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 IST-funded projects, LOBSTER and NoaH, whose goal is to roll out the necessary infrastructure to support research, development and experimental deployment of advanced cyber-defence mechanisms.

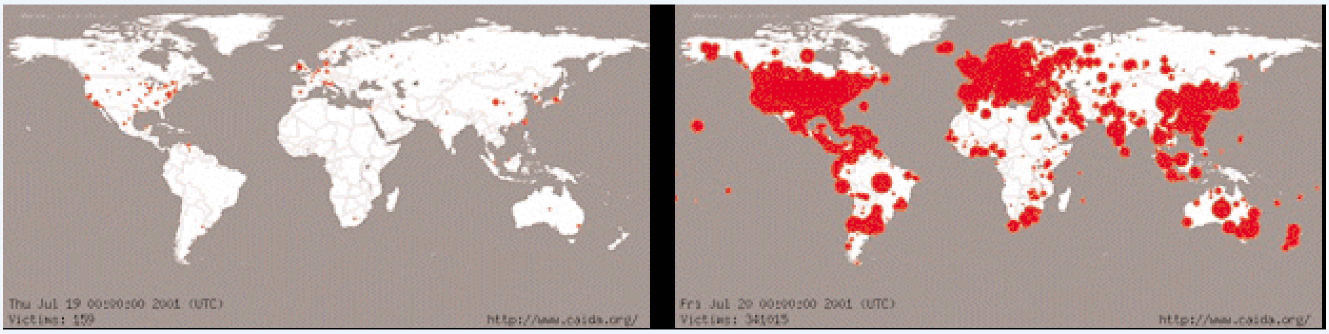
LOBSTER aims at providing a pilot infrastructure for passive Internet traffic monitoring that will improve current understanding of the Internet, and will contribute towards solving difficult performance and security problems. Based on appropriate abstractions and cooperation among several points of presence, LOBSTER will help to monitor the underlying network, providing early warning of security incidents, as well as accurate and meaningful measurements of performance. The main goal of LOBSTER is to deploy an advanced pilot European Internet Traffic Monitoring Infrastructure, based on passive monitoring sensors at speeds starting from 2.5Gbps and ranging possibly up to 10Gbps. The architecture of the system is heavily influenced by and will make use of the knowledge, software and hardware artefacts obtained by a core group of project partners in SCAMPI, a recently completed IST research project.

NoAH is a three-year project developing infrastructure for security monitoring based on honeypot technology. Honeypots are computer systems that do not provide production services, but are instead intentionally made vulnerable and closely monitored to analyse attacks directed at them. NoAH will use geographically dispersed honeypots as an early-warning system, and will correlate the data received from them to generate automated warnings and possibly trigger appropriate containment measures.

The two projects use complementary approaches towards the same goal, namely, to help ISPs and National Research Networks limit the damage to their networks, allow information security organizations to better assess threats, and provide researchers with a wealth of attack-related data to improve detection techniques. The participants will be able to gather and analyse information about the nature of Internet cyber-attacks by developing an infrastructure to detect and provide early warning of such attacks, so that appropriate countermeasures may be taken to combat them. Both efforts are exploring opportunities for supporting other related initiatives, including Geant and the global Honeynet project.

Links:
http://dcs.ics.forth.gr/
http://www.ist-lobster.org/
http://www.fp6-noah.org/

Please contact:
Evangelos Markatos, ICS-FORTH, Greece
E-mail: markatos@ics.forth.gr



Modern worms have demonstrated that they can infect tens of thousands of computers worldwide in a few hours. Source: http://www.caida.org/ analysis/security/code-red/