Leurré.com:
a worldwide distributed platform to study Internet threats

Deployed and Managed by
The Eurecom Institute

(teaching and research institute located on the French Riviera)

Contact Point:

dacier@eurecom.fr

Overview

- Leurré.com: why and how
- Web interface: a few examples
- Some ‘non trivial’ results.
- Conclusions

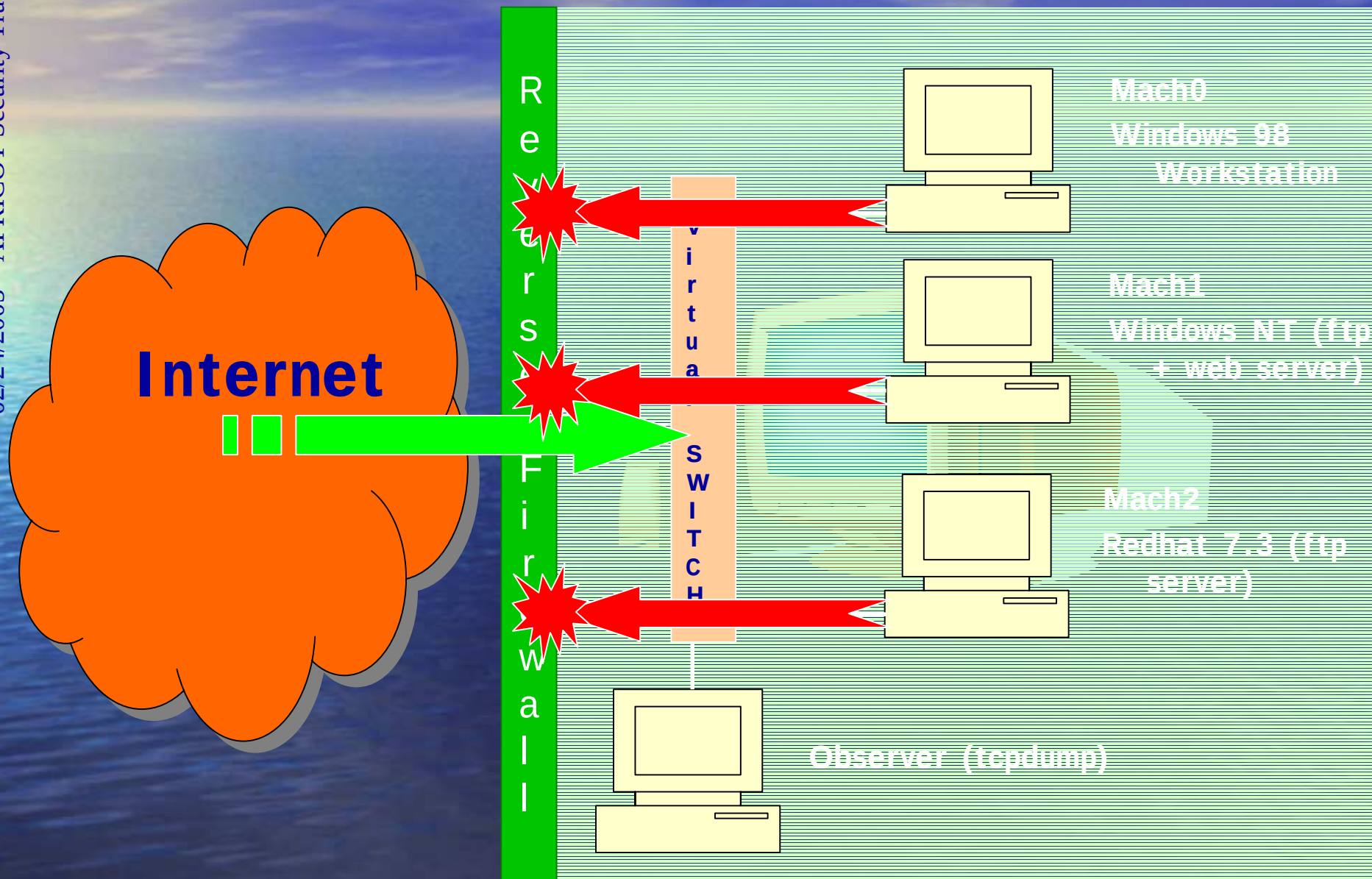
Motivations

- We do not precisely know the threats we are facing and we do not know if/how they evolve ...
- ... because of the lack of model to characterize them ...
- ... because of the lack of unbiased, quantitative data available to build such model ...
- ... because of the lack of environment to collect such data!

Leurré.com

- This project aims at deploying the very same honeypots in a large number of diverse locations.
- Early results demonstrate the complementarity of this approach to so-called *Internet telescopes* and Darknets.
- You can see this as a simple, widely distributed, fine grained network monitoring system

Experimental Set Up



30 platforms, 20 countries, 5 continents

In Europe ...


Europe
Greenland Sea
Norwegian Sea
Barents Sea
ICELAND
NORWAY
SWEDEN
FINLAND
RUSSIA
ESTONIA
North Atlantic Ocean
North Sea
IRELAND
UNITED KINGDOM
DENMARK
BELARUS
POLAND
SLOVAKIA
HUNGARY
ROMANIA
MOLDOVA
Bay of Biscay
PORTUGAL
SPAIN
Mediterranean Sea
MOROCCO
ALGERIA
TUNISIA
MALTA
GREECE
TURKEY
Black Sea

