Tracing Cyberattacks on the Internet

Evangelos Markatos
FORTH-ICS
markatos AT ics.forth.gr

http://www.ics.forth.gr/dcs/
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
and
Department of Comp. Science, University of Crete

Roadmap

- Who we are
- What do we do?
  - Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - Internet Safety
    - Safer Internet Access for children
  - Contribution to Security Policy
    - ENISA
    - FORWARD

Roadmap

- Who we are
- What do we do?
  - Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - Internet Safety
    - Safer Internet Access for children
  - Contribution to Security Policy
    - ENISA
    - FORWARD

Who we are: People

DCS

http://www.ics.forth.gr/dcs

- Distributed Computing Systems Lab
  - Created in 2004
  - 30 people
    - 6 Ph.Ds, 10 M.S., 10 B.S., 5 trainees
    - Head
      - Evangelos Markatos, Ph.D. **U of Rochester**, USA, 1992
    - **Researchers/Associated Researchers: 5**
      - Prof. Vivi Fragopoulou, Ph.D. **Queen's U**, Canada,
      - Prof. Mema Roussopoulos, Ph.D. **Stanford U**
      - Prof. George Kopidakis, Ph.D. **U of Iowa**
      - Dr. Kostas Anagnostakis, Ph.D., **U Penn**, (part-time)
      - Dr. Sotiris Ioannidis, Ph.D. **U Penn**,
    - **Engineers: 4**
      - Christos Papachristos, M.S. (GRID engineer)
      - Manolis Stamatogianakis, M.S.
      - Charis Gikas, M.S.
      - Michalis Foukarakis, M.S.
    - **MTS: 2**
      - Kallia Marakomichelaki, M.S. (part-time)
      - Meltini Christodoulaki, B.S.
    - **Research Assistants: 13**
    - **Undergraduate Trainees: 5**

Evangelos Markatos markatos AT ics.forth.gr

Roadmap

- Who we are
- What do we do?
  - – Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - – Internet Safety
    - Safer Internet Access for children
  - – Contribution to Security Policy
    - ENISA
    - FORWARD

Mission Statement

- Study planet-wide distributed systems
  - to understand the forces that drive their day-to-day operation
  - to master the dimensions that sustain their long-term evolution

- Example Questions:
  - Why do they work at all?
  - How do they break?
  - What kind of traffic is that which flows through the “veins” of such systems?
  - What holds these systems together?
  - How do they respond to various types of attacks?
  - Under what circumstances would they collapse?
  - How can we make them more robust?
  - How can we trust them?
  - How can we be safe using them?

Roadmap

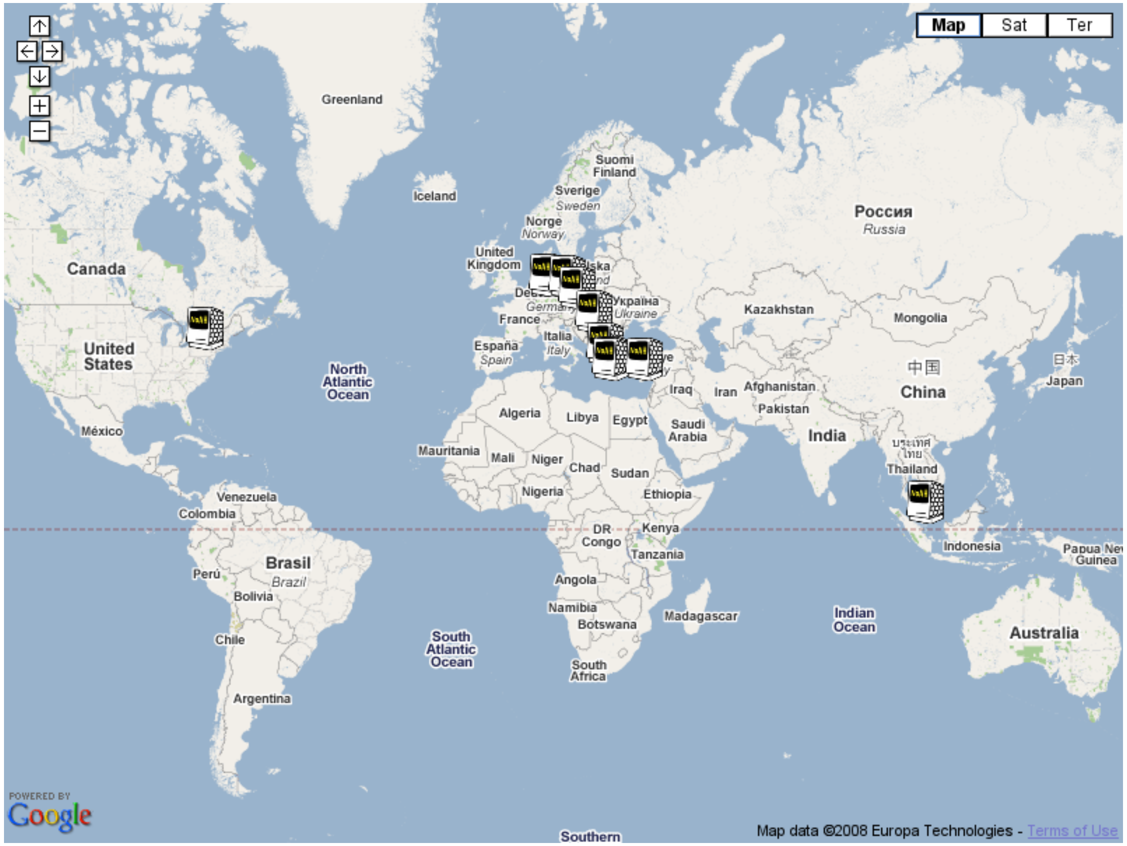
- Who we are
- What do we do?
  - Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - Internet Safety
    - Safer Internet Access for children
  - Contribution to Security Policy
    - ENISA
    - FORWARD

