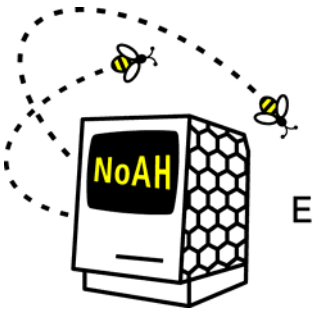
SIXTH FRAMEWORK PROGRAMME
Structuring the European Research Area Specific Programme

RESEARCH INFRASTRUCTURES ACTION



European Network of Affined Honeypots

Contract No. RIDS-011923

D4.4: Dissemination Results

Abstract:

This document summarises how public awareness of the project has been achieved, through the website, workshops, presentations at relevant events, and various publications.

Contractual Date of Delivery	30 September 2008
Actual Date of Delivery	31 October 2008
Last Update Date	31 October 2008
Deliverable Security Class	Public
Editor	Kevin Meynell
Contributors	Kevin Meynell

The NoAH Consortium consists of:

FORTH-ICS	Coordinator	Greece
VU	Partner	Netherlands
TERENA	Partner	Netherlands
FORTHnet	Partner	Greece
DFN-CERT	Partner	Germany
ETH Zurich	Partner	Switzerland
Virtual Trip	Partner	Greece
Alcatel	Partner	France

Table of Contents

1. Website

For EC-funded projects, and arguably for any activity these days, a website is the most effective method of disseminating information. As it is accessible to anyone with Internet access, this effectively means that information is available on a worldwide basis. For this reason, the development and maintenance of a high-quality website was one of the major activities in the NoAH project.

The NoAH website can be accessed at http://www.fp6-noah.org/, and includes an overview of the project, and makes available the research results and software that was developed. It also provides links to complementary websites associated with NoAH, as well as to other related activities. All informational articles, scientific papers and presentations produced during the project lifetime can be found on the website. The website is primarily targeted at the worldwide research and education community, although much of the material is relevant to other sectors as well.

A very distinctive and eye-catching design for chosen for the website, and this was later extended to other dissemination materials. In particular, the logo proved very successful, and several requests were received from around the world to use it as a generic logo for honeypots.

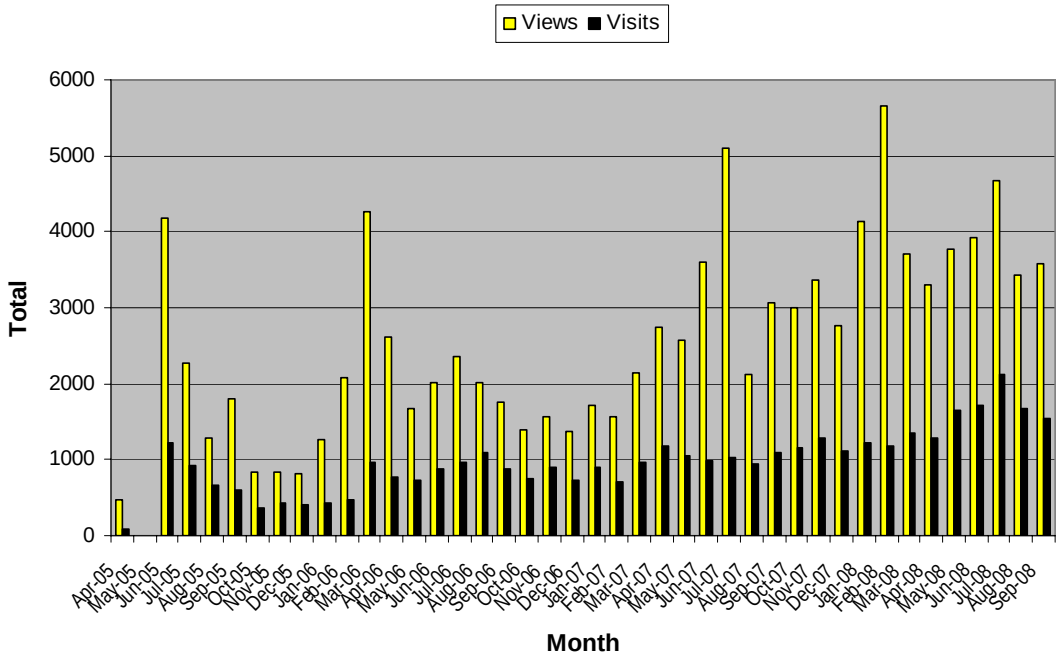
This section provides a summary of usage of the public website during the 42-month lifetime of the project (1 April 2005 – 30 September 2008), based on three main categories:

