Leurré.com: a worldwide distributed honeynet, lessons learned after 4 years of existence

M. Dacier
Director Symantec Research Labs Europe

marc_dacier@symantec.com

Foreword

- **M. Dacier joined Symantec on the first of April 2008 as the director of Symantec Research Labs Europe.**
  - » These slides present work done with partners while he was at the Eurecom Institute.
  - » The views expressed here are the ones of the author and are not necessarily shared by Symantec

Overview

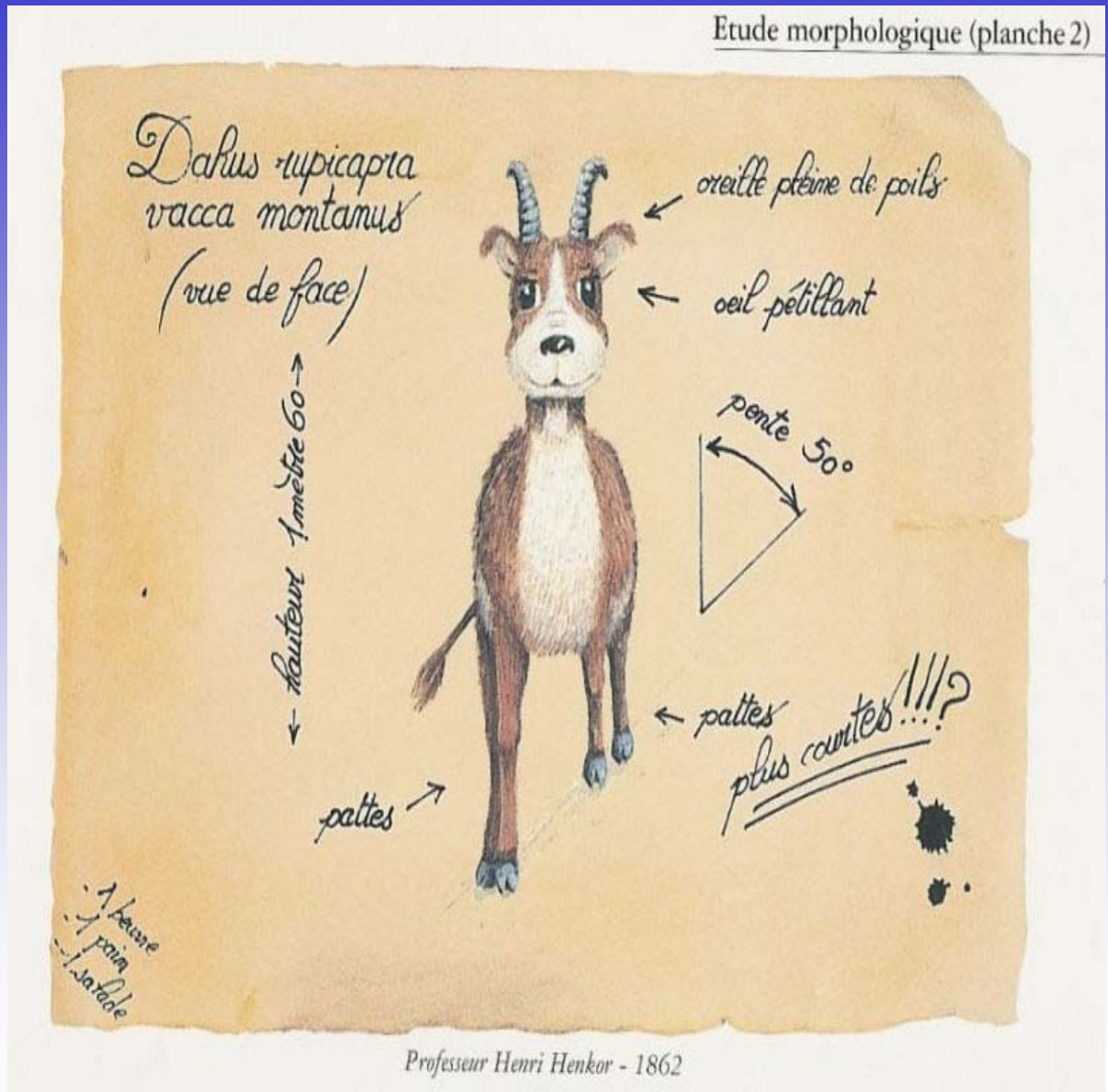
- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

Overview

- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

Dahu: definition

- **“The Dahu is an extremely shy animal living in the Alps of France and Switzerland.[…] It has adapted to its steep environment by having legs shorter on the uphill side and longer on the downhill side […] “**
  - “The Dahu, An endangered Alpine species”, Science, 2568, November 1996, pp.112:
  - http://www.vidonne.com/html/dahu-reignier.htm



symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

Food for thoughts …

- **Dahus are rare, bizarre, stimulating from an intellectual point of view but ...**
  - » Does it justify the existence of *Dahusian research*?
  - » How can we make sure we are not building tools against *Dahusian hackers*?
  - » How can we avoid inventing *Dahusian solutions*?

