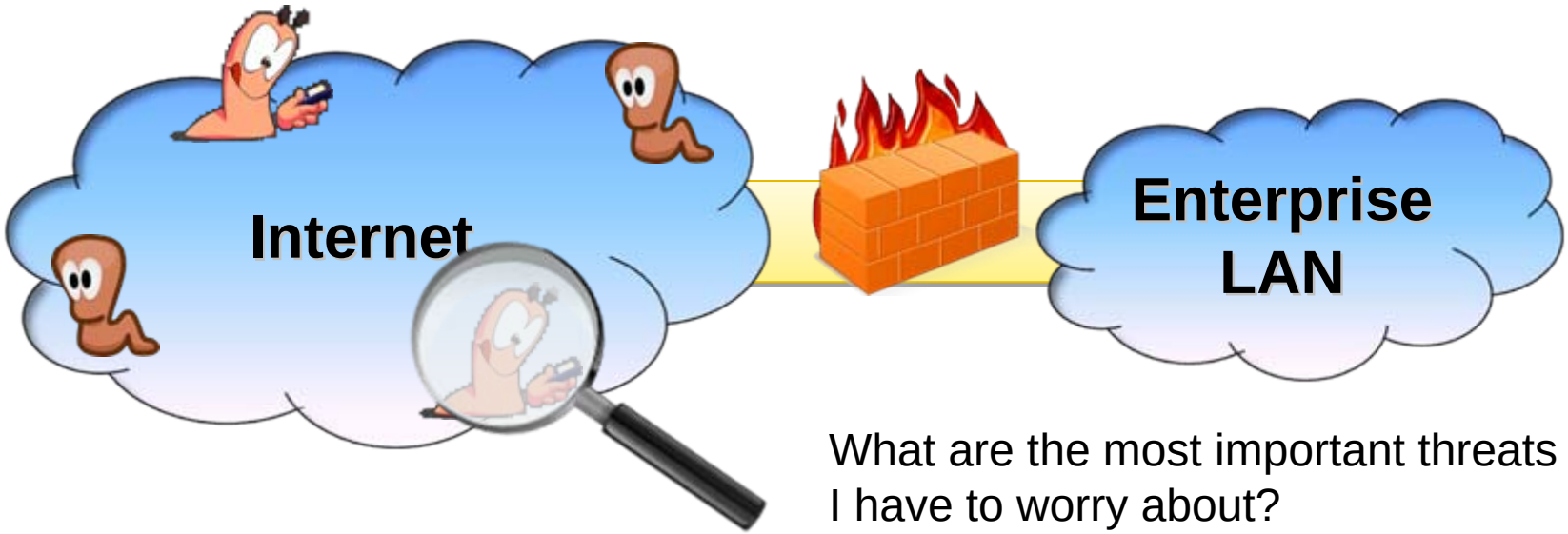
Lessons learned from the worldwide deployment of SGNET in the WOMBAT Project

Corrado Leita, Symantec Research

corrado_leita@symantec.com

WOMBAT

Data collection to improve our understanding



What are the most important threats I have to worry about?

How well am I protected?