- Visits are defined as the number of times users viewed the website. However, the viewing of several pages by a user (using the same host) within a specific time limit (20 minutes) only counts as one visit.
- Unique visitors are defined as those who have visited the website at least once during a specific period (using the same host).
- Repeat visitors are those users who returned to the website (using the same host) having previously viewed it during the same specific period.

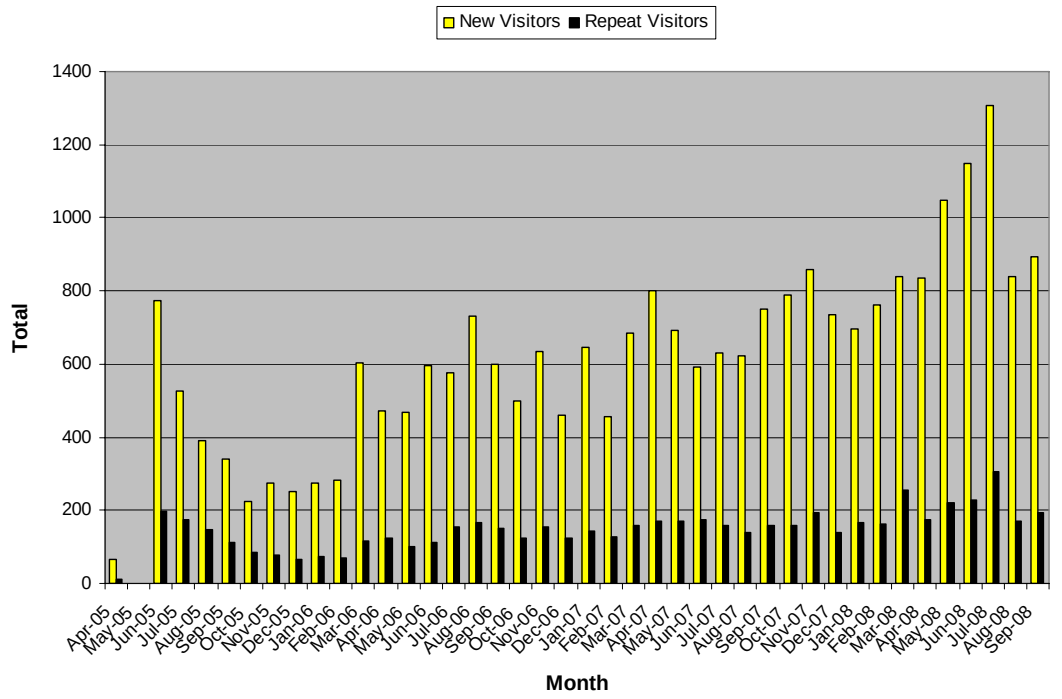
Total Visits and Visitors

Total visits	40,348
Unique visitors	29,121
Repeat visitors	6,106
Total pages viewed	210,897
Average visits per visitor	1.39
Average visits per repeat visitor	2.33
Average pages viewed per visitor	7.24

