The Honeynet PROJECT

Facing the Global Cyber Threat

Sébastien Tricaud – iAWACS 2009

Speaker

- Honeynet project Chief Technology Officer (CTO)
- Lead developer of Picviz
- Security researcher

Agenda

- Cyber-crime situation
- The (legal) information war
- The challenge
- What you can do!

CHAPTER I

The cyber-crime situation

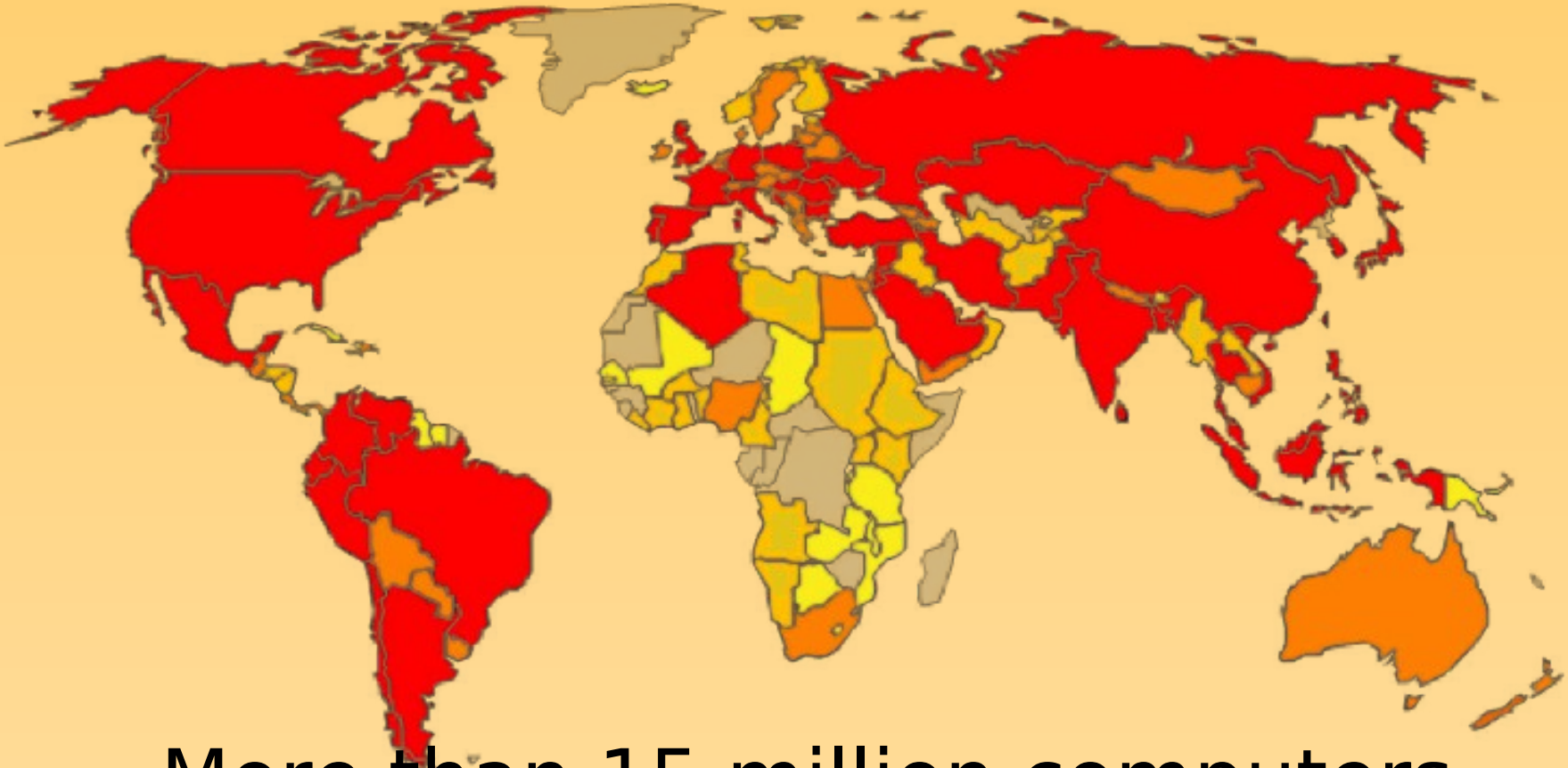
The world we live in...

- Worms
- Viruses
- Trojans
- Botnets
- Zombies
- Phishing
- Spam

- Fast-flux
- SPIT

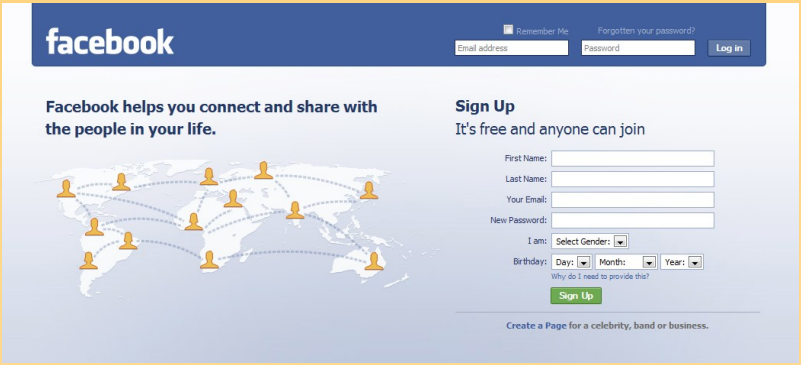
→ Buzzword Bingo!