Win-Win Partnership

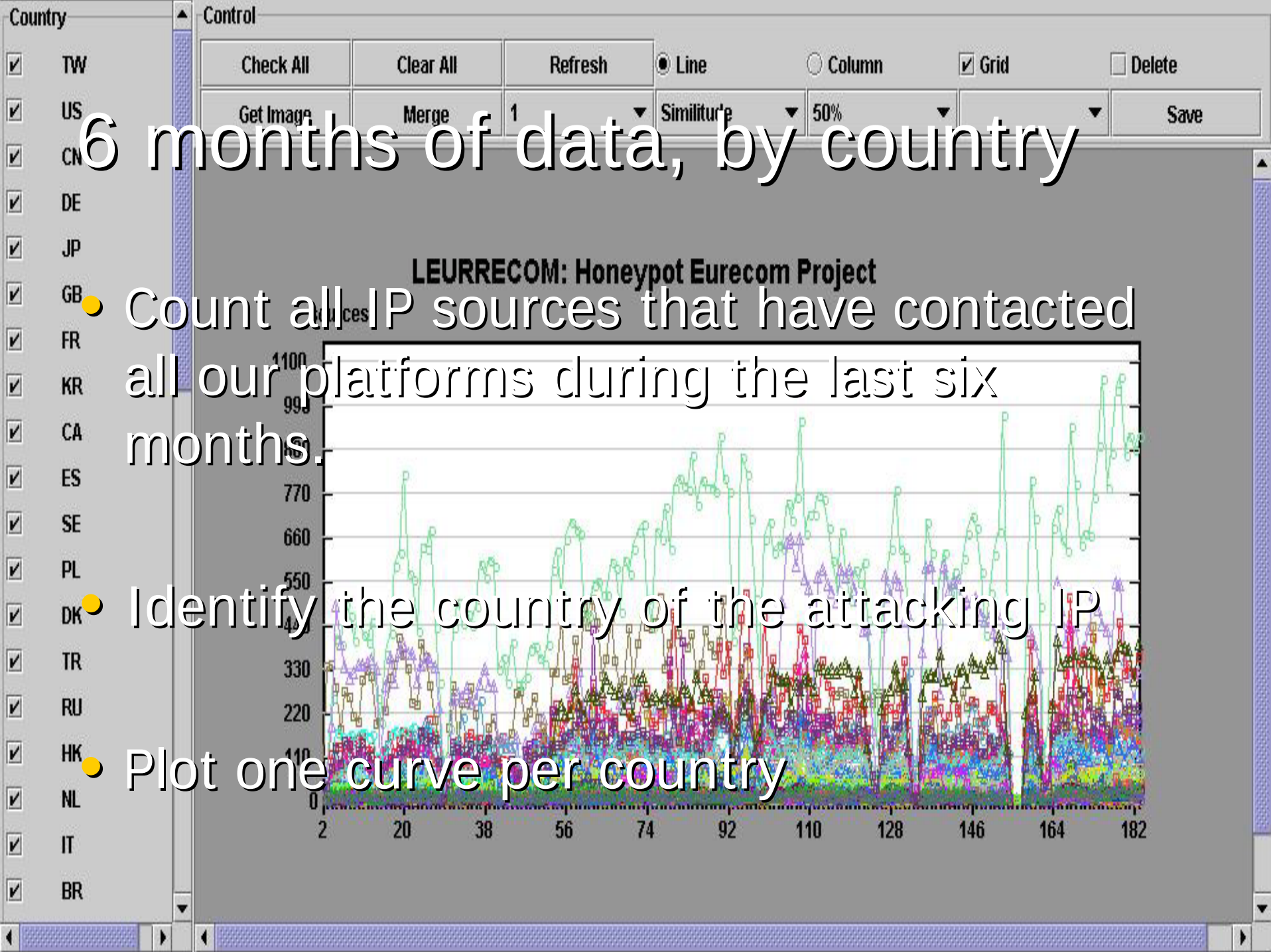
- The interested partner provides ...
  - One old PC (pentiumII, 128M RAM, 233 MHz...),
  - 4 routable IP addresses,
- EURECOM offers ...
  - Installation CD Rom
  - Remote logs collection and integrity check.
  - Access to the whole SQL database by means of a secure web access.

Overview

- Leurré.com: why and how
- Web interface: a few examples
- Some ‘non trivial’ results.
- Conclusions

6 months of data, by country

- Count all IP sources that have contacted all our platforms during the last six months.
- Identify the country of the attacking IP
- Plot one curve per country



