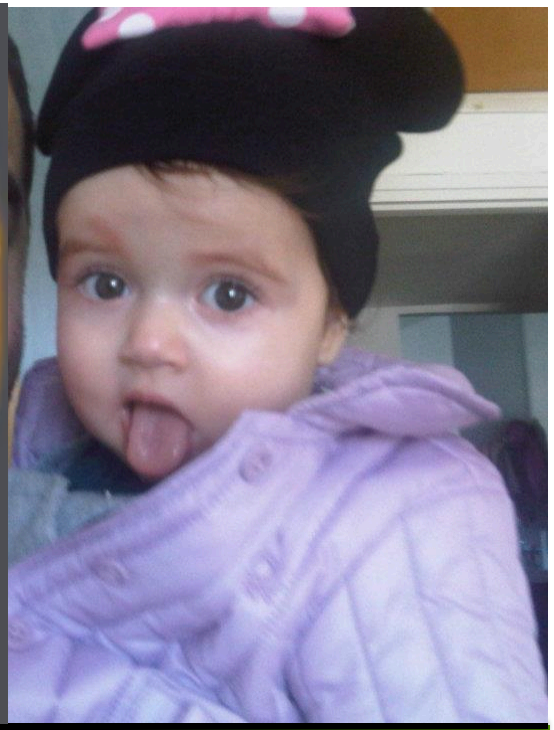
Mobile Threats:

Going Where the Money Is

Etay Maor
RSA, The Security Division of EMC

Hi

- Etay Maor, FraudAction Research Lab Manager
- etay.maor@rsa.com
- Security evangelist, father, gamer, ROCKSTAR(maybe not)



APWG

Unifying the
Global Response
to Cybercrime

2012

- Security is (mostly) up to the user… oh dear…

2009 Presentation

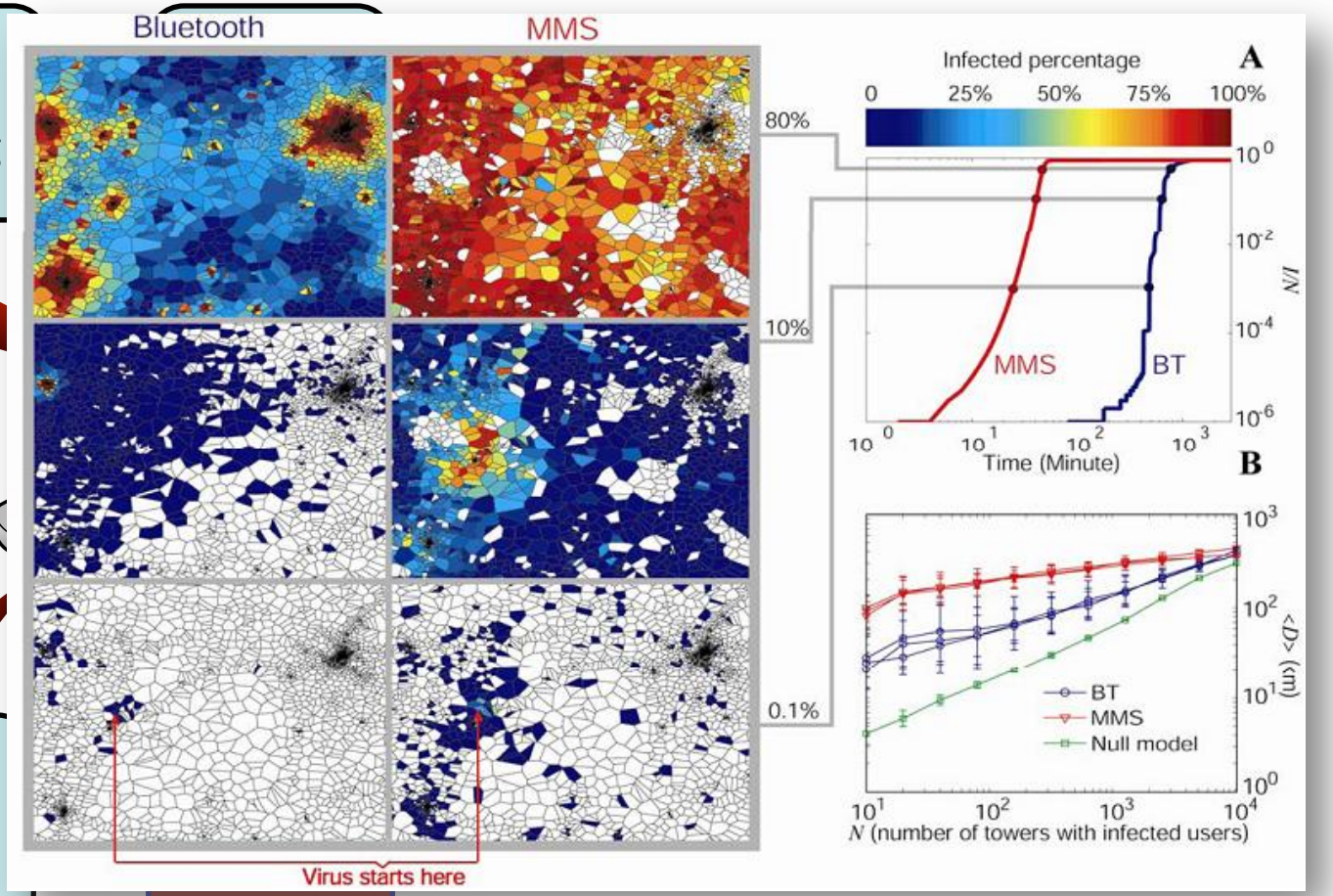
- From theory to practice!