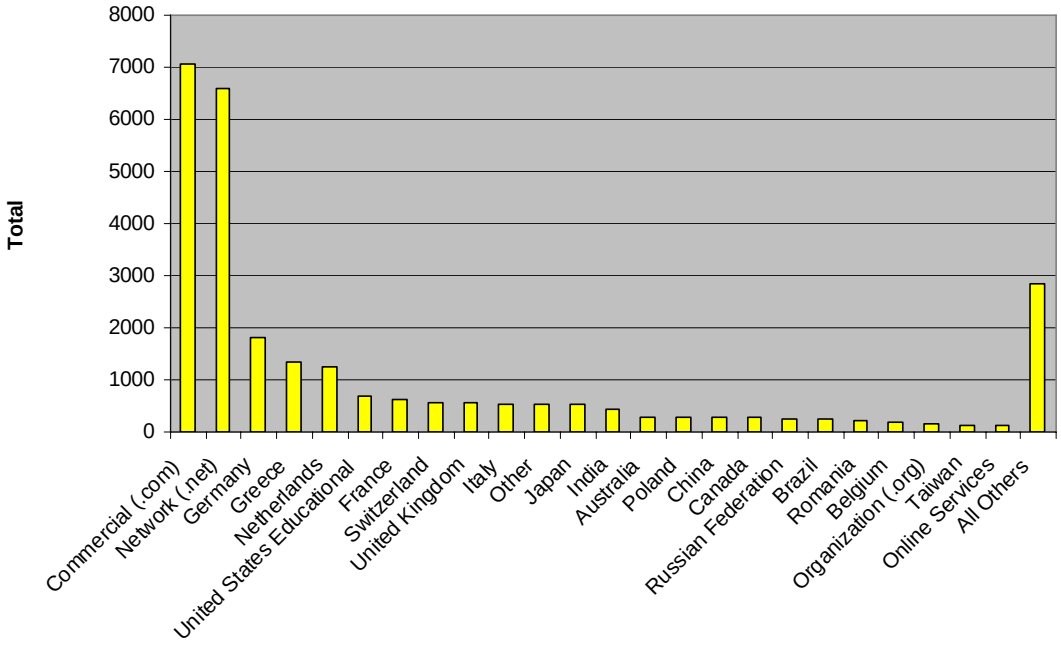
Total Views and Visits by Month



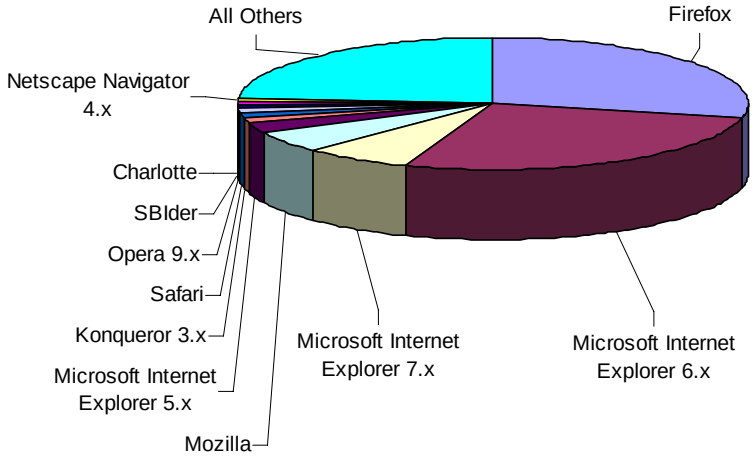
Unique and Repeat Visitors by Month



Visits by Domain (excluding unresolved domains)



Most Popular Browsers



Most Requested Pages (Top 40)

