Berlin Institute of Technology
FG Security in Telecommunications

“Rise of the iBots: 0wning a telco network”

5th IEEE International Conference on Malicious and Unwanted Software (MALWARE), Nancy, France, October 2010

Collin Mulliner and Jean-Pierre Seifert
{collin,jpseifert}@sec.t-labs.tu-berlin.de

Agenda

- Introduction
- Contributions
- Cellular Challenges
- Command and Control
- Implementation / Evaluation
- 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

Contributions

- We show a cellular botnet architecture and evaluated it with several practical implementations.
- Solved some environmental challenges of such cellular botnets.
- Implemented and evaluated a P2P-based C&C mechanism for mobile phone botnets. Based on Kademila.
- Designed, implemented, and evaluated multiple SMS-based C&C mechanisms.
- We created communication strategies for mobile phone botnets. The strategies are designed to increase the stealthiness of mobile phone botnets.

Hijacking iPhones aka the 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

Cellular Challenges

- Mobile phones present a number of challenges
- Challenges need to be addressed in order to design a mobile phone botnet
- These challenges are:
  - Absence of public IP addresses
  - Constant change of connectivity
  - Platform diversity
  - Communication costs

Absence of public IP addresses

- Most mobile operators put phones behind a NAT gateway
  - Lack of enough IPv4 addresses, etc...
- Most modern smartphones are equiped with WiFi
  - WiFi is used at home / office in order to have faster and cheaper communication
  - Wifi will put phones behind NAT again
- This is true even if operators assign public IPs to mobile phones
- Public IPs are the bases for direct bot to bot communication

Constant change of connectivity

- Mobile phones move around the physical world
  - communication possibilities change
- Disconnected vs. GPRS vs . 3G / UMTS vs. HSPA vs. Wifi
- This counts for all bots in the network
  - Therefore this has to be considered

Connectivity	Hours
WiFi	Early morning (still at home)
GSM/3G	Morning (travel to work/school)
GSM/3G	Day time (while at work/school)
WiFi	Early evening (back at home)
GSM/3G	Early Night (going out)
WiFi	Night (bed time)

Communication costs

- In the world of mobile telecommunication most types of communication result in costs
  - packet-data, SMS, MMS, ...
- Roaming will always create additional costs
  - Fix volume packages normally don't cover roaming
- Costs have to be considered
  - Increase stealthiness of bot
  - Keep to bot from communicating since packet-data my get disabled while roaming

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

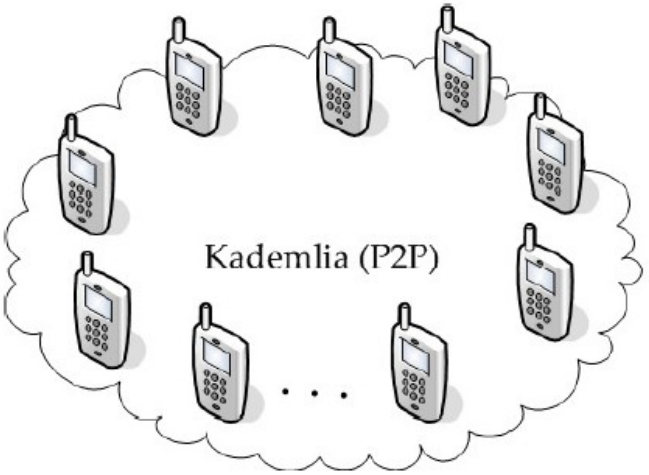
C&C for mobile botnets

- Command and Control (C&C) is the most important part of a botnet
  - Botmaster uses it to control bots
  - Defenders (we/you) it presents THE attack vector

- We investigated two major pathes for C&C
  - P2P-based approach
    - This seems to be the “industry standard”
    - Works well when NATed
  - SMS-based approach
    - This was chosen since we believe that SMS communication is hard to monitor and disrupt

Peer-to-peer C&C

- Zombies communicate using IP (GPRS/3G/WIFI)
- Communication done via P2P network
  - P2P network is used as rendezvous point
- The botmaster publish commands through the DHT



SMS C&C

- SMS seems to be the perfect C&C channel
  - Hard to monitor if not a mobile network operator
  - MNO maybe is not even allowed to monitor it
- Always available
  - World wide usable
  - GPRS/3G often disabled while roaming

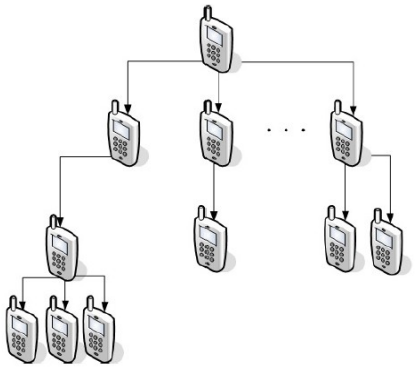
The Short Message Service (SMS): Overview