OTP Stealing

Phishing

Vishing

Smishing



Graph: P. Wang, M. Gonzalez, C. A. Hidalgo, A.-L. Barabási, Science 324, 1071-1076 (2009)

What Has Changed?

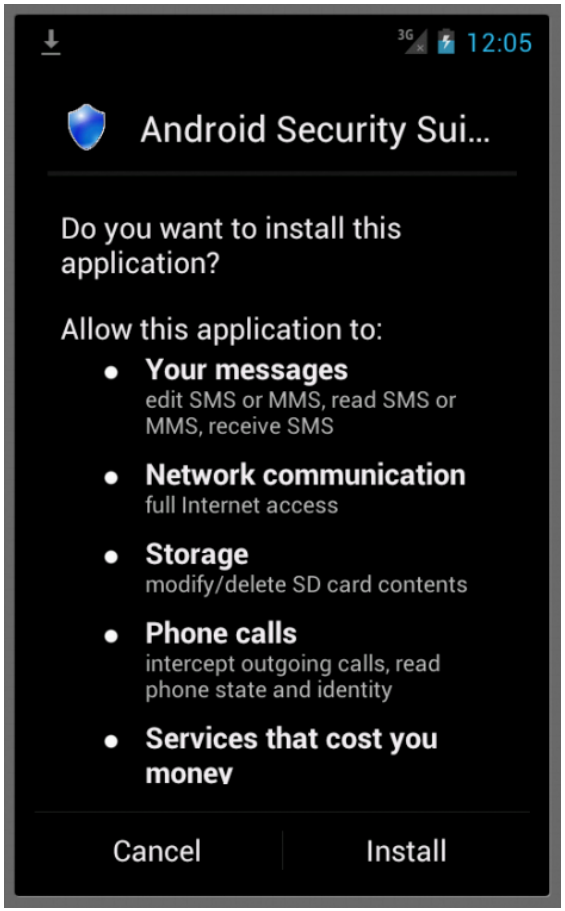
- What is your mobile device?

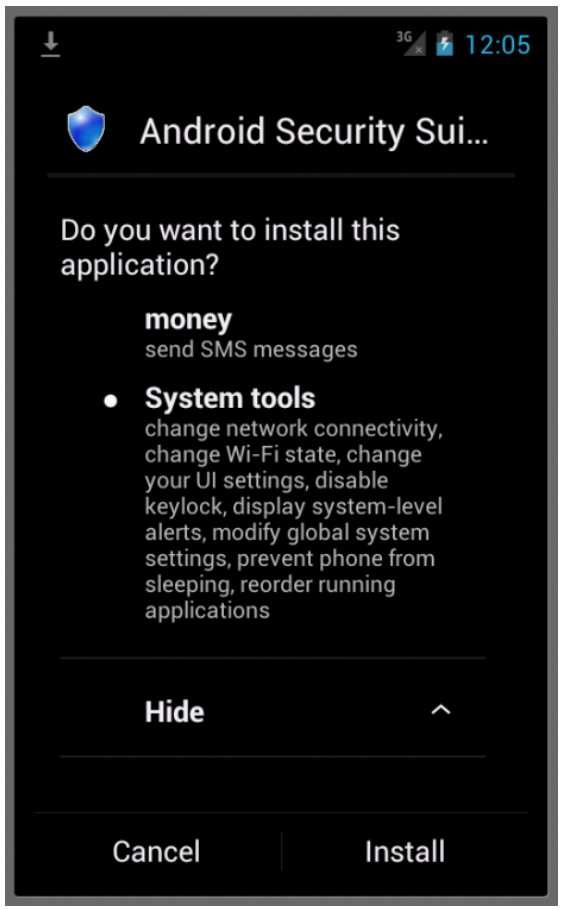
- The value of the data stored on or accessed from mobile devices has dramatically increased!

