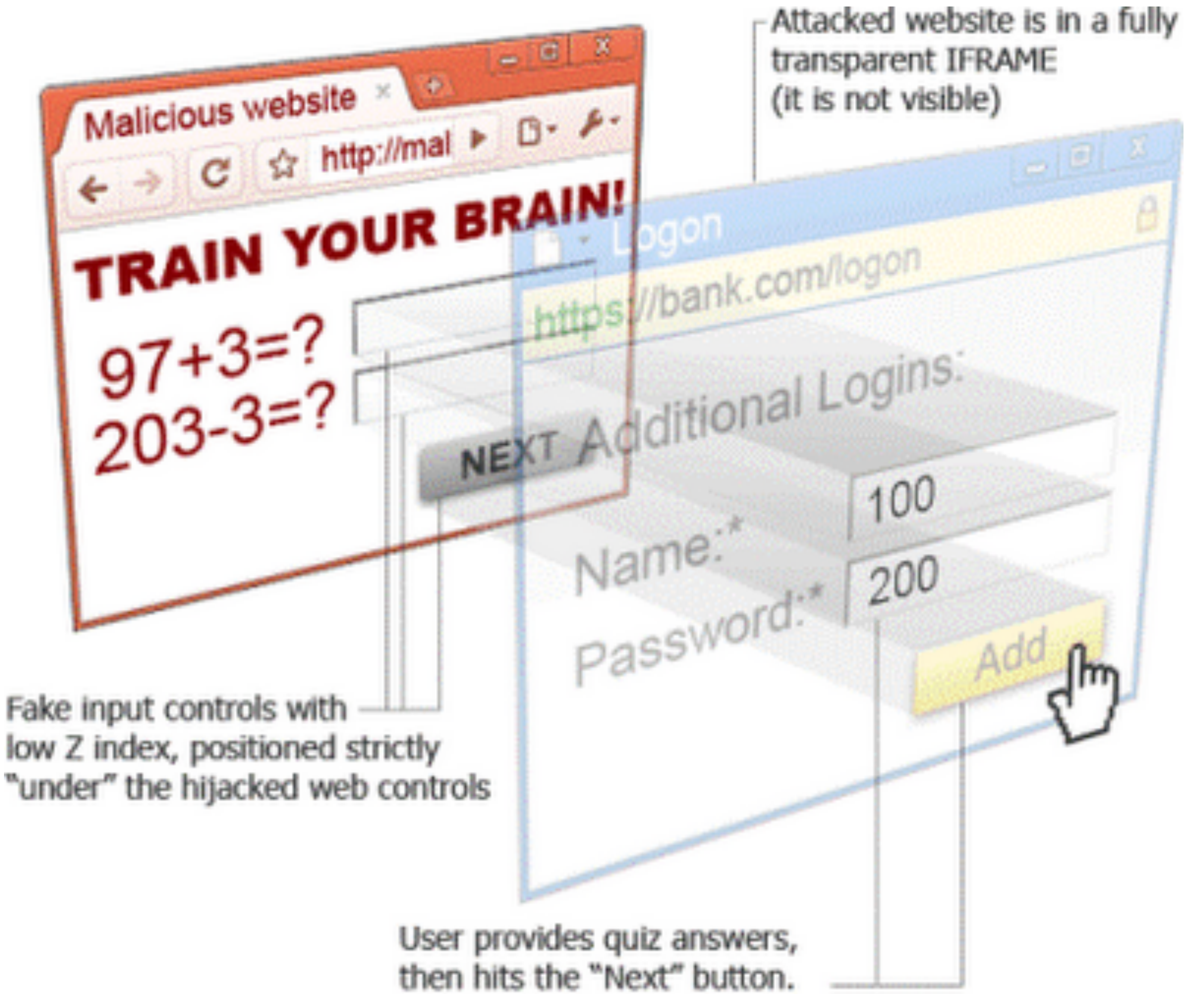
A new toolkit discovered late last year by researchers at IBM Trusteer allows even less skilled cybercriminals to steal online banking credentials and abuse them for fraudulent transactions.

The toolkit, dubbed **KL-Remote**, is used for remote overlay attacks which enable cybercrooks to access online banking accounts directly from victims' computers without raising too much suspicion.

The threat has been spotted in Brazil, a country where, according to studies, criminals made
[illegible] and the keyboard, and for presenting victims with various messages that can be used to obtain valuable information.

The threat takes a screenshot of the banking website and displays it to the user. The cybercriminal then uses the tool to push a message on top of that image. The message is different for each website and it instructs victims to enter the information needed by the attacker to gain access to the banking account. This information can include usernames and passwords, and one-time passwords generated by security devices provided by banks to their

Browser Clickjacking



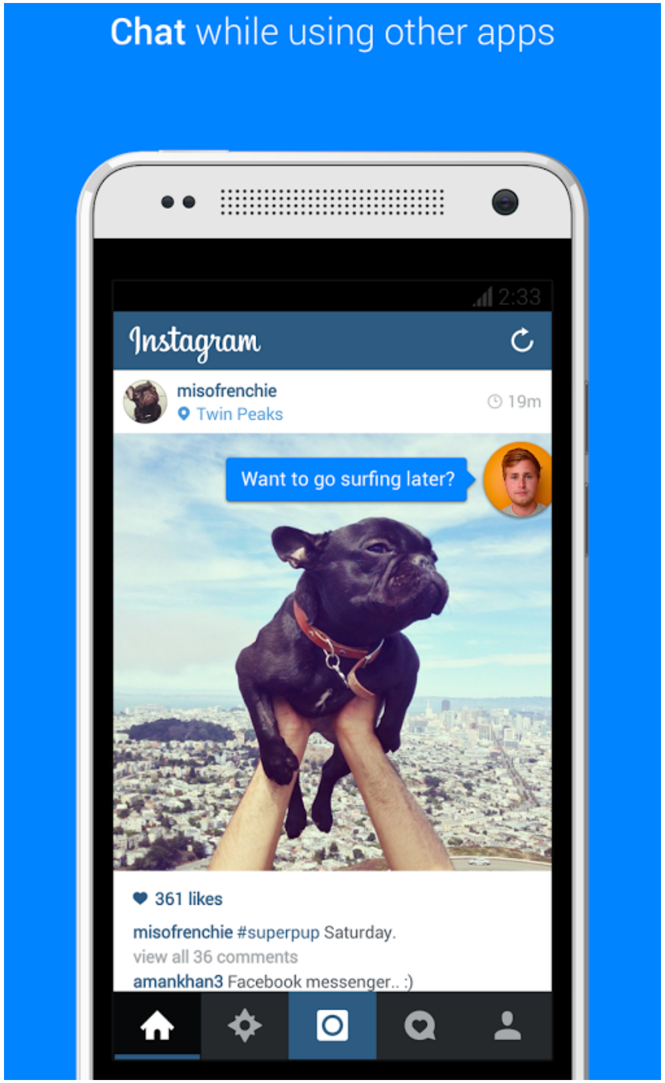
Attacked website is in a fully transparent IFRAME (it is not visible)

Fake input controls with low Z index, positioned strictly "under" the hijacked web controls

User provides quiz answers, then hits the "Next" button. All these clicks are hijacked by the invisible frame as its controls have higher (by default) Z order.