Data, data and more data

- **Experimental validation is at the core of every scientific discipline.**
  - » Computer security should not be different
  - » Data collected in a rigorous way may reveal interesting actionable knowledge

Overview

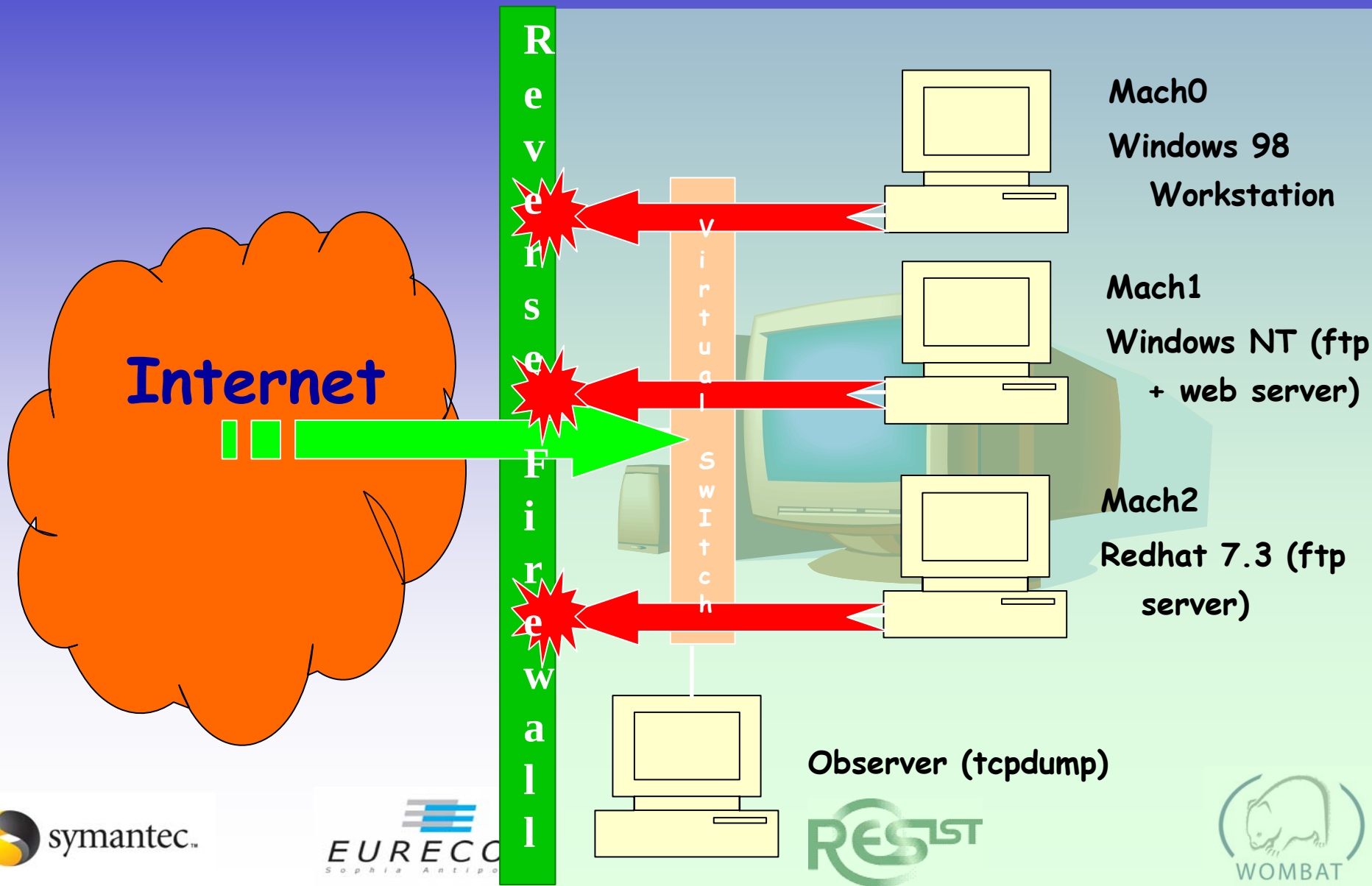
- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

Leurré.com V1.0

- **Ongoing effort since 2003**
  - » Almost 50 platforms in 30 countries today
  - » Uses low interaction honeypot (based on honeyd)
  - » Stores all enriched tcpdump (os fingerprinting, geographical location, etc.) in an Oracle DB open to all partners.
  - » Collection of tools, interfaces (java, matlab, python, etc.) and documentation available for free to all partners.

symantec. EURECOM Sophia Antipolis RESIST WOMBAT

Experimental Set Up (based on honeyd)



symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

50 sensors in 30 countries (5 continents)

Win-Win Partnership

- **The interested partner provides …**
  - » One old PC (pentiumII, 128M RAM, 233 Mhz…) and 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 GUI and a wiki (over https) + an automated alerting system

Leurré.com V1.0: Lessons learned (1/3)

- **Leurré.com, a collaborative effort:**
  - » Partially funded by the European RESIST NoE (*www.resist-noe.org*)
  - » Key element of the new European WOMBAT Project.. (*www.wombat-project.eu*)
  - » More information is available in the publications listed on the *www.leurrecom.org* web page.

Leurré.com V1.0: lessons learned (2/3)

- **Data used in this presentation:**
  - » Collected between March 14, 2004 and March 14, 2008
  - » Aggregated on a monthly basis.
  - » Names and localizations of the platforms have been anonymized (as imposed by the NDA).
  - » Available by means of dynamic applets at *www.leurrecom.org* after the conference.

