“The **Wonderful** thing about the Internet is that you’re connected to everyone else”

Vinton Cerf

"The **Terrible** thing about the Internet is that you're connected to everyone else"

--Vint Cerf

Facing the Dark Side of the Internet

Carlos Fragoso Mariscal

1st Spanish **N**etwork **O**perator's **G**roup meeting

CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA

Goal

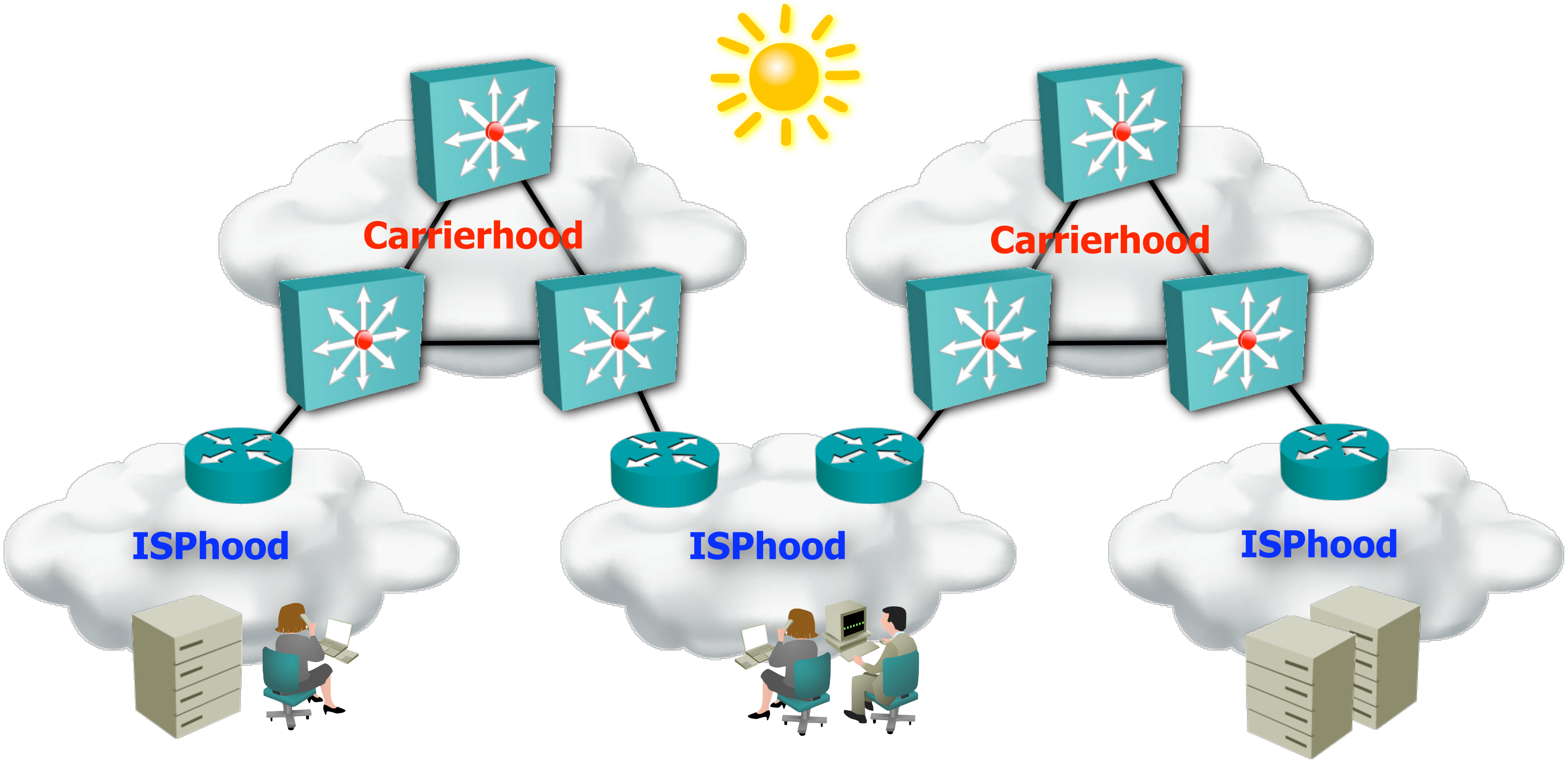
Describe **current trends** of the Dark-Side guys on the Internet and **how to face them**