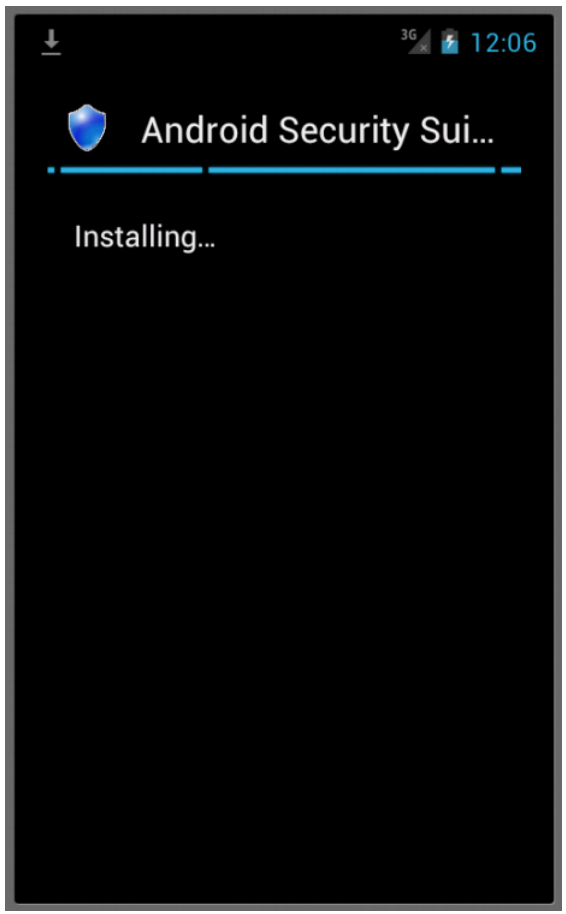
Citadel

- SMS stealer with a punch

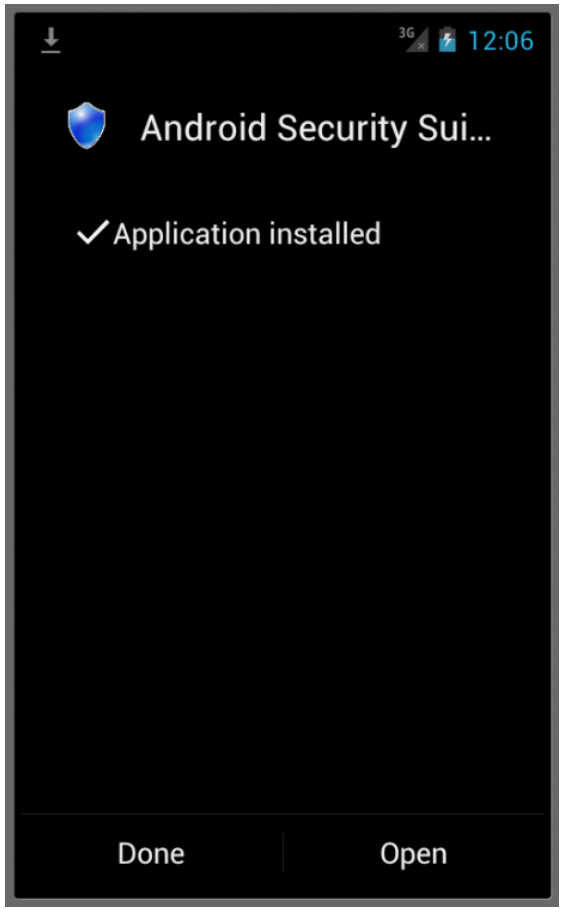
Citadel


12:05
Android Security Sui...
Do you want to install this application?
Allow this application to:
Your messages
edit SMS or MMS, read SMS or MMS, receive SMS
Network communication
full Internet access
Storage
modify/delete SD card contents
Phone calls
intercept outgoing calls, read phone state and identity
Services that cost you monev
Cancel
Install


12:05
Android Security Sui...
Do you want to install this application?
money
send SMS messages
System tools
change network connectivity, change Wi-Fi state, change your UI settings, disable keylock, display system-level alerts, modify global system settings, prevent phone from sleeping, reorder running applications
Hide
Cancel
Install

