



Internet Security: Cyber-threat detection/mitigation in the SCAMPI and LOBSTER projects



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

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



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

<http://www.ics.forth.gr/~markatos>
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)

Evangelos Markatos

FORTH





Roadmap



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

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

- The problem:
 - The trust that we used to place on our network is slowly eroding away
- We are being attacked
 - Viruses, Worms, Trojans, keyboard loggers continue to plague our computers
- What can be done?
 - Automate the
 - Detection of, fingerprinting of, and reaction to cyberattacks
- Summary and Conclusions





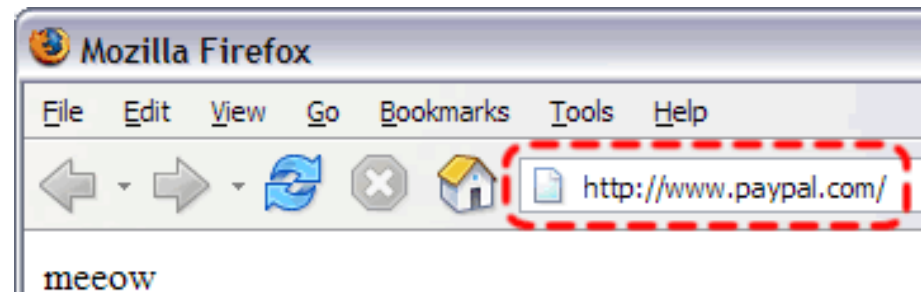
The erosion of trust on the Internet



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

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

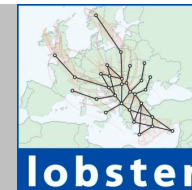
- **We used to trust computers** we interacted with on the Internet
 - Not any more...
 - Address bar spoofing:
 - Do you know that the web server <http://www.paypal.com> is the *real one*?



- We used to trust our network
 - Not any more...
 - Our network is the largest source of all attacks
- We used to trust our own computer
 - Not any more... (keyboard loggers can easily get all our personal information)



The boiling cauldron of Security



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

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

- Security on the Internet is getting increasingly important
 - **Worms, Viruses, and trojans**, continue to disrupt our everyday activities
 - **Spyware** and **backdoors** continue to steal our credit card numbers, our passwords, and snoop into our private lives
 - **Keyboard loggers** can empty our bank accounts if they choose to do so





The boiling cauldron of Security



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

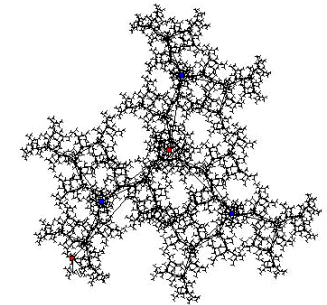
<http://www.ist-lobster.org/>

- **Viruses**

- programs that attach themselves to legitimate applications. Once the legitimate applications start running, the virus start running as well.
- They also attach themselves to email messages
- “Slow-spreading”: need user intervention (i.e. “click”) to run

- **Worms**

- **Self-replicating** programs
- They do not need our help to replicate
- How do they do it?
 - They find a vulnerable server
 - Trigger a bug in its code, hijack its execution thread and
 - They compromise the server
- They can infect 10s of thousands of computers in minutes
 - Humans have no time to react – they just clean up after the attack is over





The boiling cauldron of Security



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

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

- **Backdoors**

- Worms install “backdoors” in the compromised computers
- e.g. create a new account with login “smith” and password “me”
- The attacker can now enter the compromised computer as “smith”



- **Keyboard loggers**

- They log every key typed on the keyboard
 - Credit card numbers, bank accounts,
 - Passwords,
 - Personal email
 - Confidential information
 - They can
 - Empty bank accounts
 - Read and Forward email messages
 - Change victim’s personal data
 - Reveal financial and personal secrets
 - Destroy a person both socially and financially