Leurré.com V1.0: lessons learned (3/3)

1. **The observed attack strategy**

2. **Safe havens**

3. **Good and bad neighborhoods**

Reality vs. Representation

"*This is not a pipe*"

René Magritte (1898-1967)

symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

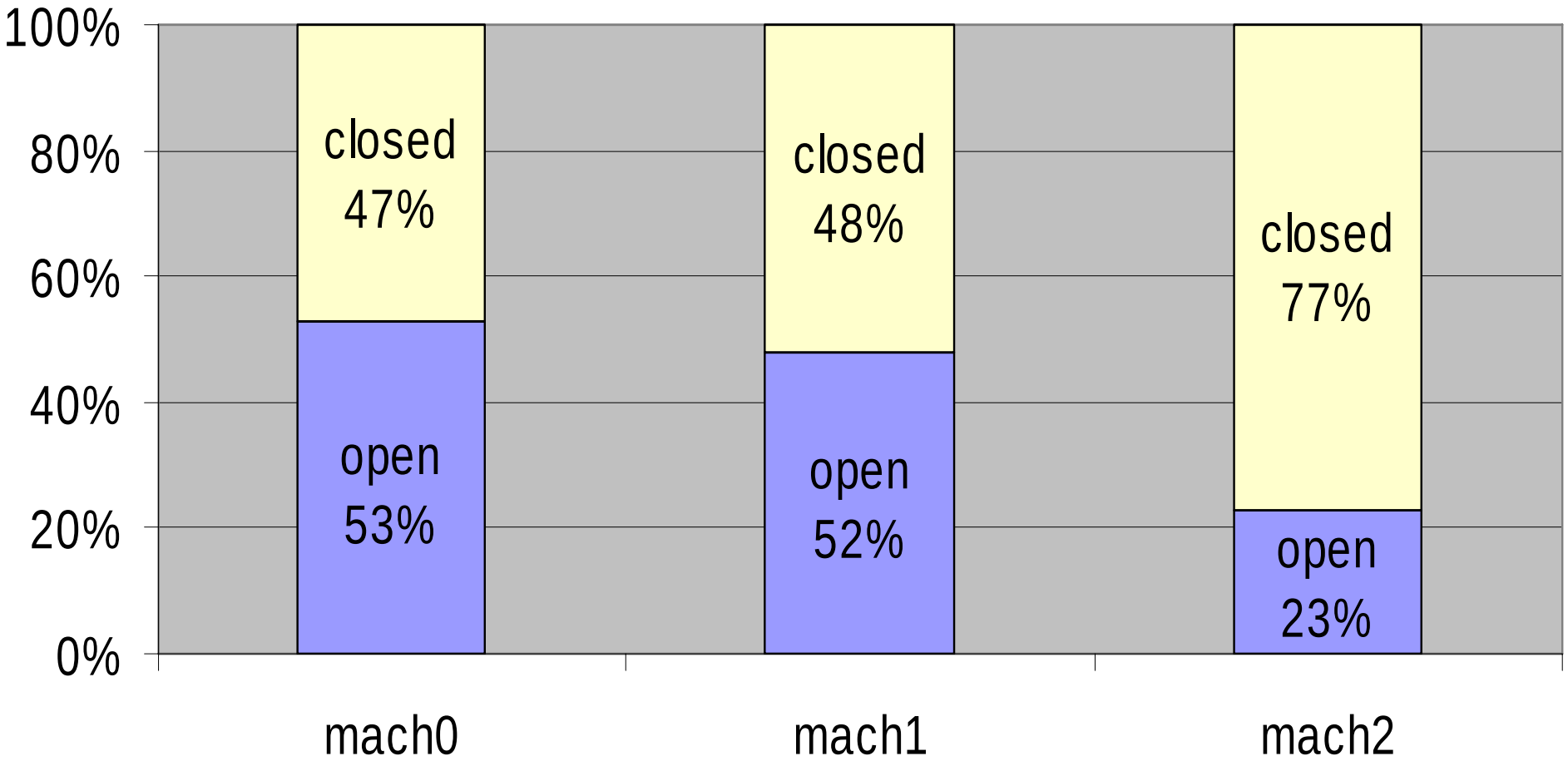
1. The observed Attack Strategy

- **Different groups of compromised machines are used for specific tasks.**
  - » Some do scan the network without attacking anyone
  - » Others do take advantage of this accumulated knowledge to attack vulnerable targets.