Agenda

- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them

Agenda

- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them


Carrierhood
Carrierhood
ISPhood
ISPhood
ISPhood

Internethood

- Roads: network
  - Carriers, ISP’s, IXP’s,
- Home/Office: end sites
  - Universities, enterprises, home
- Tools/vehicles: hardware and software
  - Vendors, developers ...
- Citizens: users and boxes
  - End users, servers ...

What’s wrong with users?

- Limited or null security knowledge
- False sense of security
- No mainteinance
- Most of them use Windows

Agenda

- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them

Who are the... BAD GUYS?

The BAD guys

- Not hackers anymore
- Cybercrime organizations
- IT well-paid professionals
- Hacktivism / Cyberterrorism

Motivation

- Distributed Denial of Service
- Identity theft
- Spam
- Crime obfuscation
- Fraud

Roles

- Infrastructure engineers
- Malware developers
- Spammers
- Operators
- Mules

Their tools

- Trojans
- Keyloggers
- Packers / crypters
- Malware creation kits

Common target

- Windows OS boxes
- Unpatched
- Unprotected (FW, AV)
- Client-side infection

2008 Menaces

- Web site attacks against browser vulnerabilities
- Sophisticated and effective botnets
- Targeted phishing
- Mobile phone threats
- Insider attacks
- Advanced Identity Theft
- Social Engineering

Source: SANS Institute

Agenda

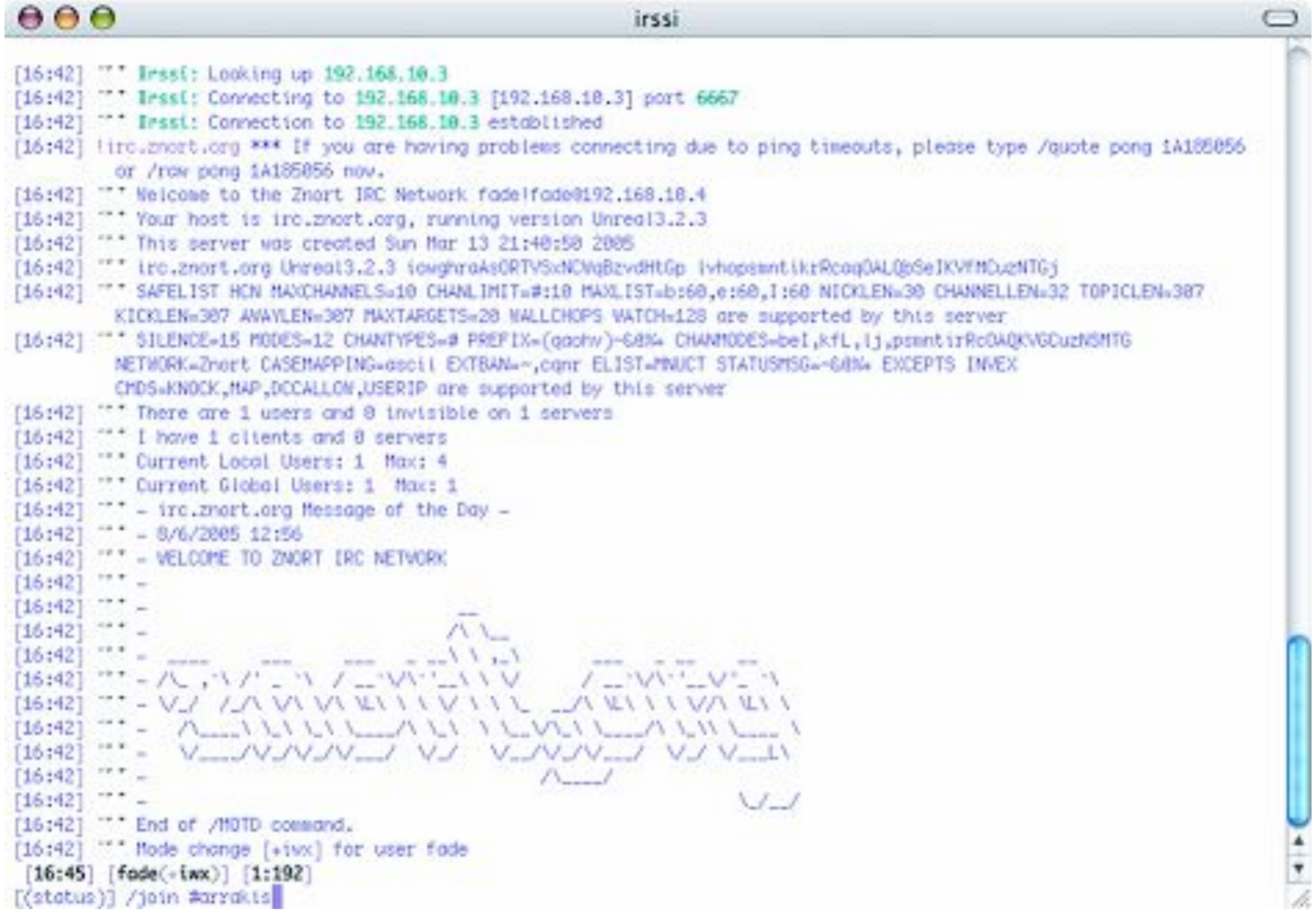
- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them