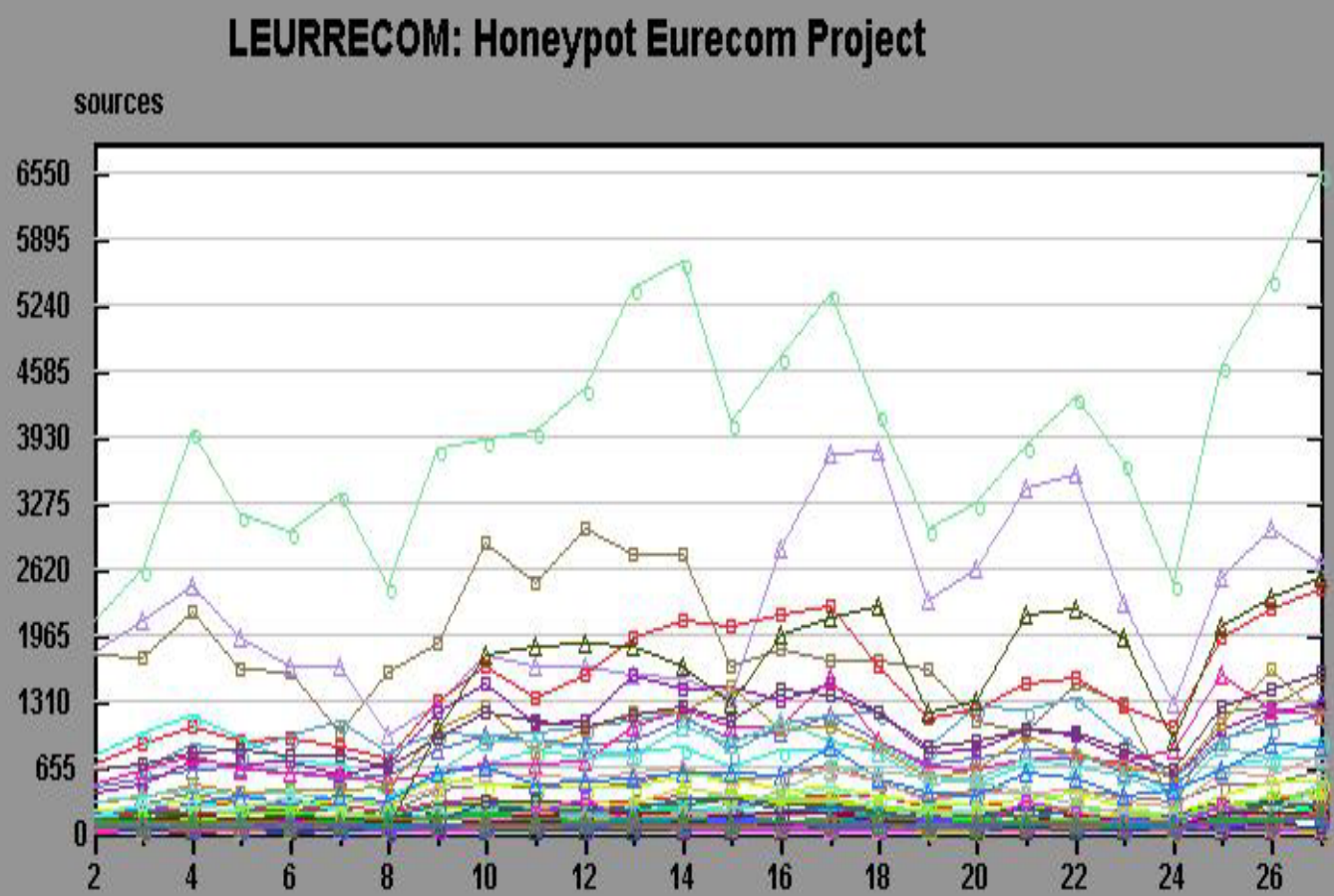
Country

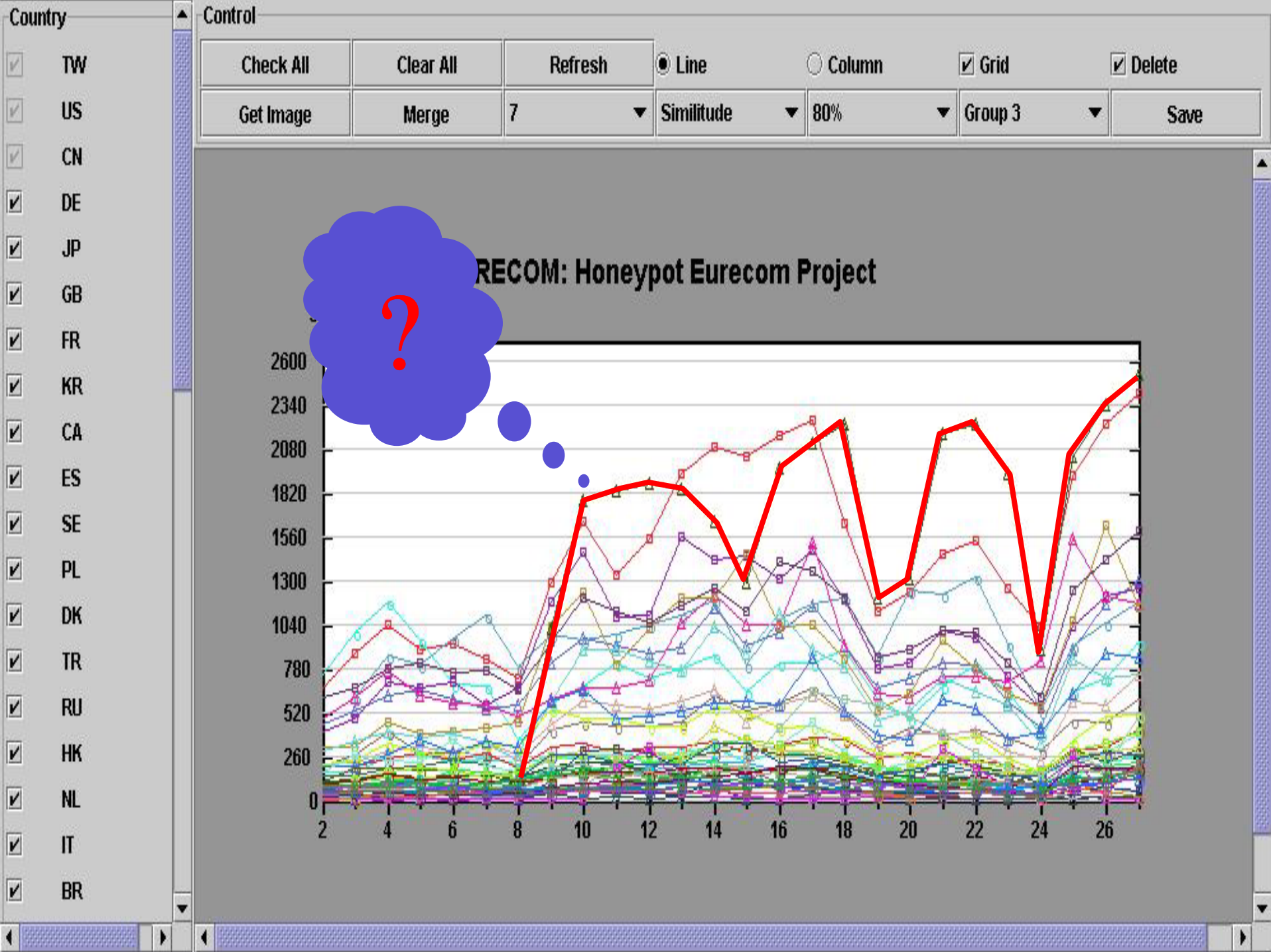
- TW
- US
- CN
- DE
- JP
- GB
- FR
- KR
- CA
- ES
- SE
- PL
- DK
- TR
- RU
- HK
- NL
- IT
- BR

Control

Check All | Clear All | Refresh | Line | Column | Grid | Delete

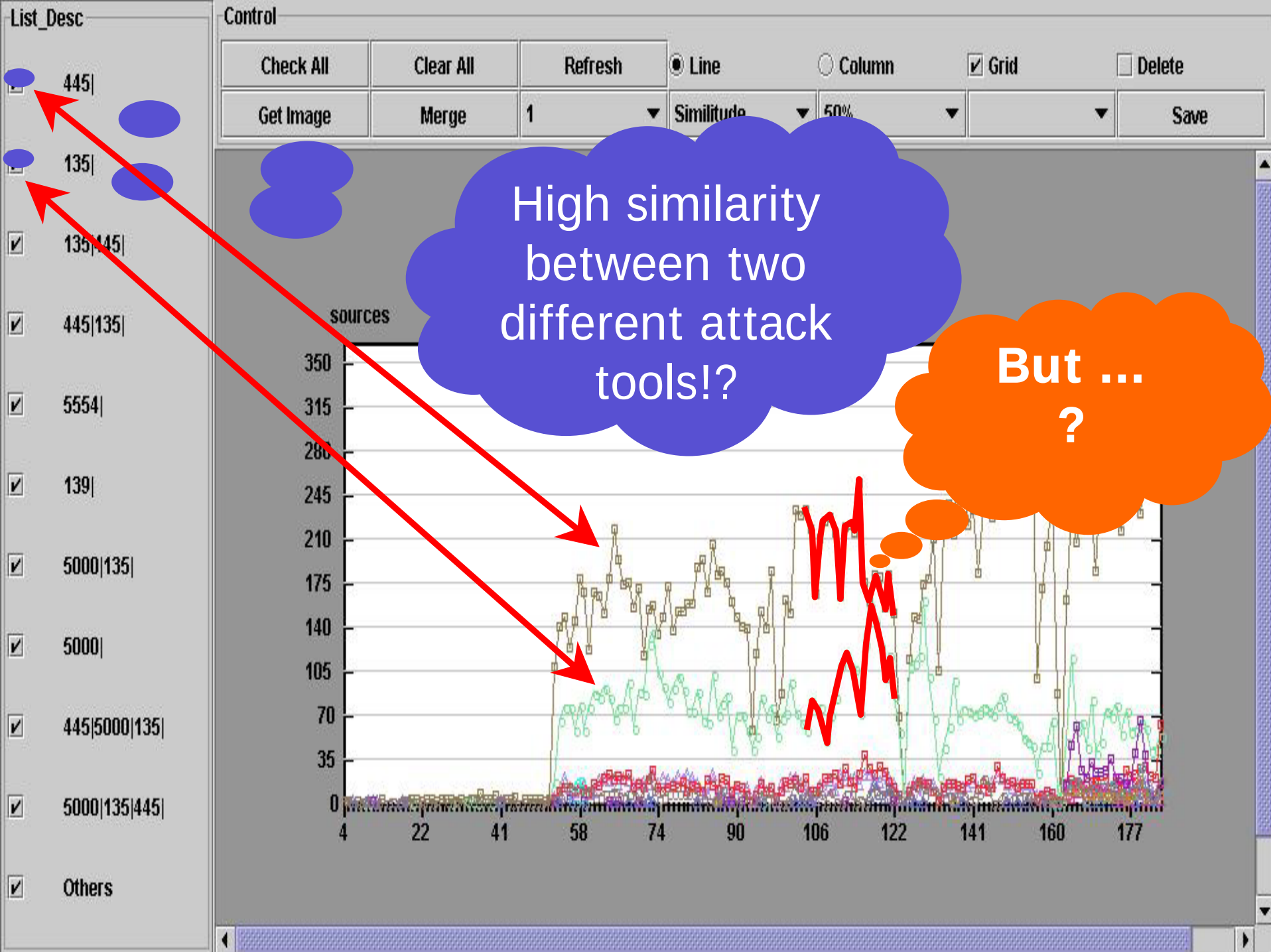
Get Image | Merge | 7 | Similitude | 50% | | Save