Image Copyright: ThreatExpert Ltd. 2008

Android overlays



Chat while using other apps

2:33
Instagram
misofrenchie
Twin Peaks
19m
Want to go surfing later?
361 likes
misofrenchie #superpup Saturday.
view all 36 comments
amankhan3 Facebook messenger.. :)

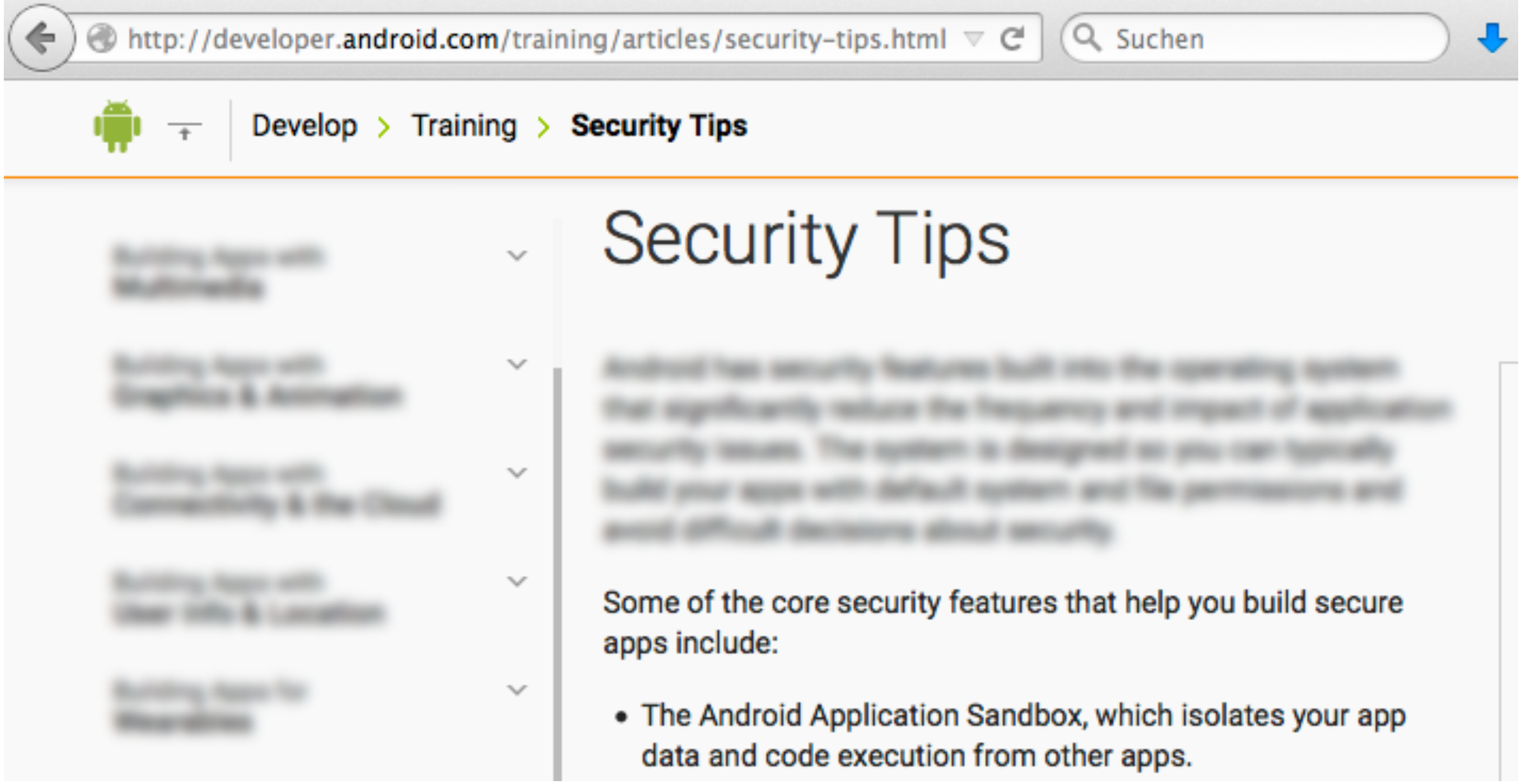
Overlaying Android apps

Android apps in sheep's clothing

What

- Stealing credentials
  - When adding a Google account to Android
  - Or from all other apps with logins
    - Enterprise containers (Good, MobileIron, etc.)
    - Password safes
    - Social media, etc.
- Manipulating sensitive data that is displayed
  - Two-factor authentication mobile banking transaction signing

How



http://developer.android.com/training/articles/security-tips.html

Develop > Training > Security Tips

Security Tips

Some of the core security features that help you build secure apps include:

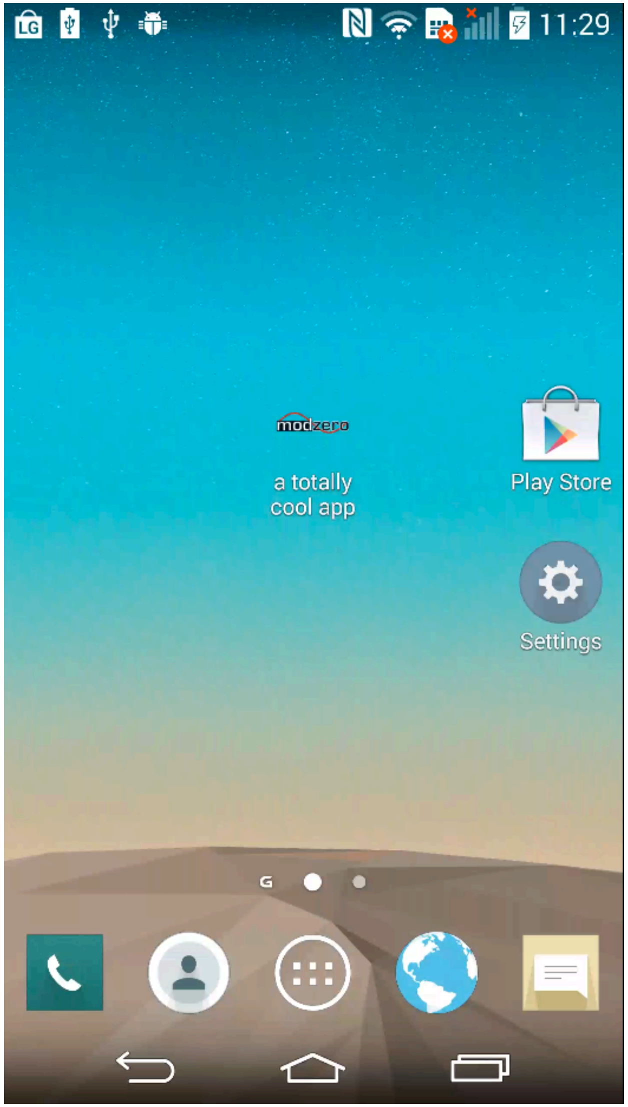
- The Android Application Sandbox, which isolates your app data and code execution from other apps.

- What about sandboxing on the User Interface (UI) level?

Prerequisites for our attack

- Installed malware app on phone
- Permissions
  - *GET_TASKS* (must)
  - *SYSTEM_ALERT_WINDOW* (recommended but optional)
  - *RECEIVE_BOOT_COMPLETED* (optional)
  - *INTERNET* (optional)