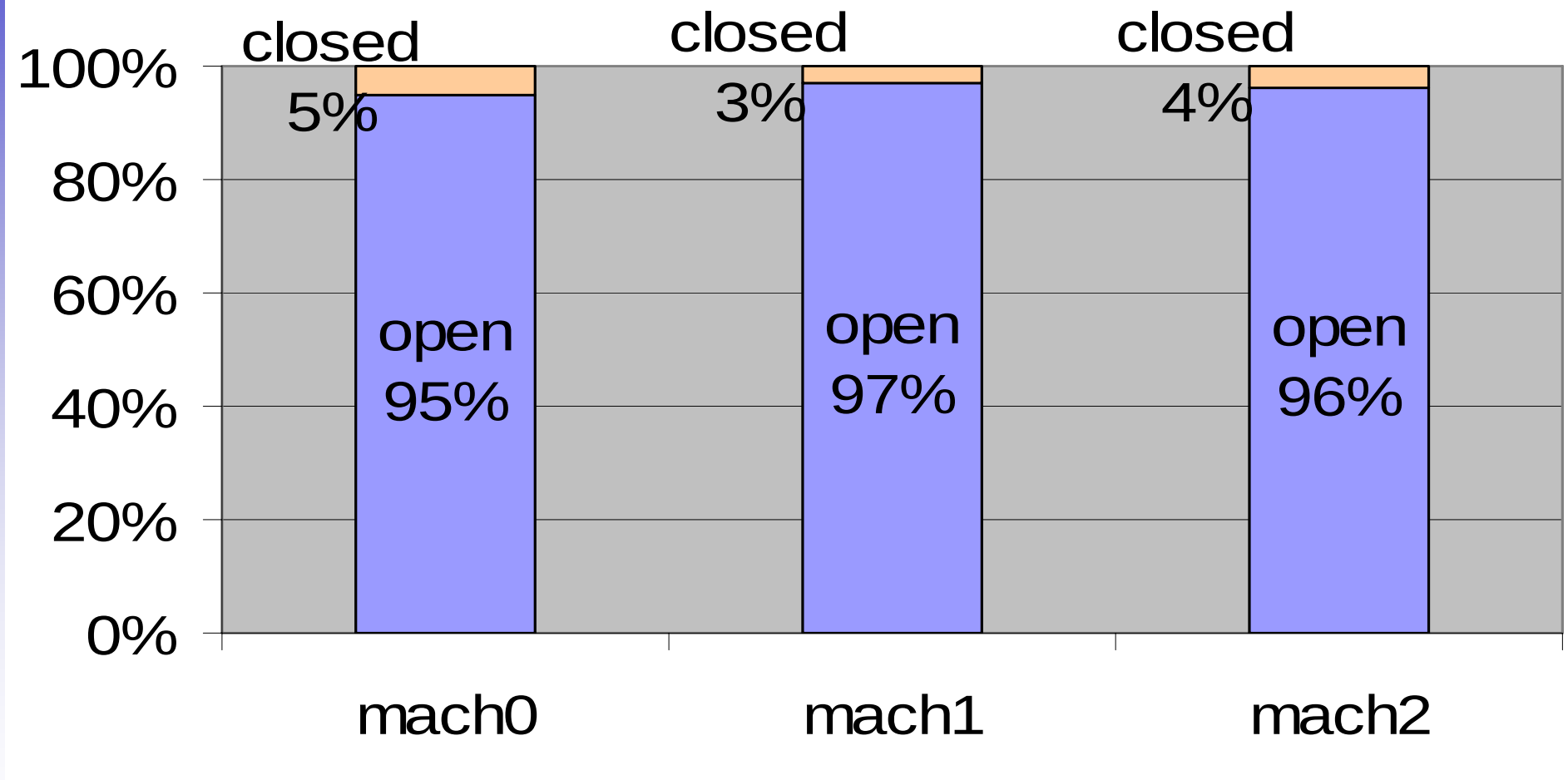
1. The observed attack strategy (ctd.)

- **Once a human being eventually logs into a compromised machine, this is achieved from a third, distinct, set of machines.**
  - » In the ssh experimentation carried out with LAAS-CNRS (E. Alata et al.), all of these machines came from a specific country, Romania.

« Scanners »


100%
80%
60%
40%
20%
0%
closed
47%
open
53%
closed
48%
open
52%
closed
77%
open
23%
mach0
mach1
mach2

« Attackers »



symantec.

