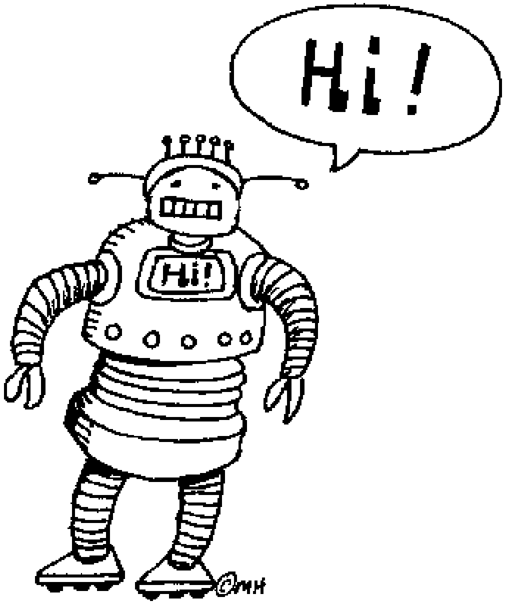
If only botmasters used Google Scholar…

The takedown of the Waledac botnet

Workshop on Botnet Detection, Measurement, Disinfection & Defence
10.03.2011

whois

Ben Stock



- Bachelor at University of Mannheim, 2009
- Now doing master‘s degree at Technische Universität Darmstadt

http://school.discoveryeducation.com/clipart/clip/robot-hi.html

Outline

- Basics on Waledac
- How to monitor Waledac?
- Back and forth with the botmaster
- Waledac Takedown
- Google Scholar?

