enisa European Network and information Security Agency

ENISA Quarterly

IN THIS EDITION

Early Detection, Warning and Alerting Systems

Vol. 3, No. 1, Jan-Mar 2007

A WORD FROM THE EXECUTIVE DIRECTOR

To mark the European Union's (EU) 50th birthday we have recently witnessed a three-day commemoration in Crete, where ENISA is based. Speaking in mythological terms, Crete is indeed the cradle of Europe, as it was here that Zeus brought Europa centuries ago. So with one of the EU's 28 'satellite' agencies scattered around Europe, ENISA, here on the island, Crete was a natural starting point for celebrations, and we participated actively in these events. Three Members of the European Parliament participated in the public debates which were organised on Europe and on the role and future of our Agency.

On 22 March we welcomed the members of the Management Board to Crete for their 10th plenary meeting. This took place in the City Hall of Heraklion, and was inaugurated by the Greek Deputy Minister for Development, Mr. Neratzis.

The Management Board discussed a series of issues and provided ENISA with long and short term recommendations, as well as broad guidelines for future operations. One of the highlights was the election of a new chairperson of the Management Board, Prof. Reinhard Posch from Austria, who was elected by acclamation.

Prof. Posch commented:
"I would like to extend my gratitude towards the Management Board for their support in the election of the new Chair. At the same time I would like to stress the constructive work of my predecessor Chair, Mrs. Kristiina Pietikainen, for her highly constructive and efficient work during the installation phase of ENISA."

As the Executive Director, I can only agree and support this statement.

Since the last issue of the EQ, I have had the pleasure of visiting the two new members of the EU family, Romania and Bulgaria, and we have established ways to strengthen our collaboration in the field of Network and Information Security (NIS) for the years to come. We have also received a visit from a Romanian delegation, which confirmed our mutual commitment.

We flew to Brussels recently, and addressed the European Parliament's committee on Industry Research and Energy (ITRE). Our presentation focussed on ENISA's achievements and was very well received by the members of the committee.

I am confident that this issue of ENISA Quarterly will provide food for thought on new concepts in NIS, and I encourage you all to participate actively and contribute to this joint forum for European NIS discussions.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

ISSN1830-3609

Real-time Monitoring and Detection of Cyberattacks

Prof. Evangelos Markatos, Kostas Anagnostakis, Spyros Antonatos and Michalis Polychronakis



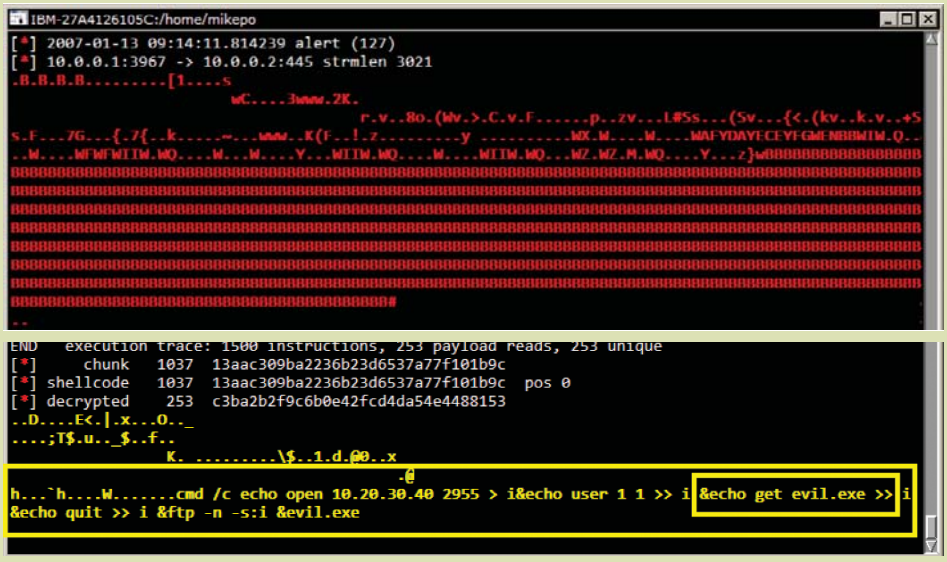

Over the last few years we have witnessed an increase in the magnitude, sophistication and speed of Internet-based cyberattacks. Motivated by fun, fame or fortune, attackers increasingly target home computers, which are then used as a springboard to perform further malicious activities, such as sending SPAM e-mail, launching Denial of Service (DoS) attacks and co-ordinating hordes of compromised computers, called 'botnets'. Such compromised computers have also been used against their legitimate owners by invading their privacy, spying on their e-mail, stealing their passwords and even blackmailing them.

