THE PARLIAMENT
POLITICS, POLICY AND PEOPLE MAGAZINE
Issue 261
18 February 2008

*INSIDE*
Brian Simpson
Bryan Gray
Leif Johan Sevland
Mary Miller

# Come together

*"THE OPENING EVENTS MARK THE START OF WHAT WILL BE A TRULY REMARKABLE YEAR"*

Everyone's invited as Liverpool and Stavanger kick off as European capitals of culture 2008

Günter Verheugen on helping Europe's SMEs

Maritime policy with Jo Borg

Who cares about carers, asks Marian Harkin

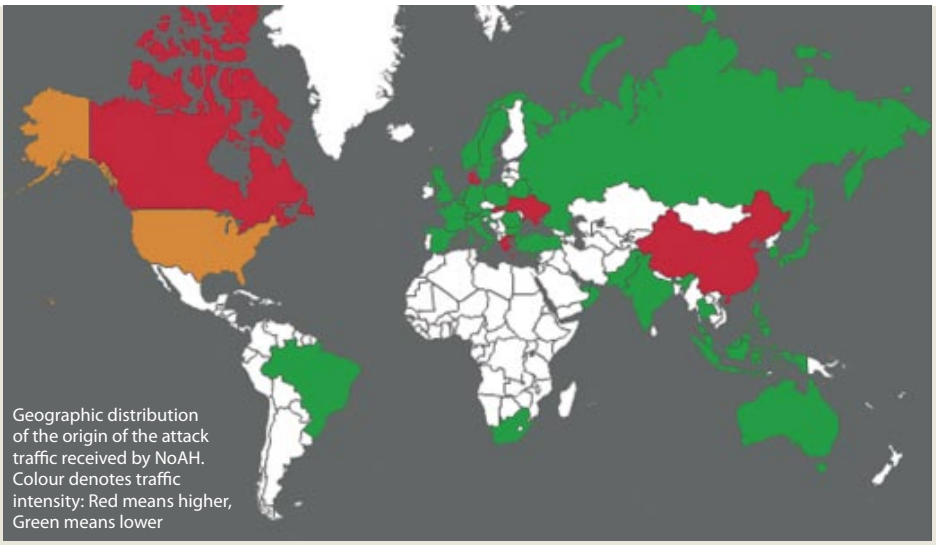
CLEAN COAL: Christian Ehler, Herbert Reul and Thorsten Diercks

EUROPEAN BUSINESS SUMMIT PREVIEW: Philippe de Buck and Rudi Thomaes

DODS

# **NoAH:** A European Network of Affined Honeypots for cyber-attack Tracking and Alerting

By Evangelos Markatos and Kostas Anagnostakis
FORTH-ICS, Crete Greece
markatos@ics.forth.gr



Geographic distribution of the origin of the attack traffic received by NoAH. Colour denotes traffic intensity: Red means higher, Green means lower

Over the past decade we have witnessed a large number of cyber attacks targeting all kinds of computing devices ranging from prominent web sites, to ordinary home computers, and, lately, mobile phones. When the Code Red Internet worm broke out in 2001, hundreds of thousands of Web servers were crippled in just a few days, causing serious disruption worldwide. Despite the increased awareness and significant effort from industry and public authorities alike, seven years later we are still exposed to threats online, primarily due to the fact that the Internet is becoming more and more lucrative as a target, and also because attackers seem to be innovating with alarming success.

The NoAH project, supported by the European Union through a Design Study implemented as a Specific Support Action in the Sixth Framework Programme, promises to make a significant contribution towards addressing the challenge of gathering and analyzing information about the nature of Internet attacks, so that appropriate countermeasures can be taken to combat them.

The guiding design practice in NoAH is that large numbers of mechanized attacks can only be tracked timely and efficiently through automated approaches. This automation is achieved through the use of **"bait" computers** called **honeypots** that are intentionally left vulnerable. Although seemingly an easy target, these honeypots are heavily monitored and record all attacks made against them. By studying the information collected by the honeypots, NoAH researchers are able to monitor and study the patterns of cyber attacks against the European cyberspace.

In this cat and mouse game, NoAH is employing a variety of smart and interesting tactics. One of these is the **honey@home** network (http://www.honeyathome.org), which extends the reach of the "bait" network to homes and small business networks. With **honey@home**, any citizen with network connectivity can participate in the NoAH network and contribute computing resources, in the same spirit as the SETI@home network tries to detect structured communication from space signals. While extra-terrestrial life may be hard to find, the NoAH infrastructure has already captured several thousands of unique attack records, which are quickly becoming indispensable as base data for guiding the design of next-generation security tools.

**Contact Person:**
Evangelos Markatos
markatos@ics.forth.gr

**Project Partners:**
Foundation of Research and Technology - Hellas, Vrije Universiteit, TERENA, FORTHnet SA, DFN-CERT, ETH Zurich, Virtual Trip Limited, ALCATEL-LUCENT

**Useful Links:**
http://www.fp6-noah.org
http://www.honeyathome.org

**Funding :**
NoAH, a Design Study implemented as a Specific Support Action, is being funded by Research Infrastructures through Contract 011923 (RIDS).

**EU Scientific Officer:**
Lorenza Saracco

**Head of Unit:**
Hervé Pero