Need to acquire intelligence On Internet Threats

A Worldwide Observatory of Malicious Behaviors and Attack Threats

EURECOM
Sophia Antipolis

Hispasec Sistemas
Seguridad y Tecnologías de la Información

NASK

symantec™

Institute for Infocomm Research
A*STAR

TU VIENNA
Technische Universität Wien
Vienna University of Technology

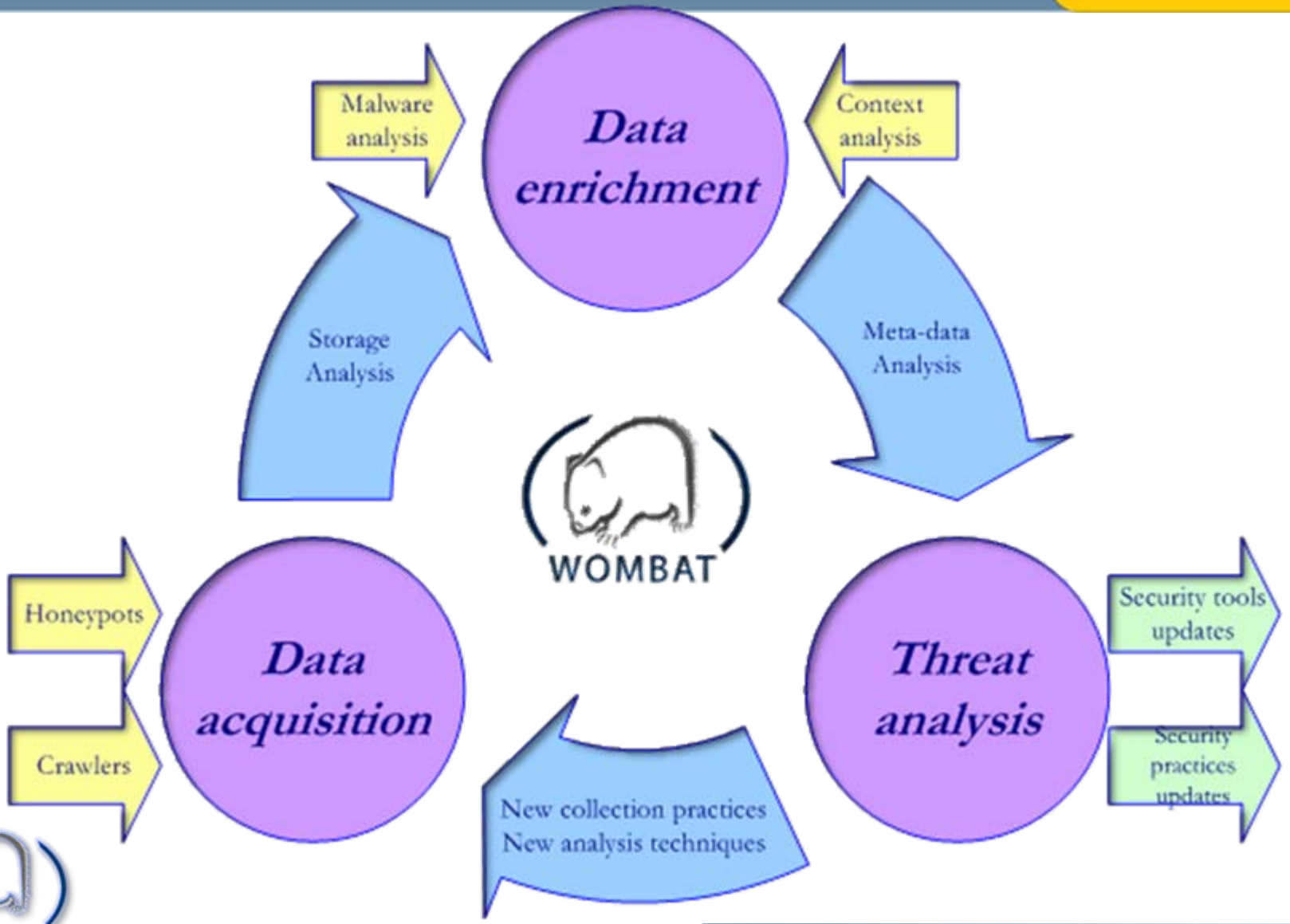
orange™

POLITECNICO MILANO

FORTH
Foundation for Research & Technology - Hellas

vrije Universiteit

WOMBAT


Malware analysis
Data enrichment
Context analysis
Storage Analysis
Meta-data Analysis
WOMBAT
Honeypots
Crawlers
Data acquisition
Threat analysis
Security tools updates
Security practices updates
New collection practices
New analysis techniques

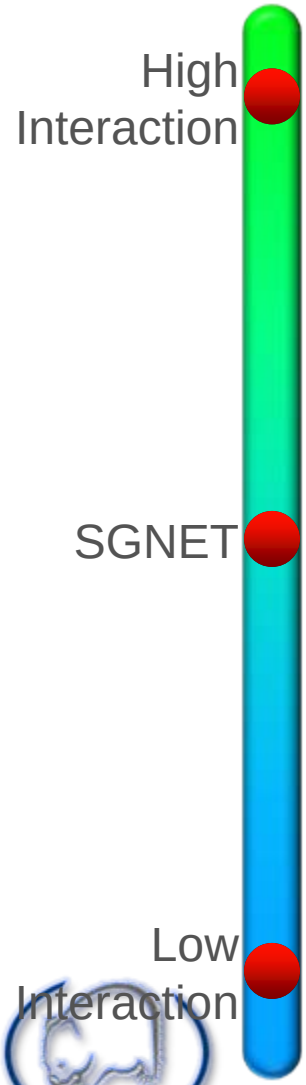
SGNET

- Distributed honeypot deployment for the analysis of server-side code injection attacks
  - Result of the integration of different tools produced by the Wombat participants (EURECOM, TU Vienna, VU Amsterdam, HispasecSystemas)
- Honeypot sensors distributed over the whole Internet
  - Deployed by volunteering partners
  - WIN-WIN partnership: hosting a sensor, the partner receives access to the whole data
  - Non-Disclosure Agreement to protect the identity of the participants and of the attackers

What is SGNET?