Having realised the scale, ferocity and potential impact of such planet-wide Internet-based cyberattacks, the Distributed Computing Systems Laboratory at FORTH-ICS has set up and is currently co-ordinating two European projects, LOBSTER and NoAH, which target the early detection, fingerprinting and mitigation of cyberattacks. Complementary in their technical approaches, but sharing the same goal of detecting sophisticated attacks early enough, both projects have already started to produce their first success stories.

LOBSTER

LOBSTER (Large Scale Monitoring of Broadband Internet Infrastructure, www.ist-lobster.org) uses a passive network monitoring approach to detect attackers trying to penetrate legitimate computers. LOBSTER has already deployed several sensors throughout Europe, which monitor the traffic on the Internet in order to gain a better understanding of its performance as well as to spot any security incidents. Capitalising on state-of-the-art monitoring software and advanced detection heuristics, LOBSTER examines the network traffic coming in to ordinary computers for possible signs of intrusion.

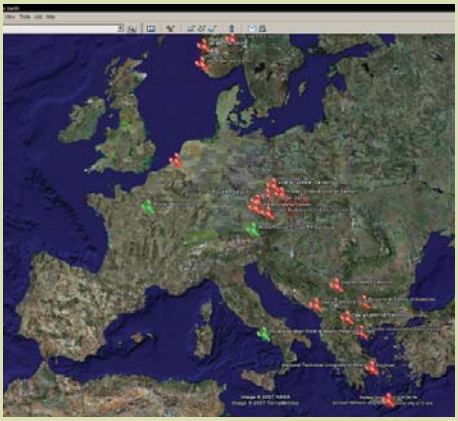
To evade such detection mechanisms, cyberattackers have developed sophisticated polymorphic attack vectors; that is, they have managed to transform their attacks into innocent-looking series of characters which at first glance do not look like part of a malicious attack. To counter polymorphic cyberattacks, LOBSTER has developed advanced polymorphism detection mechanisms that manage to inspect deep inside network packets beyond their seemingly innocent exteriors to discover any hidden attacks beneath.



The content of an incoming network packet (in red) captured by a LOBSTER sensor on the island of Crete. Although apparently innocuous, when 'executed' by a virtual machine on the LOBSTER sensor, these red characters transform themselves into the yellow characters shown in the second part of the diagram which instructs the victim computer to download and execute a cyberattack.

For example, the diagram below left shows the content of an incoming network packet (in red) captured by a LOBSTER sensor on the island of Crete. These red characters do not seem to contain any attack. However, when these red characters are 'executed' by a virtual machine on the LOBSTER sensor, they slowly but steadily transform themselves into the yellow characters shown in the second part of the diagram which, in ASCII human-readable form (shown in the big yellow box), force the target computer to connect using ftp to IP address 10.20.30.40 (anonymised form of the real IP address), to download file 'evil.exe' (shown in the small yellow box) and to execute it.

The LOBSTER sensor infrastructure has already collected dozens of such attacks which are properly anonymised and will eventually be shared in the public domain. It should be emphasised that these attacks captured by the LOBSTER sensors are against real computers (live traffic) including PCs, laptops and even IP telephones!