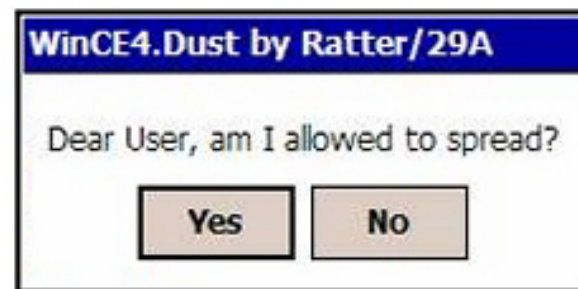
It used to be a problem of PCs



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

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

- Not any more...
- PocketPC virus:
 - Duts
- Mobile phone virus:
 - Cabir
 - Infects the Symbian operating system



Evangelos Markatos

FORTH



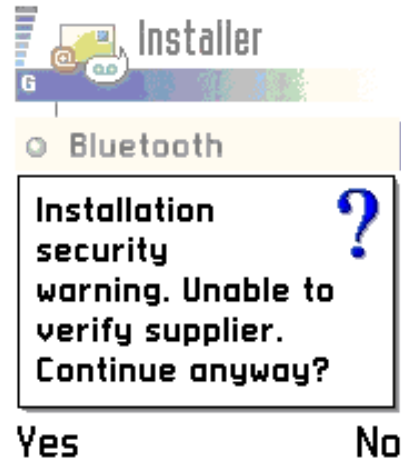


Mobile phone viruses: The Mosquitos virus



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

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



- Mosquitos Virus:
 - Attaches itself to an illegal copy of “Mosquitos” game
 - Once installed it starts sending potentially expensive SMS messages to premium numbers
 - “free to download” but “expensive to play” 😊



How much does it cost?



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

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

- **Financial Cost:** worms cost billions of euros to lost productivity
 - CodeRED Worm: \$2.6 billion
 - Slammer: \$1.2 billion
 - LoveLetter virus: \$8.8 billion
- Could cyberattacks lead to **loss of life**?
 - What if a medical equipment gets infected by a worm?
 - Wrong diagnosis? Wrong treatment?
 - What if a car gets infected by a worm?
 - Could this lead to fatal car crash?
- How about **Critical Infrastructures**?
- What if a **Nuclear power plant** gets infected?
 - Would this lead to failure of safety systems?
 - Is this possible?





How much does it cost?



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

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

- Worms have penetrated Nuclear Power plants.
 - *“The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours”*
Security Focus News
- Luckily no harm was made
 - The reactor was not operating at that time
 - There was a fall-back **analog** monitoring system
- Will we be so lucky next time?





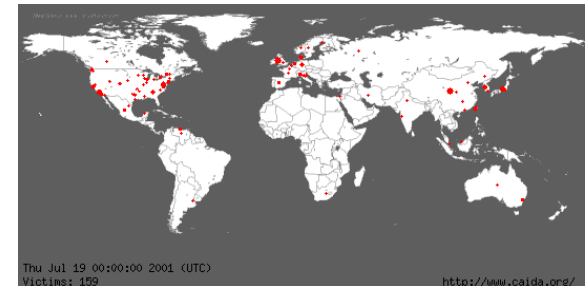
What can be done about it?



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

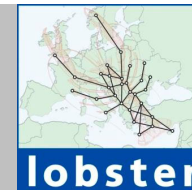
<http://www.ist-lobster.org/>

- Today the defense process is mostly manual
 - But the worms are **automated**
- Worm/Virus detection/identification is done by experts (humans)
 - It may take several hours
 - But worms multiply in **minutes**
- We need to speed-up the process of
 - Detection, fingerprinting, and reaction





What can be done about it?