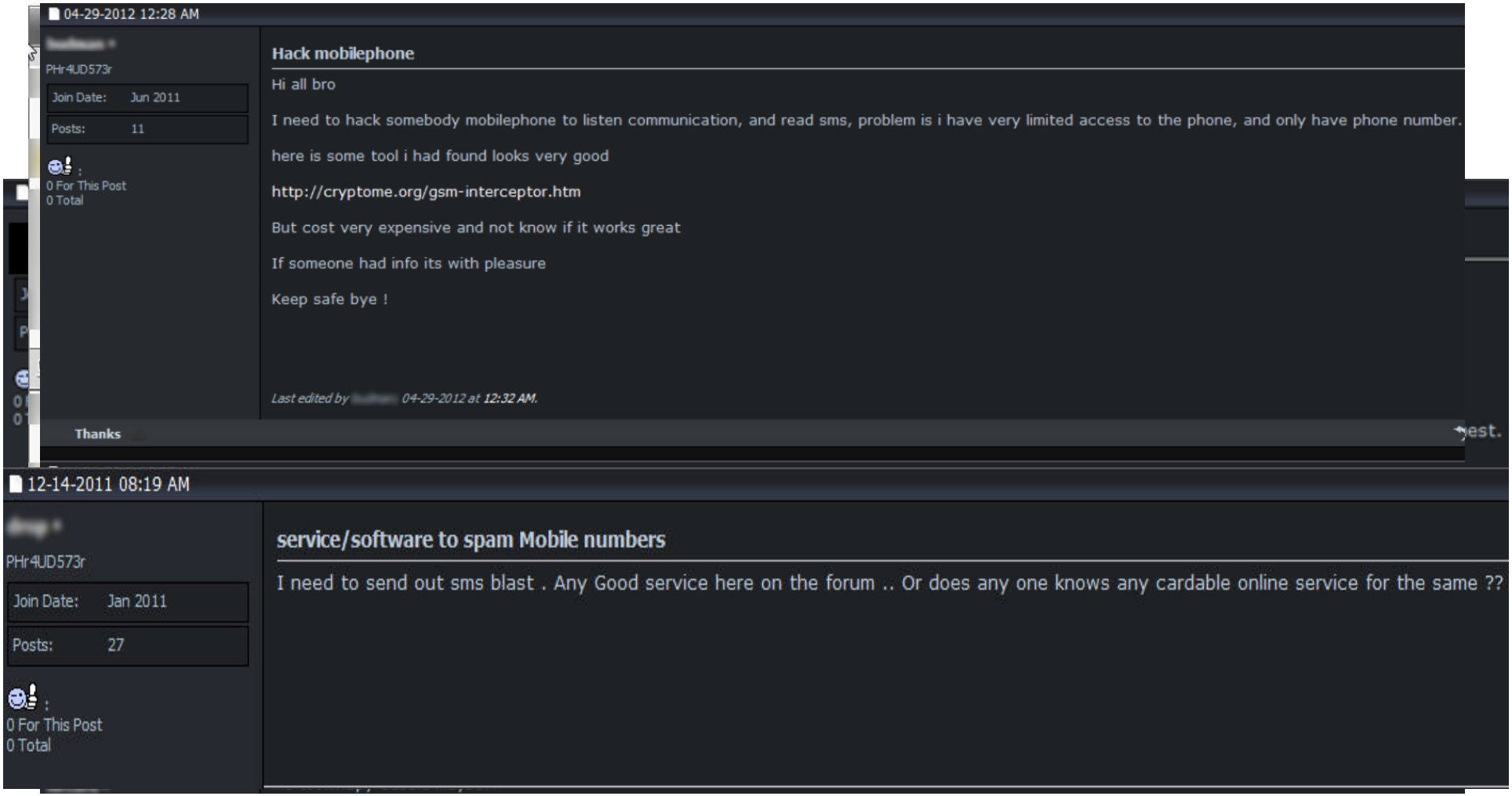

12:06
Android Security Sui...
Installing...

Citadel


12:06
Android Security Sui...
Application installed
Done
Open


12:07
Android Security Suite Premium
Activation code
103

Forums: We Put the MOB in Mobile



04-29-2012 12:28 AM

PHr4UD573r

Join Date: Jun 2011

Posts: 11

0 For This Post
0 Total

Hack mobilephone

Hi all bro

I need to hack somebody mobilephone to listen communication, and read sms, problem is i have very limited access to the phone, and only have phone number.

here is some tool i had found looks very good

http://cryptome.org/gsm-interceptor.htm

But cost very expensive and not know if it works great

If someone had info its with pleasure

Keep safe bye !