- One of the basic services of the mobile phone service
- Normally used for “text messaging”
  - 160 ascii characters
- Can transport binary payloads
  - 140 octets per message
- In order to communicate sender only needs the receivers phone number

- Message are send in store and forward manner
  - If receiver is not online, the message is kept in the network until the receiver comes online

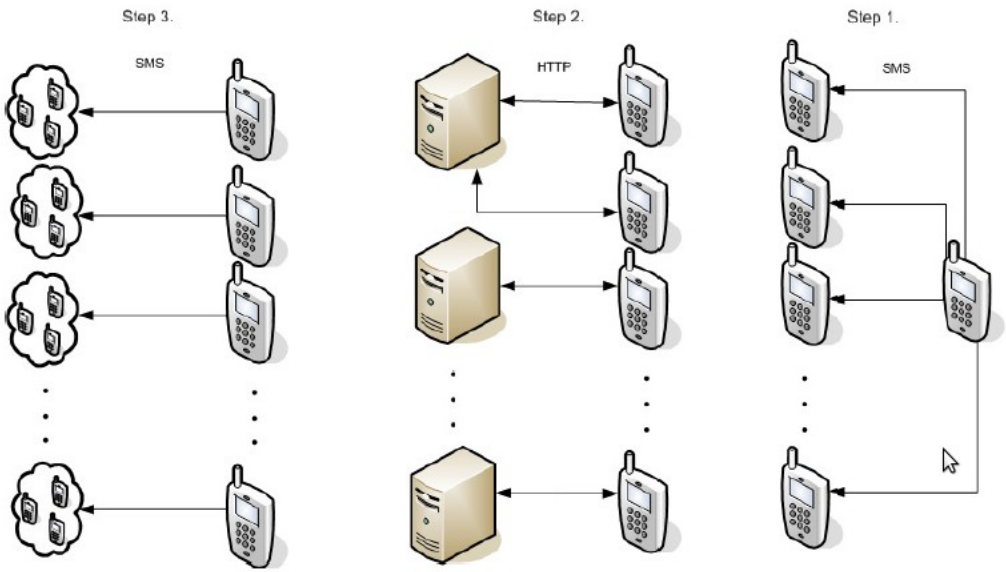
SMS-only C&C

- Communication takes place in a tree model
- Advantages:
  - Botmaster only needs to communicate with root node
  - Bot communication is hard to observe
- Disadvantages:
  - Botmaster has to check if tree is still intact
    - Need to have full list of zombies
  - Broken tree needs to be repaired
  - Requires node list on zombie phones



SMS-HTTP hybrid C&C

- Improvement over SMS-only
  - Zombies don't need a peer list anymore
  - Repair phase is easier
  - Splits up botnet in smaller parts (harder to detect)



Communication strategies

- Communication is the most important part of a botnet
  - Especially for a mobile phone botnet
- Wrong communication will lead to detection of a mobile bot
  - A battery that drains to fast, a high(er) phone bill, …

- IP
  - Only do bulk data transfer over WiFi
  - P2P traffic only over GPRS/3G (avoid detection by user)

- SMS
  - Consider not only volume but also destination
  - Group by operator/country minimize traffic between groups

Implementation

- Target platform was jailbroken iPhone
- Commands structure was build to fit both C&C methods

Content	Bytes
Signature length	1
ECDSA Signature	variable
Sequence Number	4
Command Type	1
Command	variable

- P2P
  - Based on KadC (Kademlia)
    - Only implements the DHT part
  - Command is transported in meta information of a hash
- SMS
  - Directly talks to GSM modem (via MITM technique)
  - SMS send via AT commands

Evaluation

- Installed bot(s) on a number of iPhones in the lab

- Sent commands to the bots and monitoring the actions
  - Tests:
    - Run shell commands (ping...)
    - Download URL
- P2P
  - Bots connected via either WiFi or GPRS/3G
  - Special: Change sleep interval
- SMS
  - Special: add phone number to local database

Conclusions

- We investigated the specific challenges of mobile botnets
  - Determined that a mobile bot can be easily build
- We designed and implemented multiple C&C approaches
  - P2P, SMS, SMS-HTTP
- The SMS-HTTP hybrid approach to C&C seems promising
  - Stable, hard to detect an monitor
- Mobile telcos need to think about monitoring and fighting SMS-based botnets

Questions?

Thank you!