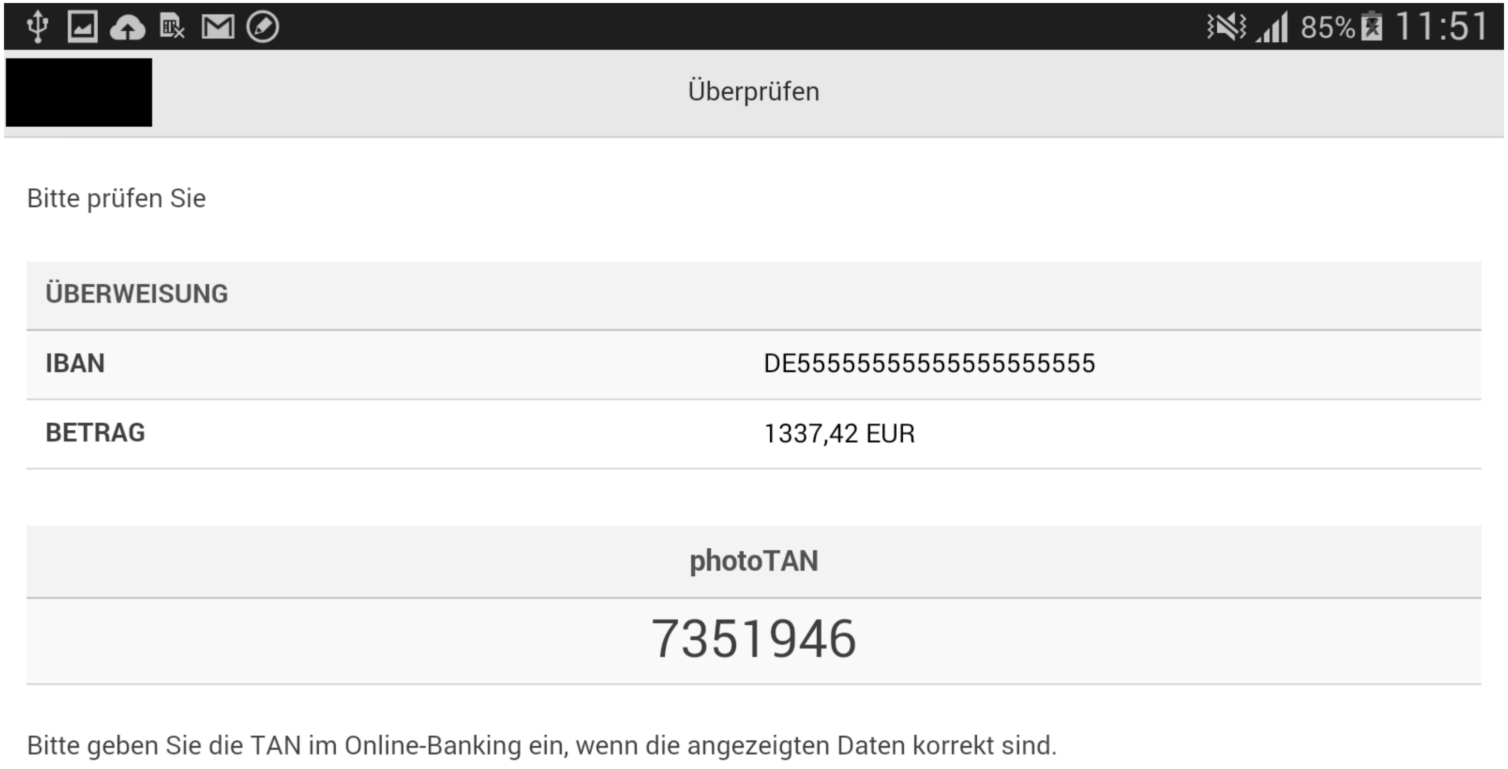
Demo: Stealing Skype credentials



How did it work?

- Exactly when the Skype app is opening the login screen, we bring our app to the foreground and show our faked login screen

Mobile banking transaction signing



[redacted]

Überprüfen

Bitte prüfen Sie

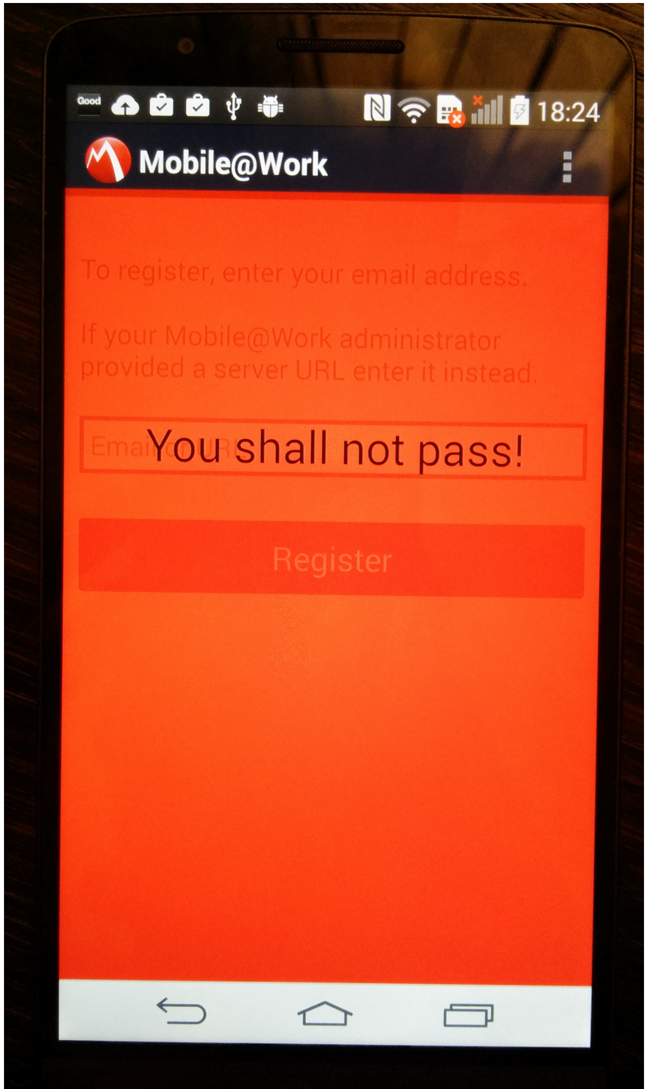
ÜBERWEISUNG	
IBAN	DE5555555555555555555
BETRAG	1337,42 EUR

photoTAN

7351946

Bitte geben Sie die TAN im Online-Banking ein, wenn die angezeigten Daten korrekt sind.

Enterprise containers – Example: MobileIron



Mobile@Work

To register, enter your email address.

If your Mobile@Work administrator provided a server URL enter it instead.

You shall not pass!

Is it fixed?

Hint: won't fix

First response Android Security Team

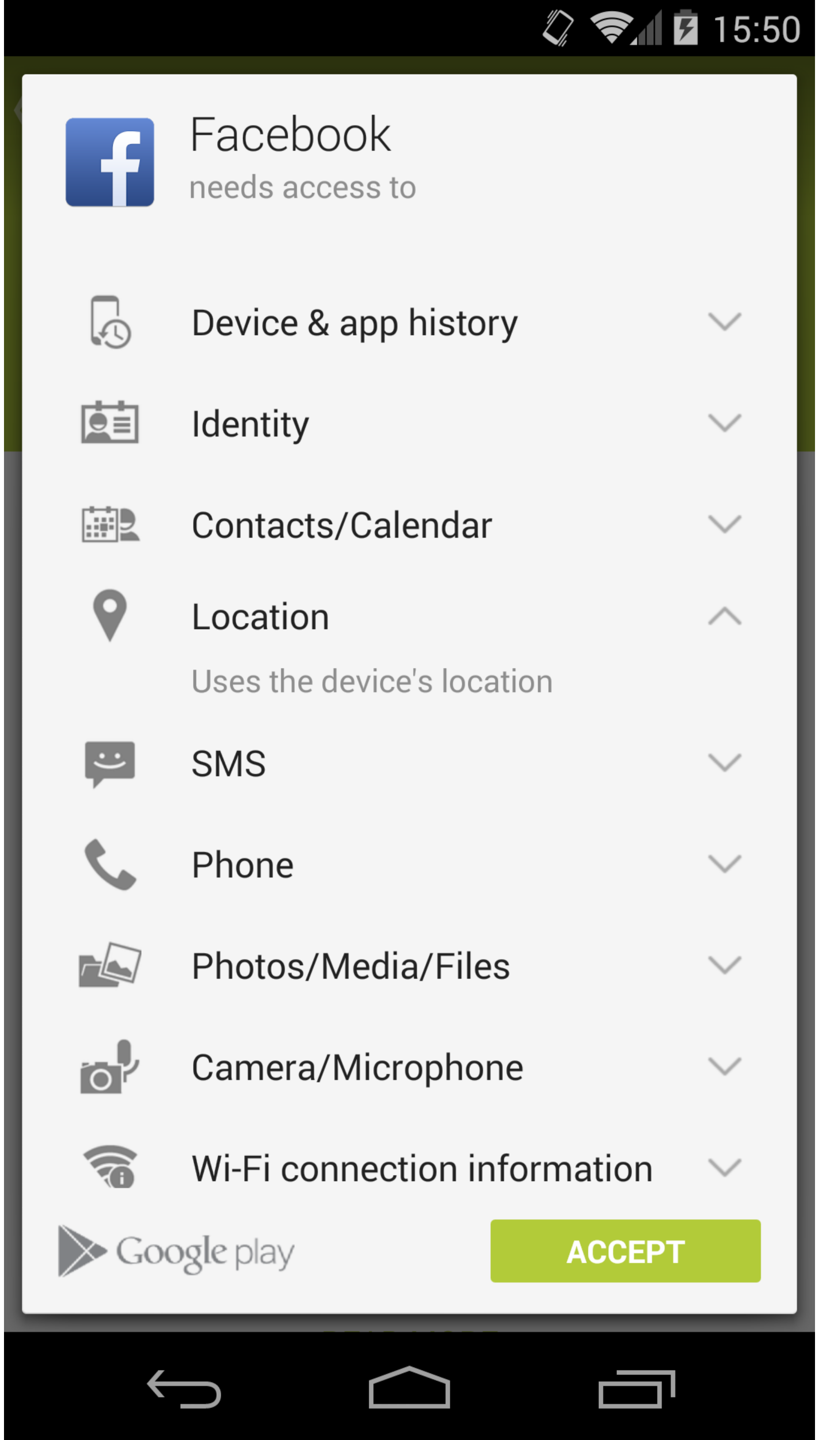
Let's talk about permissions...