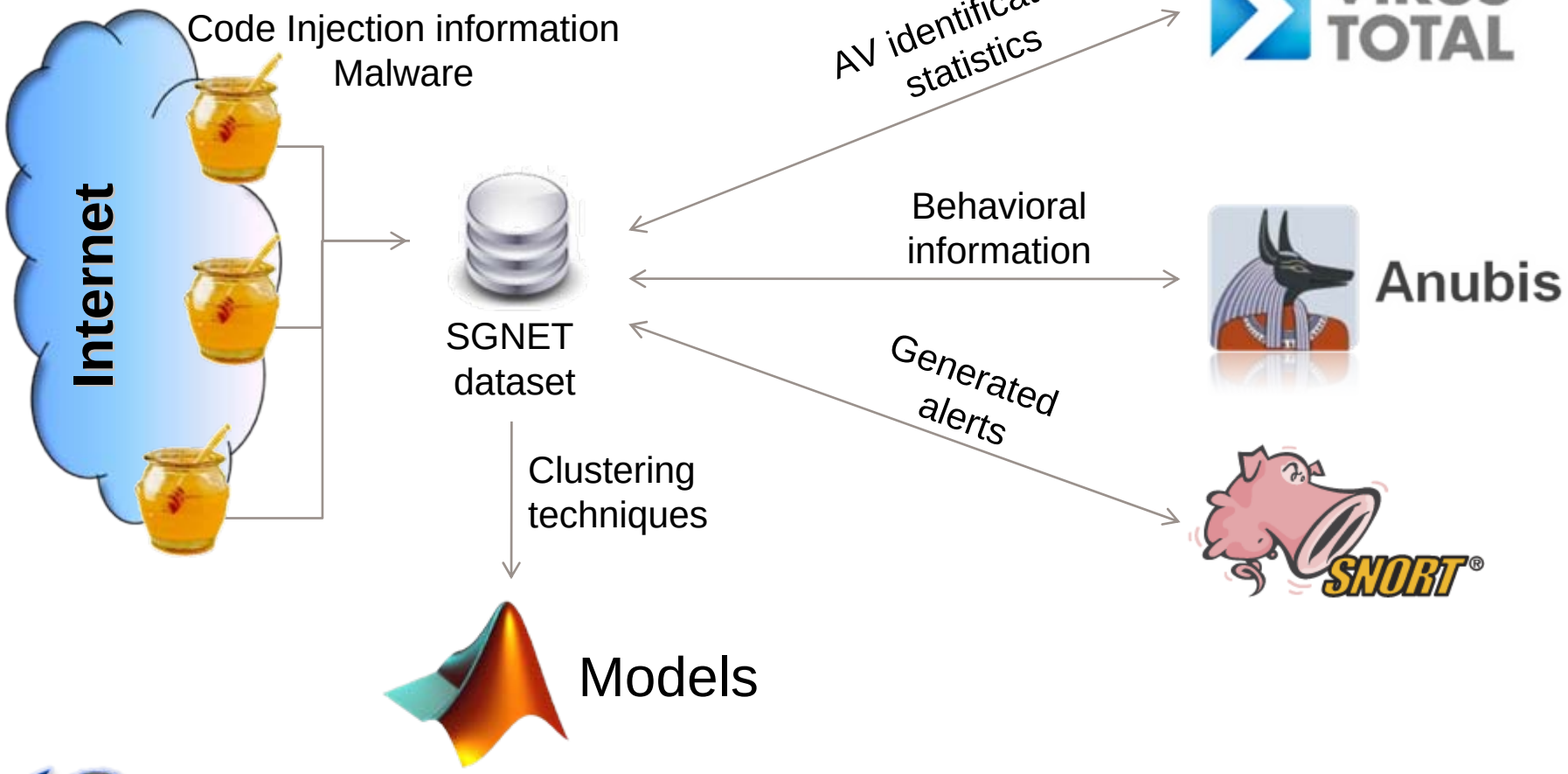
- SGNET is a “meteorological service” for Internet attacks

What makes SGNET different?