*"A **botnet** is comparable to compulsory military service for windows boxes"*

Source: Stromberg

What is a botnet ?

- Bot - Zombie - Drone
  - Malware
  - Remote control agent
- Command & Control
  - Protocol and actions



```
[16:42] -!- Irssi: Looking up 192.168.10.3
[16:42] -!- Irssi: Connecting to 192.168.10.3 [192.168.10.3] port 6667
[16:42] -!- Irssi: Connection to 192.168.10.3 established
[16:42] !irc.znort.org *** If you are having problems connecting due to ping timeouts, please type /quote pong 1A185056
          or /raw pong 1A185056 now.
[16:42] -!- Welcome to the Znort IRC Network fade!fade@192.168.10.4
[16:42] -!- Your host is irc.znort.org, running version Unreal3.2.3
[16:42] -!- This server was created Sun Mar 13 21:40:50 2005
[16:42] -!- irc.znort.org Unreal3.2.3 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCuzNTGj
[16:42] -!- SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307
          KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 WALLCHOPS WATCH=128 are supported by this server
[16:42] -!- SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVGCuzNSMTG
          NETWORK=Znort CASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT STATUSMSG=~&@%+ EXCEPTS INVEX
          CMDS=KNOCK,MAP,DCCALLOW,USERIP are supported by this server
[16:42] -!- There are 1 users and 0 invisible on 1 servers
[16:42] -!- I have 1 clients and 0 servers
[16:42] -!- Current Local Users: 1  Max: 4
[16:42] -!- Current Global Users: 1  Max: 1
[16:42] -!- - irc.znort.org Message of the Day -
[16:42] -!- - 8/6/2005 12:56
[16:42] -!- - WELCOME TO ZNORT IRC NETWORK
[16:42] -!- -
[16:42] -!- -                              __
[16:42] -!- -                             /\ \__
[16:42] -!- -  ____    ___     ___   _ __\ \ ,_\       ___   _ __   __
[16:42] -!- - /\_ ,`\ /' _ `\ / __`\/\`'__\ \ \/      / __`\/\`'__\/'_ `\
[16:42] -!- - \/_/  /_/\ \/\ \/\ \L\ \ \ \/ \ \ \_  __/\ \L\ \ \ \//\ \L\ \
[16:42] -!- -   /\____\ \_\ \_\ \____/\ \_\  \ \__\/\_\ \____/\ \_\\ \____ \
[16:42] -!- -   \/____/\/_/\/_/\/___/  \/_/   \/__/\/_/\/___/  \/_/ \/___L\ \
[16:42] -!- -                                   /\____/
[16:42] -!- -                                                           \_/__/
[16:42] -!- End of /MOTD command.
[16:42] -!- Mode change [+iwx] for user fade
 [16:45] [fade(+iwx)] [1:192]
[(status)] /join #arrakis
```