Last edited by [redacted] 04-29-2012 at 12:32 AM.

Thanks

12-14-2011 08:19 AM

PHr4UD573r

Join Date: Jan 2011

Posts: 27

0 For This Post
0 Total

service/software to spam Mobile numbers

I need to send out sms blast . Any Good service here on the forum .. Or does any one knows any cardable online service for the same ??

Mobile Botnet Management

User-Agent: Mozilla/5.0 (**iPhone; U; CPU iPhone OS 4_0** like Mac OS X; en-us) AppleWebKit/ 532.9 (KHTML, like Gecko) Version/4.0.5 Mobile/8A293 Safari/6531.22.7

Accept: application/xml,application/xhtml+xml,text/html;q=0.9

Referer:http://XXXXXXXXXXXXXXXXX/**cp2/index.php?bot_guid=&process_name=&hooked_func=&repdatestart=12%2F05%2F2011&repdateend=15%2F05%2F2011&rep_url=Login&Data_show=on&data=&limit=100**

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Connection: keep-alive

Live Mobile Malware Demo

- (Don't forget to launch the VM…)

What to Expect

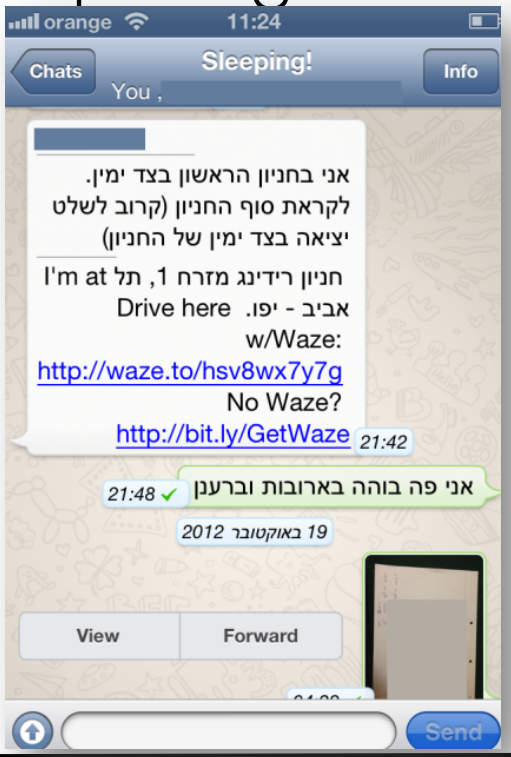
(when you are not expecting)

- **Attack methods**
  - Classic
    - Phishing
    - Apps
    - Social engineering
  - Proximity & connectivity:
    - Wifi
    - Bluetooth
    - NFC
    - Towers, targeted attacks

What to Expect

(when you are not expecting)

- **Infection & distribution**
- Your mobile device is your social network!
  - Finding trusted contacts via privileged and trusted apps is easy
  - SMSs



