



CyberSecurity Research in Crete

Evangelos Markatos

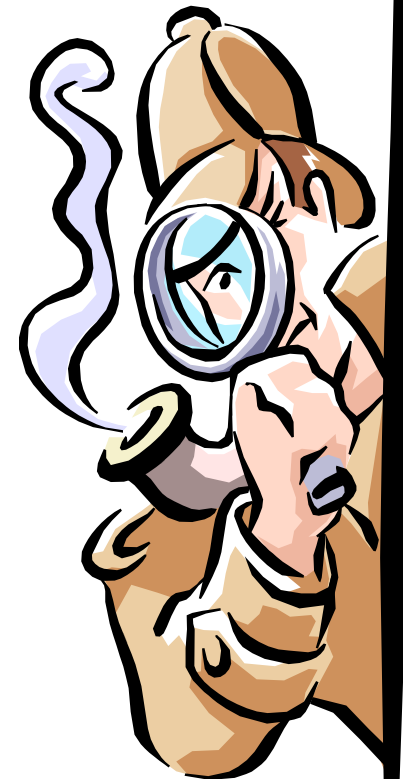
Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)

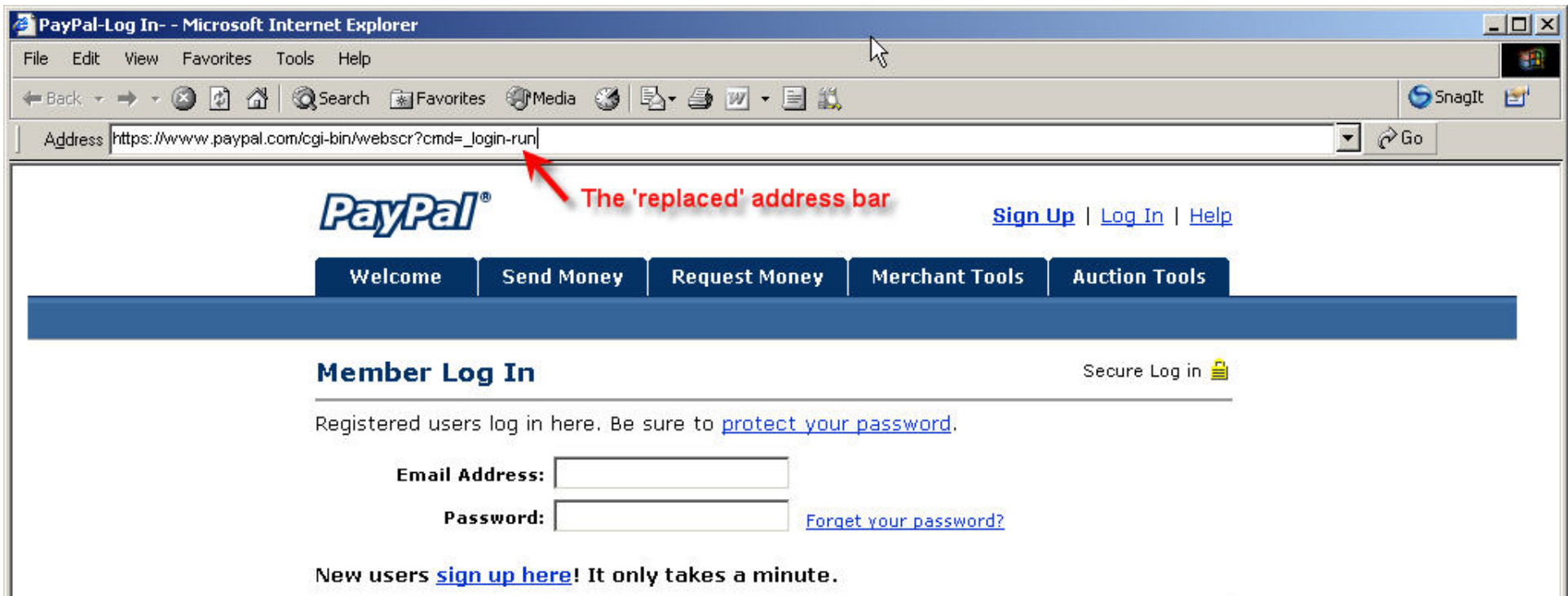
Crete, Greece



- 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 do people say about this?
 - Europe – ENISA
 - USA – PITAC
- What can be done? The DCS approach
 - Understand
 - mechanisms and causes of cyberattacks
 - Automate
 - Detection of, fingerprinting of, and reaction to cyberattacks
- Summary and Conclusions



