



An IST Project

The LOBSTER project



Information Society
Technologies

<http://www.ist-lobster.org/>

Large Scale Attacks on the Internet Lessons learned from the LOBSTER project

Evangelos Markatos

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas
(FORTH)

Crete, Greece

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



An IST Project

Agenda



Information Society
Technologies

<http://www.ist-lobster.org/>

- Motivation
- The LOBSTER Infrastructure
 - Number of sensors - deployment
 - Attacks captured
- Lessons Learned
- Policy Implications



An IST Project

Agenda



Information Society
Technologies

<http://www.ist-lobster.org/>

- **Motivation**
- The LOBSTER Infrastructure
 - Number of sensors - deployment
 - Attacks captured
- Lessons Learned
- Policy Implications



An IST Project

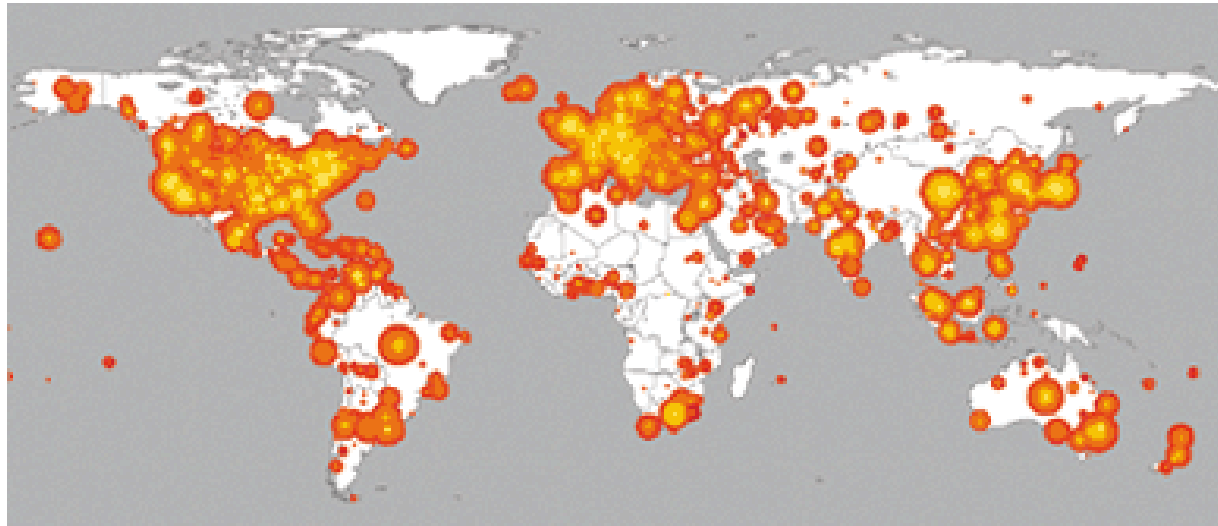
Computer Security is getting increasingly important



Information Society
Technologies

<http://www.ist-lobster.org/>

- 1988
 - The Morris worm compromised 6,000 UNIX computers
- 2001
 - The Code Red worm compromised 300,000 computers



Source: CAIDA/UCSD

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



lobster

An IST Project

Computer Security is Critical



Information Society
Technologies

<http://www.ist-lobster.org/>

- 2007: Vint Cerf (the father of the Internet and VP of Google) says:
 - 25% of all computers online are compromised
 - 100-150 million computers are compromised...



BBC NEWS | Business | Criminals 'may overwhelm the web' - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://news.bbc.co.uk/2/hi/business/6298641.stm

BBC NEWS | Business | Criminals... Vint Cerf says BotNets infect 1/4 of a...

Home News Sport Radio TV Weather Languages Search

UK version International version About the versions Low graphics Accessibility help

BBC NEWS The News in 2 minutes News services Your news when you want it

Last Updated: Thursday, 25 January 2007, 14:18 GMT

E-mail this to a friend Printable version

Criminals 'may overwhelm the web'

By Tim Weber
Business editor, BBC News website, Davos

Criminals controlling millions of personal computers are threatening the internet's future, experts have warned.

Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets, said Vint Cerf, one of the fathers of the internet.

Technology writer John Markoff said: "It's as bad as you can imagine, it puts the whole internet at risk."