Conficker



More than 15 million computers infected

Social networking



- The way teenagers email each other!
- New attacks
- More complex phishing attacks

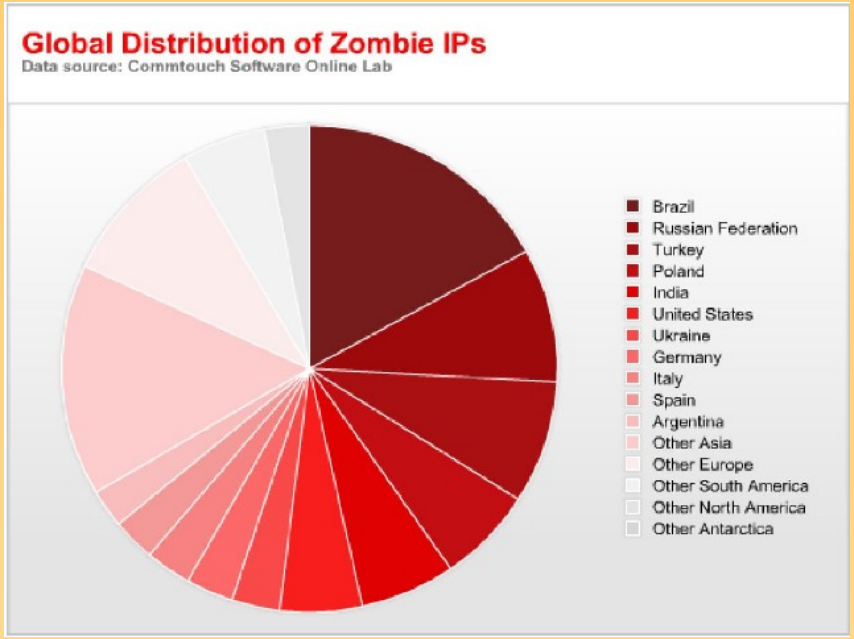
A matter of age

"Almost one half of the hackers we know about in Taiwan are between the age of 12 and 17 years old"

http://www.futuregov.net/articles/2009/sep/22/how-government-coping-cyber-crime/

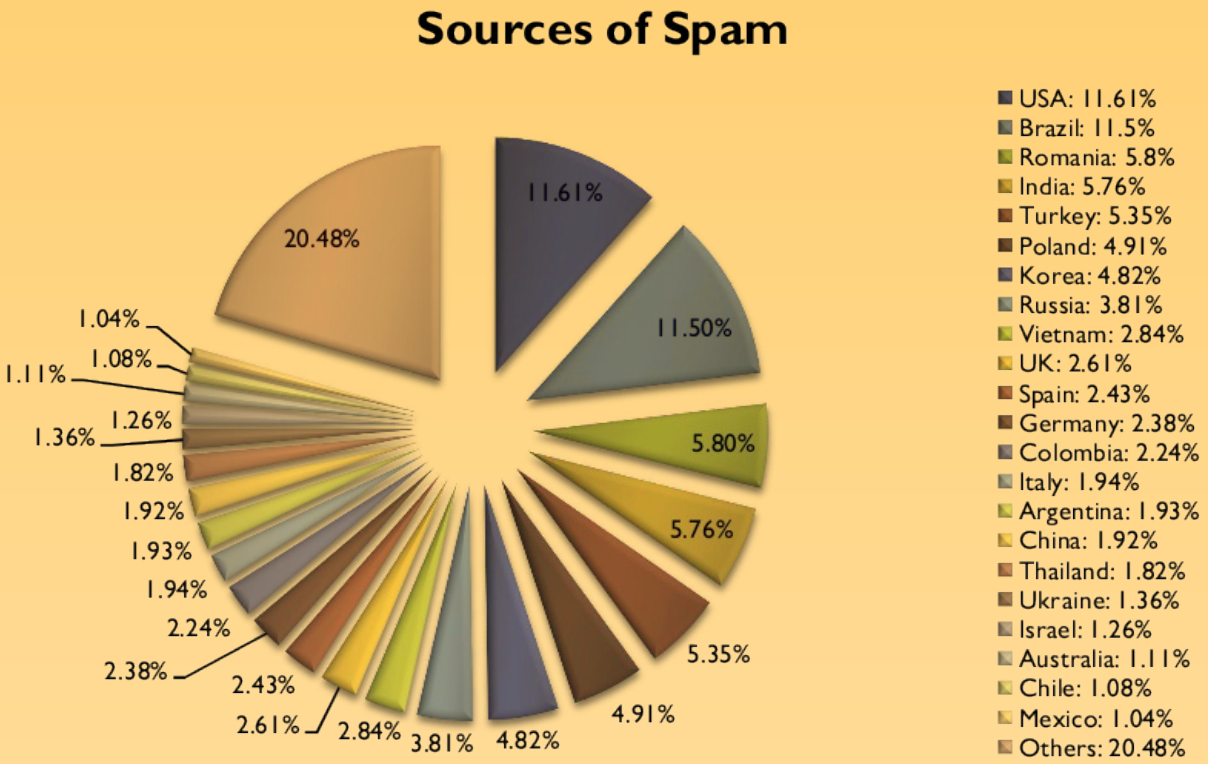

REDSKINS

Zombies: my PC is YOUR PC



- Brazil leads with 14% = 302,000 zombies activated each day

SPAM: January-March 2009



SPAMS are fun

“This message is to all the people that have been scammed in any part of the world, the United Nations have agreed to compensate them with the sum of US$500,000. This includes every foreign contractors that may not have received their contract sum, and people that have had an unfinished transaction or international businesses that failed due to Government problems etc.”