Country
TW
US
CN
DE
JP
GB
FR
KR
CA
ES
SE
PL
DK
TR
RU
HK
NL
IT
BR
Control
Check All
Clear All
Refresh
Line
Column
Grid
Delete
Get Image
Merge
7
Similitude
80%
Group 3
Save
?
RECOM: Honeypot Eurecom Project
2600
2340
2080
1820
1560
1300
1040
780
520
260
0
2
4
6
8
10
12
14
16
18
20
22
24
26

YU: Serbia and Montenegro

- YU has contacted only one platform
- Identify the sequence of ports probed by each attacking IP
- Plot one curve per sequence of ports


List_Desc
445|
135|
135|445|
445|135|
5554|
139|
5000|135|
5000|
445|5000|135|
5000|135|445|
Others
Control
Check All
Clear All
Refresh
Line
Column
Grid
Delete
Get Image
Merge
1
Similitude
50%
Save
High similarity between two different attack tools!?
But ... ?
sources
350
315
280
245
210
175
140
105
70
35
0
4
22
41
58
74
90
106
122
141
160
177

W32.Welchia.D.Worm ???

- Exploits multiple vulnerabilities, including:
  - The DCOM RPC vulnerability using TCP port 135.
  - The Workstation service buffer overrun vulnerability using TCP port 445.
  - The Locator service vulnerability using TCP port 445
- Targets Windows XP and Windows 2000

  (Windows NT also vulnerable to the first 2 attacks)

One more viewpoint

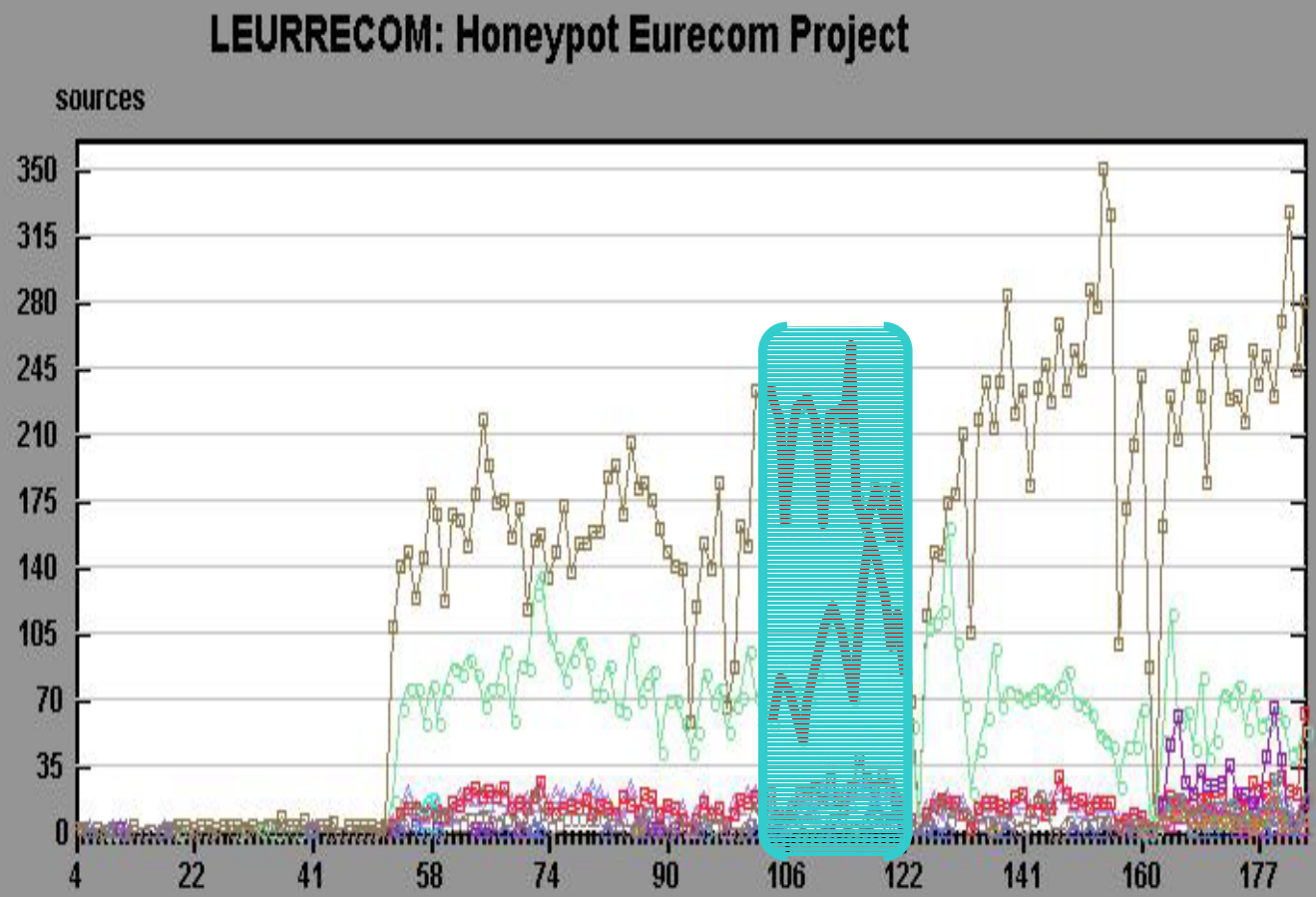
- Use passive OS fingerprinting tools (p0f, disco, ettercap) against each attacking IP.
- Plot one curve for each OS type.