Cyberattack detection: How? Honeypots

HONEYPOTS:

- Computer systems that do not provide production services
- Intentionally made vulnerable
- Closely monitored to analyze attacks directed at them

The NoAH project
http://www.fp6-noah.org

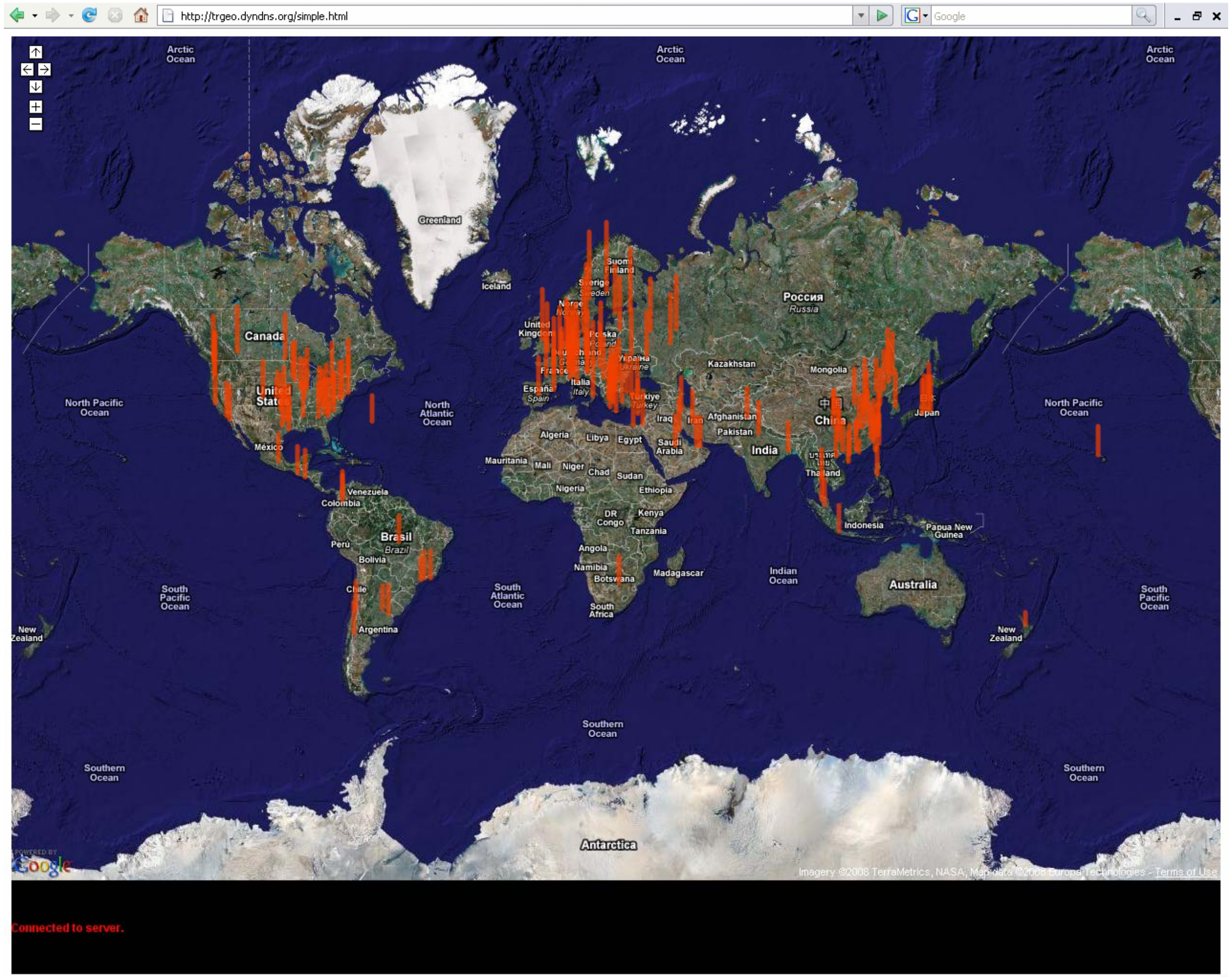