- 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)





- **We used to trust our own eyes** with respect to the content we were viewing on the Internet
 - Not any more...
 - Phishing: sophisticated social engineering
 - Attackers send users email
 - On behalf of a legitimate sender (e.g. a bank)
 - Inviting them to sign-up for a service
 - When users click they are requested to give their password
 - Which ends up in the attacker's database



ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address  http://soundforum.co.kr/asaproj/image/www/index.html



ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ

e-Banking

Help Desk:
+30 210 9479999

Log in
Πληροφορίες
Demo

ΝΕΕΣ ΥΠΗΡΕΣΙΕΣ

- Μαζικές γραμμές
- Εμβασμα σε Τράπ. Εσωτερικού ή Εξωτερικού
- Πληρωμές πιστωτικές κάρτες άλλων τραπεζών, Φόρος Εισοδήματος, ΠΛΑΣΤΙΟ COMPUTERS

Log in

Ενημερωθείτε για τους λογαριασμούς σας και διενεργείστε τις τραπεζικές / άνεση από το **Internet Banking** της Εθνικής Τράπεζας.

Εάν είστε ήδη συνδρομητής, για να ενταχθείτε στο σύστημα, συμπληρώστε τα

User ID

Password

Εισόδος

Για την ασφαλή διαβάσετε τις συ

Εάν δεν είστε συνδρομητής και επιθυμείτε να ενημερωθείτε για το Internet B

Απώλεια Κωδικών ή λίστας TAN

Η υπηρεσία απώλειας Κωδικών (User ID, Password) ή λίστας TAN είναι διαθ
Λειτουργική Στήριξη

Για λειτουργική στήριξη επικοινωνήστε με το Help Desk στο +30 210



Online Banking Alert

Need additional
up to the minute
account
information?
[Sign In >>](#)