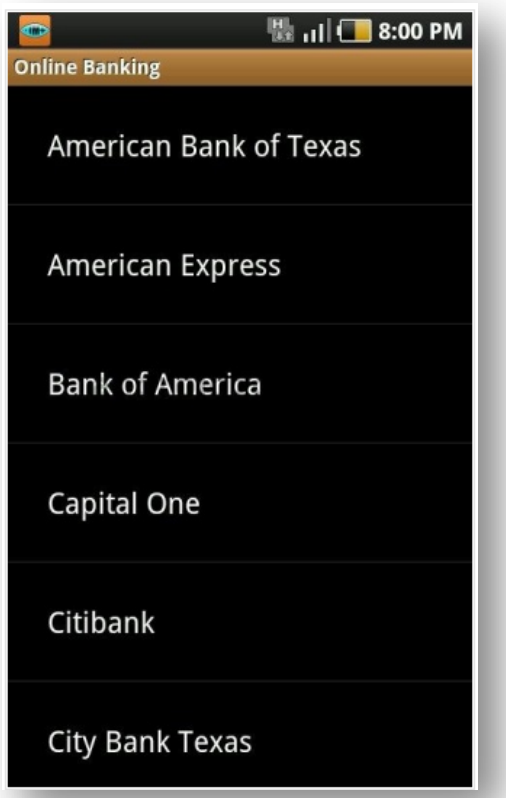
What to Expect

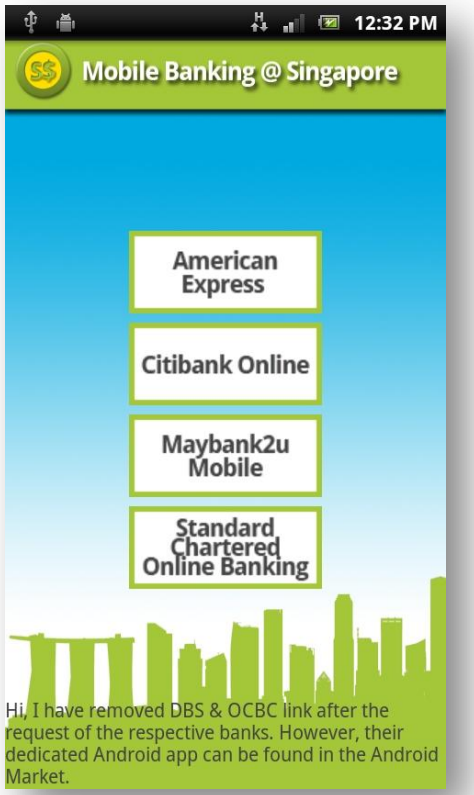
(when you are not expecting)

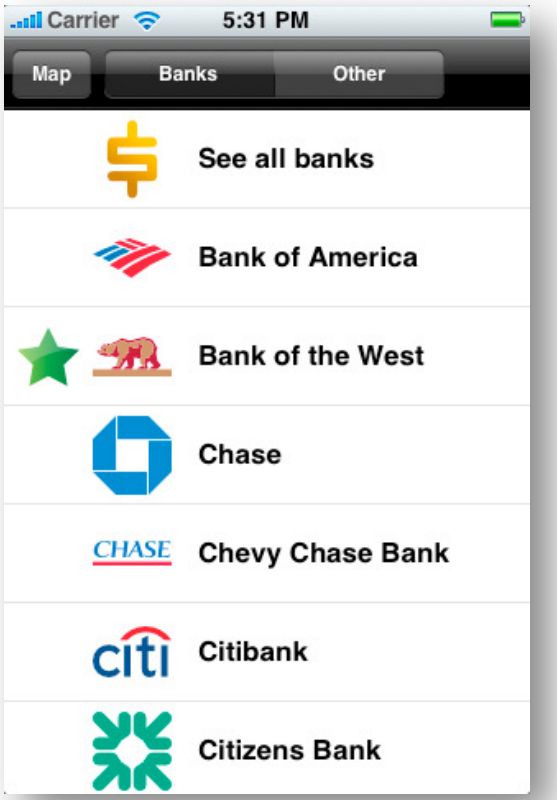
- **Infrastructure**
  - Always up
  - DDoS/spam breeding ground
  - With ever improving hardware – perfect ground for legit (and criminal) distributed computing (mobile agents)

