© Weiss

“Smartphone Botnets”

SPRING 2010

Collin Mulliner, July 7th 2010
collin@sec.t-labs.tu-berlin.de

Agenda

- Introduction
- Motivation
- Project Goals
- Command and Control
- Payloads
- Conclusions

Introduction

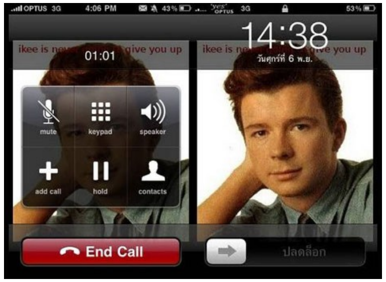
- Botnets are a serious security problem in todays Internet
  - Spam, fraud, identity theft, malware hosting, DDoS, ...
  - Anti botnet research is a big area of research

- Smartphone botnets
  - Vulnerabilities exist in all major smartphone platforms
  - Smartphones are powerful enough to host a bot
  - Smartphone-based botnets would offer additional "financial" gains for a botmaster

- Therefore, smartphone botnets are likely to appear and thus need to be studied

The iPhone iKee.B botnet

- Very simple botnet that is based on the iKee.A worm
  - Abused the default root password of jailbroken iPhones
  - Infected phones via ssh/scp
    - No user interaction required! (first one!)
  - Very simple HTTP-based C&C
    - download a shell script with new commands
  - Main payload was to steel SMS database
  - November 2009



- References

  Analysis of iKee.B [http://mtc.sri.com/iPhone/]

  iKee.A [http://f-secure.com/weblog/archives/00001814.html]

Motivation

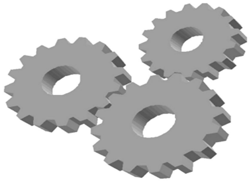
- Understand mobile botnets
  - How will they work
  - How to build one
  - Identify “general weak spots”

- Operators need to prepare for mobile botnets
  - Keep mobile network operational
  - Filter fraud (nobody likes upset customers)
  - Need to be able to detect and remove bots

Goals

- Implement smartphone bot and botnet C&C
  - Try different C&C schemas
  - Implement payloads

- Evaluate botnet
  - In test network (in test GSM network)
  - On real network (manual install, not spreading!)



- Investigate detection possibilities
  - Network side (mobile phone network)

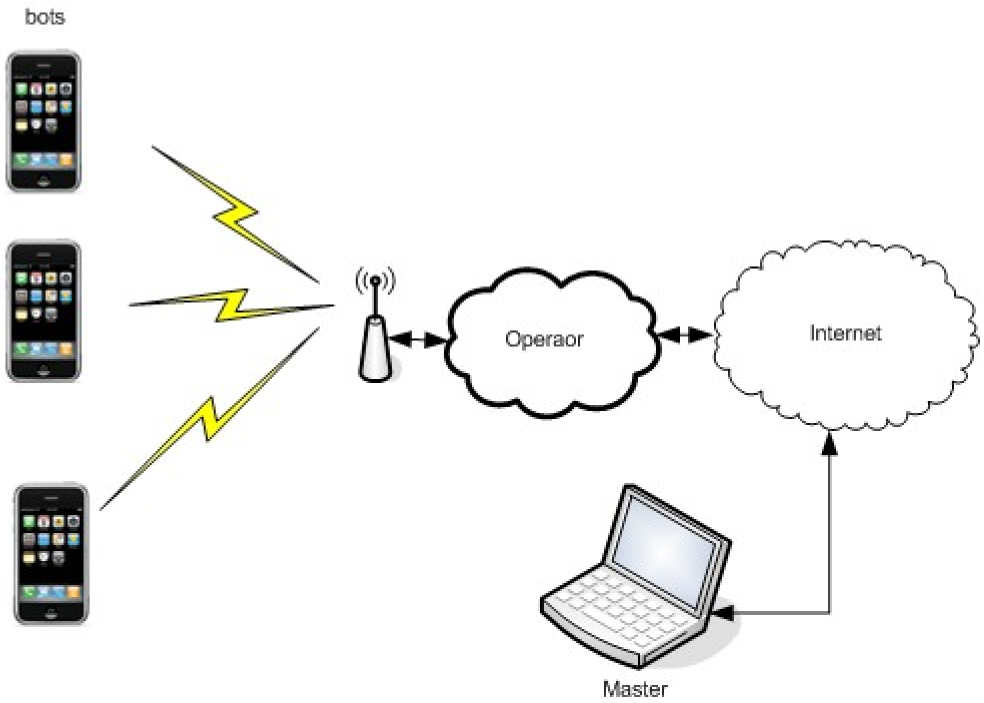
Command and Control (C&C)