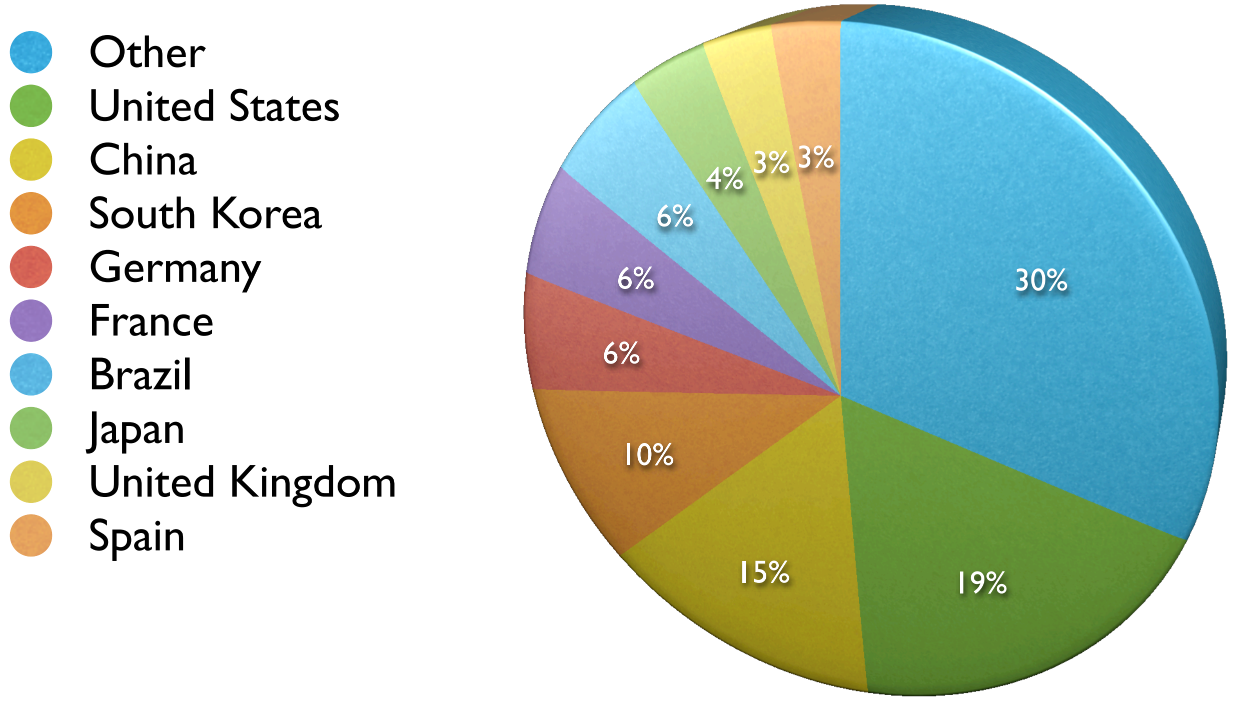
Am I a Zombie ?

Drone?

Bot?

McDonald's
NEIGHBORHOOD
ZOMBIE WATCH
WE IMMEDIATLY
REPORT ALL POSSIBLE
ZOMBIE SIGHTINGS TO
ZOMBIE SQUAD
WWW.ZOMBIEHUNTERS.ORG