EURECOM
Sophia Antipolis

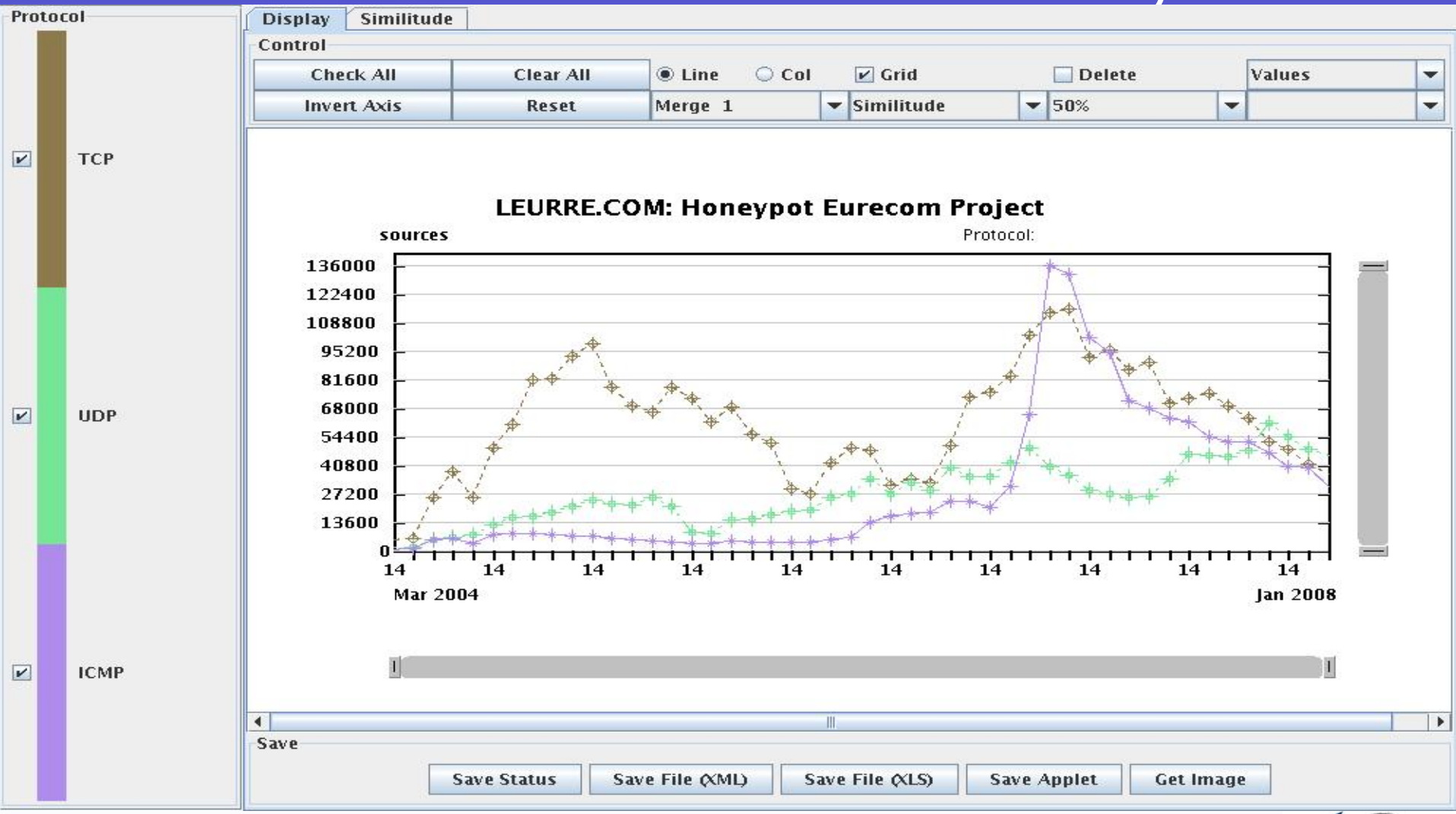
RESIST

WOMBAT

The changing observed attack strategy

- **A supplementary step seems to have emerged:**
  - » ICMP scans precede the two other steps.
  - » New *modus operandi* has appeared rapidly, worldwide.
- **Actionable Knowledge:**
  - » Machines that do not respond to ICMP echo packets will be less attacked than others
  - » Early discovery of “pingers” and/or “scanners” help protecting your network.

ICMP vs TCP vs UDP over the last 4 years



symantec.

EURECOM
Sophia Antipolis

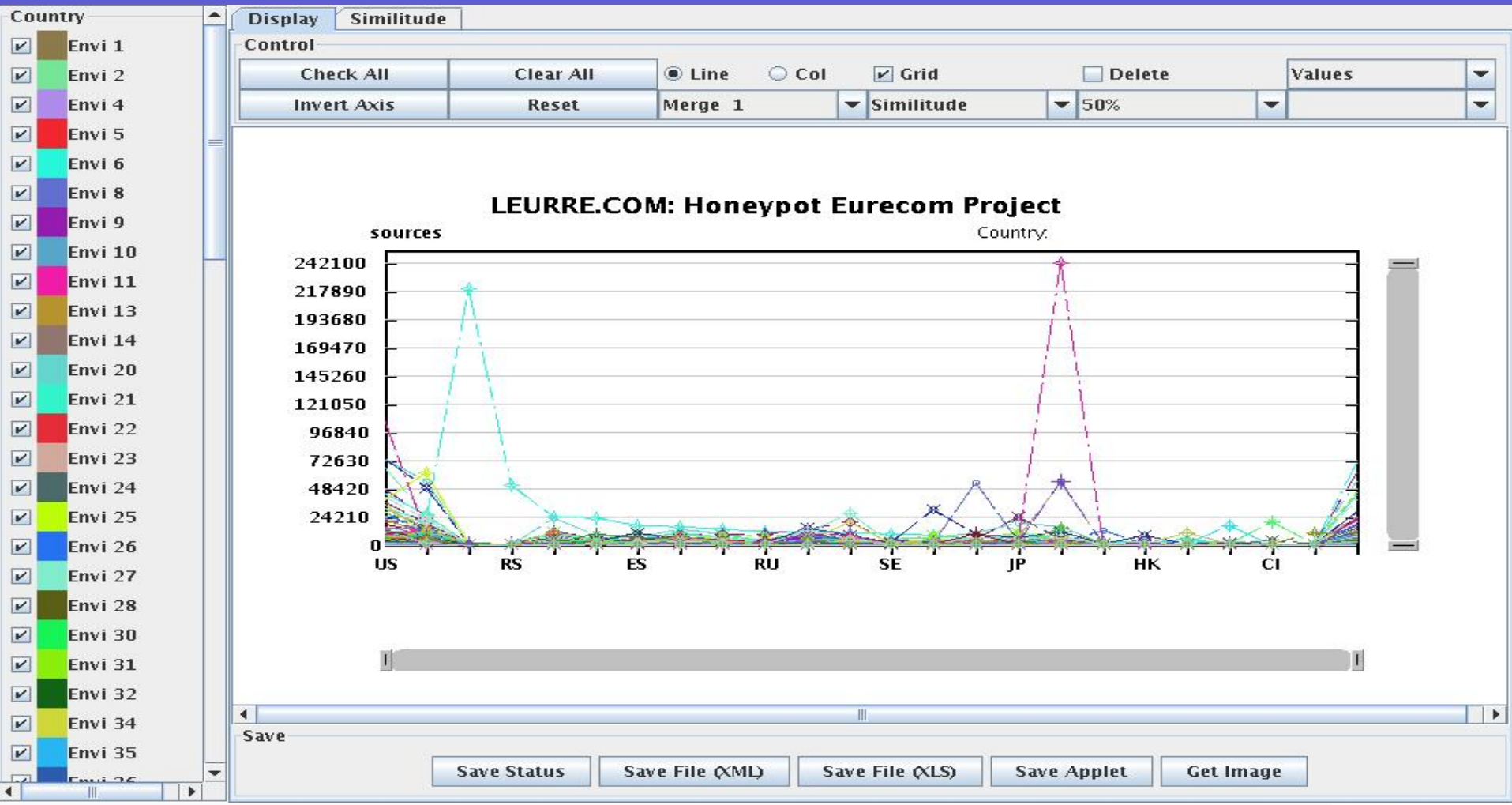
REGIST

WOMBAT

2. Safe Havens

- **Some attacks do come from a very limited number of countries**
  - » sometimes from only one
  - » They target a, sometimes very, small fraction of the Internet
  - » This is not limited to the ssh case explained before.
- **Actionable knowledge:**
  - » Enables “behavior-based” protection paradigms.

