European Commission

Participatory Honeypots: A Paradigm Shift in the Fight Against Mobile Botnets

Pasquale Stirparo (@pstirparo)
Laurent Beslay

www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

Joint Research Centre

Outline

- Introduction and Motivation
- Classical Botnet vs. **Mobile** Botnet
- **Privacy** concerns
- Current solutions
- **Participatory** Honeypot
- Conclusions

The Mission of the Joint Research Centre…

…is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies.

As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union.

Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

IRMM - *Geel, Belgium*
Institute for Reference Materials and Measurements

ITU - *Karlsruhe, Germany*
Institute for Transuranium Elements

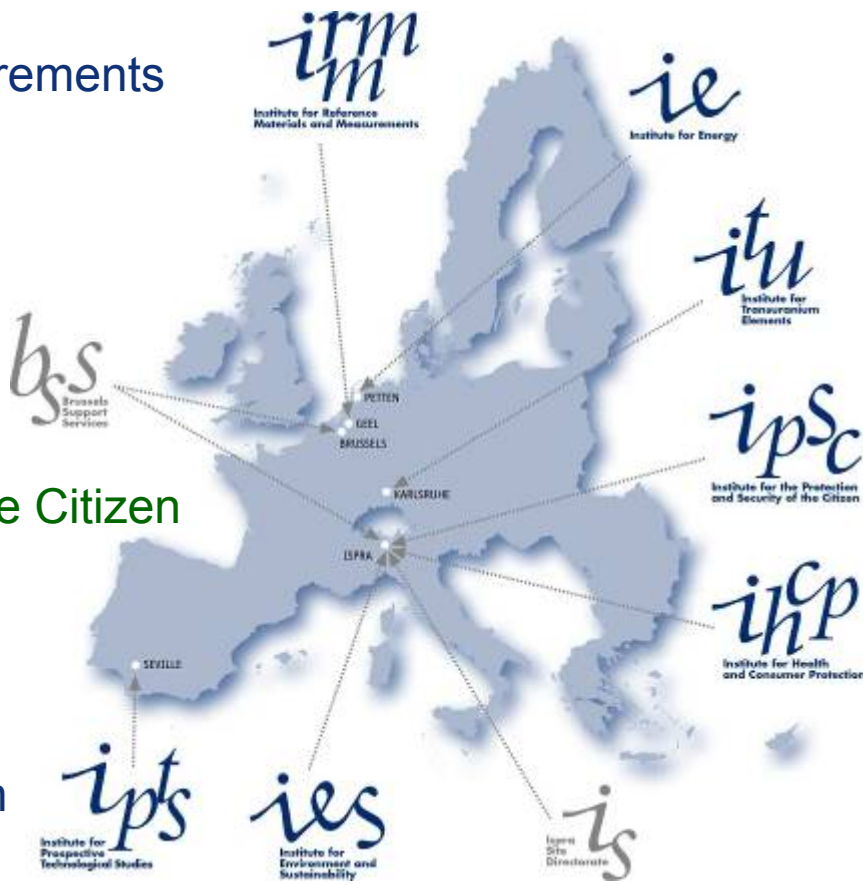
IE - *Petten, The Netherlands*
Institute for Energy

IPSC - *Ispra, Italy*
Institute for the Protection and Security of the Citizen

IES - *Ispra, Italy*
Institute for Environment and Sustainability

IHCP - *Ispra, Italy*
Institute for Health and Consumer Protection

IPTS - *Seville, Spain*
Institute for Prospective Technological Studies



Introduction

- Mobile malware has reached almost 200k samples, increasing of 1k new samples per day
- Android is leading accounting for 79% of all mobile malware
- Privacy and data protection rights are part of the European Regulatory framework
- A new trend: data subject wants to participate

Should we care?

Should we care?

Should we care?