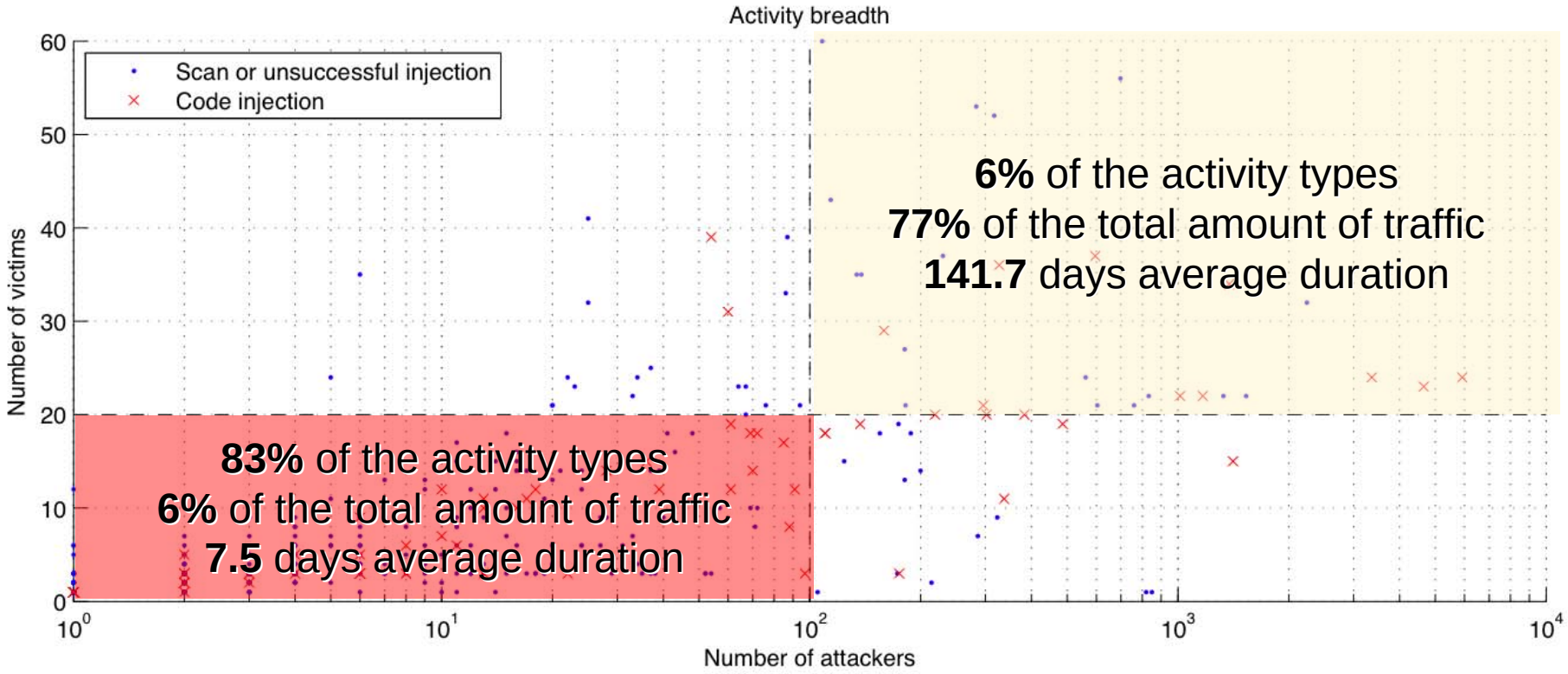
- Need to increase level of interaction
  - Required to retrieve information on the root cause of the observed activities
- Need to minimize the cost of the sensors
  - Implicit requirement of a distributed deployment of sensors hosted by volunteering partners