Making money

- If 1 in 100,000 people spend money in SPAM (not sure if women want this guy!)
- Botnets can launch Denial Of Service (DOS) attacks against anyone for money
- The BBC spent money on this for fun

CHAPTER II

The (legal) information war

<DISCLAIMER>

The companies cited here are companies who understood the importance of computers and they are models to follow for countries like France.

What is coming is not a rant against those companies.

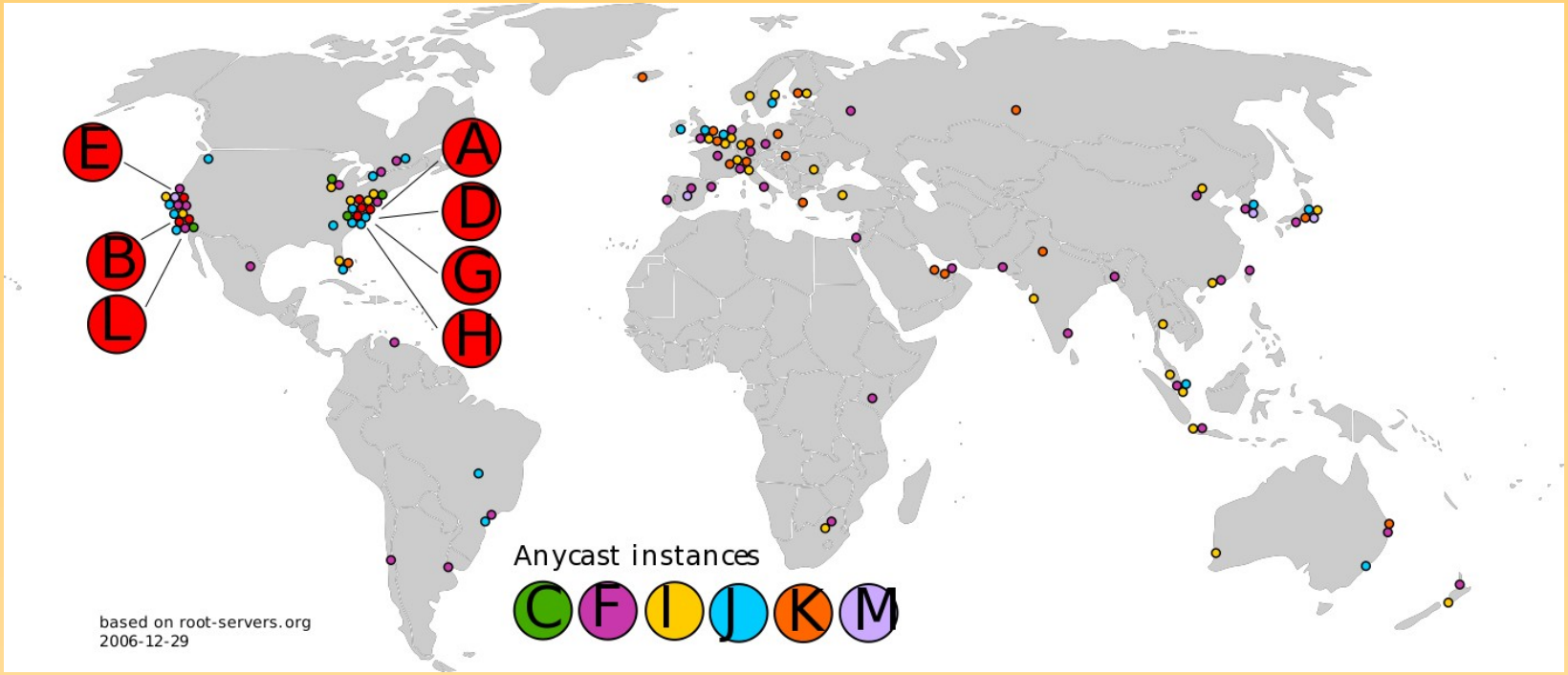
</DISCLAIMER>

What USA understood

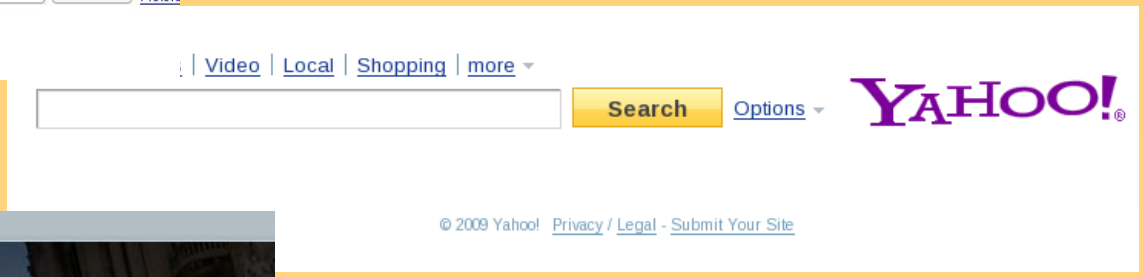
Servers

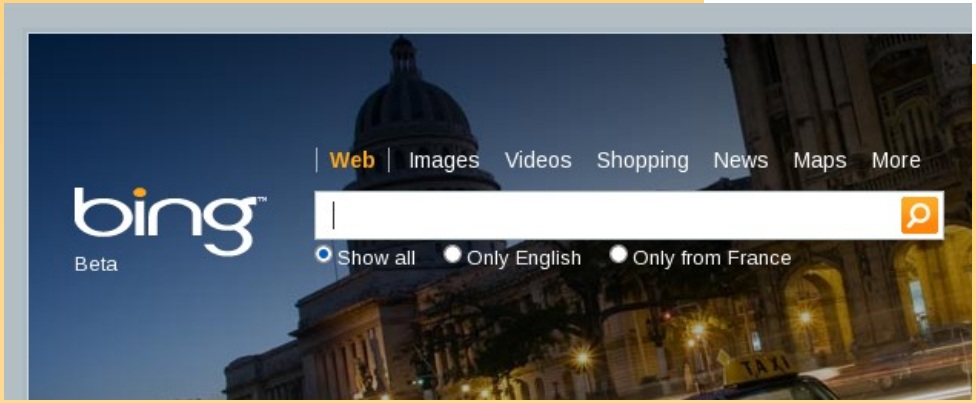
- Choices you have when you want to equip your datacenter:
  - IBM
  - HP
  - Dell
- They are nice, they replace your harddrives for free!