Evolution Timeline

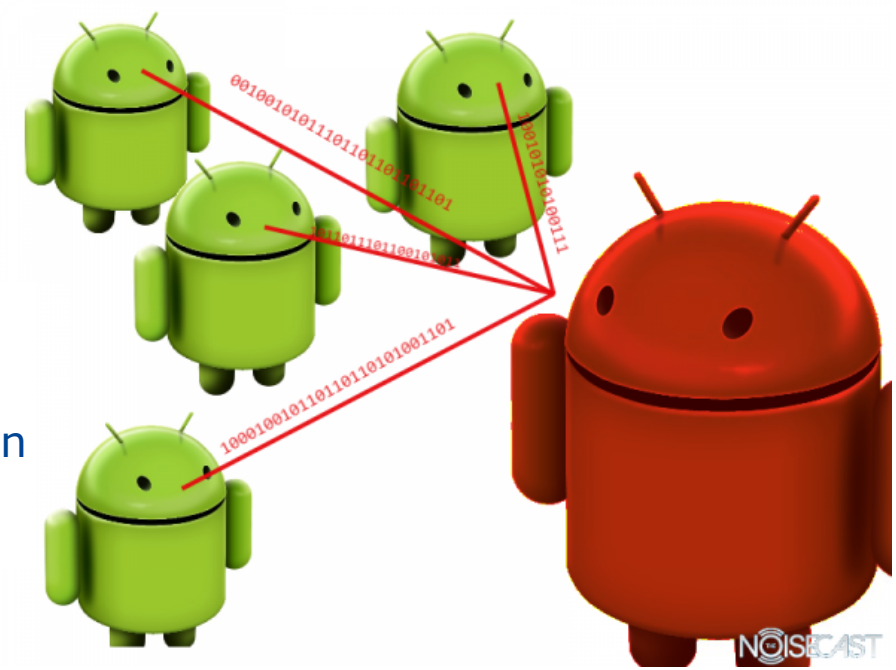
- 2009-11 iKee for (jailbroken) iPhone
- 2010-09 First Zitmo for Symbian and BB
- 2011-01 SpyEye and Zeus Merged
- 2011-02 Zitmo for WinCE
- 2011-03 Spitmo for SymbOS
- 2011-06 Zitmo for Andorid
- 2011-09 Android Spitmo Discovered
- 2012-10 SpamSoldier (Android)
- 2012-12 Citmo for Android
- 2012-12 Dexter for PoS
- ….
- 2013-09 SMS.AndroidOS.Opfake.a botnet used to distribute Backdoor.AndroidOS.Obad.a

Classical Botnet vs. Mobile Botnet

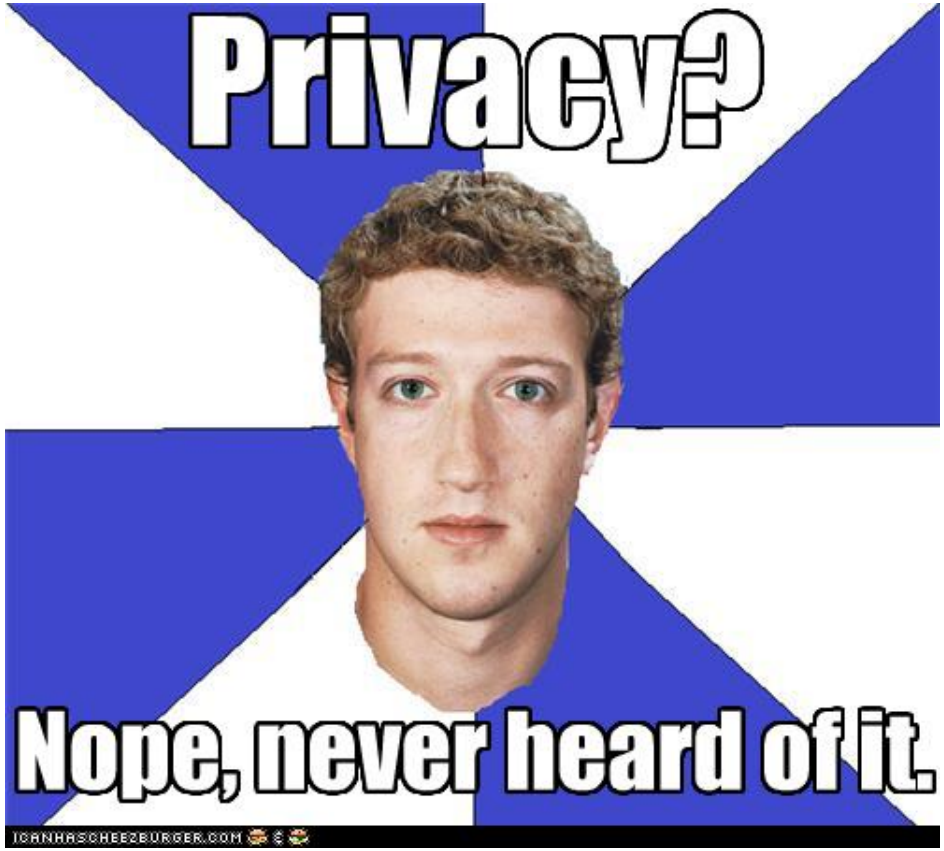
- Infection vector and botnet topology
- Honeypots
  - Def: *a computer system, built and deployed just for the goal of being attacked and compromised in order to study new attacks and to serve as an early warning system*.
- Botnet **monitoring / tracking**
  - Data collection and Analysis
- Mitigation
  - Shall we block SMSs?