The panel of leading experts was discussing the future of the internet at the World Economic Forum in Davos.

Internet pandemic

Mr Cerf, who is one of the co-developers of the TCP/IP standard that underlies all internet traffic and now works for Google, warned that the spread of botnets has become a serious threat to the internet.

WORLD ECONOMIC FORUM 2007 LATEST NEWS

- Davos misses out on the big bang
- World trade talks set to restart
- YouTube users to get ad money
- Blair sees hope of climate deal
- Skype roadmap: Trial and error
- Has Big Business gone green?
- Criminals 'may overwhelm web'
- What's the appeal of Davos?
- Germany wants globalisation push
- 'Good 2007' for world economy
- Bosses 'confident on economy'

DAVOS BLOG - LATEST POSTS

- Good-bye from Davos
- The Little Britain show
- The Google ticket

BACKGROUND

- Q&A: Davos 2007
- Green agenda for global leaders

WORLD SOCIAL FORUM

- Street kids raid poverty summit
- Vibrant 'anti-Davos' has impact

Internet guru warns of botnet pandemic

Tags: Botnet, Vint Cerf

Will Sturgeon silicon.com

Published: 29 Jan 2007 09:39 GMT

Email Trackback Clip Link Print

Father of the internet Vint Cerf has warned high-powered attendees at the World Economic Forum in Davos that the internet is at serious risk from botnets.

Vast networks of compromised PCs, used by criminals for sending spam and spyware and for launching denial of service attacks are reported to be growing at an alarming rate in terms of their

n the Internet

Policy Implications

markatos@ics.forth.gr



lobster

An IST Project

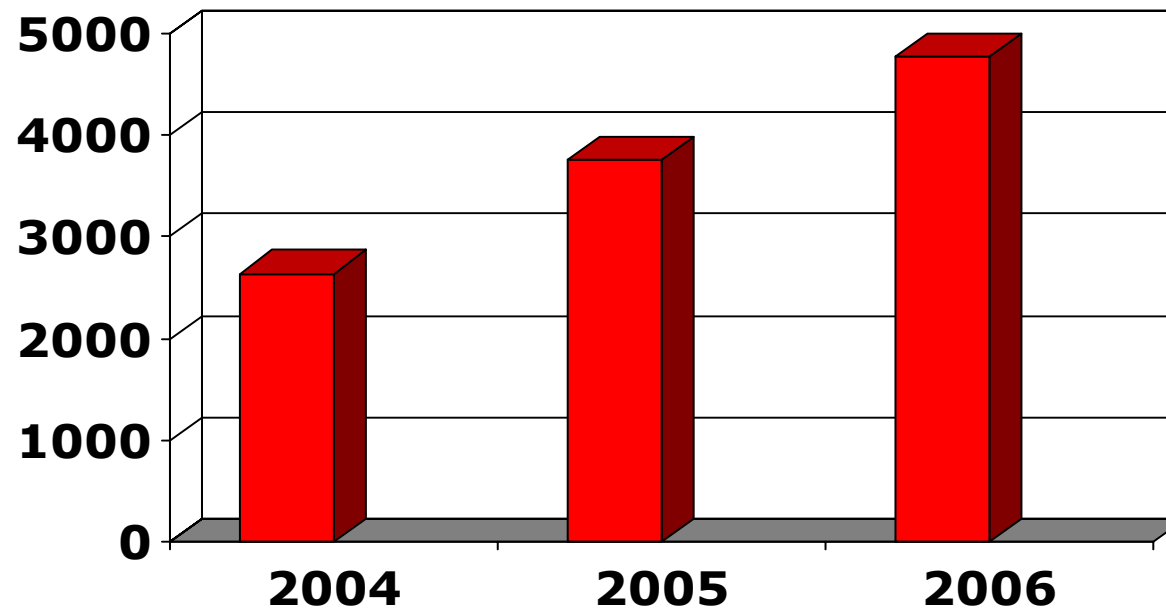
Vulnerabilities



Information Society
Technologies

<http://www.ist-lobster.org/>

Vulnerabilities found



- Total Vulnerabilities documented by Symantec Corporation
(source: Internet Security Threat Report)