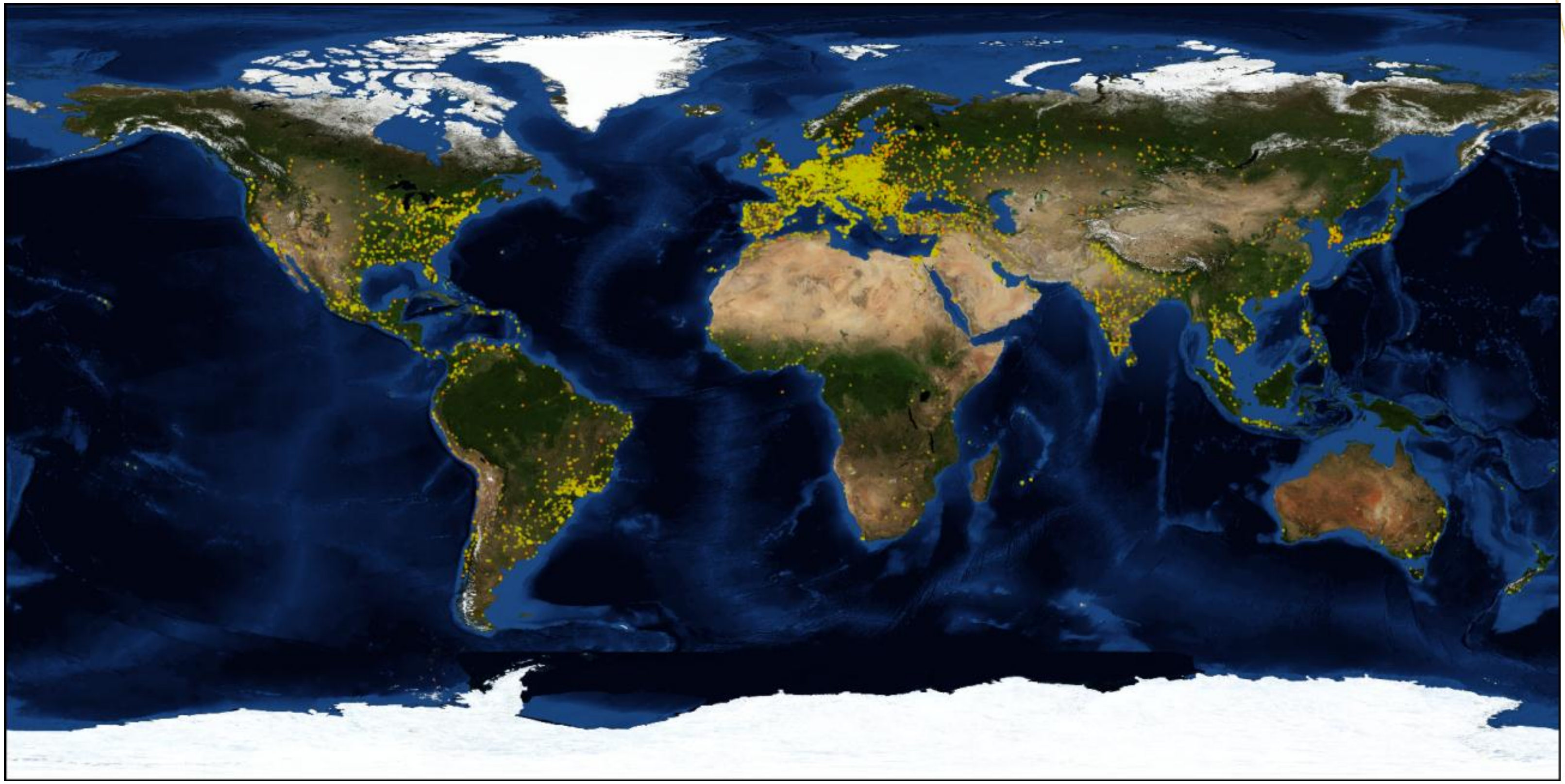
BASICS ON WALEDAC

What is (or was) Waledac?

- Spam-Bot
  - Intelligent template system
  - Reports spam success
- Fast-Flux agent
  - Used primarily for distribution
- DDoS
  - Implemented, never observed
- Harvesting credentials