Root DNS

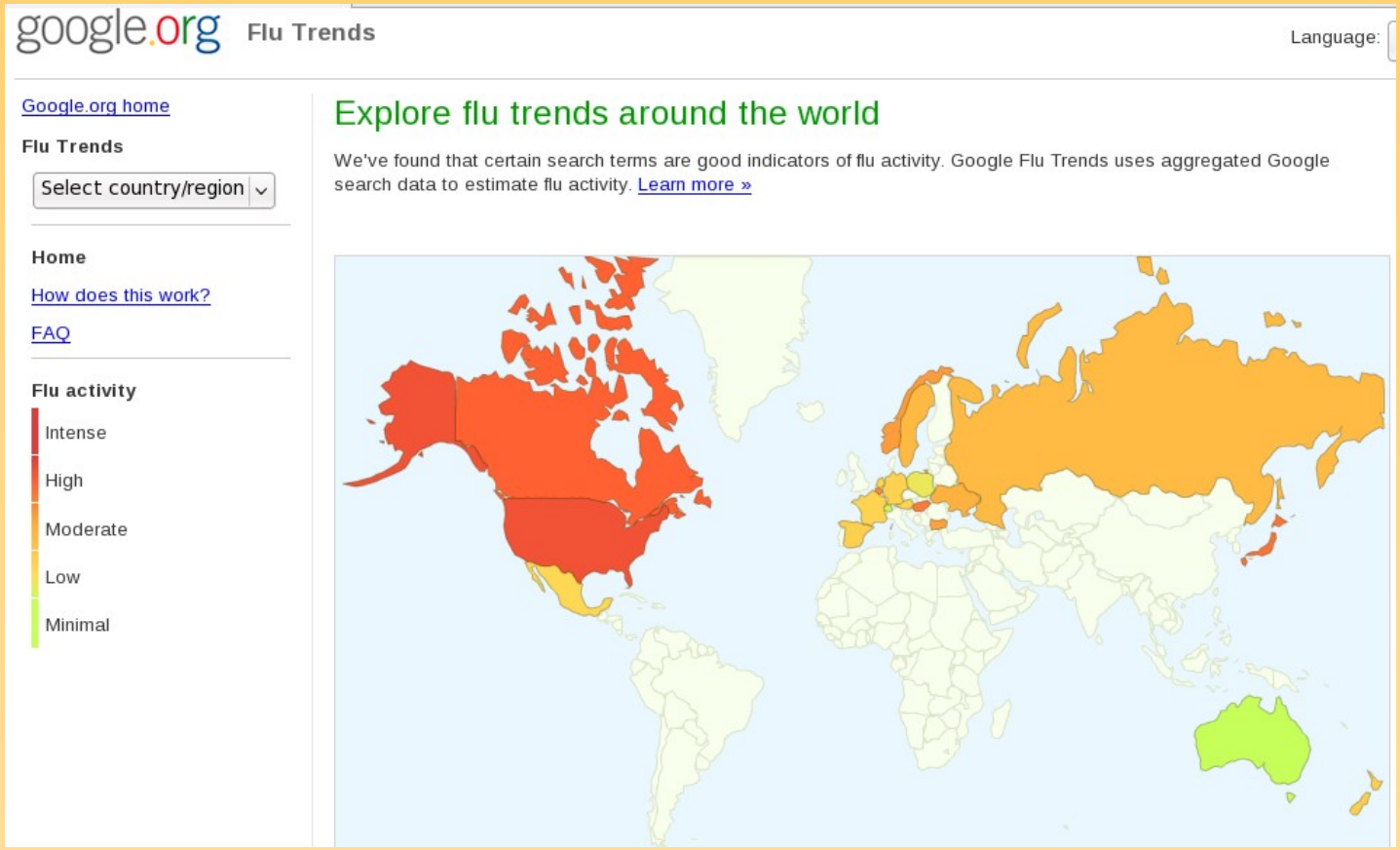

E
B
L
A
D
G
H
Anycast instances
C
F
I
J
K
M
based on root-servers.org
2006-12-29

Search engines

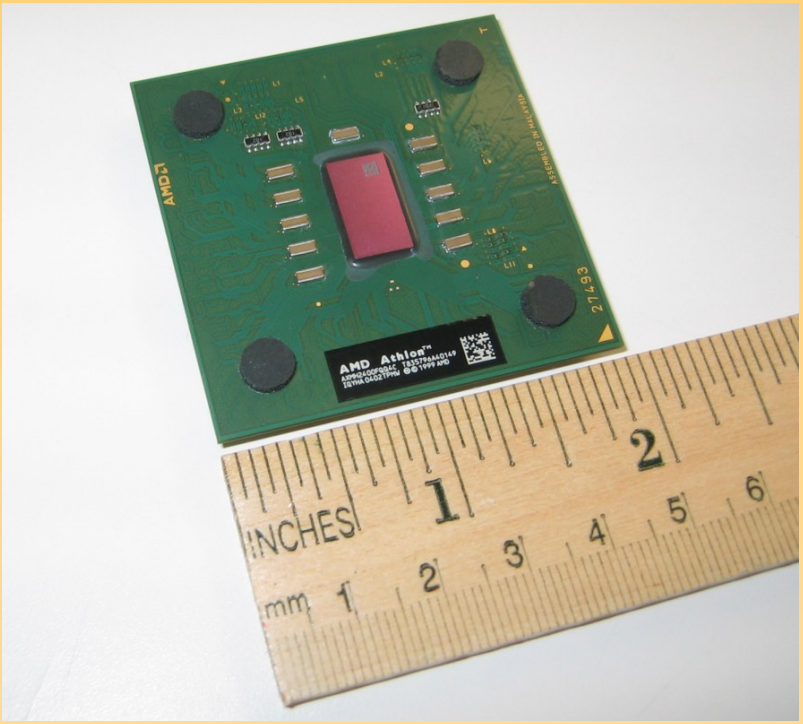




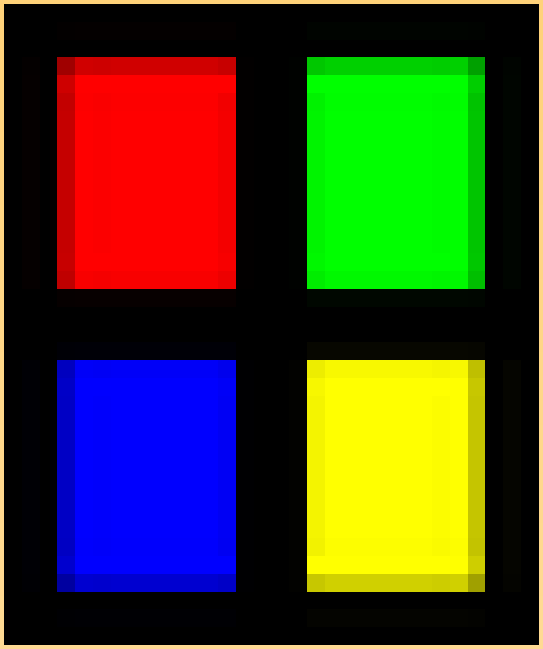