"[...] We don't consider this behavior to be a flaw in the Android security model. [...] the attack requires the victim to knowingly install an app that has permission to monitor foreground applications. [...] Google Play analyzes apps that get submitted [...] for phishing and other potentially harmful behavior. [...]"

...and analyzing for harmful behavior.

Permission system is broken

- There is no opt-in/opt-out
  - Give it all permissions it wants or uninstall it
- Cyanogenmod (an alternative Android version) has permission opt-in/opt-out called "Privacy Guard". Why not on Android?



Facebook

needs access to

Device & app history

Identity

Contacts/Calendar

Location

Uses the device's location

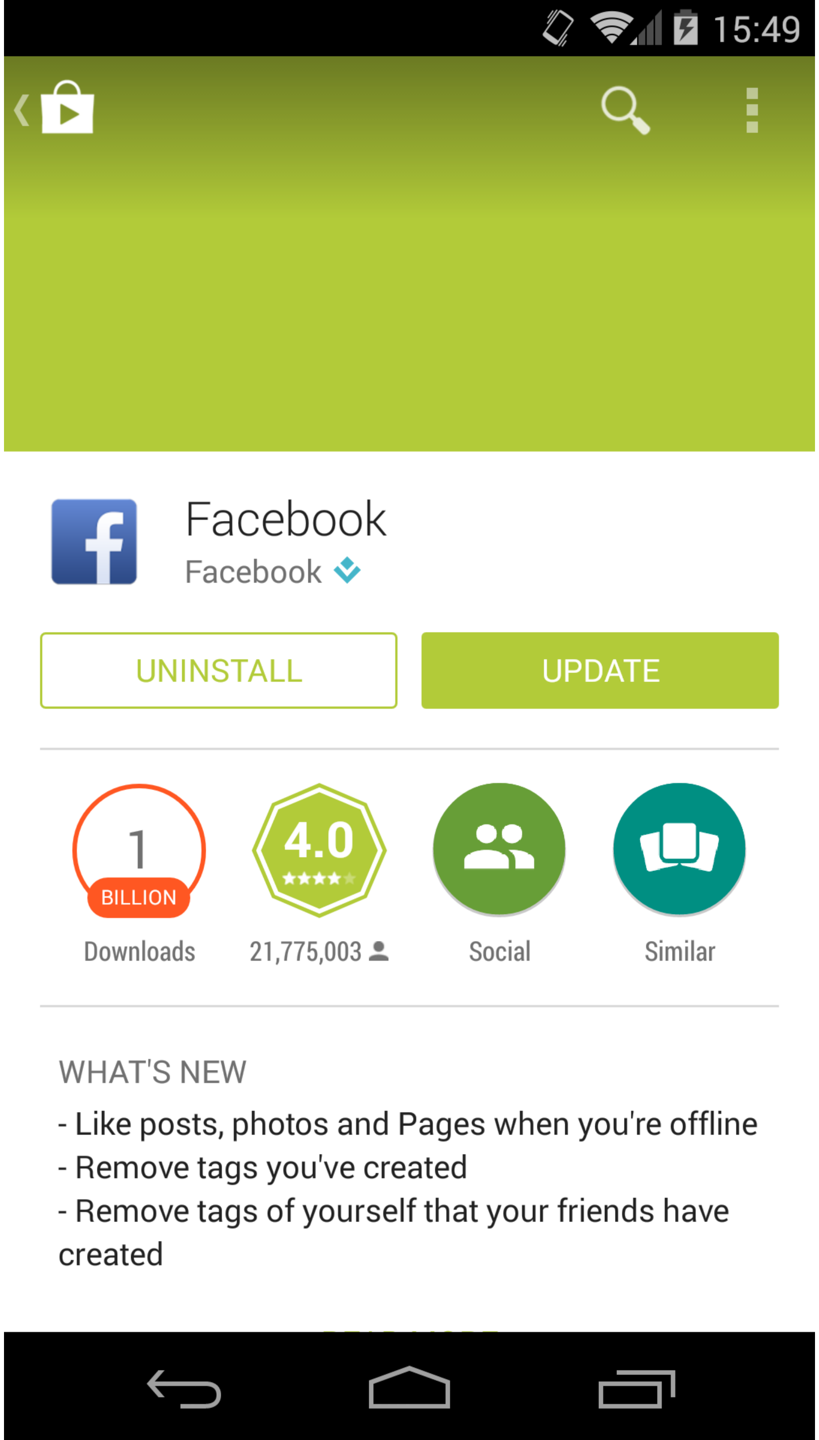
SMS

Phone

Photos/Media/Files

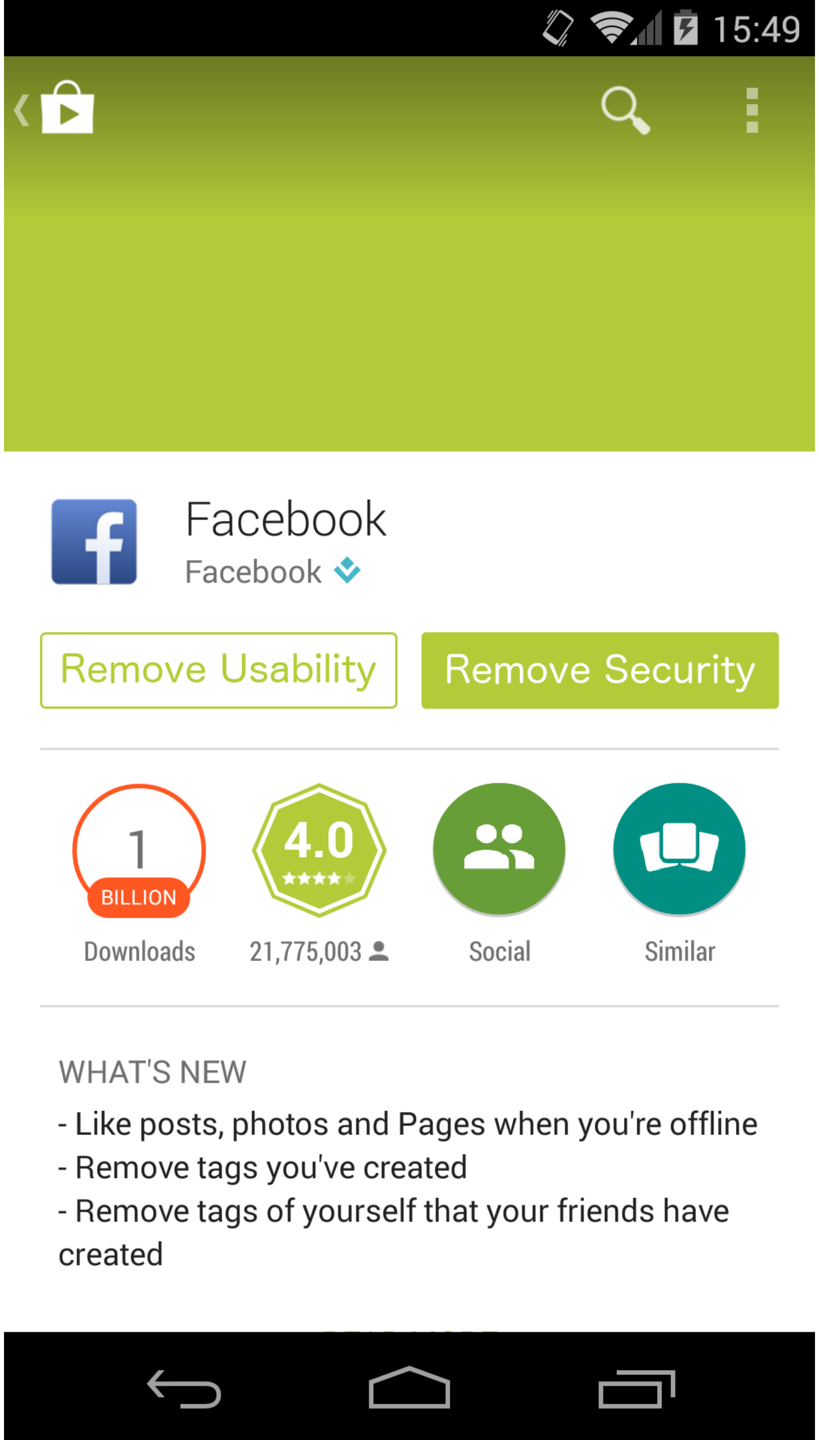
Camera/Microphone

Wi-Fi connection information



WHAT'S NEW

- Like posts, photos and Pages when you're offline
- Remove tags you've created
- Remove tags of yourself that your friends have created



Facebook

Facebook

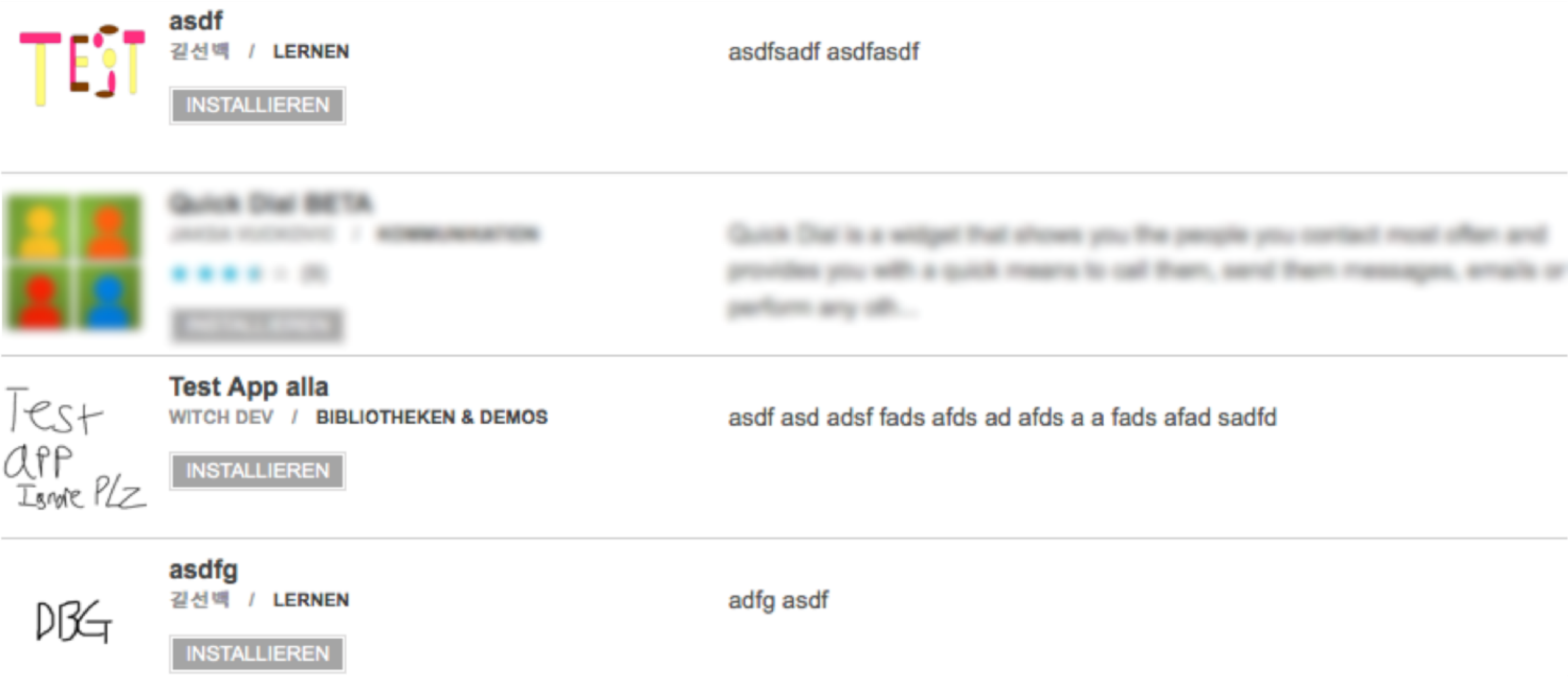