- C&C is the most important part of a botnet
  - Control channel for botmaster
  - If channel can be blocked the botnet is dead
  - Needs to be robust against attacks
    - by defenders (good guys) and other botmasters

- Challenges for mobile C&C
  - Connectivity: Wifi vs. GSM/3G → changes in bandwidth
  - Communication costs (GSM: SMS/data)
  - Computational power
  - Battery power

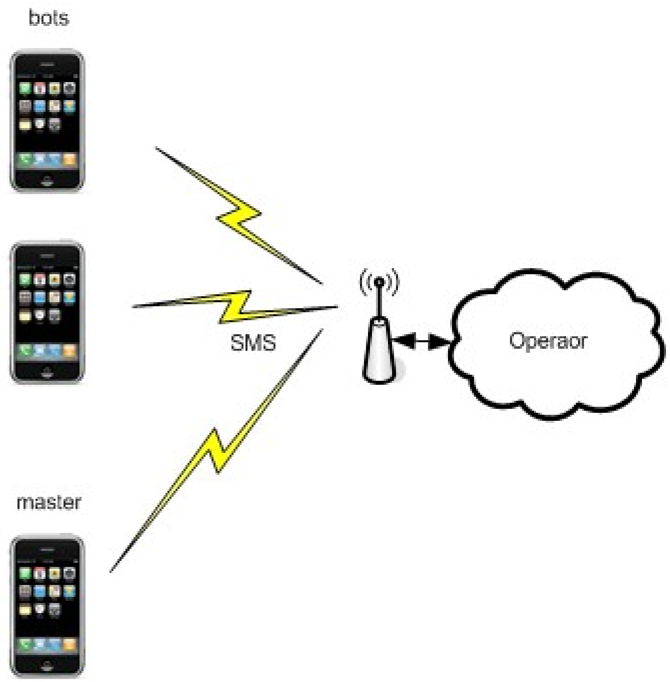
Internet-based (IP-based) C&C

- C&C via IP/Internet
  - Follow PC-based botnets using P2P



GSM-based (SMS-based) C&C

- C&C via SMS/MMS
  - Botmaster uses a phone to control the botnet
    - Phone maybe hijacked



Local Wireless C&C

- WiFi (AdHoc), Bluetooth
- Botmaster injects command and lets it travel through the net

C&C Communication Costs

- Mobile phone service cost money
  - SMS, packet-data, circuit switch data (CSD) calls, ...
- Costs could make a botnet detectable
  - more easily, faster
- Need to analyze cost factor
  - When designing a C&C system for a mobile botnet
  - When building a detection system
- Interesting because of...
  - Service plans
  - Countries, roaming

Mobile Botnet Payloads

- Mobile phones have abilities not found on desktop computers
  - Modem
    - Billing system
    - Non-IP communication
  - Data not found on desktop computer
  - Special hardware such as a GPS

- Possibilities
  - Unique kind of denial-of-Service attacks
  - Unique kind of fraud
  - Data / identify theft

Data Theft

- Smartphone store many kinds of private information
  - Addressbook
  - Calendar
  - Emails + account credentials
  - SMS/MMS
  - Voicecall records
  - Photos

- Gain for botmaster
  - Extortion (private)
  - Identity theft (private)
  - Industrial espionage (commercial)

(D)Denial-of-Service Payloads

- Operator / Network
  - DoS a single cell or cell area
  - DoS MNO backend infrastructure [1]

- “Real World”
  - DoS emergency number
  - DoS company hotline (extortion)
  - SMS flooding

[1] Trynor et al.: *On cellular botnets: measuring the impact of malicious devices on a cellular network core*, 16th ACM CCS

Conclusions

- Bots on mobile phones pose some challenges
    - Many possibilities for C&C
        - A lot of work for the defenders

- Mobile bots offer unique possibilities to a botmaster
    - Phone call / sms related fraud (easy)
    - New interesting DoS attacks

- Smartphone botnets are interesting and a hot topic right now

Questions?

Thank you!