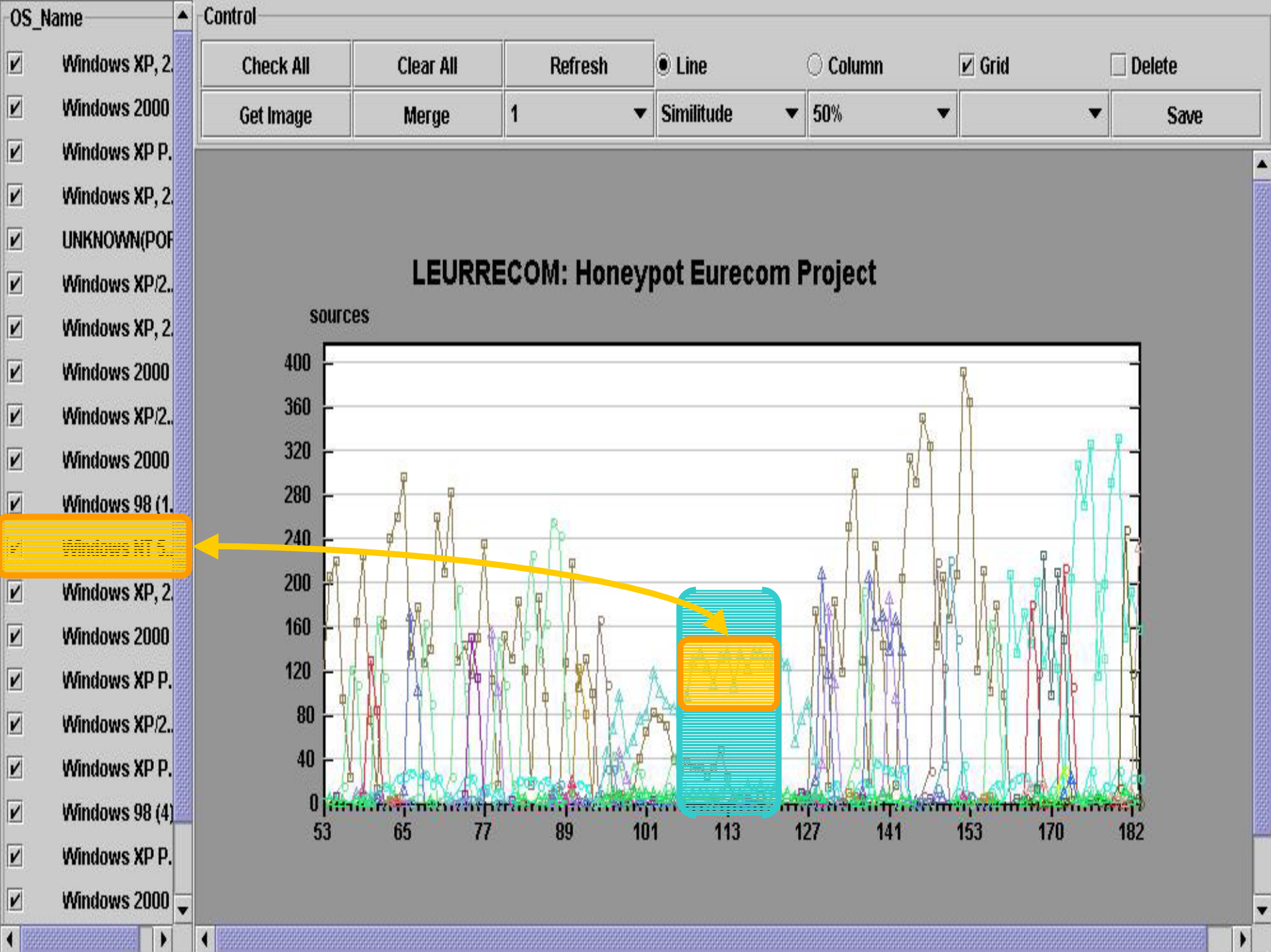
List_Desc

- [x] 445|
- [x] 135|
- [x] 135|445|
- [x] 445|135|
- [x] 5554|
- [x] 139|
- [x] 5000|135|
- [x] 5000|
- [x] 445|5000|135|
- [x] 5000|135|445|
- [x] Others

Control

Check All	Clear All	Refresh	(•) Line	( ) Column	[x] Grid	[ ] Delete
Get Image	Merge	1 ▼	Similitude ▼	50% ▼	▼	Save




OS_Name
Windows XP, 2
Windows 2000
Windows XP P.
Windows XP, 2
UNKNOWN(POF
Windows XP/2..
Windows XP, 2
Windows 2000
Windows XP/2..
Windows 2000
Windows 98 (1.
Windows XP, 2
Windows 2000
Windows XP P.
Windows XP/2..
Windows XP P.
Windows 98 (4)
Windows XP P.
Windows 2000
Control
Check All
Clear All
Refresh
Line
Column
Grid
Delete
Get Image
Merge
1
Similitude
50%
Save
LEURRECOM: Honeypot Eurecom Project
sources
400
360
320
280
240
200
160
120
80
40
0
53
65
77
89
101
113
127
141
153
170
182