Diseases knowledge



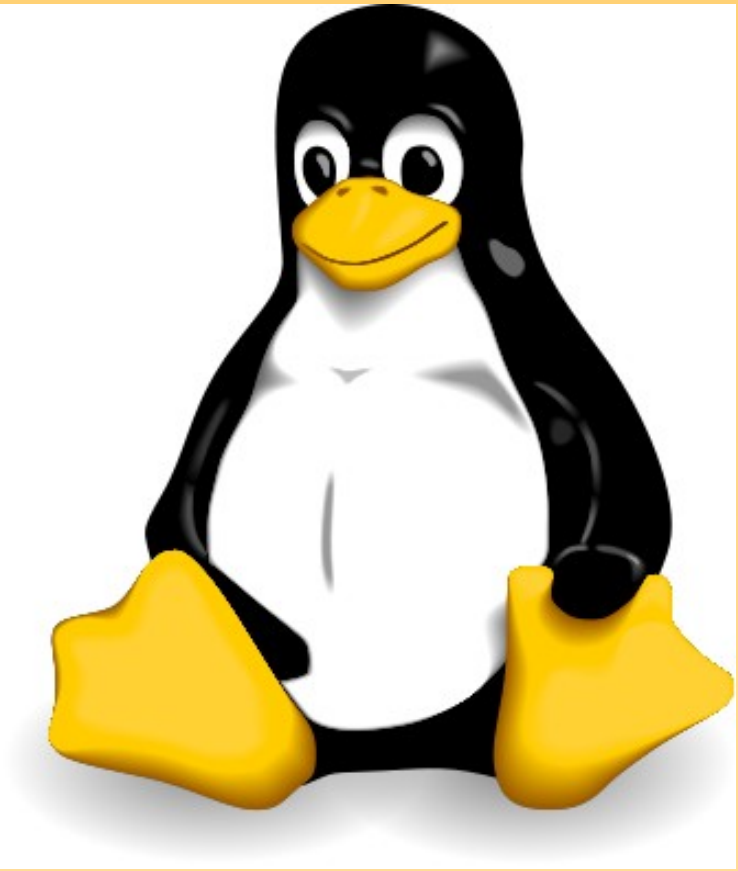
Your CPU



Your Operating System



Ah... Linux



- Fortunately there is SELinux ;)

Crypto Algorithm

- RSA
- Diffie-Hellman
- DES, Triple-DES
- AES
- ...