Page	**Visits**
NoAH Home Page	20,995
Publications	3,597
Partners	3,122
About NoAH	2,402
Calendar of Events	2,842
Related Sites	1,643
NoAH Survey	1,440
D0.1: Survey on the State-of-the-Art	1,384
Media coverage of the NoAH project	1,301
D1.2: Attack Detection and Signature Generation	1,293
D1.1: Honeypot Node Architecture	1,219
Argos: an Emulator for Fingerprinting Zero-Day Attacks paper	1,011
D1.4 Architecture Integration	817
Detecting Targeted Attacks Using Shadow Honeypots	816
1st NoAH Workshop	780
D0.2: Requirements Collection and Analysis	756
Downloads	739
D2.2 Prototype Implementation	708
SafeCard: a Gigabit IPS on the network card paper	707
NoAH Flash Demo	665
Network-level Polymorphic Shellcode Detection using Emulation paper	656
NoAH Honeynet Project	561
D2.2 Prototype Implementation	512
2nd NoAH Workshop	446
D1.5: Shadow Honeypots	444
D2.1 Core components implementation	441
D1.3 Containment Environment Design	393
Writing a successful proposal: the NoAH approach presentation	314
Detecting Targeted Attacks Using Shadow Honeypots paper	312
D2.3: Containment mechanisms for commodity switches	296
EU-Projekt NoAH zur Früherkennung und Bekämpfung von neuen Cyberattacker paper	275
The NoAH approach to zero-day worm detection presentation	272
NoAH Leaflet	269
Eudaemon: Involuntary and On-Demand Emulation Against Zero-Day Exploits paper	243
The Impact of Honeynets for CSIRTs paper	231
D2.4: Enhanced NoAH implementation and optimizations	212
Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart paper	191
Honey@home: Trapping Attacks on the Internet	186
NoAH: A European Infrastructure for Cyberattack Detection presentation	177

2. Workshops

NoAH organised two informational workshops during the lifetime of the project. The first workshop focused on explaining the rationale of the NoAH infrastructure and presented some preliminary results. The second workshop focused on disseminating achieved results and motivating participation in the NoAH infrastructure.

1st NoAH Workshop

The 1st NoAH workshop was held on 17 May 2006 in Catania, Italy (in conjunction with TNC 2006). It attracted around 70 participants.

This workshop presented the pilot honeypot infrastructure being developed by the NoAH project. It also outlined the techniques being developed for the automatic identification of cyberattacks, and the mechanisms used to distribute this information to firewalls and other containment systems.

More information can be found at http://www.fp6-noah.org/events/workshop-1/

2nd NoAH Workshop

The 2nd NoAH workshop was held on 20 May 2008 in Bruges, Belgium (in conjunction with TNC 2008). It attracted more than 60 participants.

This workshop presented the current activities of the NoAH project, along with other relevant work related to honeypots. It included talks on the Argos secure system emulator, the honey@home client that can be used on end-systems, and on signature generation and analysis.

NoAH also organised a booth at TNC 2008, where several demos of the working project prototype showed in real-time the network attacks being captured by the NoAH Honeypots. Several participants visited the booth, and expressed their interest in collaborating with the NoAH partners.

More information can be found at http://www.fp6-noah.org/events/workshop-2/

3. Publications

Promotional Material

NoAH produced an informational leaflet for promotional purposes that outlined the aims and goals of the project, whilst highlighting the Argos and honey@home software. This was distributed at variety of conferences and other events, as well as being made available on the NoAH website at http://www.fp6-noah.org/publications/noah-leaflet-print.pdf.

To accompany the leaflet, an attractive A3-sized poster was also produced for displaying at relevant events (see http://www.fp6-noah.org/publications/NoAH-posterA3.pdf). To complement this, an interactive demonstration was produced in Adobe Flash (see http://www.fp6-noah.org/demo_flash.html). This was primarily used for the NoAH display stands, but both the poster and demonstration are available on the NoAH website.

News Items & NoAH Blog

NoAH issued several news items during the course of the project that were circulated via the NoAH informational mailing list, and TERENA's established PR channels (e.g. website, inter-NREN news exchange, and relevant mailing lists). These were used to promote the project and highlight important developments such as the release of honey@home, Argos, and the NoAH workshops.

The NoAH Blog (http://blogs.fp6-noah.org/) was started in early-2008 as a more proactive way of providing information about the project, and highlighting the most recent developments. It allowed individual members of the project to publish articles on particular aspects of their work, and to discuss real-world experiences with the NoAH technology.