SIXTH FRAMEWORK PROGRAMME

Research infrastructures

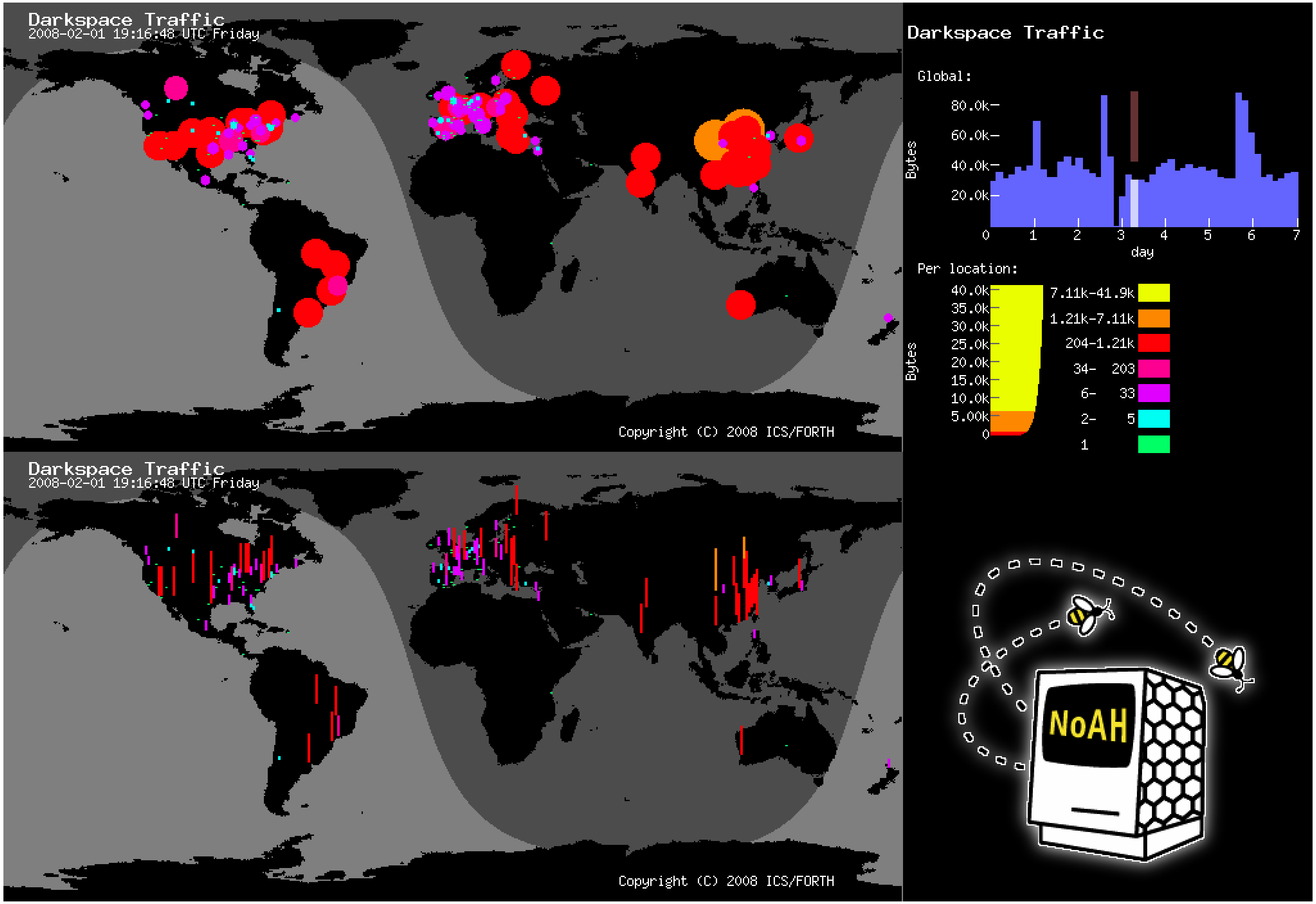
- Implemented a pilot honeypot infrastructure
- Duration: 1/4/05-30/9/08, DG Research, FP6
- Coordinator: FORTH. Partners: ALCATEL, VU, DFN-CERT, FORTHNET, VTRIP, ETHZ