Platforms targeted by country of origin



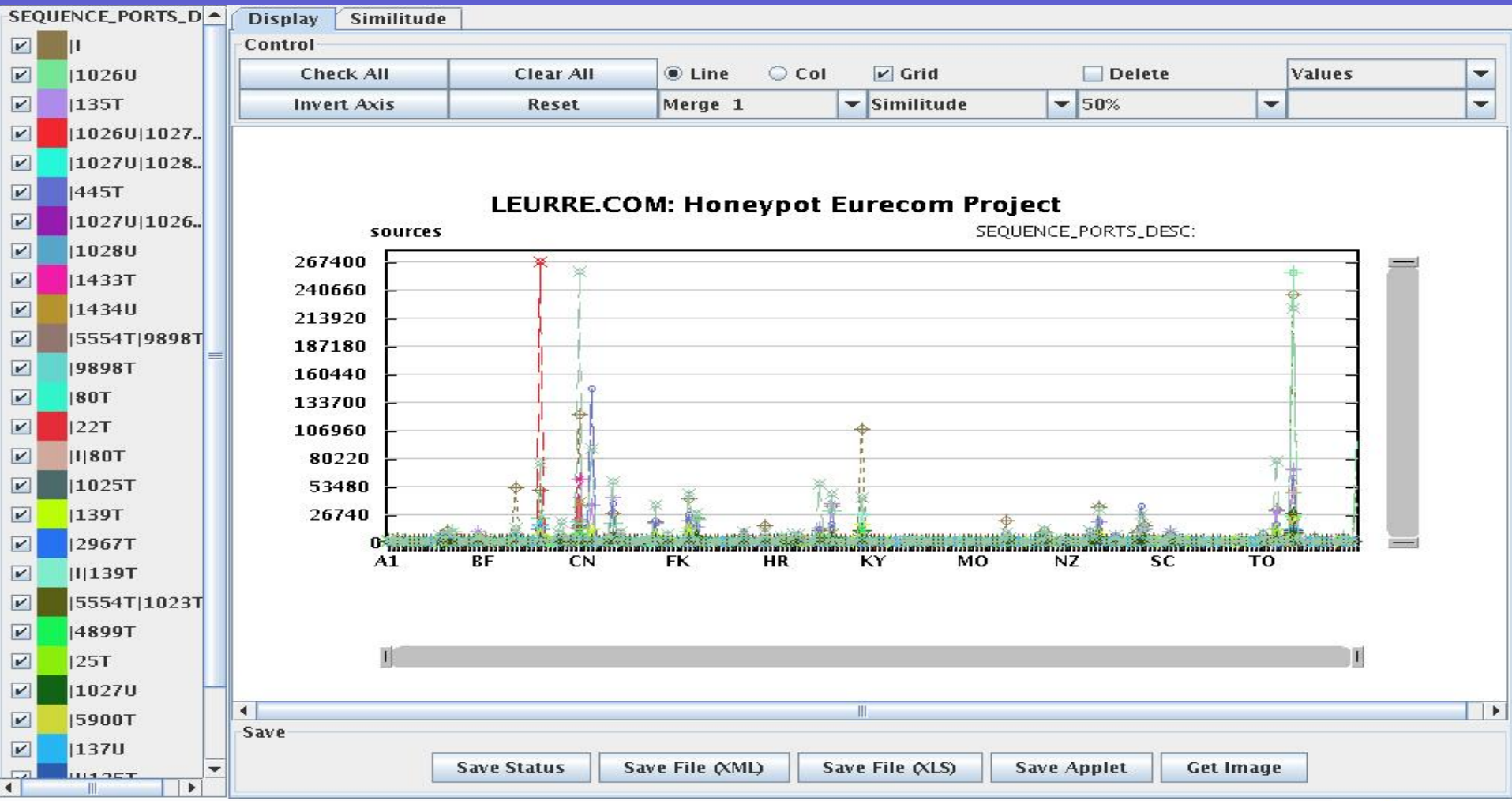
symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

Ports sequence targeted by country of origin



symantec.

EURECOM
Sophia Antipolis

REGIST

WOMBAT

3. Good and bad neighborhoods

- **Your IP matters:**
  - » The amount of attacks is more a function of *where* you are than of *who* you are.
  - » Other sites in the same environment exhibit similar attack profiles as yours
- **Actionable knowledge:**
  - » Pick the quieter places for your servers
  - » Others can tell you if you are subject to a targeted attack

Overview

- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

Leurrécom V2.0, SGNET: Goals

- **Continue the conversation with the attacker up to the point where a malware is downloaded (resp. uploaded).**
- **Avoid using high interaction honeypots**
- **Data collected with V2.0 enrich the ones obtained with V1.0**