http://minalex.lima-city.de/aio/pages/wissen/woher-kommt-der-begiff-spam.php

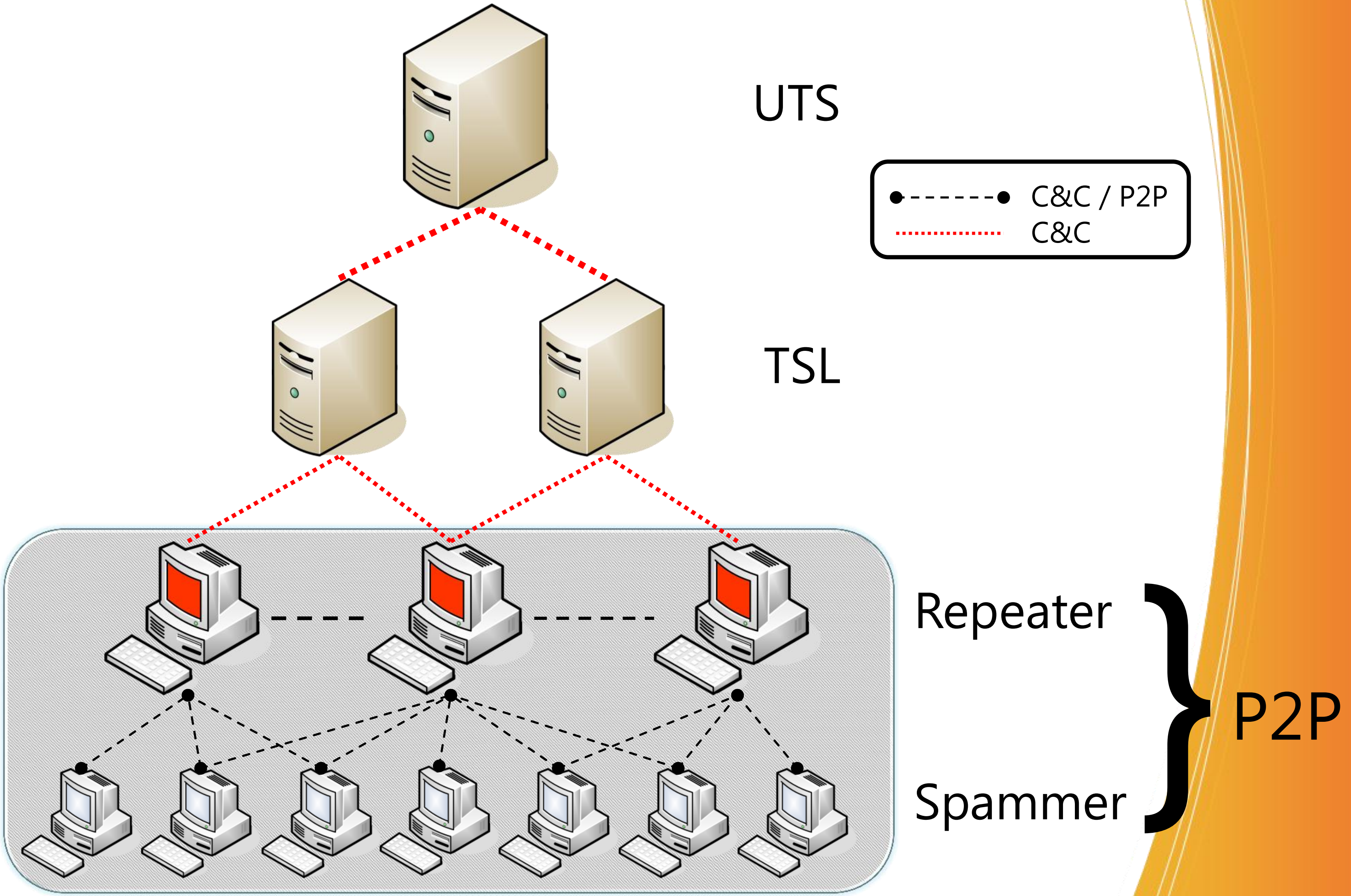
A global threat



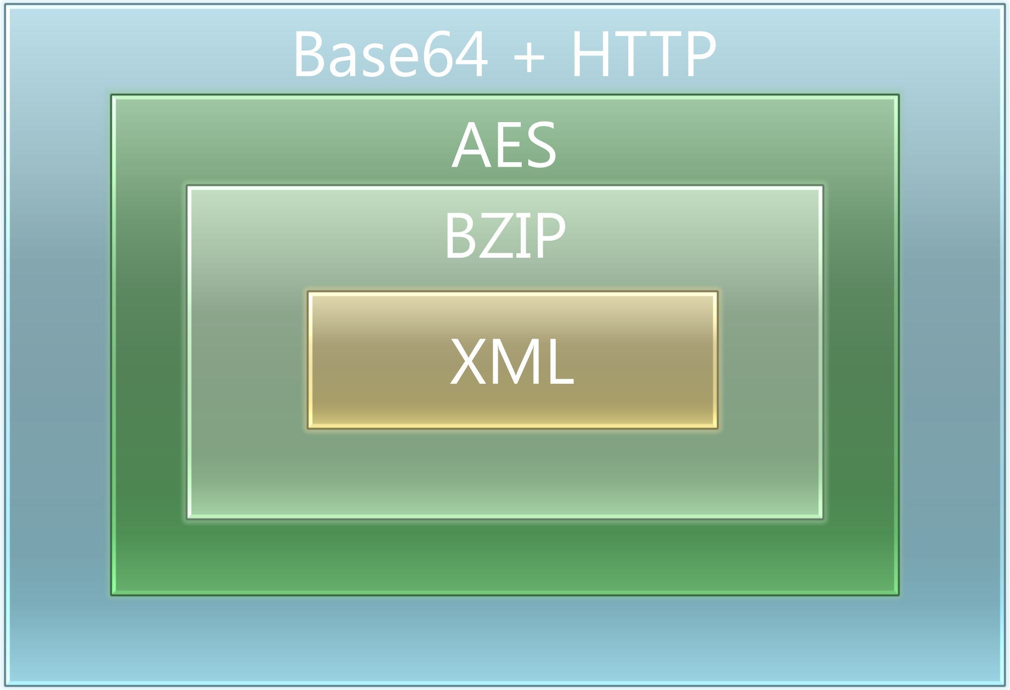
Botnet structure

- Waledac consisted of four layers
  - lowest: **Spammer** (behind NAT)
  - second layer: **Repeater** (direct connection to the Internet)
  - third layer: **Backend Server** (TSL)
  - Highest layer: **Mothership** (UTS)

Botnet structure (contd)



Communication protocol



Base64 + HTTP

AES

BZIP

XML

P2P protocol: Node updates

- Each node stores 500 nodes