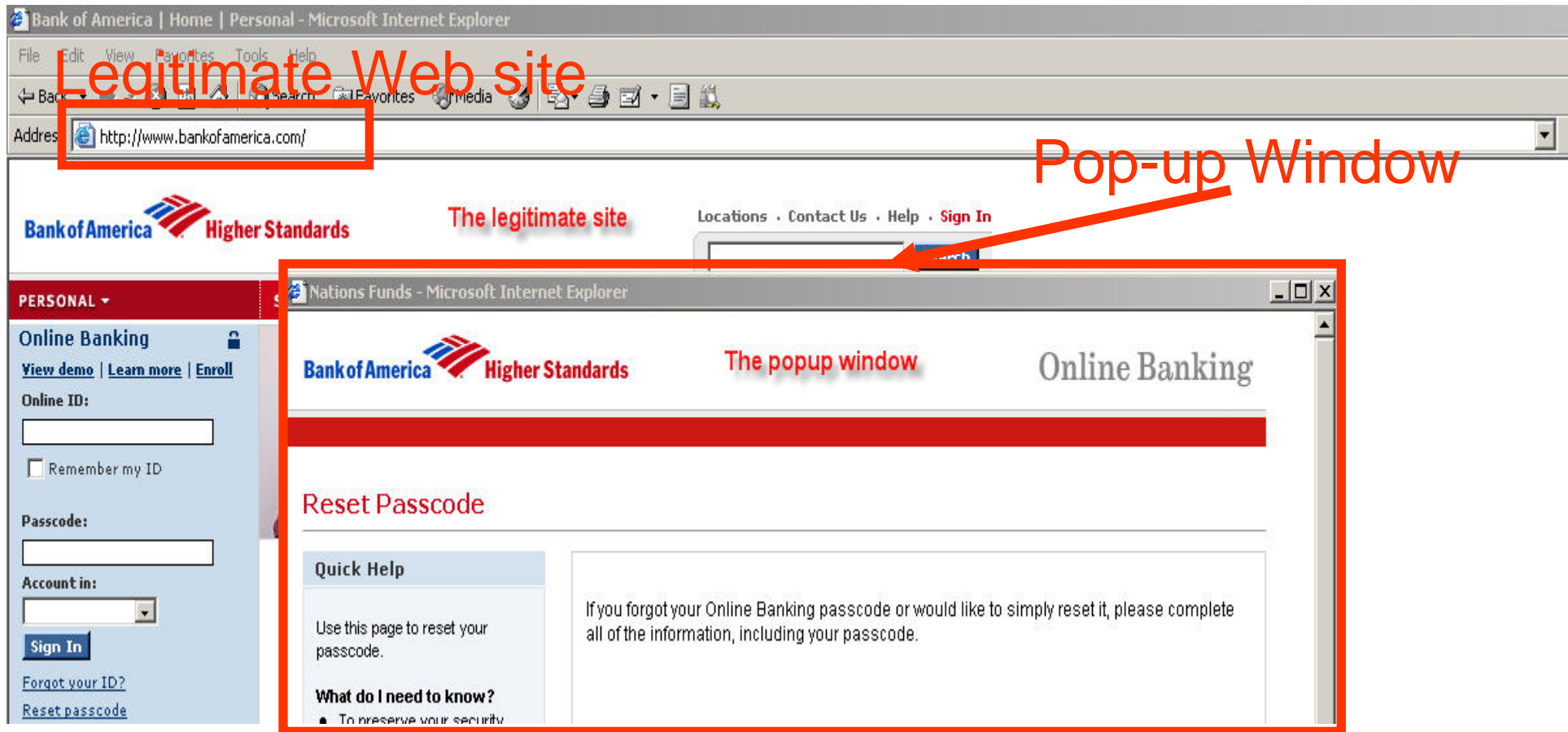
Change of Email Address

Your primary e-mail address for Bank of America Online Banking has been changed.

Did You Know? You can change your address, order checks and more online. [Sign in to Online Banking](#) and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of America with questions or comments, please [sign in to Online Banking](#) and visit the customer service section.

- Attackers send email inviting Bank of America customers to change their address on-line

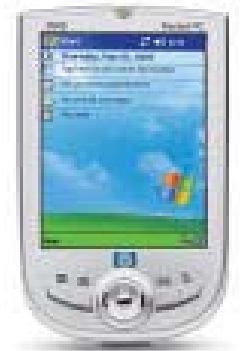
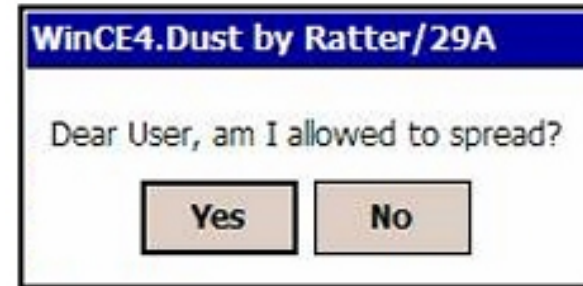


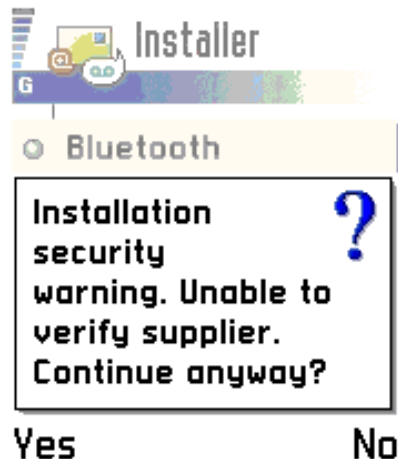
- Bank of America web site opens in the background
- Pop-up window (from www.bofalert.com!) requests user name and password