Informational Articles

NoAH had several articles about the project published in the Economist (Greek Edition) and European Parliament magazines, a Greek scientific newspaper, as well as the ERCIM and the ENISA newsletters:

- S. Antonatos, E. Athanasopoulos, K. Anagnostakis & E. Markatos; *Honey@home: Trapping Attacks on the Internet*; Economist (Greek Edition), September 2007. (Greek language)
- E. Markatos and K. Anagnostakis; *NoAH: A European Network of Affined Honeypots for Cyber-Attack Tracking and Alerting*; The Parliament Magazine, Issue 262, 3 Mar 2008.
- E. Markatos, K. Anagnostakis, S. Antonatos and M. Polychronakis; *Real-time Monitoring and Detection of Cyberattacks*; ENISA Quarterly, Vol. 3, No. 1, Jan-Mar 2007.
- E. Markatos, S. Antonatos and K. Anagnostakis; *Honeypot Computer, "Discovering Hackers, with a honeypot as bait"*; "Pro[ek]taseis", Special Issue of Naftemporiki Newspaper, December 2006. (Greek language)
- S. Antonatos, K. Anagnostakis and E. Markatos; *A European platform for the detection and containment of cyber-attacks* - The Economist (Greek Edition), February 2006. (Greek language)
- K. G. Anagnostakis & E. Markatos; *Towards a European Malware Containment Infrastructure*; ERCIM News No.63, October 2005.

Published Papers

NoAH had twelve scientific papers accepted for publication during the course of the project:

- K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos & A. D. Keromytis; *Detecting Targeted Attacks Using Shadow Honeypots*; Proceedings of the 14th USENIX Security Symposium, Baltimore, USA, August 2005.
- B. Tellenbach; *EU-Projekt NoAH zur Früherkennung und Bekämpfung von neuen Cyberattacken*; Security Zone Newsletter, March 2006. (German language)
- G. Portokalidis, A. Slowinska & H. Bos; *Argos: an Emulator for Fingerprinting Zero-Day Attacks*; Proceedings of ACM SIGOPS Eurosys 2006, April 2006.
- J. Kohlrausch, J. Schönfelder *The Impact of Honeynets for CSIRTs*; 18th Annual FIRST Conference, Baltimore, USA, June 2006.
- M. Polychronakis, K. G. Anagnostakis, and E. P. Markatos; *Network-level Polymorphic Shellcode Detection using Emulation*; Proceedings of the GI/IEEE SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), Berlin, Germany, July 2006.
- W. de Bruijn, A. Slowinska, K. van Reeuwijk, T. Hruby, L. Xu, and H. Bos; *SafeCard: a Gigabit IPS on the network card*; Proceedings of RAID'06, Hamburg, Germany, September 2006.
- E. Athanasopoulos and S. Antonatos; *Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart*, Proceedings of CMS'06, Heraklion, Greece, October 2006.
- M. Polychronakis, K. G. Anagnostakis, and E. P. Markatos; *Emulation-based Detection of Non-self-contained Polymorphic Shellcode*; Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID); Gold Coast, Australia, November 2007.
- M. Valkering, A. Slowinska and H. Bos; *Tales from the Crypt: fingerprinting attacks on encrypted channels by way of retainting*; 3rd European Conference on Computer Network Defense (EC2ND 2007), Heraklion, Greece, October 2007.
- S. Antonatos, K. G. Anagnostakis and E P. Markatos; *Honey@home: A New Approach to Large-Scale Threat Monitor*; Proceedings of the 5th ACM Workshop on Recurring Malcode (WORM 2007), Alexandria, USA, November 2007.
- A. Slowinska and H. Bos; *The Age of Data: pinpointing guilty bytes in polymorphic buffer overflows on heap or stack*; Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC'07), Miami, USA, December 2007.

- G. Portokalidis & H. Bos; *Eudaemon: Involuntary and On-Demand Emulation Against Zero-Day Explorts*; Proceedings of ACM SIGOPS/EUROSYS 2008, Glasgow, UK, April 2008.

4. Software

The software developed by the NoAH project has been made available on the NoAH website for download:

Argos Secure System Emulator -This is a full and secure system emulator designed for use in honeypots. It is based on Qemu, an open source emulator that uses dynamic translation to achieve a fairly good emulation speed. It supports multiple operating systems and CPU types, and does not require any modification of the guest operating system.

honey@home client - This is a client-side implementation of the NoAH project, aiming to facilitate the gathering of information on cyber-attacks. It can be installed on either a Window or Linux system and is designed to be simple to manage and lightweight on system resource usage. It runs as a background process and interacts with a centralised honeypot when it receives traffic of interest.