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



lobster

An IST Project

Black Market Trading



Information Society
Technologies

<http://www.ist-lobster.org/>

PC Pro: News: Black market thrives on vulnerability trading - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.pcpro.co.uk/news/84523/black-market-thrives-on-vulnerability-trading.html

pc PRO COMPUTING IN THE REAL WORLD

Worry Free Security Solutions for Small Business Free trial >

CERTIFIED FOR Windows Vista™ TREND MICRO

SEARCH FOR: IN: All IT Sites Search Advanced Search

Guest Level 00 in Register | Log

Home > News
News [Security]
 Tuesday 7th March 2006
Black market thrives on vulnerability trading
 6:09PM, Tuesday 7th March 2006

Security giant Symantec claims that anonymous collusion between hackers and criminals is creating a thriving black market for vulnerability trading.

As criminals have woken up to the massive reach afforded to their activities thanks to the Internet, hackers too are now able to avoid risking prison sentences by simply selling on their findings.

Graeme Pinkney, a manager at Symantec for trend analysis, told us: 'People have suddenly realised that there's now a profit margin and a revenue stream in vulnerabilities... There's an element of anonymous co-operation between the hacker and criminal.'

The evidence comes from Symantec's latest biannual security report: vulnerabilities are up. Nearly 2,000 new holes were identified, the largest rise in seven years. And it's not Microsoft's fault. Two-thirds affected web applications rather than the operating system. Four in five were found to be trivial to exploit, and 97 per cent were moderately or highly severe.

Symantec Offers
 Find Symantec at Ask.com

Latest News
 Windows Home Server: ready to install?
 Poor WAN performance hobbles staff productivity
 Microsoft retunes its IPTV platform
 Technology becomes key influence for campus choice
 Ballmer derides Google complaint as "baseless"
 Microsoft mobilises MSN

The Xerox Phaser™ family of printers and MFPs
 SEE LIVE PRICES

http://www.pcpro.co.uk/news/115852/windows-home-server-ready-to-install.html

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



An IST Project

So?



Information Society
Technologies

<http://www.ist-lobster.org/>

- One out of four computers is compromised
- Hackers penetrate all different kinds of computers
- Vulnerabilities are increasing every year
- They are being sold in the black market

- We need to react:
 - Monitor large scale attacks
 - Understand mechanisms and motives of attackers



An IST Project

Agenda



Information Society
Technologies

<http://www.ist-lobster.org/>

- Motivation
- The LOBSTER Infrastructure
 - Number of sensors - deployment
 - Attacks captured
- Lessons Learned
- Policy Implications



An IST Project

The LOBSTER project



Information Society
Technologies

<http://www.ist-lobster.org/>

- **Research Networking Test-Bed** project

- 2005-2007 Funded by IST



- Installed a monitoring infrastructure

- To study performance and security issues in European Research and Educational networks