Zombie demography



Source: Ciphertrust

Agenda

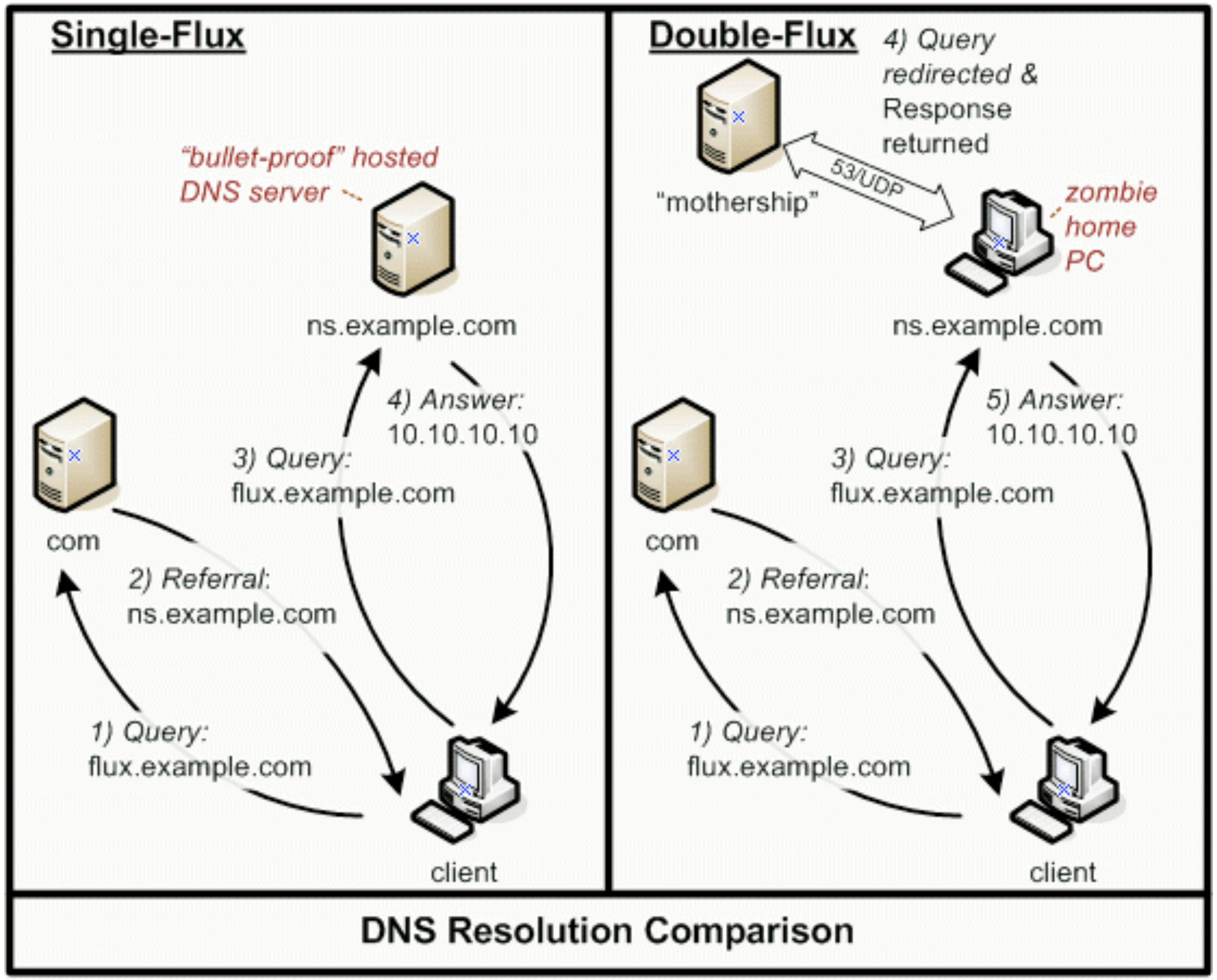
- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them

Trends

- Encryption
- Stealthy
- New control protocols
- Distributed architecture

Fast-Flux

- Multiple IP addresses to same FQDN
- Round-Robin DNS RR with low TTL
- Load distribution


Single-Flux
"bullet-proof" hosted DNS server
ns.example.com
4) Answer: 10.10.10.10
3) Query: flux.example.com
com
2) Referral: ns.example.com
1) Query: flux.example.com
client
Double-Flux
4) Query redirected & Response returned
"mothership"
53/UDP
zombie home PC
ns.example.com
5) Answer: 10.10.10.10
3) Query: flux.example.com
com
2) Referral: ns.example.com
1) Query: flux.example.com
client
DNS Resolution Comparison