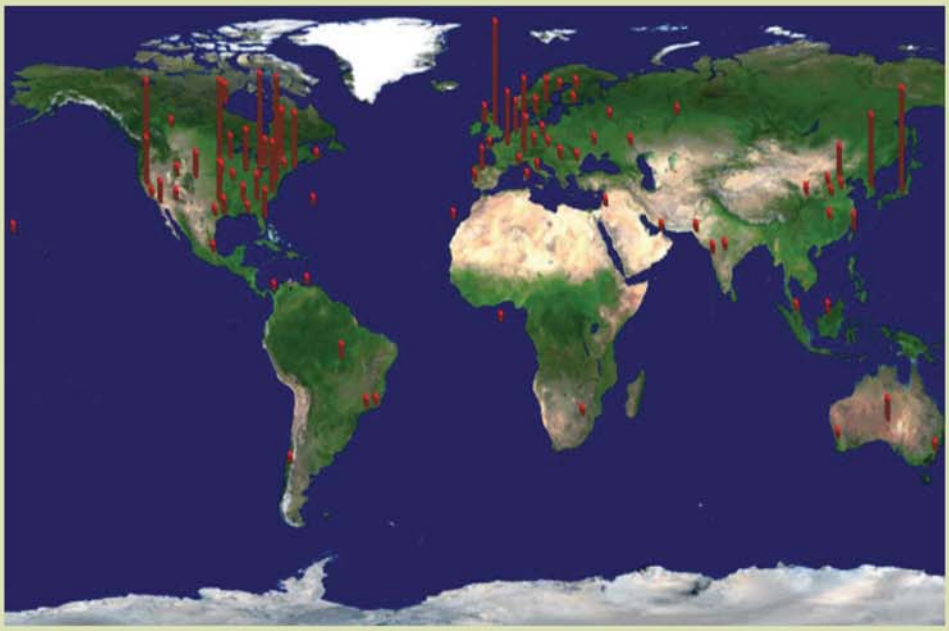


The geographic location of LOBSTER sensors

NoAH

While LOBSTER sensors monitor real-time network traffic aimed at live computers, the NoAH project, a European Network of Affined Honeypots (www.fp6-noah.org), monitors the shadows, the dark spaces and the back corners of the Internet in its quest to detect, fingerprint, and mitigate cyberattacks based on state-of-the-art honeypot technology.

A honeypot is a computer which usually does not serve any ordinary users and whose main value is in being compromised by attackers. Thus, honeypots usually listen to unallocated IP addresses on the Internet (which are usually called 'dark address space') in order to detect any unusual activity. By luring attackers and by willingly getting compromised, a honeypot captures a wealth of information about the attackers, about the mechanisms they use to



Graphical representation of the geographic origin of cyberattacks captured by FORTH's honeypots.

penetrate computers, about the software they download and about other computers they communicate with.

The attack information can be used then to understand the attacker's tactics, provide a fingerprint for it, and generate a signature that can be used by Intrusion Detection/Prevention Systems (IDS/IPS) for example, to defend against this kind of attack in the future. The diagram above shows the geographic origin of such attacks captured by NoAH honeypots installed at FORTH.

To empower ordinary home (and small business) users in the fight against cyberattacks, FORTH has developed 'Honey At Home' (honey@home, www.honeyathome.org/), which is a light-weight software-only honeypot that monitors unused IP addresses or port ranges of home-users, reporting to central NoAH honeypots all suspicious activity which might be a potential attack to that home-user. Based on sophisticated taint-based analysis, the central NoAH honeypots in turn differentiate between random activity and targeted attacks.

Conclusion

In conclusion, by monitoring live network traffic and unused IP address space and searching to detect, fingerprint and mitigate attacks spreading on the Internet, both projects LOBSTER and NoAH are already making tangible contributions towards early real-time cyberattack detection.

Evangelos Markatos (markatos@ics.forth.gr) is the director of the Distributed Computing Systems laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete and a member of the Permanent Stakeholders Group established by ENISA.

Kostas Anagnostakis (kanag@ics.forth.gr) is a researcher at I2R in Singapore and visiting associated researcher at FORTH-ICS.

Spyros Antonatos (antonat@ics.forth.gr) is a member of the Distributed Computing Systems laboratory at FORTH-ICS and a Ph.D. Candidate at the University of Crete.

Michalis Polychronakis (mikepo@ics.forth.gr) is a member of the Distributed Computing Systems laboratory at FORTH-ICS and a Ph.D. Candidate at the University of Crete.