- Normal case
  1. Any node sends 100 peers to Repeater
  2. Repeater merges list
  3. ➔ Repeater always has fresh list
  4. Repeater answers with merged list
  5. ➔ Requesting bot repeats steps 2 and 3

HOW TO MONITOR WALEDAC?

Measurement?

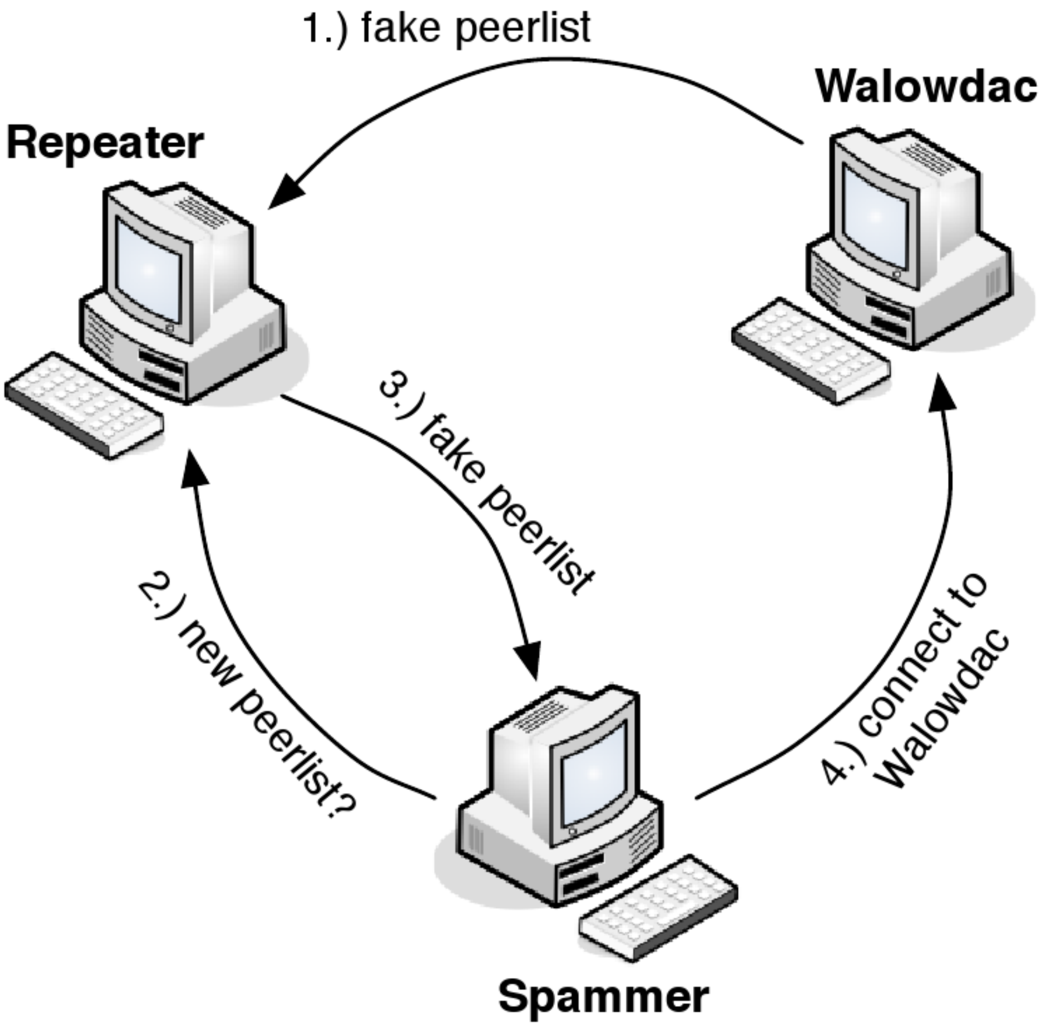
- Problem: we can only reach Repeaters
  - Later analysis shows ratio of 1:17
- Idea: bots need to connect to us
  - Inject own IPs into botnet
  - Are distributed in the botnet automatically
  - Let‘s keep a low profile: inject 10 entries each time