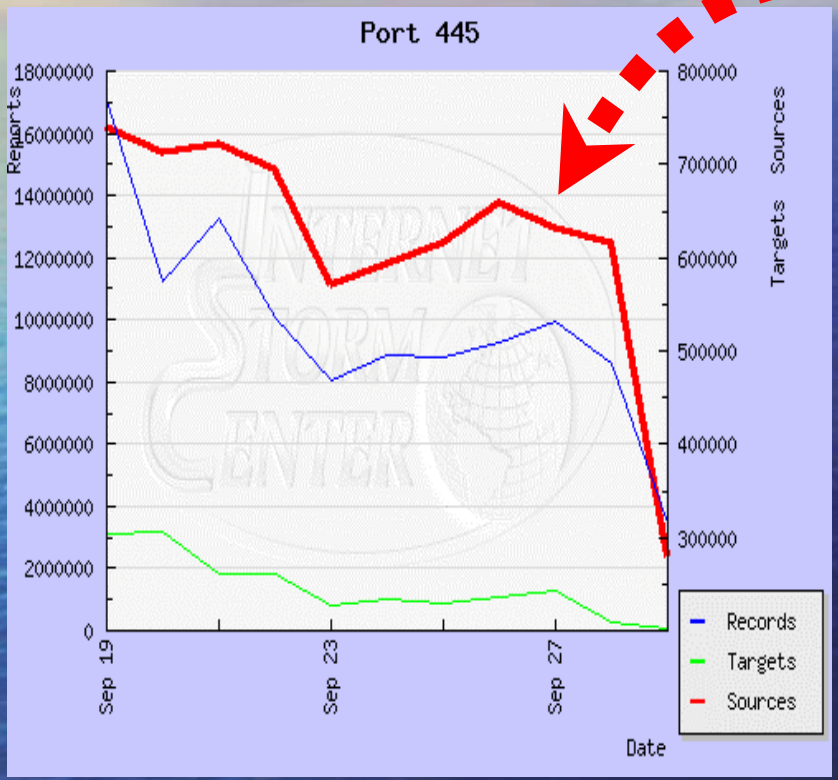
Discussion

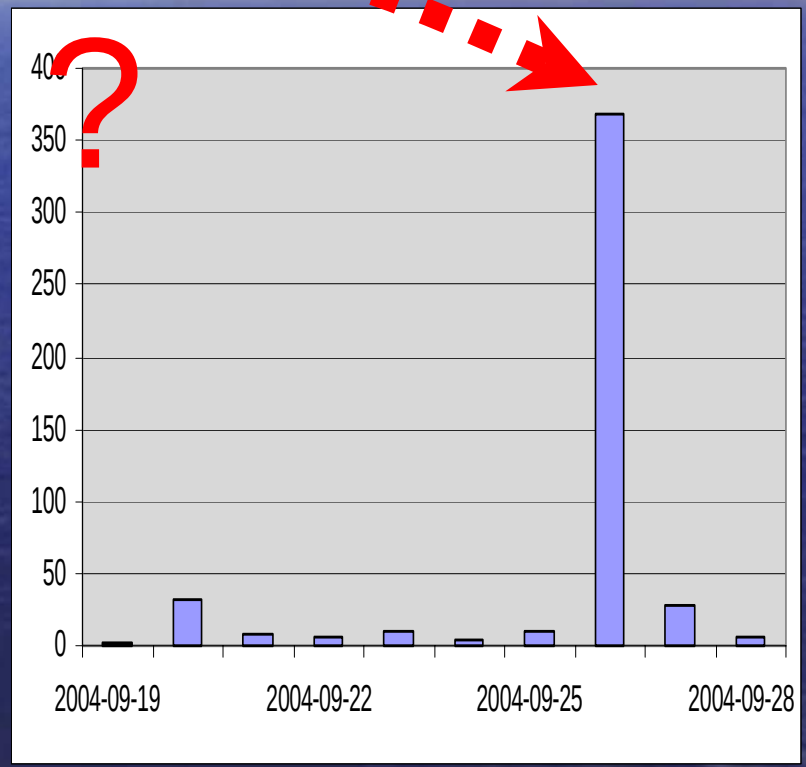
- Welchia does not seem to be the only cause of these attacks because of:
  - The bizarre peak of attacks coming from NT boxes
  - The fact that only one platform is targeted by this country
- Are there attackers ‘surfing’ on the traces of other attacks in order to hide themselves?
- More research is required.

Overview

- Leurré.com: why and how
- Web interface: a few examples
- Some ‘non trivial’ results.
- Conclusions