Source: The Honeynet Project

Distributed C&C

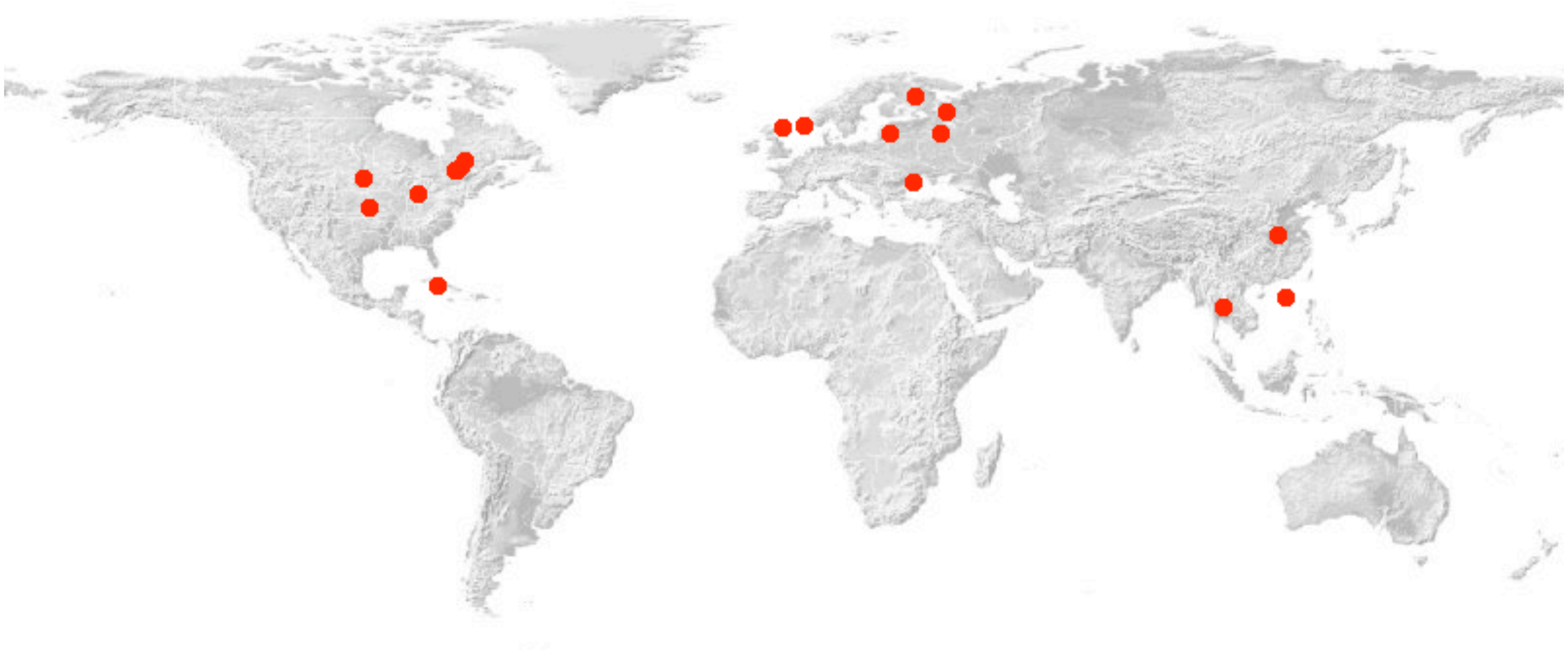
- Drones as botnet controllers
- Smaller botnets
- Difficult and time consuming tracking
- P2P protocols using supernodes