- 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

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





- 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” 😊

- Once installed
 - Searches for nearby phones
 - Sends itself to the owner's address list through MMS
 - Using random names
 - Difficult to filter out

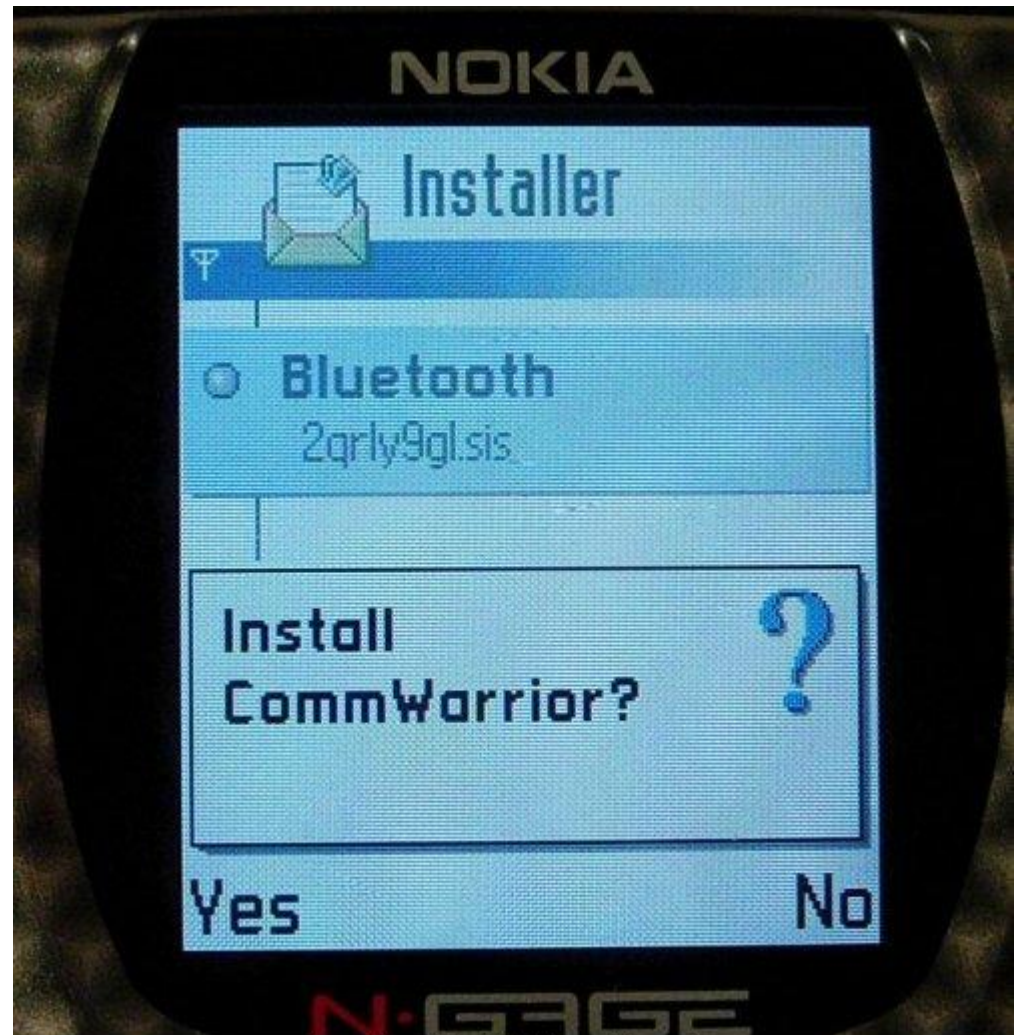


Image Copyright © F-Secure Corporation

- **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?



- 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?