Means

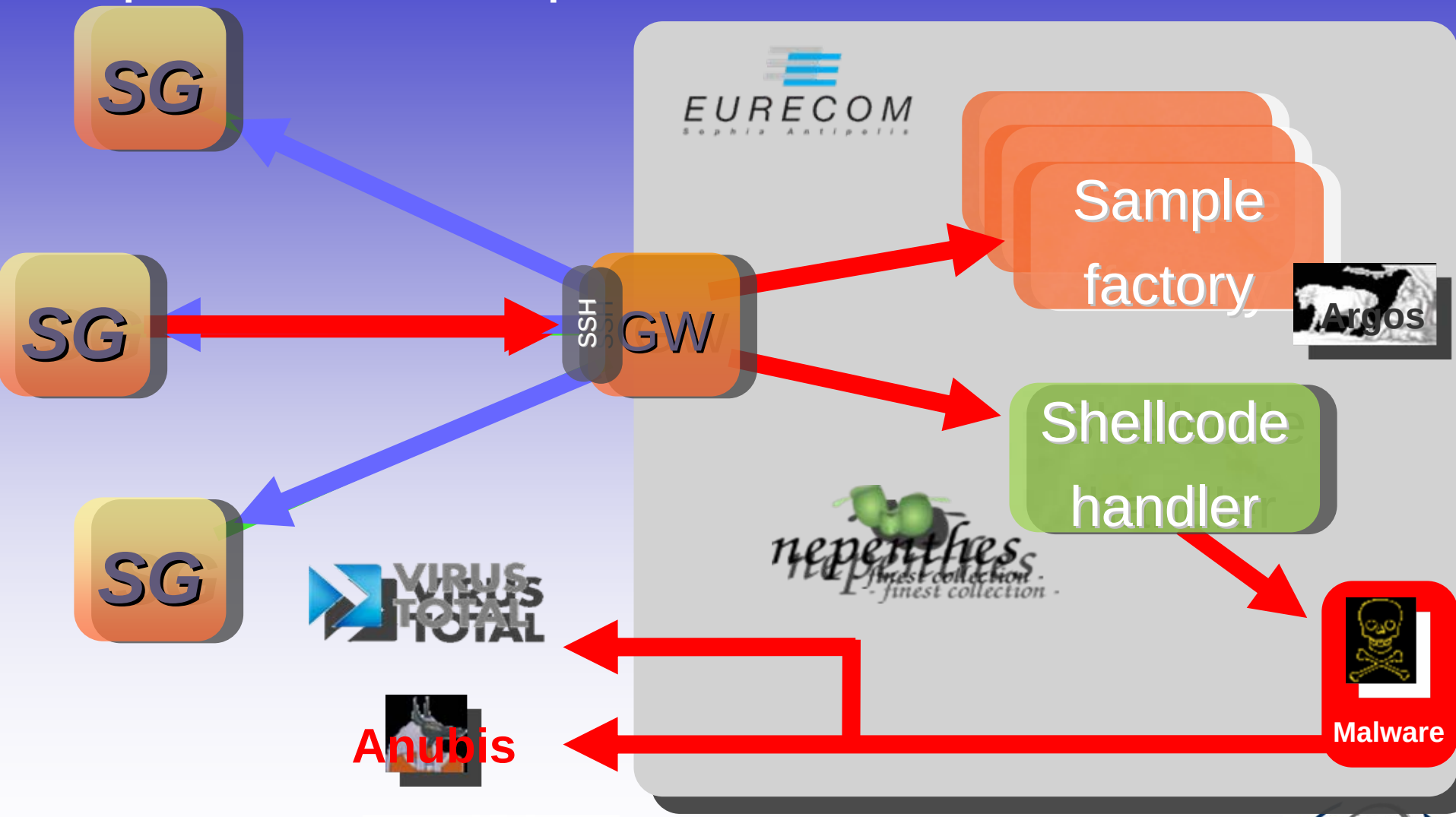
- **Scriptgen: a novel 'medium-interaction' honeypot**
- **SGNET =**
  - Scriptgen (Eurecom) +
    Argos (VU Amsterdam) +
    Nepenthes (TU Manheim) +
    Anubis (TU Wien) +
    Virustotal (Hispasec).

symantec. EURECOM Sophia Antipolis RESIST WOMBAT

Scriptgen

- **Basic idea** (see ACSAC05, RAID06, NOMS08, EDDC08)**:**
  - » Learn protocol semantics from the interactions with a real server
    - – Represent learnt behavior in a state machine
  - » Protocol agnostic approach
    - – No assumption is done neither on protocol structure, nor on its semantics.

Operational setup



symantec.

EURECOM

RESIST

WOMBAT

Current status

- **A couple of SG sensors deployed to study the feasibility of the approach.**

- **Important contribution to the newly funded WOMBAT European project.**

symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

Overview

- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

IST-216026-WOMBAT

- **Worldwide Observatory of Malicious Behaviors and Attack Threats**
- **3 Years research project**
- **See *www.wombat-project.eu* for more information**

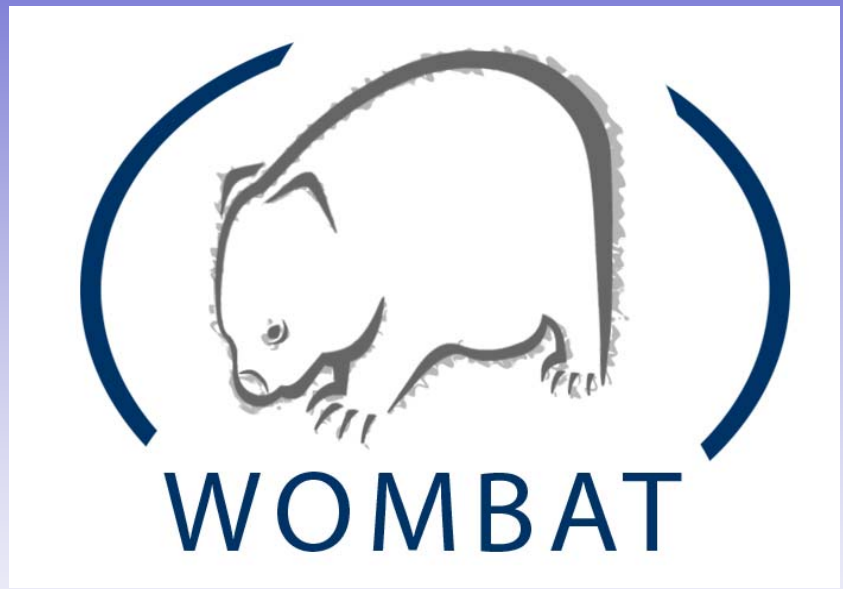
symantec.