WHAT'S NEW

- Like posts, photos and Pages when you're offline
- Remove tags you've created
- Remove tags of yourself that your friends have created

Google is scanning for harmful behavior?

- What about other app stores?
- The malware app will be disguised as a legitimate app
  - Functionality will require those permissions
- Other malware made it in the Play store
- Our malware code can be loaded after the app is already in the store

Talking about quality assurance in the Google Play store...



asdf
길선택 / LERNEN
INSTALLIEREN

asdfsadf asdfasdf

Quick Dial BETA
[illegible] / KOMMUNIKATION
★★★★☆ (8)
INSTALLIEREN

Quick Dial is a widget that shows you the people you contact most often and provides you with a quick means to call them, send them messages, emails or perform any oth...

Test App alla
WITCH DEV / BIBLIOTHEKEN & DEMOS
INSTALLIEREN

asdf asd adsf fads afds ad afds a a fads afad sadfd

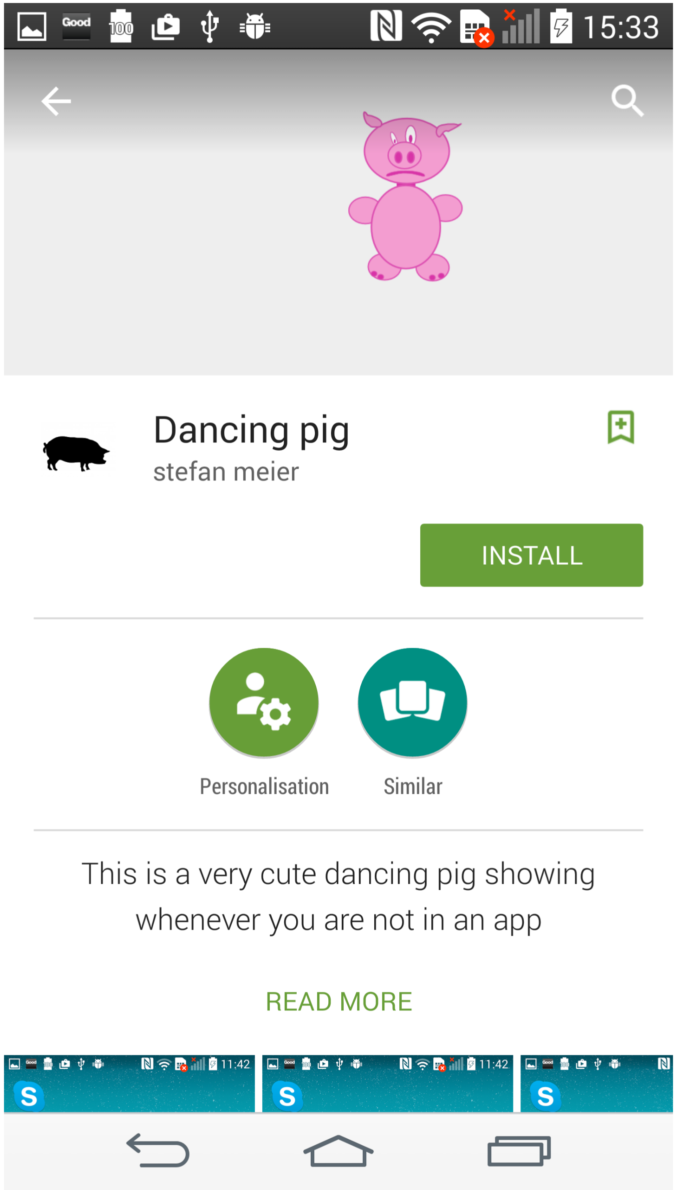
asdfg
길선택 / LERNEN
INSTALLIEREN

adfg asdf

"Given a choice between dancing pigs and security, users will pick dancing pigs every time."