Current Mobile Botnets "Tasks"

- Fraudster
  - Zitmo, Spitmo, Citmo
- SMS Spam
  - SpamSoldier
- DDoS
  - TheAndroid.DDoS.1.origin
- … what's next?



What about Privacy?



What about Privacy and Data Protection?

- Stealing **contacts, personal information**;
- Opening a **backdoor** on the device and sending the IP address to the remote server;
- Sending **SMS messages** to premium numbers;
- Sending copies of SMS messages, **IMSI** and **IMEI**;
- GPS **tracking**;
- **Recording calls** and uploading to a server;
- Capturing unencrypted web sessions;
- Capturing **keyboard inputs**;
- Building profile without the consent of the data subject;
- Etc…

Mobile Honeypot: current solutions

1. "Nomadic Honeypot"
   - Two VM, a HoneypotVM running Android and an InfrastructureVM, which implements the communication part with the sensors, logging capabilities and a backchannel to communicate with the operator.
   - Potential risks are that a) if for any reason, the VM separation get compromised the device will be out of control from the infection point of view; and b) it may be very invasive, and not many users may be willing to participate/collaborate knowing that everything (SMS, calls, Internet traffic, etc.) is being monitored by a third party.

Liebergeld, S., Lange, M., Mulliner, C.; "**Nomadic honeypots: A novel concept for smartphone honeypots**." In: *Proc. Workshop on Mobile Security Technologies (MoST13)*, in conjunction with the 34th IEEE Symp. on Security and Privacy

Mobile Honeypot: current solutions

2. "Mobile Honeypot"
   - Honeypot systems implemented using well-known honeypot tools and connected to the UMTS network via USB stick;
   - The attempt is to make the honeypot looking like a mobile phone;
   - The choice of such architecture has also been driven by the aim to focus on remote attacks via the Internet;
   - The authors state that "*there is no need to operate the mobile honeypot on real device"*.