- Deployed

- more than 40 sensors
- in 10 countries

- Monitors incoming traffic to see if it contains network attacks from hackers

Funded by the European Commission

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



lobster

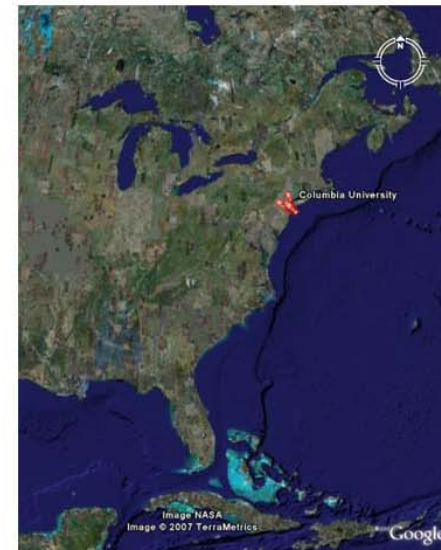
An IST Project

LOBSTER Deployment



Information Society
Technologies

<http://www.ist-lobster.org/>



Learn
Policy Implications

markatos@ics.forth.gr



An IST Project

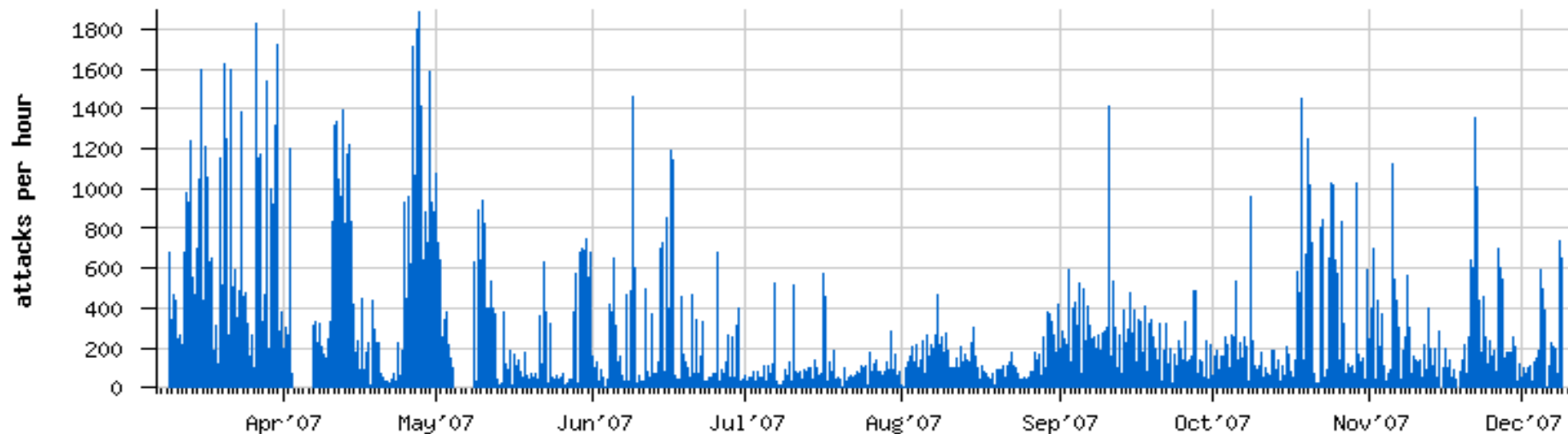
Attacks Captured: focus on polymorphic attacks



Information Society
Technologies

<http://www.ist-lobster.org/>

- Close to one million attacks captured
- One attack every 30 seconds!
- One attack every two seconds (peak rate)!



Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



lobster

An IST Project

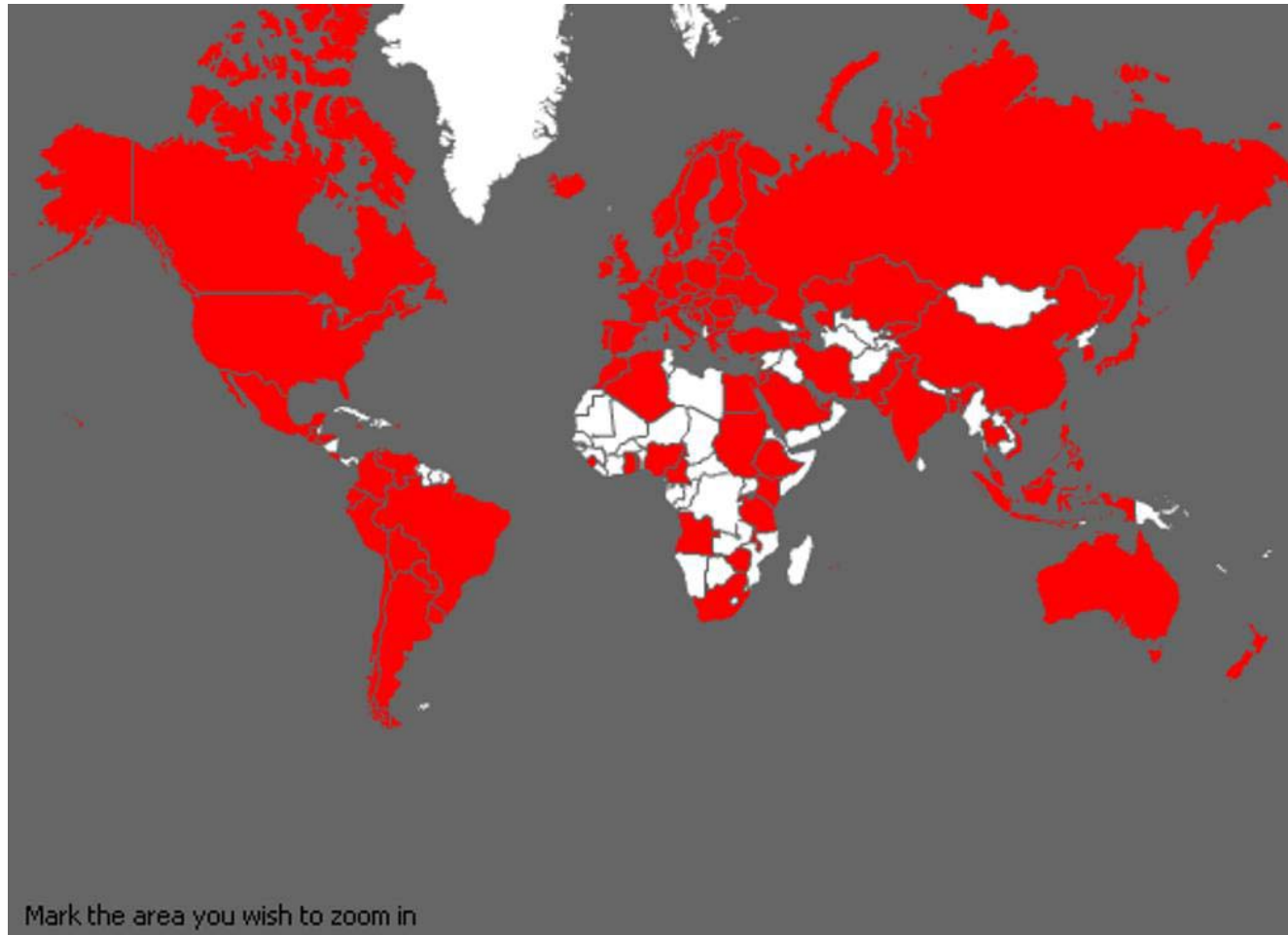
Where do attackers come from?