http://tux.crystalxp.net/de.id.2024-novadk-tortux-ninja.html

Walowdac

- Low-interaction clone of Waledac
- Speaks Repeater-level protocol
- Speaks C&C protocol
  - Does not relay requests
- Logs all incoming data

Measurement



Reaction by botmaster

- Botmaster detected high number of University of Mannheim IPs at some point
- Patched out peerlist exchange

Protocol change

- Each node stores 500 nodes
- Normal case
  1. Any node sends 100 peers to Repeater
  2. **Repeater merges list**
  3. ➔ Repeater always has fresh list
  4. Repeater answers with **empty** list

Thus: How to get back in?

- Bots have a fail-safe: fail-over URL
- Thus, let's see how we get listed in there
  - List of last 100 repeaters that checked in
  - ➔ Check in as a repeater

THE CAT AND MOUSE GAME

Repeater check

- Introduce ourselves as a repeater
- First: simple check from botmaster
- GET /readme.exe
  - Content: „MZ“
- Let‘s reply to readme.exe with „MZ“ then ☺
- (we don‘t want to relay malicious download requests)

And we are in…

Again, the botmaster reacted

- Check changed to getting a random filename with random content
  - GET /wj72az.exe
    - Content: <random>
  - But: coming from UTS mothership
    - Just proxy incoming connections from that IP to TSL servers (we know those)

And we are in…again

Tag, you're it

- This time, the botmater really went out of his way
  - GET for random filename…
  - And using different repeaters as proxies
  - ➔ random filename, random content, random connecting IP address