Data collection and enrichment

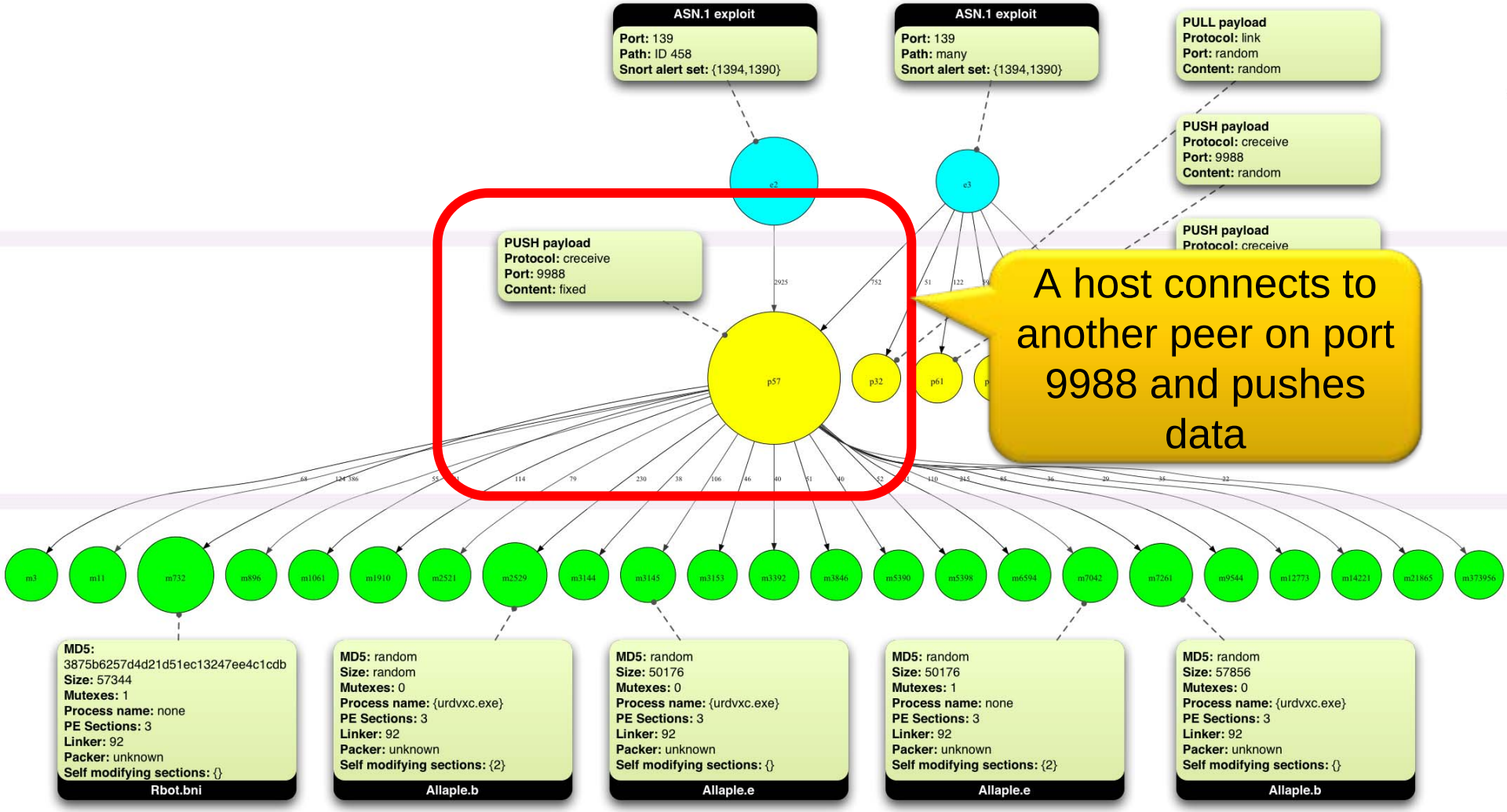


A frightening picture

- Each different activity type is plotted according to the number of involved attackers and victims (its “size”)



Studying the malware ecosystem



Threats and economy

- We need to understand the “underground economy”
- Revenues
  - Phishing/spam campaigns
  - Botnets
  - …
- Costs
  - Sophistication
  - Development of new exploits
  - …?

- Can we “attack” the ROI?

There is more

- The “Future Internet” will be different from nowadays Internet
- We will need to face different patterns and develop new strategies
- How will these changes impact the “underground economy”?
- Some food for thoughts:
  - Highly connected mobile devices: new threats?
  - IPv6: no more NAT?
  - Cloud computing, or better “outsourcing”:
    - New data confidentiality problems
    - Larger scale of what we are starting to see now with social networks

Joining SGNET

- Contact: **corrado_leita@symantec.com**
- What is needed
  - 4 routable IP addresses
  - An old host
    - At least Pentium II, 256 MB RAM, 1GB Hard Disk
  - Non-Disclosure Agreement
    - Protects identity of the participants to the project
- What you get
  - Access to the whole dataset
  - Wiki for sharing interesting results
  - Data mining tools
  - Web interface (demo at http://www.leurrecom.org/event2/index.html)

Thank You!

CorradoLeita

Corrado_Leita@symantec.com

© 2007 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.