– Edward Felten (Securing Java)

Demo: I just couldn't resist



Dancing pig

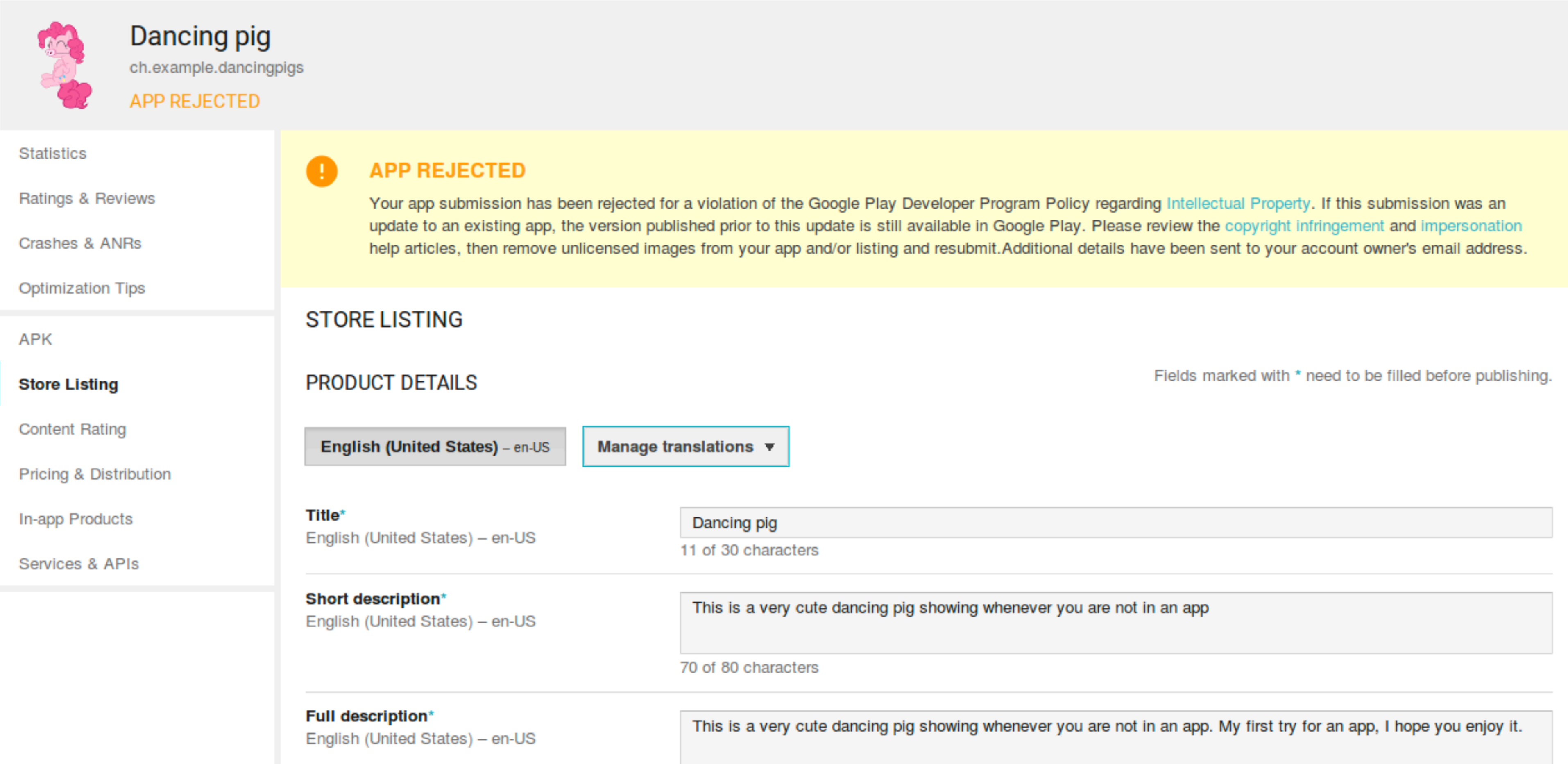
stefan meier

This is a very cute dancing pig showing whenever you are not in an app

I just couldn't resist

- Uploaded yesterday
- This particular demo works only on LG g3 with Android 5
- Download the malware:
  - https://play.google.com/store/apps/details?id=ch.example.dancingpigs

I just couldn't resist



Dancing pig
ch.example.dancingpigs
APP REJECTED

! APP REJECTED

Your app submission has been rejected for a violation of the Google Play Developer Program Policy regarding Intellectual Property. If this submission was an update to an existing app, the version published prior to this update is still available in Google Play. Please review the copyright infringement and impersonation help articles, then remove unlicensed images from your app and/or listing and resubmit.Additional details have been sent to your account owner's email address.

STORE LISTING

PRODUCT DETAILS

Fields marked with * need to be filled before publishing.

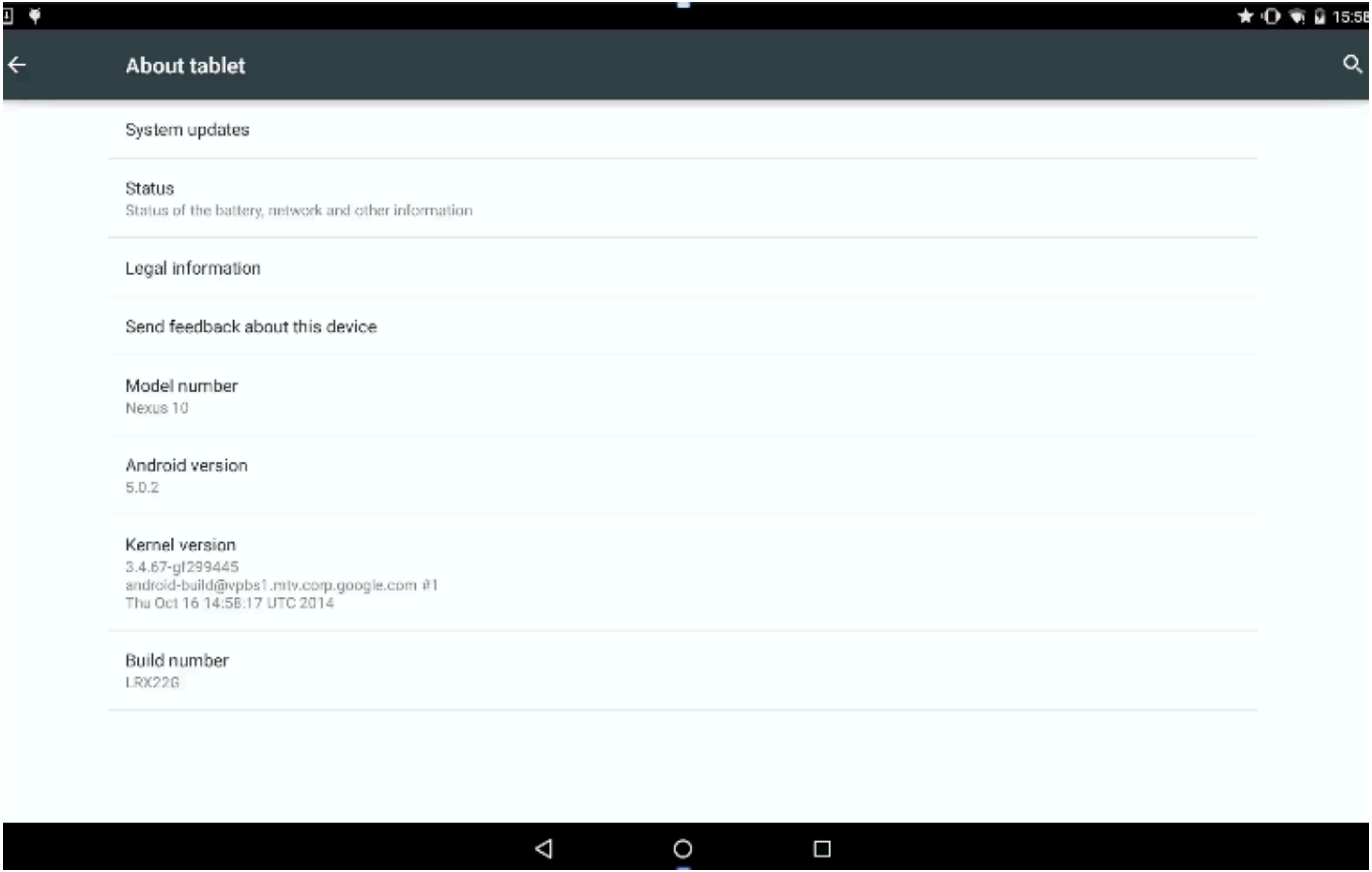
Title*
English (United States) – en-US
Dancing pig
11 of 30 characters