BlackEnergy botnet

- HTTP-based
- Small binary (<50KB)
- DDoS as main purpose

BlackEnergy

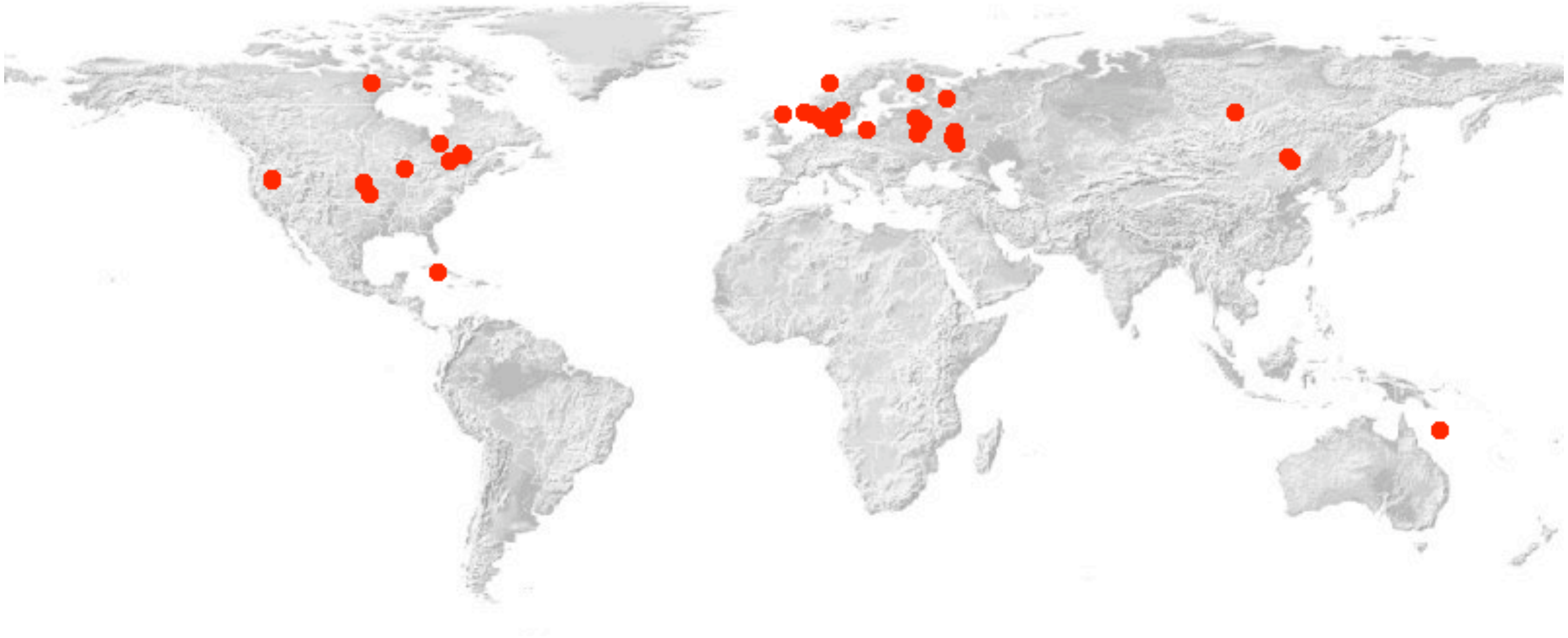
HTTP C&C locations



Source: Arbor Networks

BlackEnergy

DDoS Targets



Source: Arbor Networks

Agenda

- Internethood
- The Dark Side
- Botnets
- Trends
- Facing them

Fight !!!

Please...

Fight against them

- Build your own IR team
- Join IR communities
- Get and deploy your tools
- Train your users/customers
- Get in touch with LEOs

Join and share ...
Incident Response Communities

- FIRST
- TF-CSIRT
- NSP-SEC
- NSP-SEC-LEO
- SANS ISC

Got

tools?

Tools

- Flow consolidation
- Network Forensics
- Anomalous Detection Systems
- Blackhole Route Servers
- Security lab (analysis)
- Communication (IM, VoIP)

Summing up

Cybercrime will become more and more aggresive...

...but we will be here to fight them back!

Some references

- CSI Survey 2007
- ENISA Botnets paper
- The Honeynet project
- Arbor Networks' blog

Greetings

- Spanish CSIRT’s
- NSP-SEC community
- The Honeynet Project
- Jose Nazario and John Kristoff
- ESNOG guys

Tragedy?

Comedy?

http://carlos.fragoso.es

carlos@fragoso.es

CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA

E3B5 8908 57CA 5B67 83DD 9400 085A 29FF D539 69A3