Business decision

- Snort is a NIDS developed by Sourcefire
- Checkpoint tried to acquire Sourcefire for $225 million
- The DoD objected to the sale
- Sourcefire was not acquired

Conclusion

- USA, as a developed country understood the importance of computers
- Developing countries such as Brazil, China, Malaysia etc. act also in a smart way
- Western countries such as France do not get it right (HADOPI etc.)

CHAPTER III

The Computer Security Challenge

Sometimes bugs are interesting

```
    static unsigned int tun_chr_poll(struct file *file,
poll_table * wait)
    {
    struct tun_file *tfile = file->private_data;
    struct tun_struct *tun = __tun_get(tfile);
    struct sock *sk = tun->sk;
    unsigned int mask = 0;

    if (!tun)
        return POLLERR;
```

The fun can be in your logs

```
Feb  26 07:59:03 kirk useradd[27475]: new user: name=vnc,
UID=1342, GID=1342, home=/home/vnc, shell=/bin/bash

Feb  26 07:59:16 kirk passwd(pam_unix)[27628]: password
changed for vnc

Feb  26 07:59:31 kirk sshd[27988]: reverse mapping
checking getaddrinfo for 18924012215.user.veloxzone.com.br
failed - POSSIBLE BREAK-IN ATTEMPT!

Feb  26 07:59:33 kirk sshd[27988]: Accepted keyboard-
interactive/pam for vnc from 189.24.12.215 port 1206 ssh2

Feb  26 07:59:33 kirk sshd(pam_unix)[28075]: session
opened for user vnc by (uid=0)
```

Finding traces

- Logs are often not enough
  - Exploit bypassing the authentication
  - Exploit not using syslog() to tell it exploited ;)
- However, traces are always in:
  - Network traffic
  - Syscalls
- Tricks: auditd loging a segfault

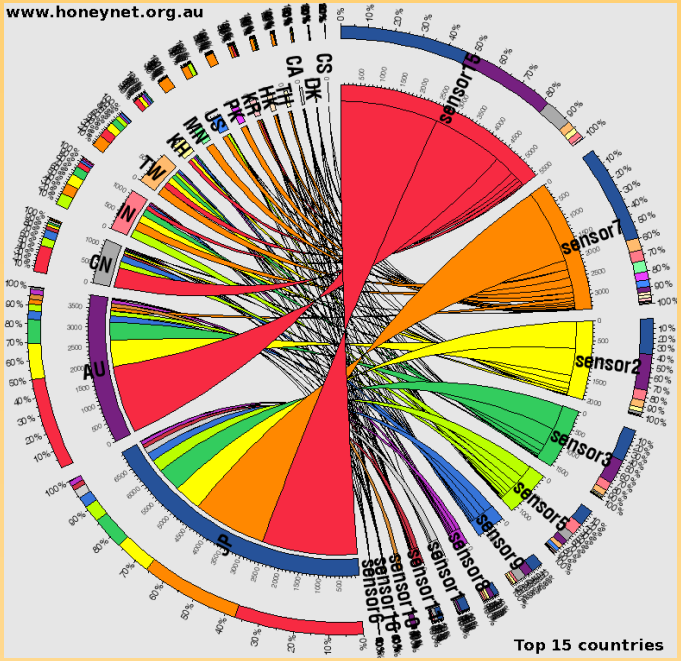
The problem

- Too many different ways of bypassing security (and I even did not talk about SQL injections!)
- When people deploy IDS, it is funny in a short term, unusable in a longer term
- We detect stuff on known patterns/signatures

Going visual

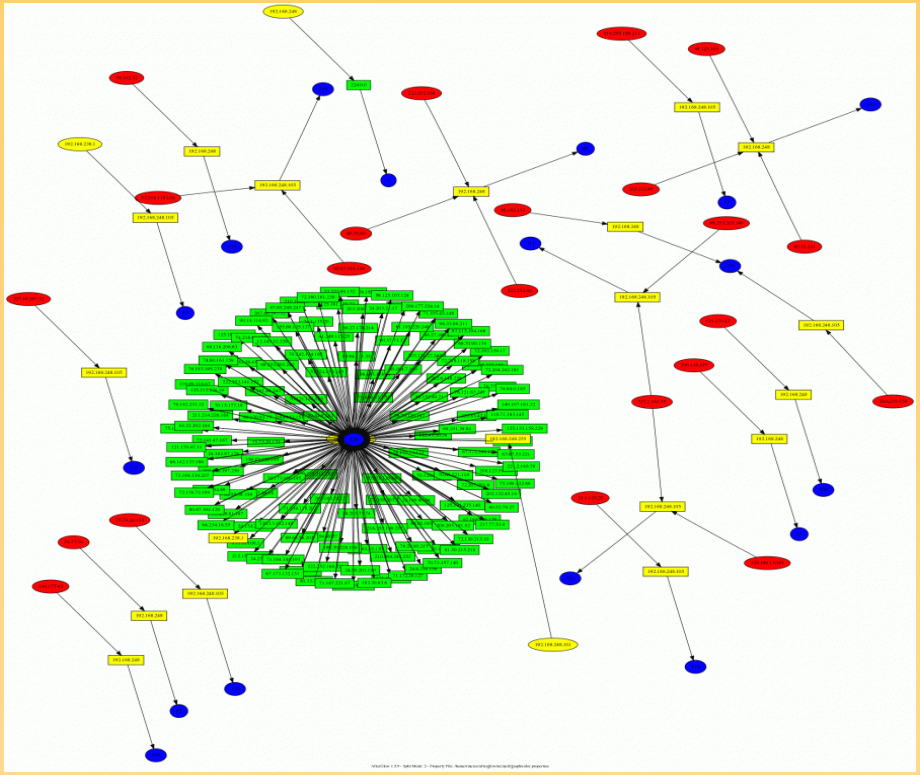
- How to understand big volumes and be efficient?
- Not interested in what we know already
- We can visualize!
- http://www.secviz.org