EURECOM
Sophia Antipolis

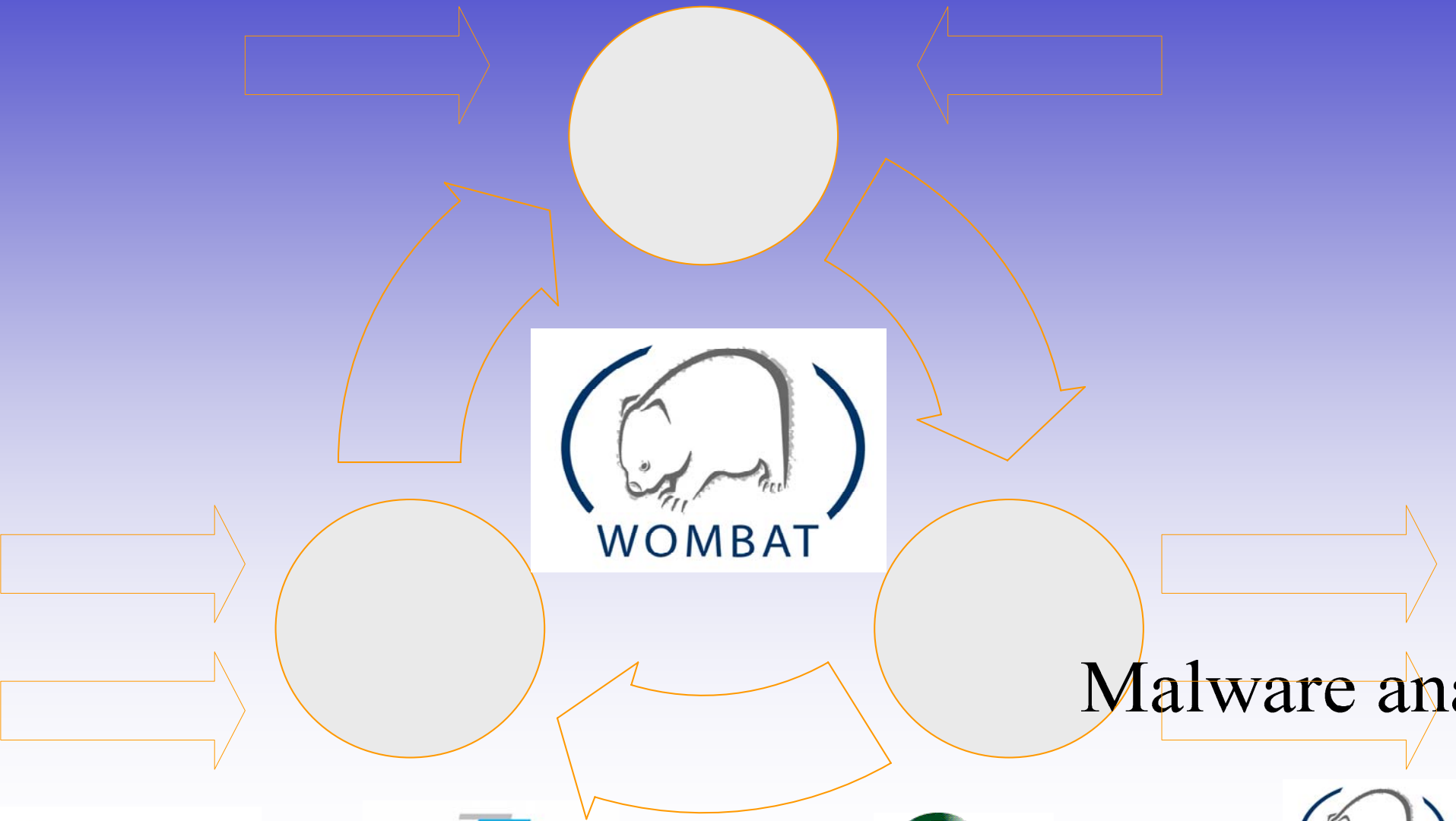
RESIST

WOMBAT

The WOMBAT Consortium



Main objectives and principles



symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

Project results and innovation

- **New data gathering tools**
  - » Advanced features (high interaction, real-time analysis)
  - » New targets (wireless, bluetooth, RFID, …)
- **Tools and techniques for characterization of malware**
  - » Malware-based analysis AND Contextual analysis
- **Framework and tools for qualitative threat analysis**
  - » Early warning systems

symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

The WOMBAT is welcoming you

- **The philosophy of the WOMBAT project is to join forces to address the current and future threats**
- **If you are interested in being involved in this effort or in learning more about it, feel free to contact me:**
  - marc_dacier@symantec.com

symantec.

EURECOM
Sophia Antipolis

RESIST

WOMBAT

Overview

- **Introduction**
  - » Leurré.com V1.0 set up and lessons learned
  - » Leurré.com V2.0 set up
  - » WOMBAT
- **Conclusions**

Data, data and more data

- **Collecting threats-related data all over the world in such a way that a systematic and rigorous analysis can be carried out is a key element to help us all fight cybercrime as it leads to the discovery of actionable knowledge.**

Data, data and more data (ctd.)

- **The Leurrécom dataset has contributed to this task over the last four years.**
- **Trends are changing and highlight the need for novel sources of data**
- **The WOMBAT project is looking forward to address these issues. Feel free to be part of it.**

Questions ?