Short description*
English (United States) – en-US
This is a very cute dancing pig showing whenever you are not in an app
70 of 80 characters

Full description*
English (United States) – en-US
This is a very cute dancing pig showing whenever you are not in an app. My first try for an app, I hope you enjoy it.

Is the attack still feasible on Android 5?

Demo: Android 5.0.2 (verified on 5.1)



15:5

About tablet

System updates

Status
Status of the battery, network and other information

Legal information

Send feedback about this device

Model number
Nexus 10

Android version
5.0.2

Kernel version
3.4.67-gf299445
android-build@vpbs1.mtv.corp.google.com #1
Thu Oct 16 14:58:17 UTC 2014

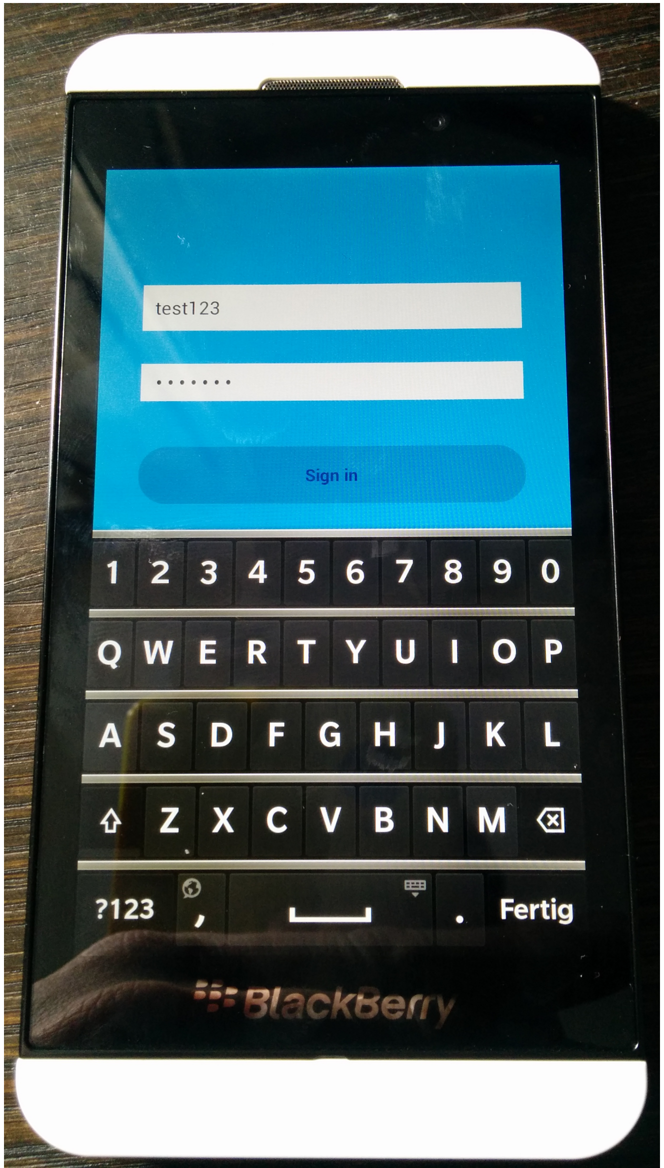
Build number
LRX22G

What about BlackBerry?

Blackberry

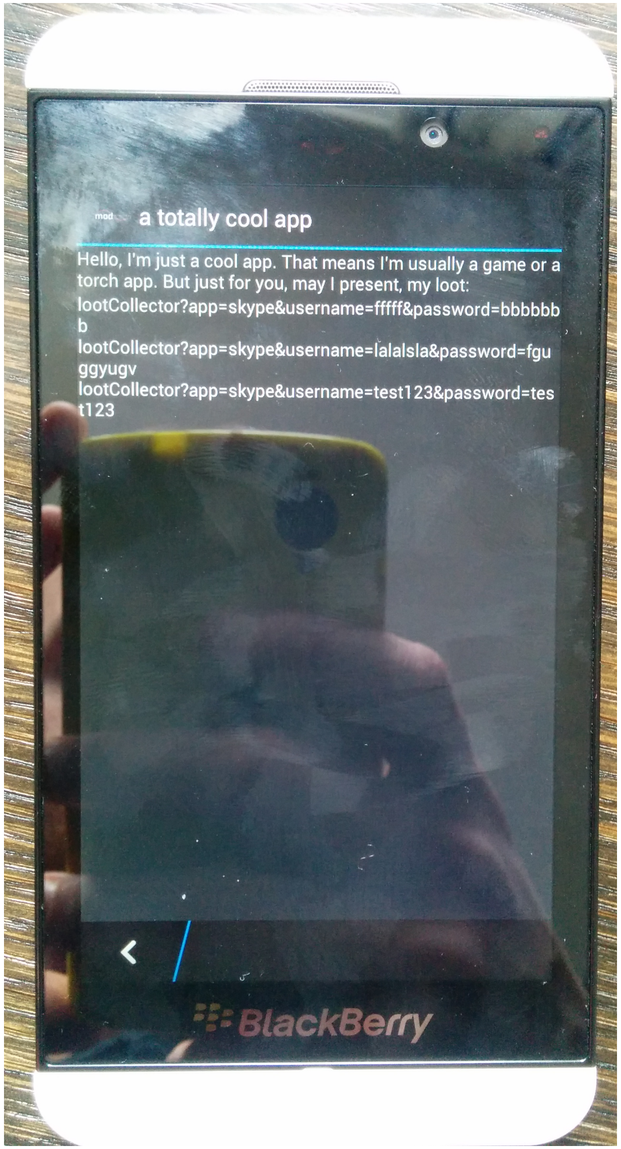
- Blackberry supports Android apps
- You can attack another Android app on Blackberry
  - With our technique you are not able to figure out which native Blackberry app is in the foreground