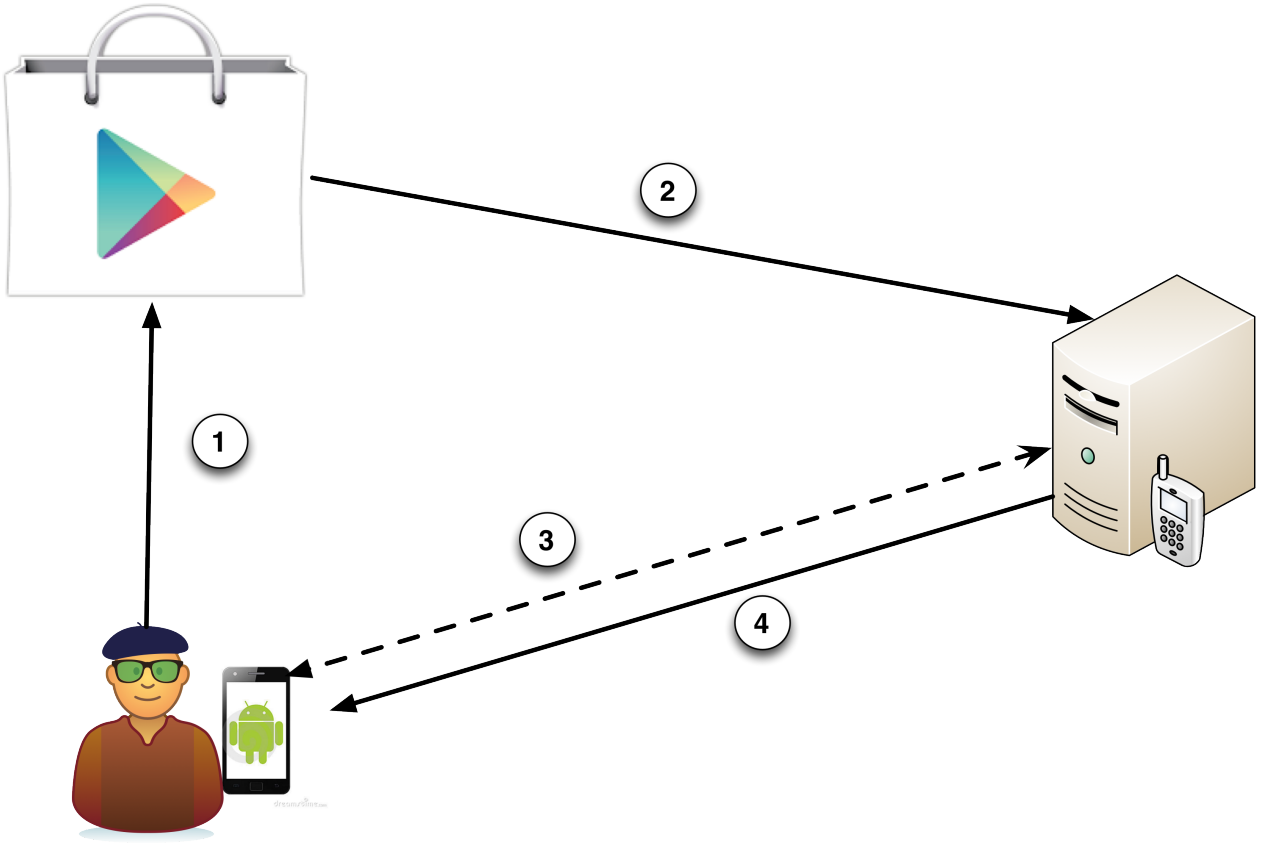
W ahlisch, M., Vorbach, A., Keil, C., Sch onfelder, J., Schmidt, T.C., Schiller, J.H.; "**Design, implementation, and operation of a mobile honeypot**". *arXiv preprint arXiv:1301.7257 (2013)*

Participatory Honeypot

We introduce the concept of Participatory Honeypot, a privacy-by-design system where users become partners of the collection of meaningful information subsequently used for the analysis.

- Remote sandbox system
- The user downloads the application he intend to purchase
- He will use it during a limited test phase remotely on our system from his mobile phone, via a mobile application provided by us

Usage Scenario



Advantages of this solution

- **Meaningful touches**
  - Modern malware can detect random touches on the screen, meaning that they are being under dynamic analysis
  - Therefore they may keep the malicious activity dormant;

- **Privacy by design principle**
  - Being executed outside the user's real device, we avoid to over-collect extra information related to the user private activities that may not be always indispensable for the analysis.
  - The system is based on an anonymity preserving reputation framework using periodic pseudonyms generated by blind signatures as proposed by Delphine Chrisitin and Matthias Hollick

Advantages of this solution (cont'd)

- The success of such system depends on the active contributions of the users, **rewards and voting schemes** will be put in place as **incentive to participate**, as well as for the **operator to grade the level of users' contribution.**

- As a contribution for a trustworthy relationships between the PBDS and the user acting as a partner, a **Data Protection Impact Assessment will be conducted and its results provided to the user** prior to his/her registration to our system.

Conclusions

- **Mobile botnet will be a growing concern** and we should care about it;
- Due to its nature, **classical approaches may not work** in the mobile environment;
- The mobile dimension brings **high risks** also for user **privacy**:
  - Attackers have access to many personal data;
  - Analyst may over-collect information for analysis;
- Novel concept of **Participatory Honeypot**;

Joint Research Centre (JRC)

Web: www.jrc.ec.europa.eu

Contacts:
pasquale.stirparo@jrc.ec.europa.eu
laurent.beslay@jrc.ec.europa.eu