Shelia client-side honeypot - This is a simple intrusion detection client for Windows. It comes with a client emulator that scans through a mail folder (typically the spam folder) specified on the command line, and is capable of opening every attachment and following URLs. It monitors the processes and generates alerts when these attempt to execute invalid operations.

Signature Generator - This is used to receive alerts from another application (e.g. Argos) and generate a signature for the attack. It is designed and implemented as a framework, and features a plug-in structure and a template mechanism. It also features a logging component and load balancing for efficient operation on multi-core systems.

5. Presentations

A number of presentations about the NoAH project were given at various conferences and other events during the lifetime of the project:

- Writing a successful proposal: the NoAH approach - *Evangelos Markatos, Information Day on Research Infrastructures, Athens, 21 December 2004.*
- Detecting Targeted Attacks Using Shadow Honeypots - *Kostas Anagnostakis, 14th USENIX Security Symposium, Baltimore, 4 August 2005.*
- CyberSecurity Research in Crete - *Evangelos Markatos, Safeline Focus Group on "Safety in the Mobile Internet", Athens, Greece, 10 May 2006*

- NoAH Honeynet Project - *Klaus Moeller, 17th TF-CSIRT Meeting, Amsterdam, 24 January 2006.*
- The NoAH approach to zero-day worm detection - *Asia Slowinska, 19th TF-CSIRT Meeting, Espoo, 22 September 2006.*
- NoAH: A European Infrastructure for Cyberattack Detection - *Catalin Meirosu, 23rd APAN Meeting, Manila, 25 January 2007.*
- Honey@home - *Spiros Antonatos, 20th TF-CSIRT Meeting, Budapest, 30 January 2007.*
- NoAH: A European Infrastructure for Cyberattack Detection - *Catalin Meirosu, IUCC-TERENA Workshop, Tel Aviv, 16 March 2007.*
- Intrusion Detection Systeme: Trends und Herausforderungen - *Bernhard Tellenbach, Zuercher Tagung 2007, Zürich, 3 May 2007.*
- Prospector: Analysis of Heap and Stack Overflows using Emulated Hardware - *Asia Slowinska, NLUUG 2007 Conference, Ede, 10 May 2007.*
- The NoAH Project - poster presentation - *S. Antonatos, D. Brauckhof, B. Tellenbach, A. Slowinska, TNC 2007, Copenhagen, 20-24 May 2007.*
- Network of Affined Honeypots - More Than an Infrastructure - *Spiros Antonatos, TNC 2007, Copenhagen, 23 May 2007.*
- Fingerprinting Intruders - *Herbert Bos, TNO Security Knowledge Network Meeting, Groningen, 31 May 2007.*
- Emulation-based Detection of Non-self-contained Polymorphic Shellcode - *M. Polychronakis, RAID'07, Gold Coast, 6 September 2007.*
- Automated Signature Generation: Overview and the NoAH Approach - *Bernhard Tellenbach 22nd TF-CSIRT meeting, Porto, 21 September 2007.*
- Emerging Ways to Protect your Network: From Vulnerability Scanning to Real-time Monitoring and Detection of Cyberattacks - *Konstantinos Xinidis, 3rd Regional Electronic Security Forum, Thessaloniki, 11-12 October 2007.*
- Tales from the Crypt: fingerprinting attacks on encrypted channels by way of retainting – *M. Valkering, EC2ND 2007, Heraklion, 4 October 2007.*
- Honey@home: A New Approach to Large-Scale Threat Monitor - *S. Antonatos, WORM 2007, Alexandria, 2 November 2007.*
- The Age of Data: pinpointing guilty bytes in polymorphic buffer overflows on heap or stack - *A. Slowinska, ACSAC'07, Miami, 14 December 2007.*
- Eudaemon: Involuntary and On-Demand Emulation Against Zero-Day Exploits - *G. Portokalidis, ACM SIGOPS/EUROSYS 2008, Glasgow, 4 April 2008.*