The NoAH traffic



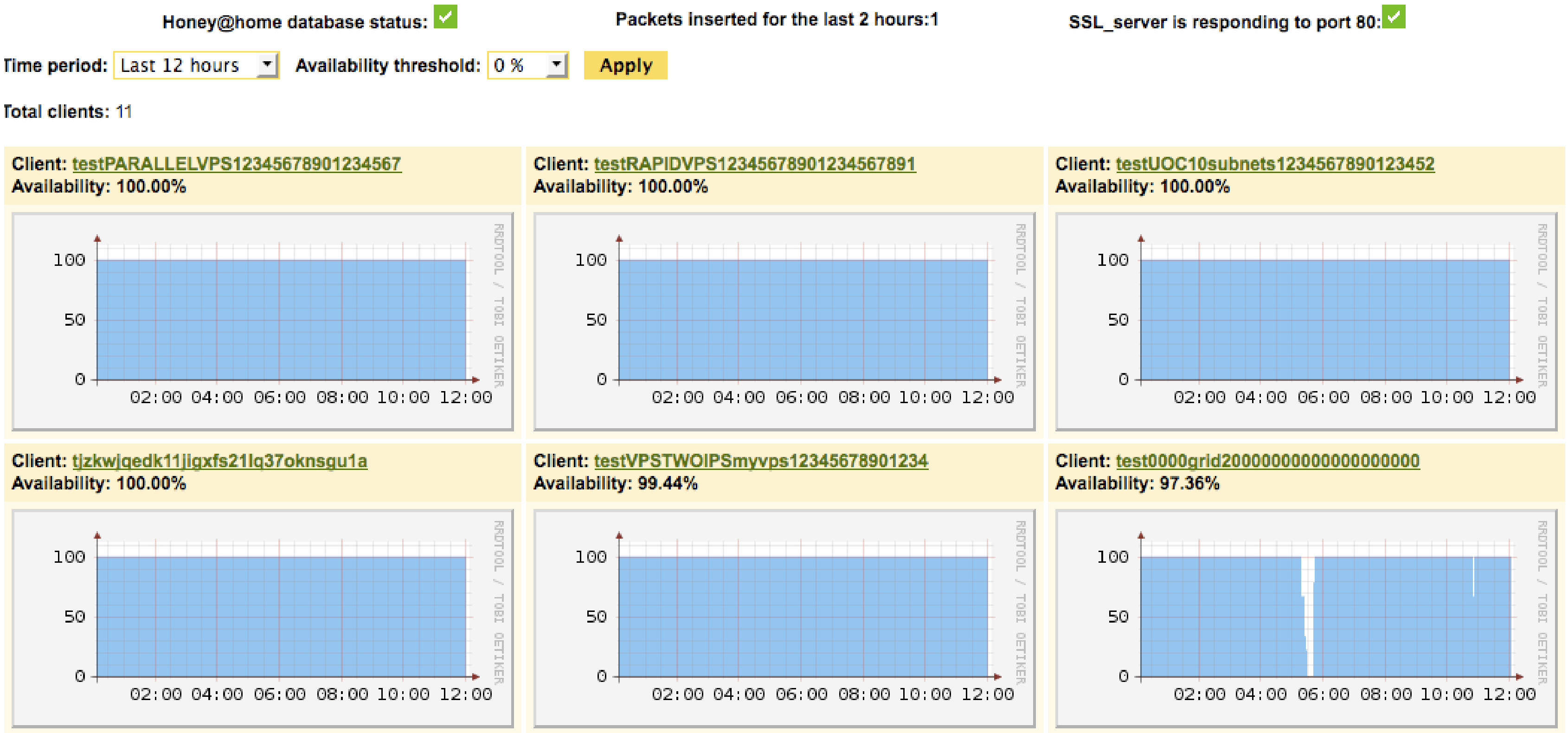
Connected to server.

Scan traffic received by NoAH



Honey@Home

- Empower the end user
- We designed a easy-to-install “homey honeypot”: The Honey@Home