- ENISA: European Network and Information Security Agency
- PSG: Permanent Stakeholders Group
- Vision Document



- *“The longer-term impact of ... worm compromised hosts is likely to be greater in total than at present”*
- *“... Organized Crime and terrorists ... introduce a level of sophistication and funding of (cyber)attacks that is far beyond what we have commonly seen in the previous 20 years of cyber security”*

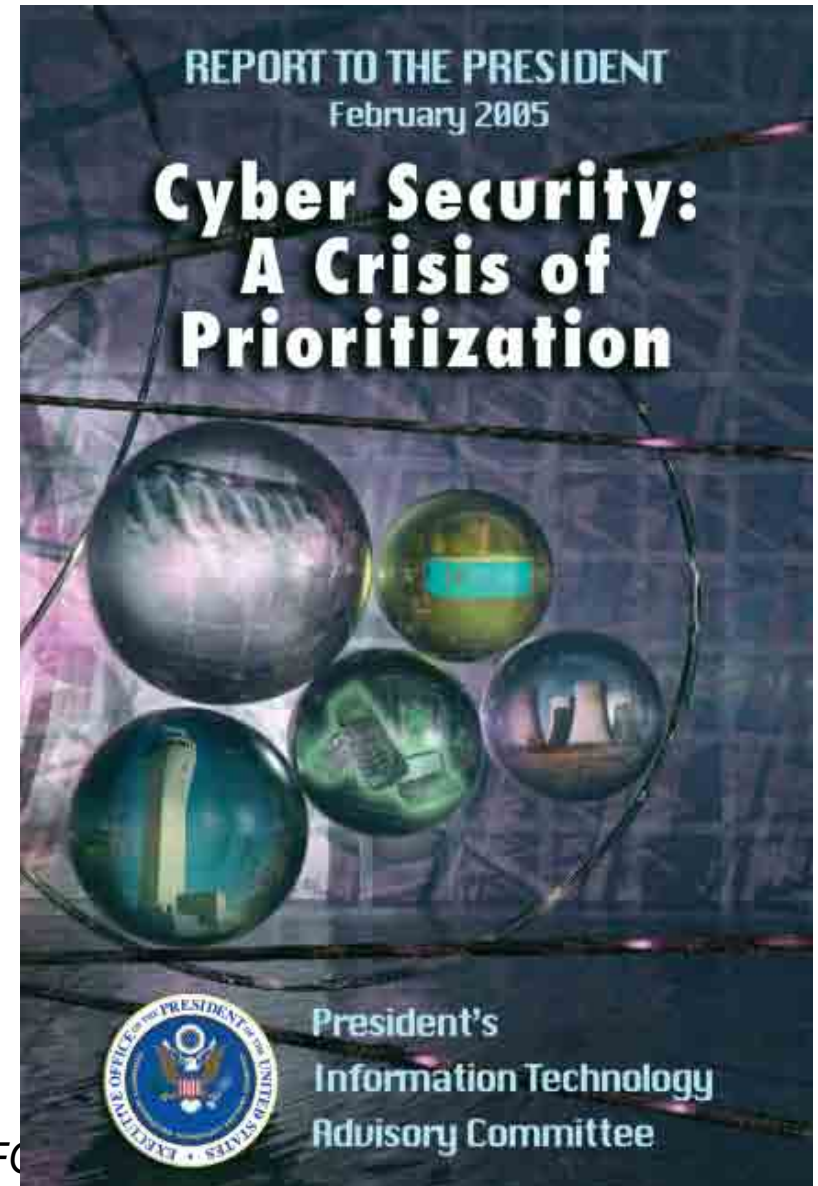
ENISA PSG

i.e. **things are bad and are going to get worse!**

- Feb. 2005
- President's Information Technology Advisory Committee (in U.S.)
- Cyber-Security Sub-committee
 - David Patterson, UC Berkeley
 - Tom Leighton, MIT,
 - and several others



- Provide expert advice
 - In IT security

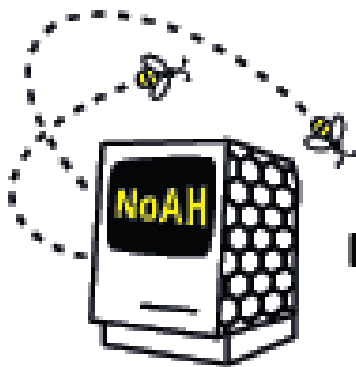


- They identified 10 Research Priorities
- We should do Research in:
 - Global Scale Monitoring (*for cyber-attacks*)
 - Real-time Data collection storage and analysis (*for cyberattacks*)
 - Automated (*cyberattack*) discovery from monitoring data
 - Develop forensic-friendly architectures