6. NoAH in the Media

There proved to a great deal of interest in the NoAH activities from both the online and printed media, which reflected the impact of the project's dissemination efforts. This interest was not just restricted to specialist media, but extended to mainstream publications as well. In addition to the articles written by project itself (that are listed in Section 2), articles mentioning the NoAH project and/or its activities appeared in the following publications:

- Groot onderzoek VU naar computervirussen - *De Telegraaf, 19 January 2005.* (Dutch language)
- Groot onderzoek VU naar computervirussen - *De Volkskrant, 19 January 2005.* (Dutch language)
- Universiteit doet onderzoek naar virussen en wormen - *Computer Idee, 20 January 2005.* (Dutch language)
- Grootscheeps computervirusonderzoek bij de VU - *Computable (Dutch), 20 January 2005.* (Dutch language)
- VU haalt recordsubsidie virusonderzoek binnen – *Edusite, 25 January 2005.* (Dutch language)
- Condoom voor het netwerk – *Computable, 25 February 2005.* (Dutch language)
- Electronic "burglars" of the Internet - *Tolmi Newspaper, 13 August 2005.* (Greek language)
- Vrije Universiteit werkt aan 'vaccin' voor internet - *Nu.nl, 14 Jan 2006.* (Dutch language)
- Opsporing Verzocht - *Computable, February 2006.* (Dutch language)
- EU-Projekt NoAH zur Früherkennung und Bekämpfung von neuen Cyberattacken - *Security Zone Newsletter, March 2006.* (German language)
- Feature: "Lab rats" - *Bright Magazine, April 2006.* (Dutch language)

NoAH activities were also mentioned on the following websites:

- Worm blog reporting on SweetBait TR - *Worm blog, 13 October 2005.*
- Argos: an Emulator for Capturing Zero-Day Attacks - *Nepenthes/mwcollect news, 22 December 2005.*
- Evolutions in the honeypot/honeynet arena - *Geek Log, 26 December 2005*
- Mit mwcollect, QEMU, nepenthes und Argos kommen neue Techniken zur Malwareanalyse - *Network Secure News, 27 December 2005.* (German language)
- Argos: An Emulator for Capturing Zero-Day Attacks - *The gaetano Honeypots Archive, 31 December 2005.*

- NoAH: European Network of Advanced Honeypots - *Thorsten's Holz Honeyblog, 3 March 2006.*
- Argos: An Emulator for Capturing Zero-Day Attacks - Thorsten's Holz Honeyblog, 9 March 2006.
- Argos: Un emulador para capturar ataques 0 day - Sergio's Hernando Blog, 12 March 2006. (Spanish language)
- Features a description of Argos, as well as links to the papers on Argos and SweetBait - honeypots.net, 30 March 2006.
- HoneyBlog reporting on SweetBait TR - *HoneyBlog, 30 March 2006.*
- The EuroSys'06 paper about Argos was recommended reading material in the Astalavista Group Security Newsletter - A*stalavista Group Security Newsletter, 31 March 2006.*
- Argos: An Emulator for Capturing Zero-Day Attacks - *Del.icio.us, May 2006.*
- Argos: An Emulator for Capturing Zero-Day Attacks - *SWiK, 7 June 2006.*
- Shelia: A Client-side Honeypot for Attack Detection - *Honeyblog, 6 March 2007.*
- Interview with Niels Provos and Thorsten Holz about their book 'Virtual Honeypots: From Botnet Tracking to Intrusion Detection' which writes about Argos in some detail – *NetworkWorld, 10 August 2007.*
- Research that matters - more insights into NOAH the European Network of Affined Honeypots research project - *CyTRAP Labs, 1 November 2007.*
- NoAH jagt Buffer Overflows und Zero-Day-Exploits - *SearchSecurity.de, 4 July 2008.* (German language)