Honey@home database status: ✓

Packets inserted for the last 2 hours:1

SSL_server is responding to port 80:✓

Time period: Last 12 hours ▾ Availability threshold: 0 % ▾ Apply

Total clients: 11

Client: testPARALLELVPS12345678901234567
Availability: 100.00%

Client: testRAPIDVPS1234567890123456789 1
Availability: 100.00%

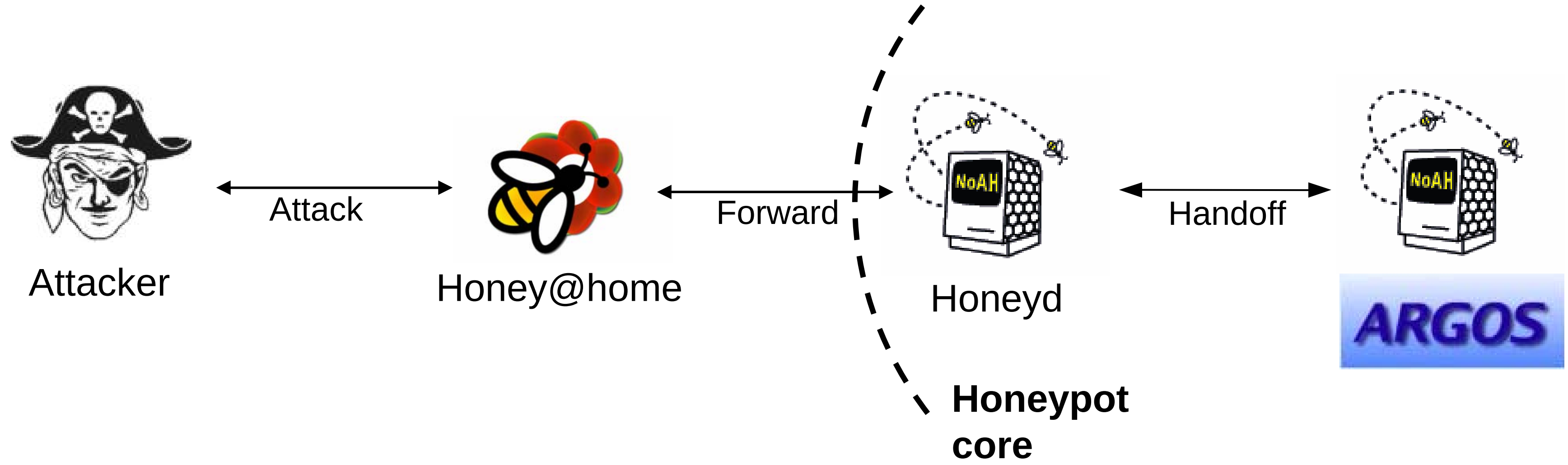
Client: testUOC10subnets1234567890123452
Availability: 100.00%

Client: tjzkwjqedk11jigxfs21lq37oknsgu1a
Availability: 100.00%

Client: testVPSTWOIPSmyvps12345678901234
Availability: 99.44%

Client: test0000grid20000000000000000000
Availability: 97.36%

The NoAH Backend architecture



- Honey@home clients connect to a honeypot core
- Communication is done over port 80 and looks like HTTPS traffic
- Honeyd as front-end to filter out scans
  - Filters out scans and unfinished connections
- Honeyd hands off connection to Argos
- Argos is an instrumented virtual machine able to catch zero-day exploits without the danger of getting infected
  - http://www.few.vu.nl/argos/

NoAH Publicity

DCS

http://www.ics.forth.gr/dcs

enisa
European Network and Information Security Agency
ENISA Quarterly
IN THIS EDITION
Early Detection, Warning and Alerting Systems
A Word from the Executive Director
A Word from the Editor
From the World of Security – A Word from the Experts
Page
A WORD FROM THE EXECUTIVE DIRECTOR
Real-time Monitoring and Detection of Cyberattacks
NoAH
LOBSTER
The Economist
The Economist
Μία ευρωπαϊκή πλατφόρμα ανίχνευσης & αναχαίτισης ηλεκτρονικών επιθέσεων στο Διαδίκτυο
Ανακαλύπτοντας τους hackers
με δόλωμα ένα «βάζο μέλι»
Adobe Acrobat Professional - [tellenbach-noah.pdf]
File Edit View Document Comments Tools Advanced Window Help
Search
Create PDF
Comment & Markup
Send for Review
Secure
Sign
Forms
Select
164%
Help
ERCIM NEWS online edition
Special: Embedded Intelligence
European Digital Library
Special: Space Exploration
Special: Emergent Computing
ERCIM NEWS
Special: Security and Trust Management

subscribe | search | back issues on-line | order back issues | advertise

ERCIM website quick index

< Contents ERCIM News No. 63, October 2005 **SPECIAL: Security And Trust Management**

Towards a European Malware Containment Infrastructure

by Kostas G. Anagnostakis and Evangelos Markatos

'LOBSTER' and 'NoaH' are two projects designing the necessary infrastructure to support research, development, and experimental deployment of advanced cyber-defence mechanisms.

Over the last few years, we have witnessed increasing levels of innovation among cyber-attackers, which, combined with the increasing penetration of broadband Internet service and the persistent vulnerabilities of host software systems, has led to new classes of rapid and scalable mechanized attacks on information infrastructure. Levelling the playing field requires scalable, automated responses to malicious code that can react as quickly as modern network worms propagate. Traditional approaches have relied on signatures, manual containment and quarantine. However, while tools are improving, progress in the development and deployment of the necessary technology is widely regarded as too slow for a threat that is so clear and imminent.

To address this problem, the Distributed Computing Systems Laboratory at FORTH-ICS has initiated and is currently coordinating two EU-funded projects, LOBSTER and NoaH, whose goal is to roll out the necessary infrastructure to support research, development and experimental deployment of advanced