Information Society
Technologies

<http://www.ist-lobster.org/>

All over the world



Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



An IST Project

Where do attackers come from?

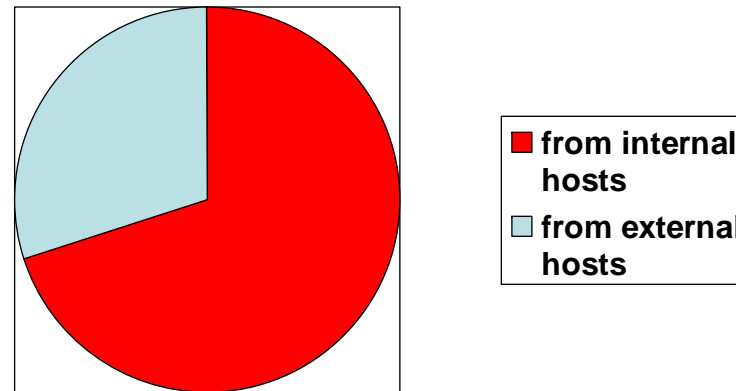


Information Society
Technologies

<http://www.ist-lobster.org/>

- 70% of the attacks to an organization originate from “inside” hosts
 - Maybe compromised computers which attack the local network

Attacks Launched





An IST Project

Agenda



Information Society
Technologies

<http://www.ist-lobster.org/>

- Motivation
- The LOBSTER Infrastructure
 - Number of sensors - deployment
 - Attacks captured
- **Lessons Learned**
- Policy Implications