Mobile Security Threats

- **Apps**
  - Rouge

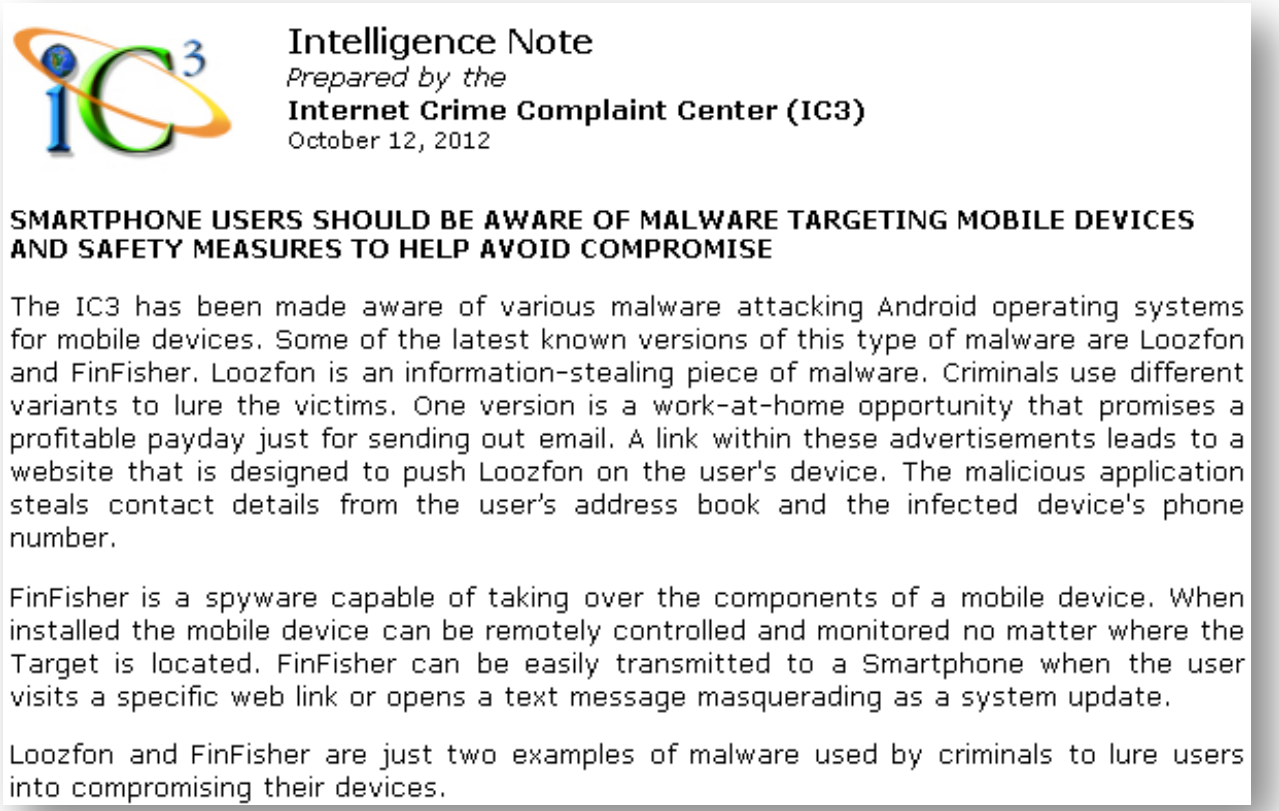






Mobile Security Threats

- **Apps**
  - Malware



Intelligence Note
Prepared by the
Internet Crime Complaint Center (IC3)
October 12, 2012

SMARTPHONE USERS SHOULD BE AWARE OF MALWARE TARGETING MOBILE DEVICES AND SAFETY MEASURES TO HELP AVOID COMPROMISE

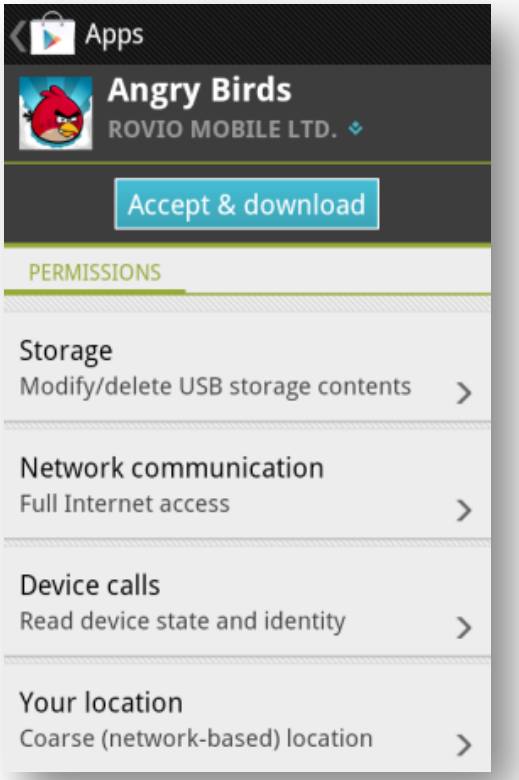
The IC3 has been made aware of various malware attacking Android operating systems for mobile devices. Some of the latest known versions of this type of malware are Loozfon and FinFisher. Loozfon is an information-stealing piece of malware. Criminals use different variants to lure the victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out email. A link within these advertisements leads to a website that is designed to push Loozfon on the user's device. The malicious application steals contact details from the user's address book and the infected device's phone number.

FinFisher is a spyware capable of taking over the components of a mobile device. When installed the mobile device can be remotely controlled and monitored no matter where the Target is located. FinFisher can be easily transmitted to a Smartphone when the user visits a specific web link or opens a text message masquerading as a system update.

Loozfon and FinFisher are just two examples of malware used by criminals to lure users into compromising their devices.

Mobile Security Threats

- **Apps**
  - No "least privilege" policy



Fake Angry Birds ensnares 80,000 on Chrome Store

by **Seth Tipps** | Email a friend | Print

Add a comment | Tweet 10 | Share | Like 2

Scam scores big with free games, conceals dangerous permissions

Thousands of browser game fans have been tricked into installing knock-off versions of Rovio games that alter ad content on many of the web's biggest hubs.

The Google Chrome Web Store is well known for its hands off approach to screening what games are allowed on the platform, but as more users flock to the speedy browser, this could have dangerous consequences.