ISC (Dshield) Limitations



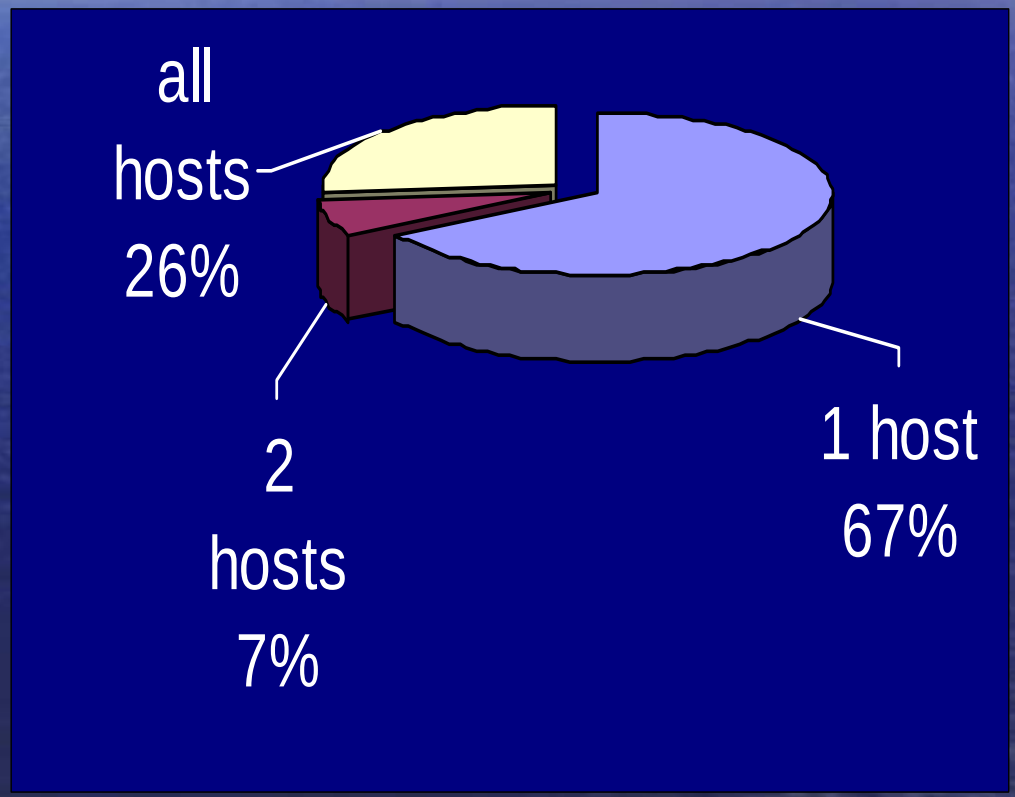


Source: Internet Storm Center

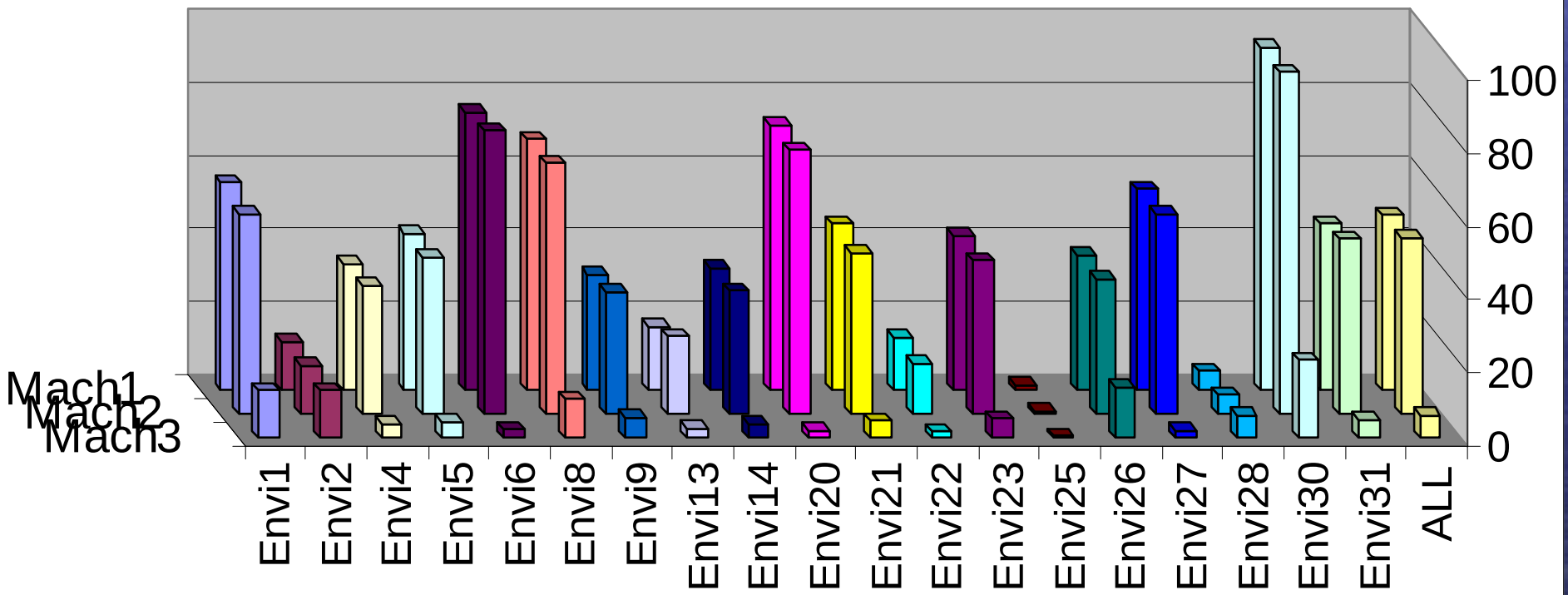
Source: Leurré.com

During the last 6 months

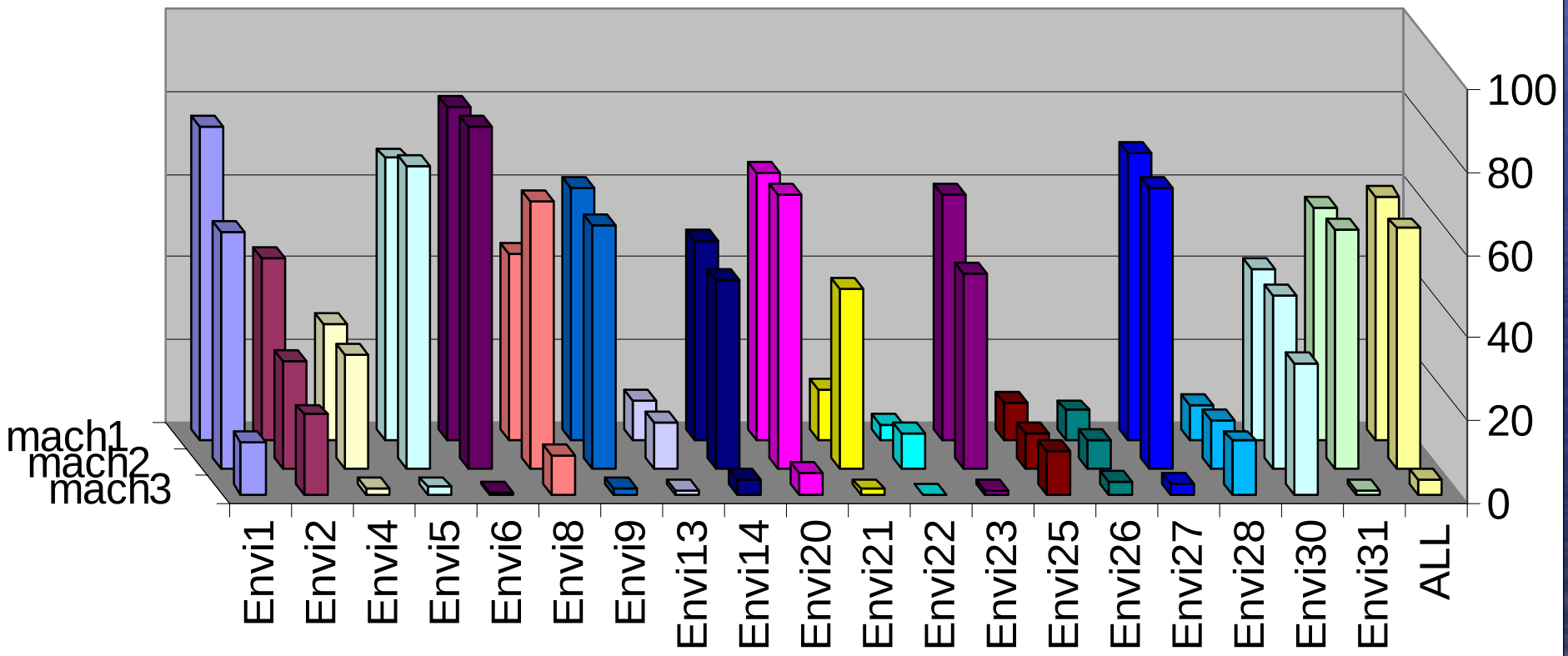
- 345718 IPs have probed only 1 host per platform
- 36287 have probed only 2 hosts per platform
- 136331 IPs have probed all hosts of a given platform



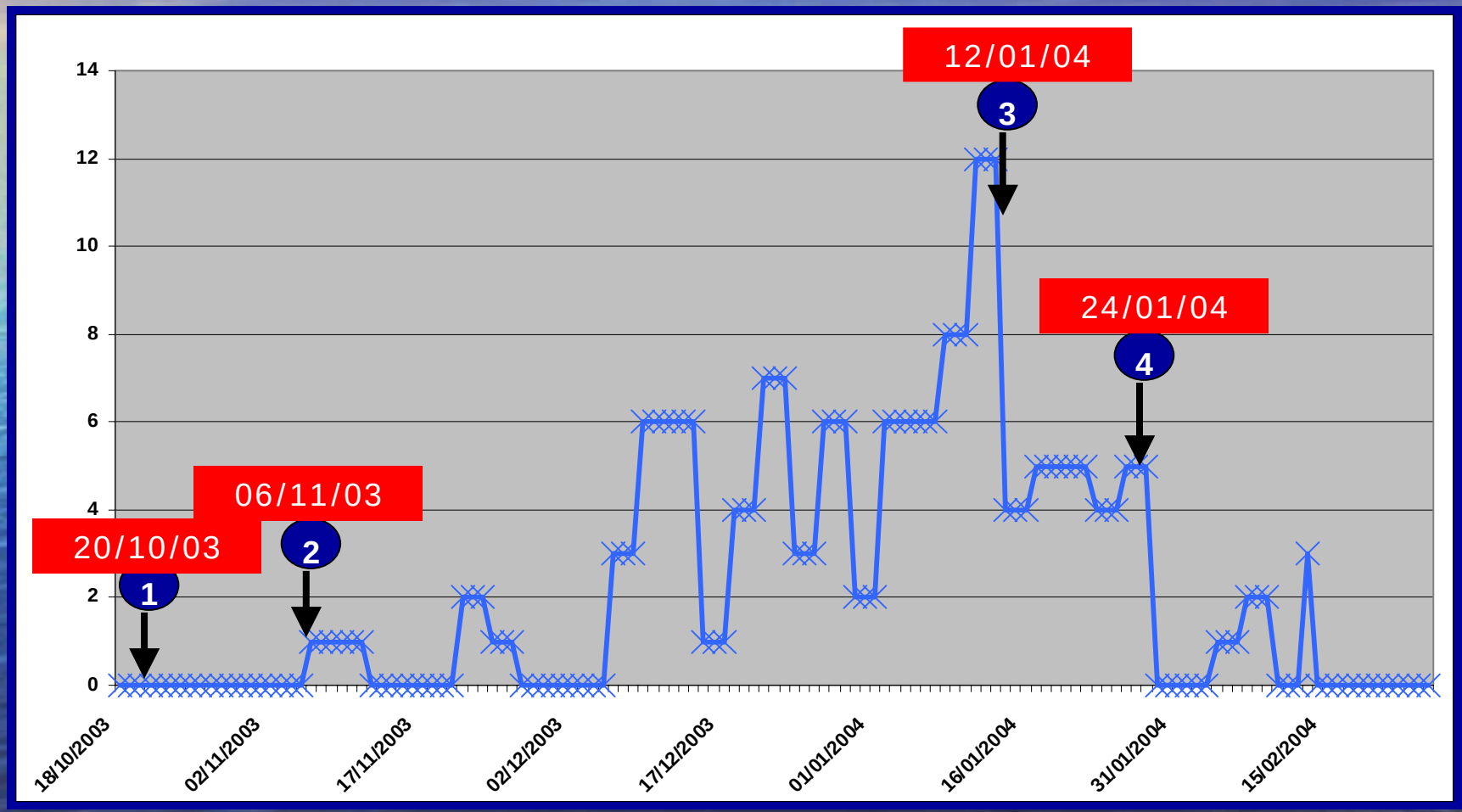
P(sending a packet to an open port) for an attacker who sends packets to all machines of a given environment