To summarize:

Monitor for cyber-attacks and detect them early

- At DCS we do just that
- Monitor, detect, and fingerprint
 - Cyberattacks



European Network of Affined Honeypots



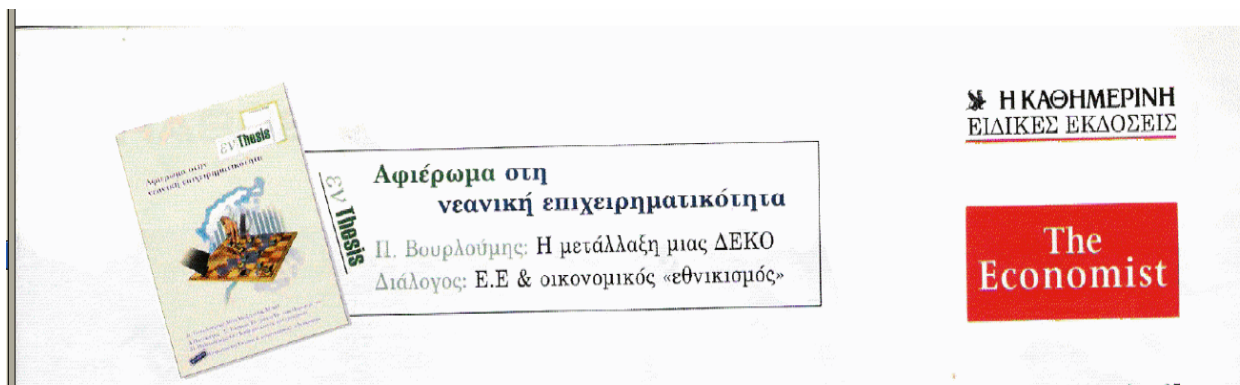
- **LOBSTER: Large Scale Monitoring of Broadband Internet Infrastructure**
 - SSA, Research Networking Testbed, funded by IST, 9 partners
- **NoAH: Network of Affined Honeyspots**
 - SSA (Design Study), Research Infrastructure
 - Funded by DG Research, 8 partners



Information Society
Technologies



European Network of Affined Honeyspots

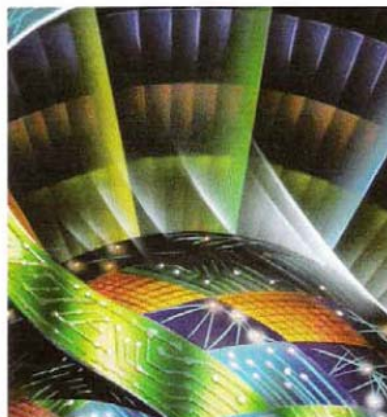


Μία ευρωπαϊκή πλατφόρμα ανίχνευσης & αναχαίτισης ηλεκτρονικών επιθέσεων στο Διαδίκτυο

Των Σπύρου Αντωνάτου, Κώστα Αναγνωστάκη και Ευάγγελου Μαρκάτου*

Τα τελευταία χρόνια γινόμαστε μάρτυρες ολοένα και περισσότερων ηλεκτρονικών επιθέσεων, οι οποίες, προερχόμενες από κακοπροαίρετους χρήστες και χρησιμοποιώντας ως μέσο μεταφοράς το Διαδίκτυο, έχουν στόχο να διεισδύσουν σε υπολογιστές ανυποψίαστων χρηστών, τόσο στον επαγγελματικό όσο και στον προσωπικό τους χώρο.