And yet…

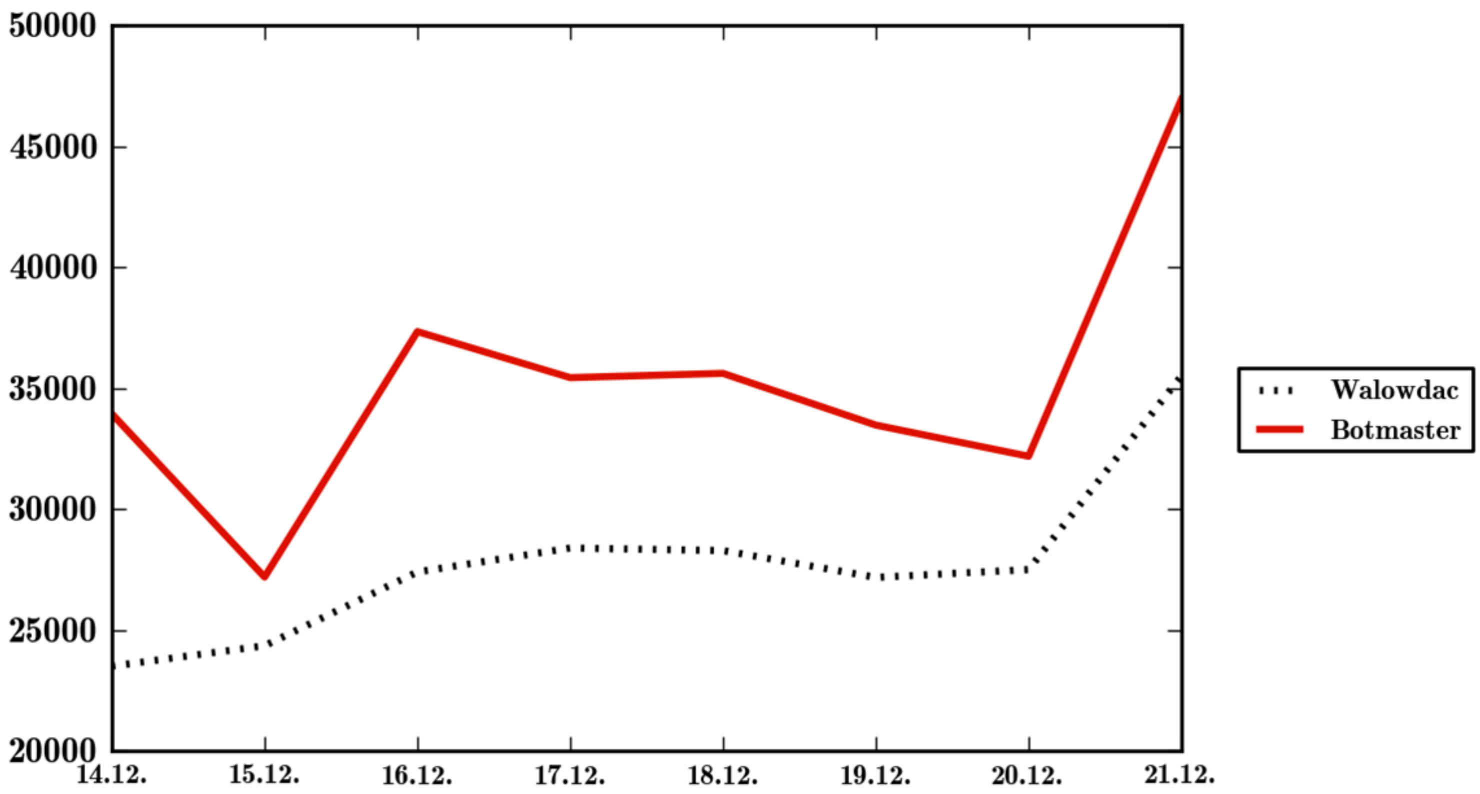
- Still one possibility to determine check
  - Normal fast-flux request: `http://somewaledacdomain.com/mal.exe`
  - Botmaster check: `http://199.2.137.X/wj72az.exe`
  - i.e. just check HTTP `Host` header and redirect request accordingly

Once more, we are in

Monitoring Waledac

- Monitoring went on for months afterwards
- Between 50k and 130k bots
  - Difficult to get good numbers:
    - Number of IPs: way too high
    - Number of nodeIDs: too low
      - Lots of collisions
    - Criteria: ASN/nodeID

Overlap



- between 69% und 90% data overlap

Source Data Botmaster: Greg Sinclair

ACTUAL TAKEDOWN

Steps taken

1. Making sure, our IPs are in fail-over URL (started mid February)
2. On Feb, 22nd: raising the number of poisonous IPs sent out by Walowdac
   - 1000 crafted entries per request
3. Using crawler to poison any new repeaters
   - Source: the botmasters fail-over URL

Impact

- Any bot connecting to Walowdac once is trapped
  - No valid repeaters left in list
  - At the same time: fail-over URL no longer available
- All communication to the C&C infrastructure is redirected to our infrastructure
- → **Waledac rendered ineffective**