P(sending a packet to an open port) for an attacker who sends packets to only one machine of a given environment



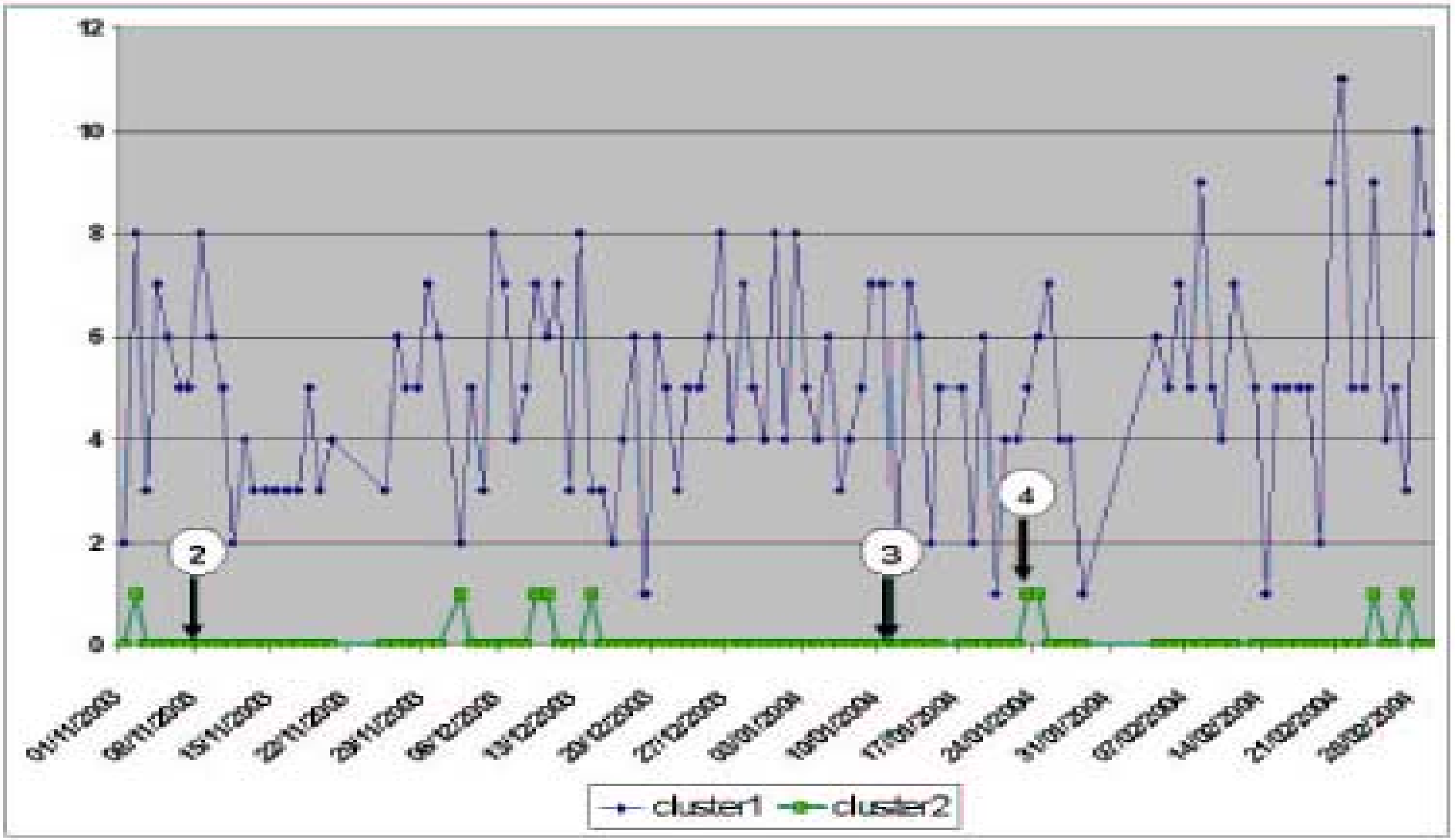
Targeted attacks: Port 1433 example



Results: identification of the scanner

- 5 different types of scans have probed that port between point 1 and point 2
- Only 2 of these 5 have been observed between point 3 and 4.
- The scanning tool is quite likely one of these two.

Results: identification of the scanner (ctd.)



Overview

- Leurré.com: why and how
- Web interface: a few examples
- Some ‘non trivial’ results.
- Conclusions

Conclusions

- Experience shows that this data set is a gold mine for researchers.
- It can provide the foundations to build a new generation of early warning information systems
- We, at Eurecom, can only take advantage of a fraction of it.

We need you ...

- ... to deploy more platforms in Asia Pacific.
- ... to see other teams carrying out their own research with our data sets.
- ... to build a truly international cooperative environment to fight Internet threats.

Contact: dacier@eurecom.fr

References

- F. Pouget, M. Dacier, “Honeypots-based Forensics”, *Proc. Of the AusCERT2004 Conference* (refereed stream), May 23-27 2004, Brisbane, Australia.
- M. Dacier, F. Pouget, H. Debar, “Attack Processes found on the Internet”, *Proc. NATO Symposium on Adaptive Defense in Unclassified Networks*, April 2004.
- M. Dacier, F. Pouget, H. Debar, “Honeypots: Practical Means to Validate Malicious Fault Assumptions on the Internet”, *Proc. 10th IEEE International symposium Pacific Rim Dependable Computing (PRDC10),*March 2004, pages. 383-388.

Exhaustive and up to date list of publications available at
http://www.eurecom.fr/~pouget/papers.htm