Εκμεταλλευόμενες την εξάπλωση της κοινωνίας της Πληροφορίας, την ολοένα και ευρύτερη χρήση εικοσιτετράωρων διαδικτυακών συνδέσεων τύπου DSL και την ευρεία χρησιμοποίηση ευάλωτου, αν όχι διάτρητου, λογισμικού, οι επιθέσεις αυτές τείνουν να γίνουν πια καθημερινό φαινόμενο. Έχοντας, όπως άλλωστε όλοι οι κακοποιοί, πολλά παράξενα ονόματα μεταξύ των οποίων και οι (αίσιμα) ακούσιες



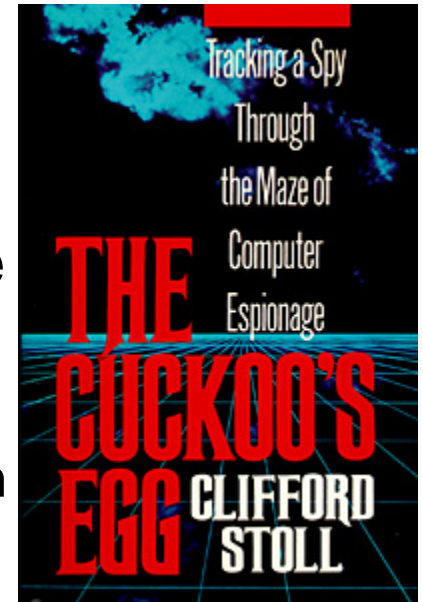
λεια και την προστασία των προσωπικών τους δεδομένων.

Αν και έχουν γίνει πολλά βήματα για την ανίχνευση και την καταπολέμηση αυτών των ηλεκτρονικών επιθέσεων, τα περισσότερα από αυτά βασίζονται στην ανθρώπινη παρέμβαση και στην καταλυτική βοήθεια εμπειρογνομόνων, οι οποίοι μόνο αυτοί έχουν τις απαραίτητες γνώσεις να αναγνωρίσουν και να απομονώσουν τέτοιες επιθέσεις. Αυτή η παρέμβαση του ανθρώπινου παράγοντα έχει ως αποτέλεσμα η διαδικασία ανίχνευσης και αναχαίτισης αυτών των ηλεκτρονικών επιθέσεων να είναι αργή, επίπονη και να ολοκληρώνεται πολλές φορές ακόμα και μετά το πέρας της επίθεσης. Πράγματι, πρόσφατες επιθέσεις έχουν αποδείξει ότι μπορούν να κυριεύσουν δεκάδες χιλιάδες υπολογιστές και να προ-

- An “undercover” computer
 - which has no ordinary users
 - which provides no regular service
 - Or a few selected services if needed
 - Just waits to be attacked...
- Its value lies on being compromised
 - Or in being exploited, scanned, etc.
- Honeypots are an “easy” target
 - But heavily monitored ones
 - If attacked, they log as much information as possible



- Widely publicized: The cuckoo's egg
 - By Cliff Stoll
- Cliff Stoll noticed a 75-cent accounting error in the computer he managed
 - This led Cliff to discover an intruder named “Hunter”
 - Instead of shutting “Hunter” out, Cliff started to study him
 - He connected the modem lines to a printer
 - He created dummy “top-secret” directories to “lure” “Hunter” into coming back
 - He was paged every time “Hunter” was in
 - He traced “Hunter” to a network of hackers
 - Paid in cash and drugs and
 - Reporting directly to KGB



- Three types of sensors:
 - **Traditional honeypots** who wait to be attacked
 - **Collaborating organizations** who install low-interaction honeypots and forward “interesting” attacks to NoAH core
 - **Honey@Home**: A “screensaver” who forwards all unwanted traffic to NoAH
 - Unwanted traffic received at
 - unused IP addresses
 - unused TCP/UDP ports



- In a week from today (May 17th) is the
 - World Telecommunication Day 2006 (WTD)
 - Commemorates the founding of ITU
 - WTD 200 is Dedicated to
 - “Promoting Global Cybersecurity”



- Let us take this opportunity
 - Of the World Telecommunication Day
 - Dedicated to promoting Global Cybersecurity
 - And promote cybersecurity and Internet Safety
 - By promoting awareness
 - By empowering small organizations
 - By empowering people to contribute and make a difference
- Thank you all...



CyberSecurity Research in Crete

Evangelos Markatos

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)

Crete, Greece