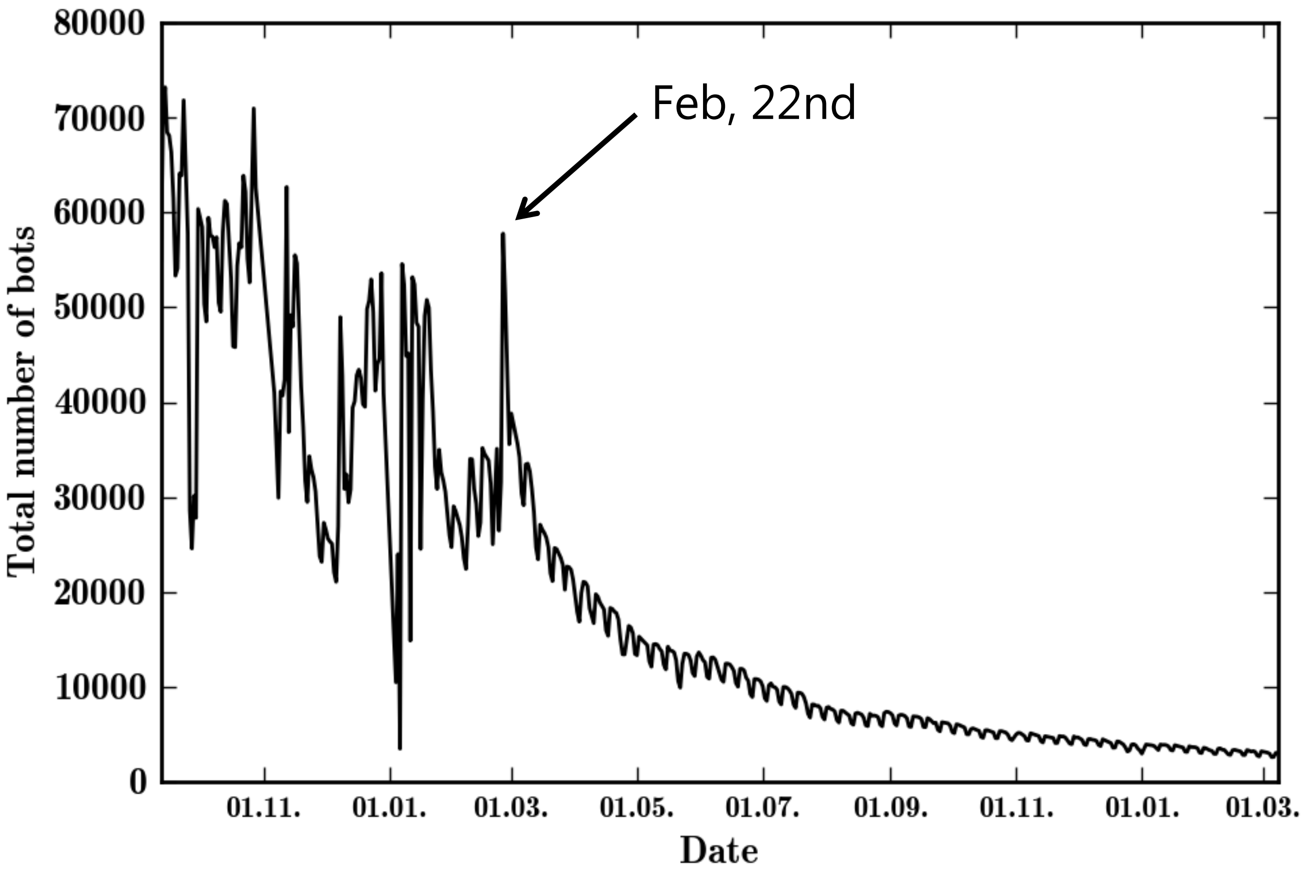
For the legal details…

- Catch Mark Debenham's talk
  - But watch for coffee mugs near him!
  - And also for small bottles with other content