Circos



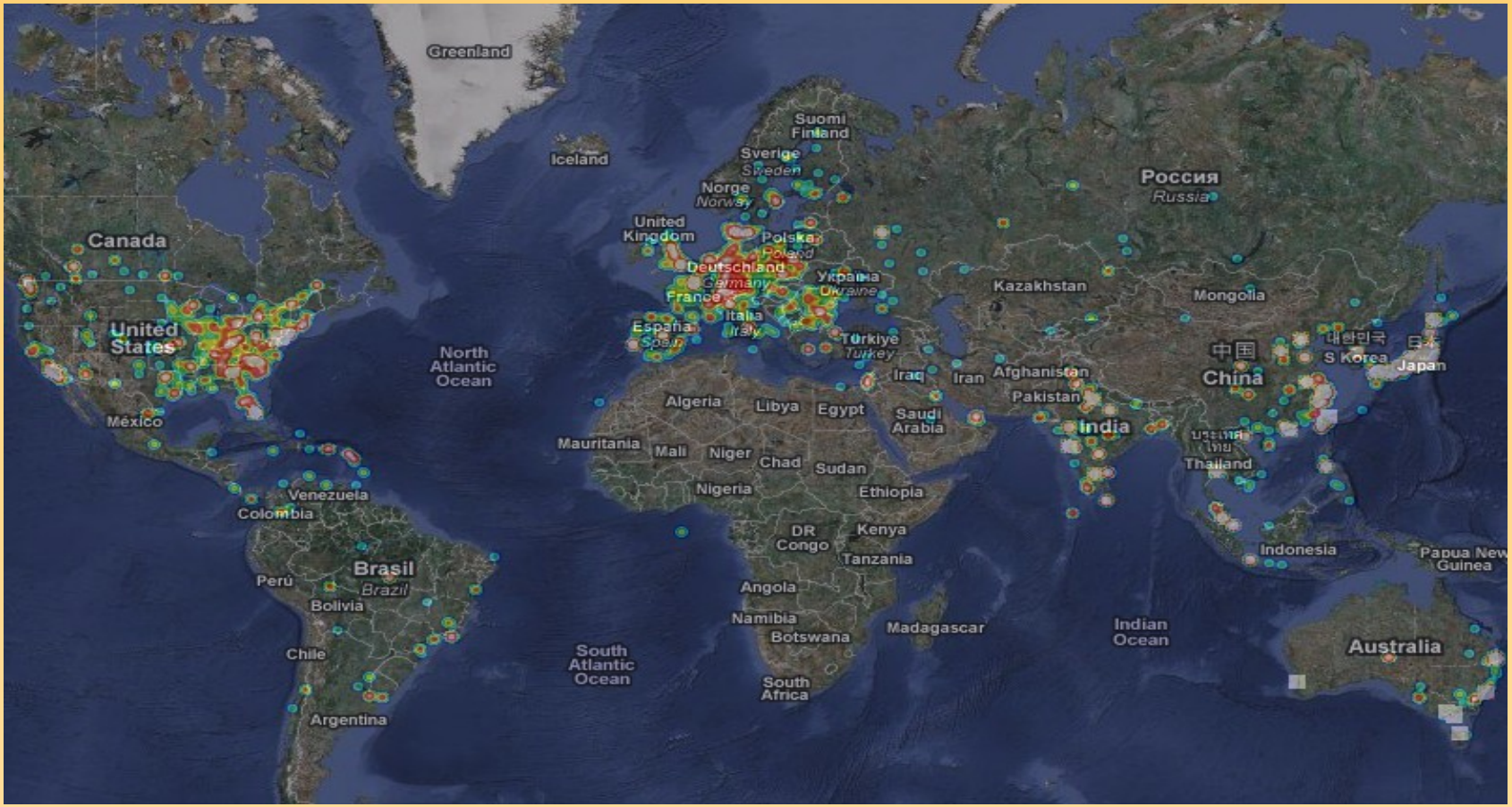
http://mkweb.bcgsc.ca/circos/

Afterglow



http://afterglow.sourceforge.net

Worldmap


Greenland
Iceland
Suomi
Finland
Sverige
Sweden
Norge
Norway
Россия
Russia
United
Kingdom
Polska
Poland
Deutschland
Germany
Україна
Ukraine
Canada
France
Italia
Italy
España
Kazakhstan
Mongolia
United
States
North
Atlantic
Ocean
Türkiye
Turkey
Iraq
Iran
Afghanistan
Pakistan
中国
China
대한민국
S Korea
日本
Japan
México
Algeria
Libya
Egypt
Saudi
Arabia
India
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Thailand
Venezuela
Colombia
DR
Congo
Kenya
Tanzania
Indonesia
Papua New
Guinea
Brasil
Brazil
Perú
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian
Ocean
Australia
Chile
South
Atlantic
Ocean
South
Africa
Argentina