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

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

- In SCAMPI, LOBSTER, EAR
- We work towards the automated
 - Detection of,
 - Fingerprinting, and
 - Reaction to cyberattacks





Automated Worm Detection



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

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

Challenges

- We do not know what we are looking for
 - Note: we are looking for a “new” worm – we do not know what it looks like
- Lots of **false positives**:
 - There are lots of times where things seem to be wrong without any cyber-attack going on
 - If we cry “wolf” too often, our systems will be useless

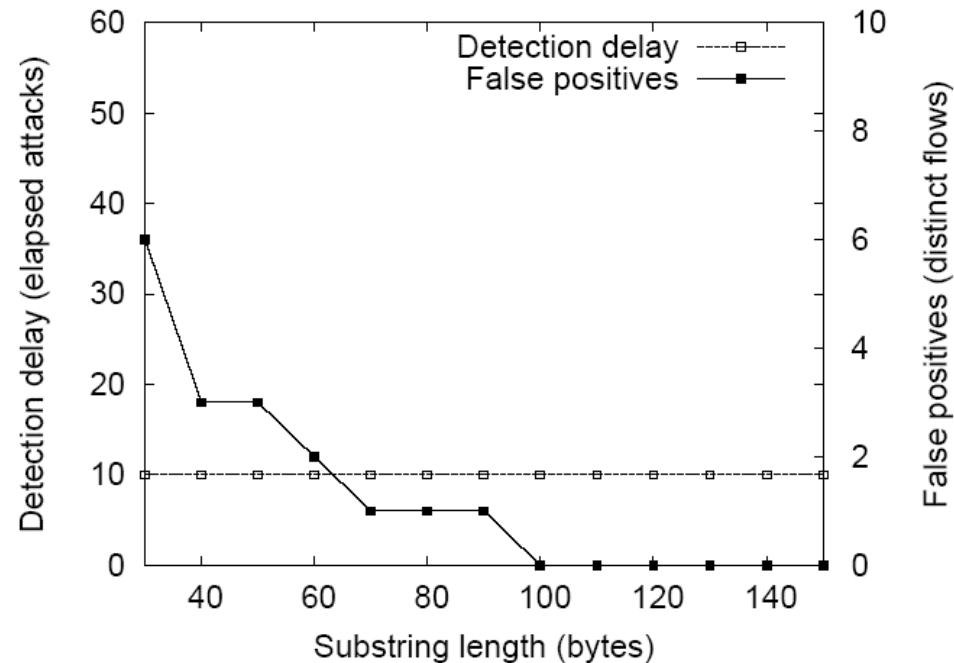


Automated Worm Detection



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

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



- Use heuristics to find out that “something is wrong”
 - e.g. unusual large number of packets in some ports (a peak)
 - abnormally high number of **identical packets** [ICC 2005]
 - That have not been seen before in the past
 - at least at such numbers
 - From several sources to several destinations

Evangelos Markatos

FORTH





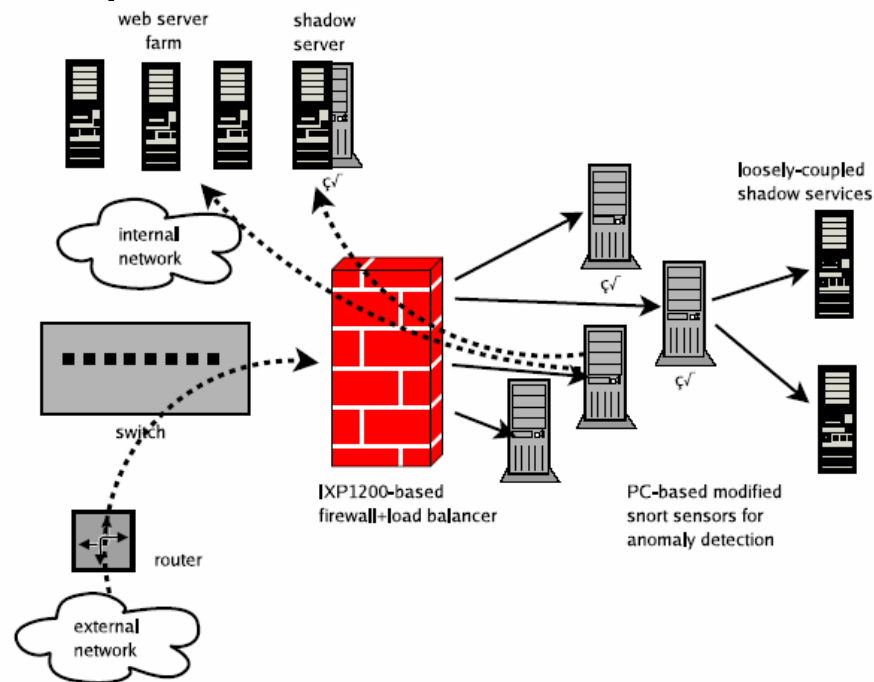
Automated Worm Detection



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

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

- Need to distinguish between false positives and real attacks
 - Forward some “suspicious” packet flows to virtual machines (shadow servers) for further execution [TR 2005]