An IST Project

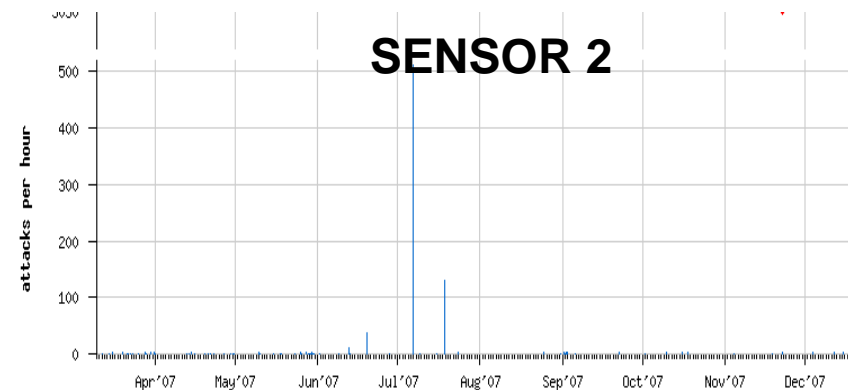
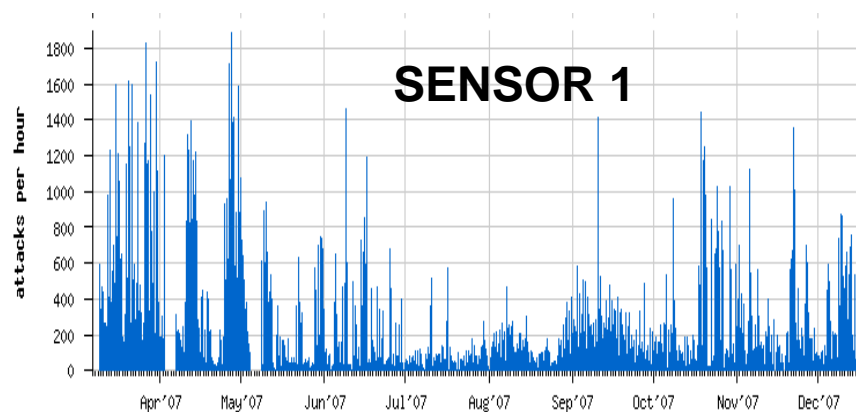
Lessons Learned



Information Society
Technologies

<http://www.ist-lobster.org/>

- Attackers launch attacks **from all over the world**
- Several attacks originate **from “internal” hosts**
 - Probably compromised computers of the organization
- Isolated viewpoints provided a “narrow point of view” of the attack plane, i.e.
 - One sensor reported heavy attack while
 - Another sensor reported very little attacks



Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr



An IST Project

Agenda



Information Society
Technologies

<http://www.ist-lobster.org/>

- Motivation
- The LOBSTER Infrastructure
 - Number of sensors - deployment
 - Attacks captured
- Lessons Learned
- **Policy Implications**



An IST Project

What needs to be done?



Information Society
Technologies

<http://www.ist-lobster.org/>

- The knowledge of large scale attacks may be fragmented today
 - Individual organizations know their status but do not know the status of other organizations/networks
- Very few people/organizations have a global view of the attack landscape
- Even fewer publish this information on the public domain
- We need to work towards a “broad viewpoint” by sharing of data
- Large-scale attack monitoring needs “**broadened points of view**”



An IST Project

What has been done



Information Society
Technologies

<http://www.ist-lobster.org/>

- ENISA has started work in this area:
 - Examining the feasibility of a data collection framework
- Unit A3 of ICT promotes the “Learning from Large-Scale Attacks on the Internet”
- Individual projects/organizations in Europe provide some form of data/information (NoAH, WOMBAT, Arakis, Leurre.com, etc.)
- BUT
- We need to **share more information/data**



An IST Project

What needs to be done?



Information Society
Technologies

<http://www.ist-lobster.org/>

- Facilitate sharing of knowledge – facilitate sharing of data
 - Encourage Organizations to **share attack-related data**
 - Universities are usually willing to provide information but
 - they may need technical and legal advice before doing so
 - Help organizations **exchange attack-related data**
 - Create repositories for all data provided by individual organizations
- Provide a **legal framework** for data sharing
 - **Who** can access the data, **when** and for **which** purposes



An IST Project

Summary



Information Society
Technologies

<http://www.ist-lobster.org/>

- Lots of attacks out there
- Vulnerabilities are increasing
 - They are being traded in the black market
- One out of four computers is compromised
- Existing projects/initiatives/organizations provide attack-related information-data but
 - Most of them provide narrow viewpoints
- We need to find a formula to broaden our point of view
 - And to share data and information
- Large-scale attacks need large-scale viewpoints



An IST Project

The LOBSTER project



Information Society
Technologies

<http://www.ist-lobster.org/>

Large Scale Attacks on the Internet Lessons learned from the LOBSTER project

Evangelos Markatos

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas
(FORTH)

Crete, Greece

Learning from Large Scale Attacks on the Internet
Policy Implications

markatos@ics.forth.gr