THE PARLIAMENT

POLITICS, POLICY AND PEOPLE MAGAZINE

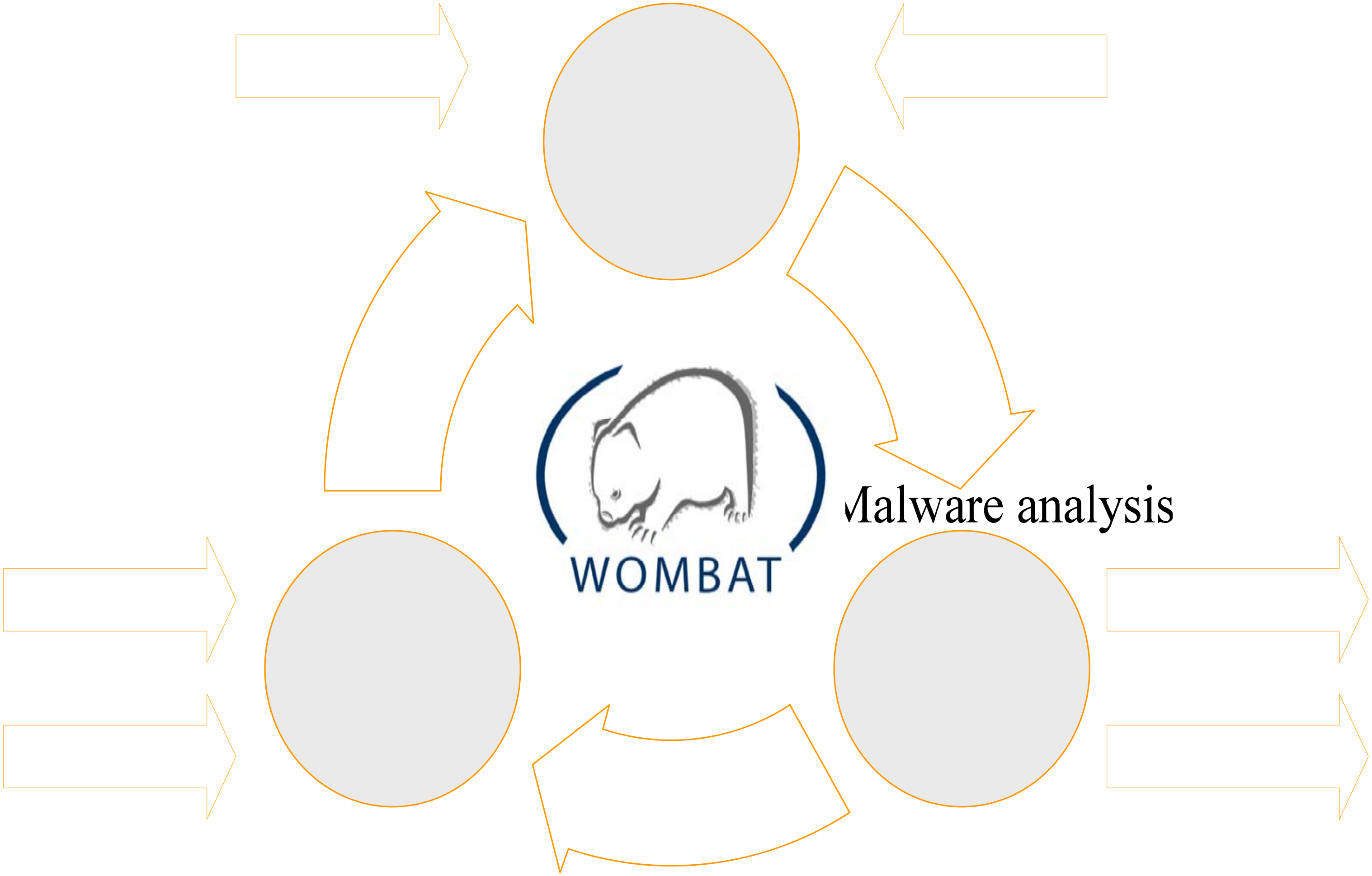
Roadmap

- Who we are
- What do we do?
  - – Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - – Internet Safety
    - Safer Internet Access for children
  - – Contribution to Security Policy
    - ENISA
    - FORWARD

WOMBAT

- WOMBAT: World Wide Observatory of Malicious Behaviors and Attack Threats
  - Develop a repository of attack-related information
  - Develop novel approaches to malware detection
  - Partners: Orange, Eurecom, TUV, NASK, FORTH, VU, Poli Milano, Hispasec

Main objectives and principles



en

ge

is

Evangelos Markatos markatos AT ics.forth.gr

The WOMBAT Consortium

EURECOM
Sophia Antipolis

orange™

TU WIEN
Technische Universität Wien
Vienna University of Technology

WOMBAT

symantec.

HISPASEC SISTEMAS

FORTH

POLITECNICO DI MILANO

vrije Universiteit

NASK

Roadmap

- Who we are
- What do we do?
  - Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - Internet Safety
    - Safer Internet Access for children
  - Contribution to Security Policy
    - ENISA
    - FORWARD

Safer Internet Access

- Founder and host of Safeline: The first Greek Hotline for Safer Internet Access http://www.safeline.gr
- Partner in the newly formed Greek node of Safer Internet (Awareness/Hotline/HelpLine)
- Host of the web site of the Greek Safer Internet node http://www.saferinternet.gr

Safer Internet Access: what do we do?