Effects

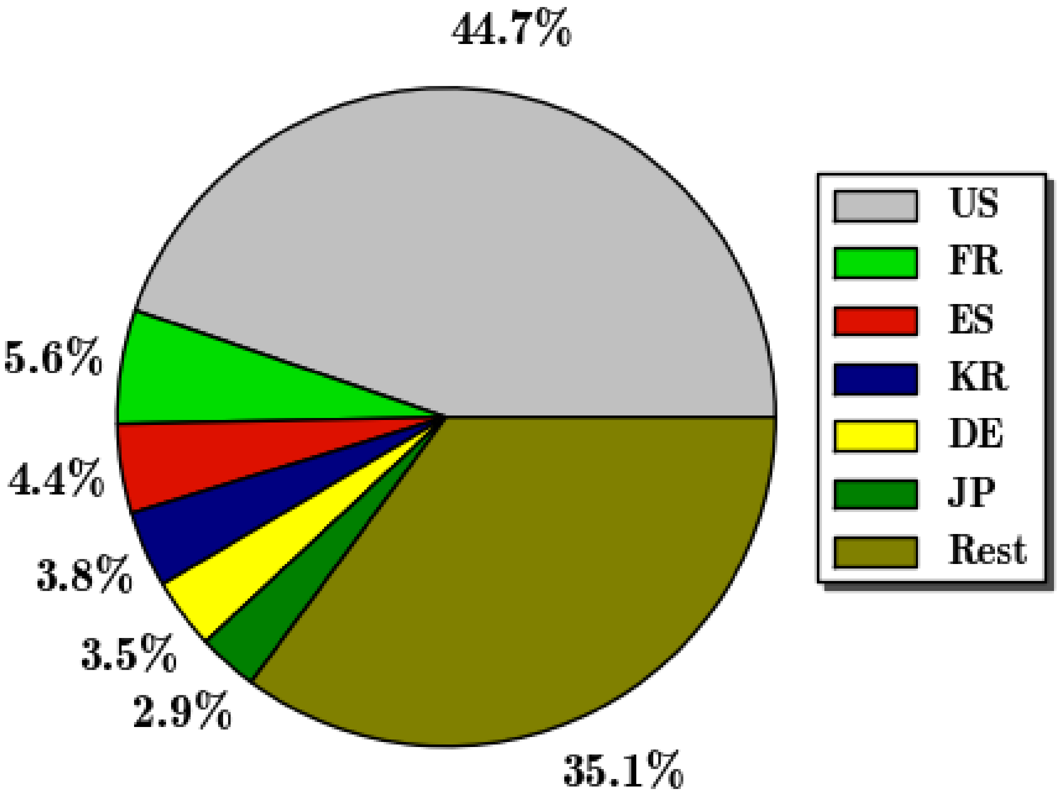
- Fast-flux domains offline (due to court‘s decision)
- Fast-flux infrastructure offline (due to redirection of C&C traffic)
- → no new infections possible

Effect on botnet size



- 30% per-day fluctuation before takedown
  - Without fast-flux infrastructure, no new infections

Germany is not that bad…



GOOGLE SCHOLAR…

Botmaster could have prevented takedown

- Go to Google Scholar, search for „Waledac“
  - Second and third entry from my thesis (in german, though)
  - Fourth hit: Greg Sinclairs paper from MALWARE, October 2009
  - Tenth hit: Our paper from EC2ND, November 2009
- All of them discuss the attack! (even more than half a year before it started)

That begs the question

- Should academia publish ideas like this?
  - Feel free to discuss this with me right now or after the talk

Thanks to

- Felix Leder for inviting me
- Greg Sinclair for the data (and a looot of other stuff)
- Microsoft
  - esp. TJ Campana and Mark Debenham

Questions?

OK