Publication in “Pro[ek]taseis”, special issue of Naftemporiki Newspaper, December 2006

Honeypot Computer, "*Discovering Hackers, with a honeypot as bait*",

By Evangelos Markatos, Spyros Antonatos and Kostas Anagnostakis,
Institute of Computer Science, Foundation for Research and Technology-Hellas

Lately we are witnessing an increasing aggression activity over the Internet. Indeed, the Internet attackers widely known as “hackers” take advantage of the computers’ software weaknesses and manage to gain control and access to these computers, which they subsequently use for their illegal purposes.

Initially by curiosity and sometimes to gain acceptance by their peers, the hackers have proved that they can conquer and control thousands of computers within less than half an hour, by using a new generation of auto-multiplying programs, called worms.

The hackers are aware of their significant technical abilities and in the last few years they begun to exploit this knowledge for financial gains. Where in the beginning they aimed at conquering as many computers as possible in a small time frame to attract publicity, currently their priorities mainly focus on gaining control over computers as quietly as possible, so that sometimes even the computer’s owner is not aware of being attacked. In this way, they manage to have under their control a great number of computers for a long time and thus a huge financial profit. These attacked computers, called bots (from robots) can be used to send spam emails, to download advertisements, to attack other computers, or even to be hired (news.bbc.co.uk/1/hi/technology/5407478.stm). Recent disclosures demonstrate that hackers gain five thousand dollars per month, just by hiring the computers they control. By offering full anonymity, these computers are ideal for conducting all sorts of illegal activities over the Internet.

In an effort to fight against the Internet hackers, researchers from the Foundation for Research and Technology-Hellas designed and are currently coordinating the European Project NoAH (A European Network of Affined Honeypots). In order to find and study the hackers, the researchers from FORTH use specialized computers, widely known as honeypots. A honeypot becomes easy bait that attracts the hacker, as a pot of honey would attract a bee. To be more precise, a honepot waits to be attacked by the hacker and when this happens, it records as much information as possible about the hacker’s tools, starting point, techniques and the attack’s profile in general. This profile will be then shared with other computers and then, based on the data recorded by the honeypot these computers will be able to identify and subsequently confront the same or similar attacks.

In their effort to conquer as many computers as possible, the hackers currently apply a method of arbitrary attacks, known as “random scanning”. With this technique the hackers produce “random” computer names, with purpose to communicate and take over their control. An analogous example from the typical telephone communication would be the random selection of digits to make a phone call, in the hope to access an existing phone number. The NoAH takes advantage of this arbitrary process through its advanced infrastructure and addresses these attacks by responding on behalf of non-existent computers. That is, if a honeypot becomes aware of initiating communication with a computer whose name is non-existent, one of NoAH computers temporarily disguises into that computer, in order to communicate with the hacker and gain as much information as possible about the attack.

NoAH wishes to give to all the computer users the opportunity to help trace the hackers and has developed a program called “HoneyAtHome”. The HoneyAtHome is software running on ordinary

computers, forwarding the incoming attacks to the NoAH computers for further study and analysis. The HoneyAtHome is lightweight, easy to use and can be run on all networks, households and enterprises. It offers features such as automatic updates, detailed statistics of attacks and users' anonymity.

Based on honeypots' attraction, on users' cooperation and on reserachers' effort, the NoAH project aims to make a significant step towards a safer Internet.

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