Evangelos Markatos

FORTH





Fingerprinting



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

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

- Create a “signature” or “fingerprint” of a worm
 - e.g. the worm attacks applications on port 135 and it contains the string “I_AM_A_BAD_WORM” in the first 100 bytes of its attack packet
- Create a rule for the worm
 - SNORT rule:
 - `alert tcp any any -> any 135`
`(msg: “new worm”;`
`content: “I_AM_A_BAD_WORM”;`
`depth: 100)`





Fingerprinting



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

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

- Challenges
 - Create a short signature
 - e.g. that can be used by firewalls
 - Create an accurate signature
 - e.g. which does not match innocent packets



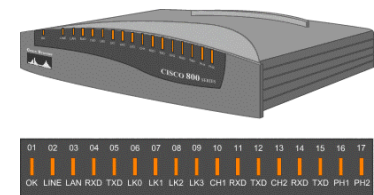
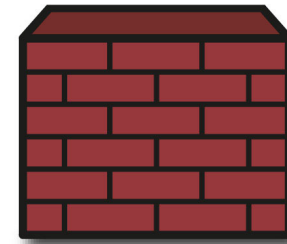
Reaction



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

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

- Place protection/reaction devices in place
- What are the available protection/reaction devices?
 - Firewalls
 - They can not inspect packet payload
 - They drop packets based only on header information
 - What if a worm starts spreading on port 80?
 - Are they going to drop all packets to port 80?
 - Are they going to shut down the web?
 - Routers
 - More effective – they are in the core of the network
 - Do they have the processing capacity to filter packets at 10-40 Gbps based on a set of fingerprints?
 - Intrusion Prevention Systems (IPSeS)
 - Most effective: they inspect both headers and payloads
 - They can filter out packets based on their payloads
 - How many organizations have an IPS in place?
 - Personal shields and firewalls
 - Most effective
 - How many have they been deployed?





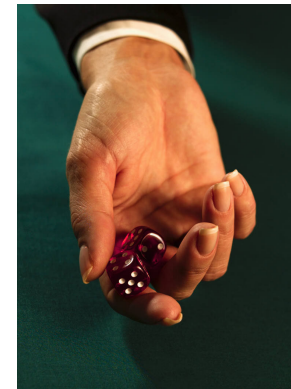
Reaction: IP Address randomization



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

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

- Hit list worms gather intelligence offline:
 - They gather IP addresses of vulnerable servers at low speed:
 - They evade detection
 - They gather a “hit list” that enables rapid spread
- At the time of the attack they attack only computers on the “hit list”
- Our approach: Change IP addresses of computers frequently [TR 2005]
 - Hit list easily becomes stale
 - e.g. use DNS DHCP
 - Worms now shoot at a moving target



Evangelos Markatos

FORTH





Summary



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

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

- We have just scratched the surface
- Cyberattacks continue to plague our networks because
 - They replicate on their own
- We need to respond faster and automate
 - the detection, fingerprinting of, and reaction to cyberattacks
- SCAMPI, LOBSTER, EAR
 - Detection – Fingerprinting
 - Find identical packets [ICC 2005]
 - Find server requests which contain executable code [SEC 2005]
 - Forward suspicious packets to “shadow servers”
 - Reaction
 - Randomize IP addresses so that worms shoot a moving target [TR 2005]



Internet Security: Cyber-threat detection/mitigation in the SCAMPI and LOBSTER projects



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

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



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

<http://www.ics.forth.gr/~markatos>
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)

Evangelos Markatos

FORTH