The suspects in question are a series of games designed to look like games in the hit Angry birds series.

Barracuda Networks has revealed these titles contain code that could potentially lead to a user having their browser hijacked.

Over 80,000 users have granted the apps permission to run on their browser, despite the warning the games will receive full access to a player's web activity.

HOT TOPICS

- The iOS 6 App Store 'is a disaster' for developers 17
- Notch refuses Windows 8 certification 13
- [Correction] Millions of PlaySpan user IDs and passwords leaked online 8
- Crowdfunding 'should be a red flag' to backers 7
- App Store rejects game for in-app purchase remark 5
- Autodesk bolsters Scaleform SDK and plug-in

Mobile Security Threats

- **WiFi**
  - Unsecure networks

- **Device physical security**
  - New York, SF – start paying attention to your devices
  - In the US – a device is lost/stolen every 3.5s
  - 70% don't use passwords

Mobile Security Threats

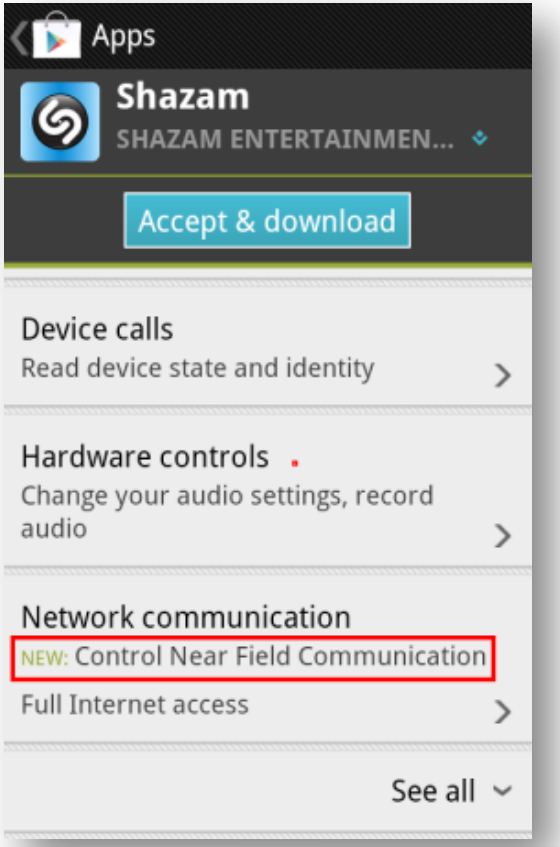
- **Data storage**
  - Encryption
  - Is the device properly secured and monitored

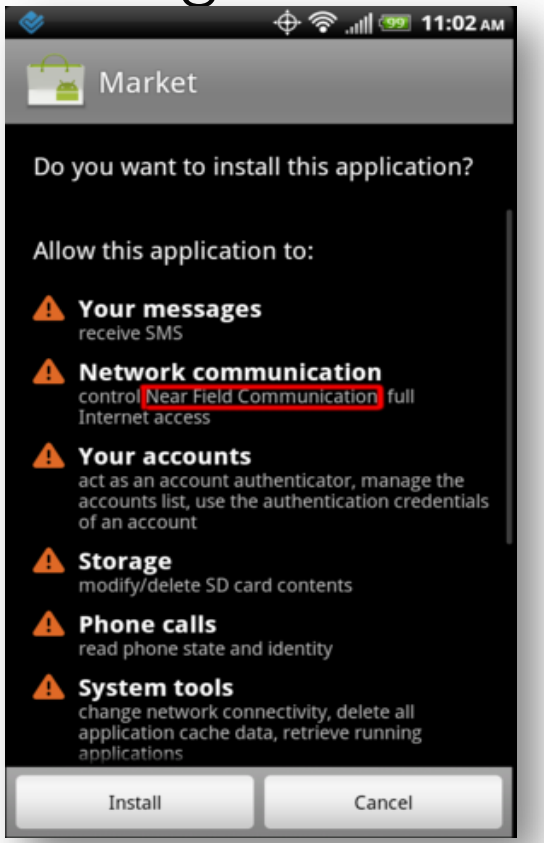
- **BYOD**
  - Can security policies be enforced?
  - Privet Vs Corporate – where is the line drawn?

- **Rooted / Unpatched / Old OS devices**

Mobile Security Threats

- **NFC**
  - A new take on POS fraud, skimming and hacking





Stay Vigilant

- (vid)

Thank You

APWG

Unifying the
Global Response
to Cybercrime