- Promote visibility of Safer Internet
- Provide advice for parents and teachers
- Provide advice for children on how to surf safely on the Internet
- Access and forward reports about illegal content on the Internet
- We are part of the INHOPE: The International Association of Internet Hotlines

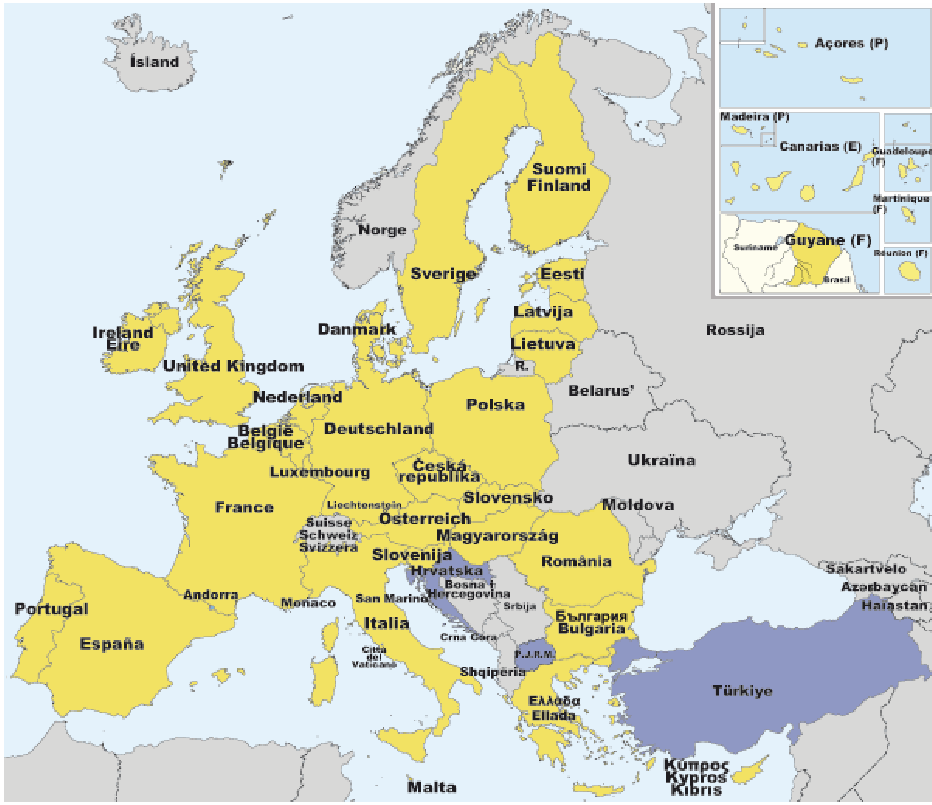
SAFELINE: Safer Internet

- Since 2001 we host
  - SAFELINE: The first Greek hotline in the fight against cyber-crime
  - We educate teachers and parents about Safer Internet Access by children
  - Part of the **European Union** "Safer Internet Plus Programme”