Blackberry



test123

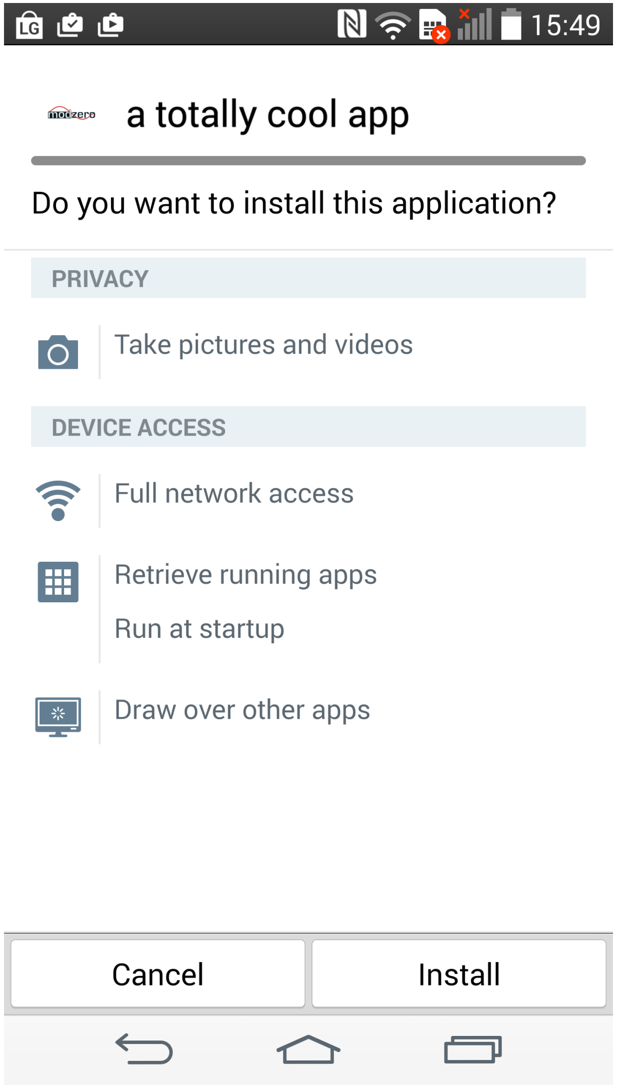
•••••••



a totally cool app

```
Hello, I'm just a cool app. That means I'm usually a game or a
torch app. But just for you, may I present, my loot:
lootCollector?app=skype&username=fffff&password=bbbbbb
b
lootCollector?app=skype&username=lalalsla&password=fgu
ggyugv
lootCollector?app=skype&username=test123&password=tes
t123
```

Blackberry – spot the permission difference



15:49

a totally cool app

Do you want to install this application?

PRIVACY

Take pictures and videos

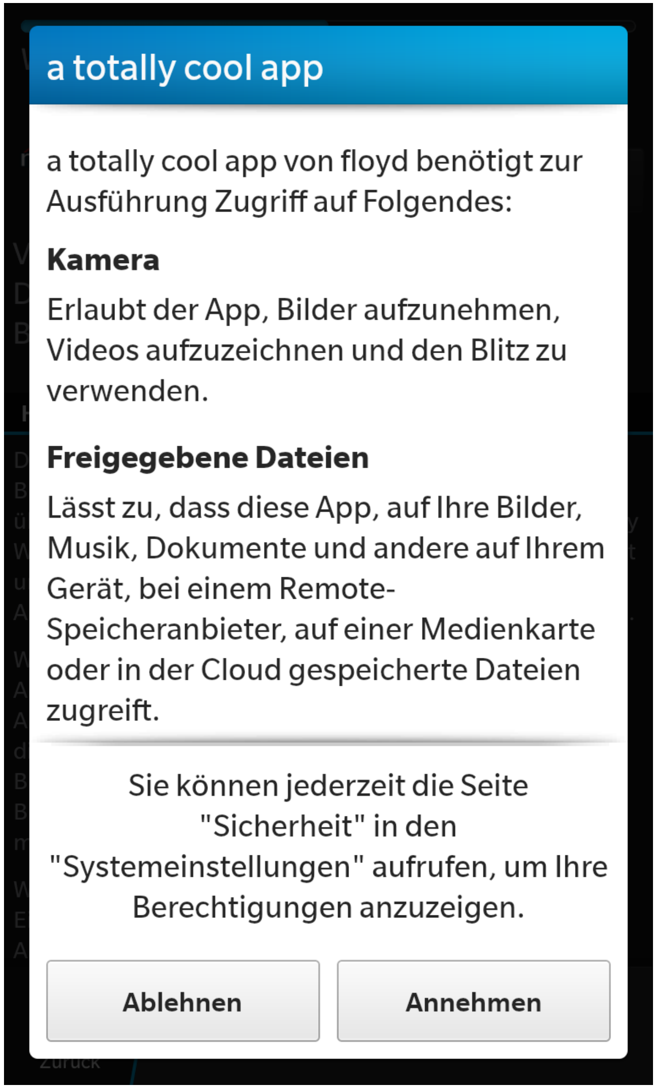
DEVICE ACCESS

Full network access

Retrieve running apps

Run at startup

Draw over other apps



a totally cool app

a totally cool app von floyd benötigt zur Ausführung Zugriff auf Folgendes:

Kamera

Erlaubt der App, Bilder aufzunehmen, Videos aufzuzeichnen und den Blitz zu verwenden.

Freigegebene Dateien

Lässt zu, dass diese App, auf Ihre Bilder, Musik, Dokumente und andere auf Ihrem Gerät, bei einem Remote-Speicheranbieter, auf einer Medienkarte oder in der Cloud gespeicherte Dateien zugreift.

Sie können jederzeit die Seite "Sicherheit" in den "Systemeinstellungen" aufrufen, um Ihre Berechtigungen anzuzeigen.

Countermeasures

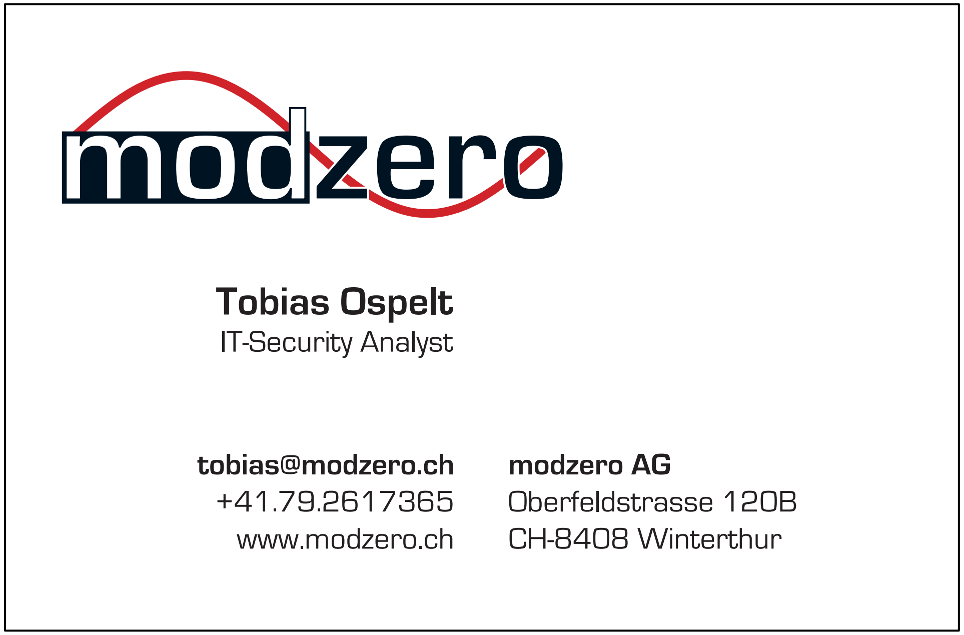
- If you have a HTML5 app (one WebView) the attack is "harder"
  - Android 5 situation on all Android versions

Summary

- Is this technique rocket-science? Not at all
- Does it matter? Yes, the impact is huge
- Android app separation is broken
  - Don't trust the sandboxing promises
- Bring-your-own-device is still a bad idea from a security perspective
  - private apps and business apps/data
- Come and play with devices here at the front

Thank you

- http://www.modzero.ch/modlog/index.html
- Twitter: @floyd_ch
- Twitter: @mod0
- http://floyd.ch



Tobias Ospelt
IT-Security Analyst

tobias@modzero.ch
+41.79.2617365
www.modzero.ch

modzero AG
Oberfeldstrasse 120B
CH-8408 Winterthur