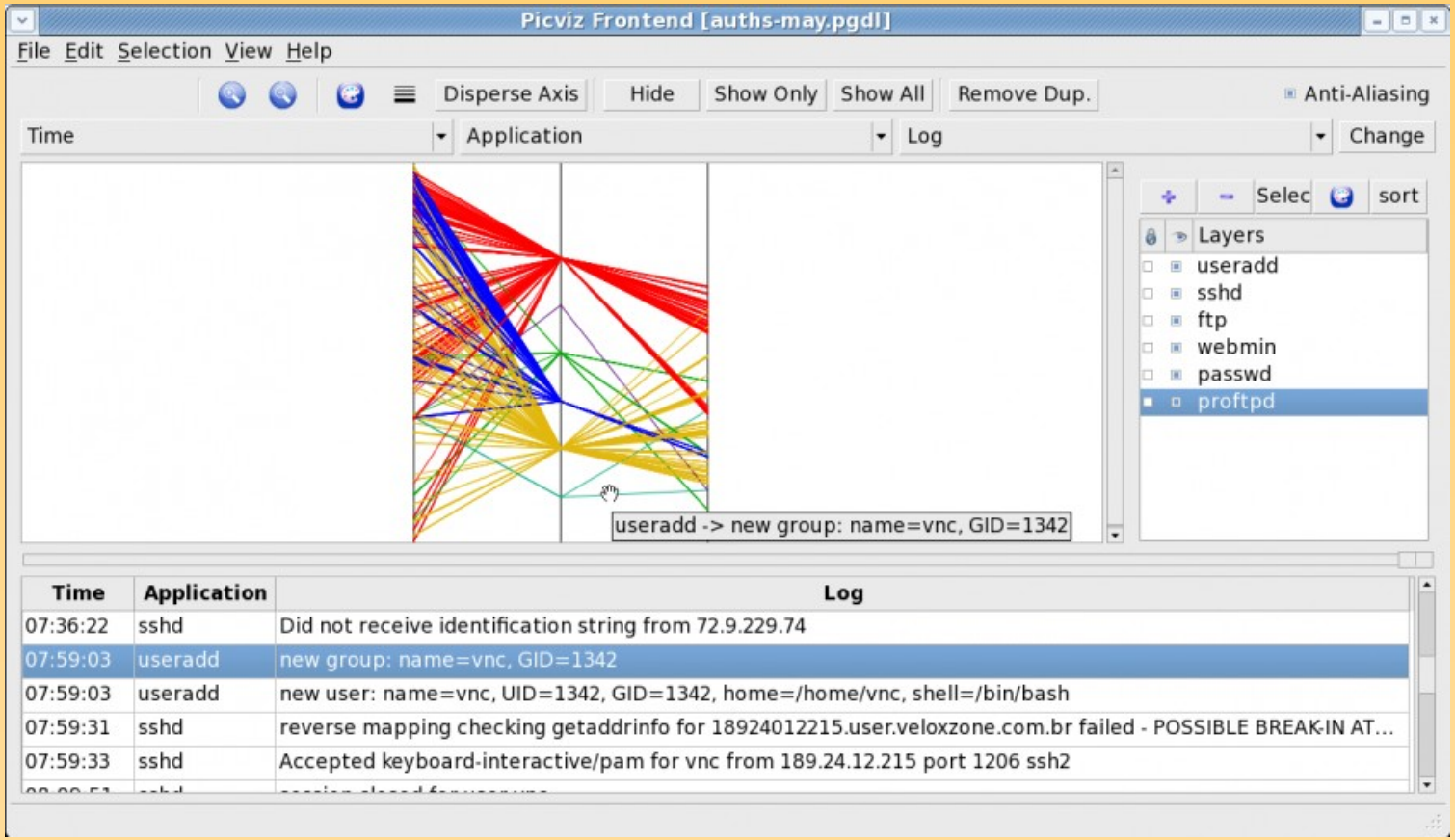
Some questions

- How to represent the time?
- How to have more than 3 dimensions?
- How to have an infinity of events?

Picviz

- http://www.wallinfire.net/picviz
- Created by Philippe Saadé and myself in summer 2008
- Use parallel coordinates
- Use maths in computer security

Picviz


Picviz Frontend [auths-may.pgdl]
File Edit Selection View Help
Disperse Axis
Hide
Show Only
Show All
Remove Dup.
Anti-Aliasing
Time
Application
Log
Change
Selec
sort
Layers
useradd
sshd
ftp
webmin
passwd
proftpd
useradd -> new group: name=vnc, GID=1342
Time
Application
Log
07:36:22 sshd Did not receive identification string from 72.9.229.74
07:59:03 useradd new group: name=vnc, GID=1342
07:59:03 useradd new user: name=vnc, UID=1342, GID=1342, home=/home/vnc, shell=/bin/bash
07:59:31 sshd reverse mapping checking getaddrinfo for 18924012215.user.veloxzone.com.br failed - POSSIBLE BREAK-IN AT...
07:59:33 sshd Accepted keyboard-interactive/pam for vnc from 189.24.12.215 port 1206 ssh2

CHAPTER IV

Share your data!

Some initiatives

- http://www.loganalysis.org/sample-log-files/
- http://www.pcapr.net
- http://2009.hack.lu/index.php/InfoVisContest

Why sharing?

- Allow researchers to work on real stuff
- Improve parsers
- Improve tools
- Anonymization? Argus has tools, or you can write your own

Conclusion

- The cyber-crime is an economy and is complex
- People use the internet in a way that can surprise you (social networks for email...)
- There is too many data containing much information
- Logs are usually not normalized, especially syslog
- Sharing is a key to improve this situation

Questions?

sebastien@honeynet.org