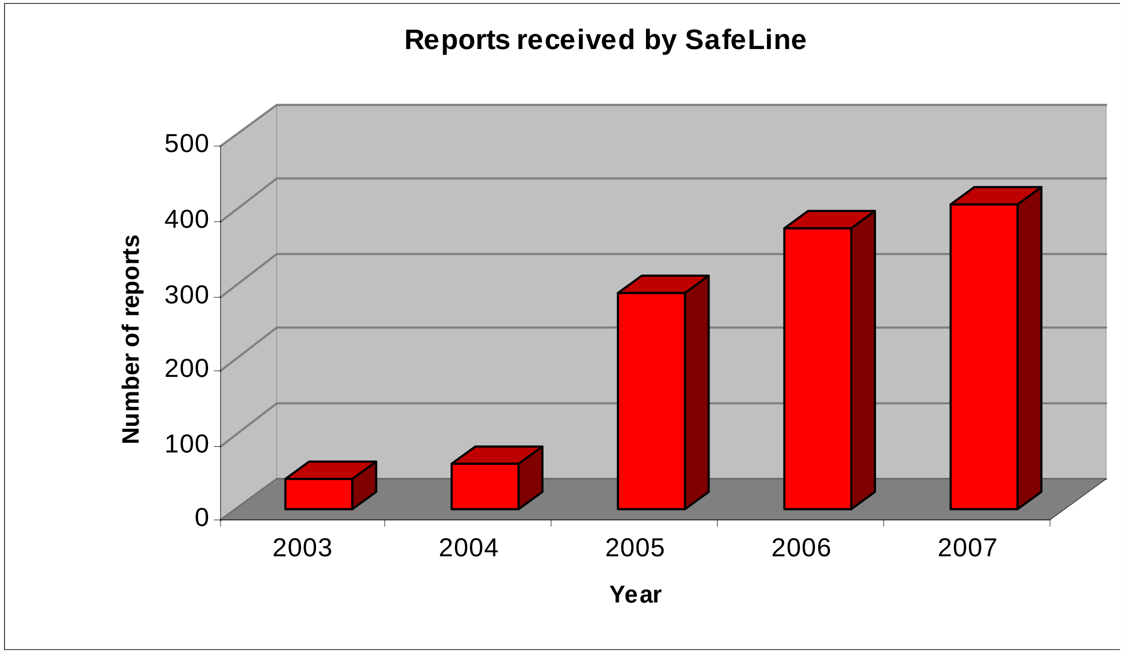
SAFELINE: Safer Internet

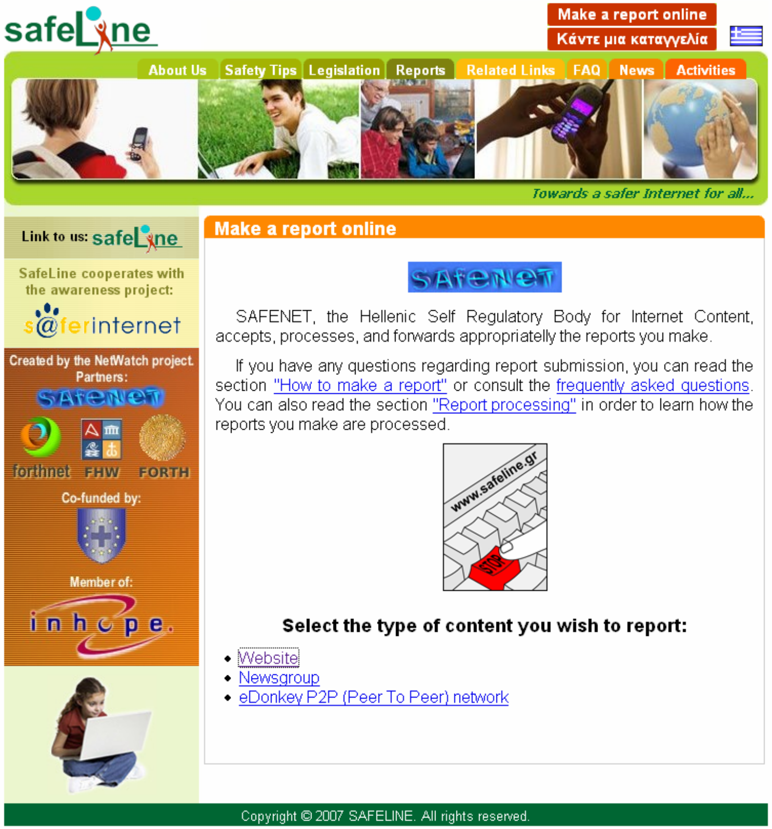
- Safeline is a member of INHOPE
- INHOPE is the International Association of Internet Hotlines fighting Internet illegal content. Founded in 1999 under the [EC Safer Internet Action Plan](#).

inhope.
Internet Hotline Providers



- Reports received by Safeline regarding Internet illegal content found on the Internet are rapidly increasing





Make a report online

SAFENET, the Hellenic Self Regulatory Body for Internet Content, accepts, processes, and forwards appropriately the reports you make.

If you have any questions regarding report submission, you can read the section "How to make a report" or consult the frequently asked questions. You can also read the section "Report processing" in order to learn how the reports you make are processed.

Select the type of content you wish to report:

- Website
- Newsgroup
- eDonkey P2P (Peer To Peer) network

Copyright © 2007 SAFELINE. All rights reserved.

Roadmap

- Who we are
- What do we do?
  - Internet Security
    - Cyberattack detection
    - Repositories for Security-related data
  - Internet Safety
    - Safer Internet Access for children
  - Contribution to Security Policy
    - ENISA
    - FORWARD

Contribution to Policy

- ENISA: European Network and Information Security Agency
- Member of ENISA’s
  - Permanent Stakeholders Group
  - Emerging and Future Risks (EFR) Stakeholders Forum
  - Awareness Community
- Evaluator of ENISA deliverables

FORWARD

- The FORWARD initiative will
  - Identify future security threats
  - Identify a road map for security in Europe
  - Focuses on “system” security
- Funded by the European Commission
  - Coordination and Support Action
  - Coordinator: TUV
  - Partners: EURECOM, VU, FORTH, IPP-BAS, Chalmers

The future

- WOMBAT: Worldwide Observatory of Malicious Behaviors and Attack Threats
  - FORTH designs the largest European Data base of Internet attack-related information
- FORWARD: Design the roadmap for Internet Security Challenges & Research
- MOMENT: Participate in the largest European Repository of Internet measurement/monitoring data
- WISDOM: Participate in the design and development of an all-optical firewall at 40 Gbps

Tracing Cyberattacks on the Internet

Evangelos Markatos
FORTH-ICS
markatos AT ics.forth.gr

http://www.ics.forth.gr/dcs/
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
and
Department of Comp. Science, University of Crete