

LURING HACKERS INTO HONEYPOTS

- Network sponsored by several Norwegian companies
- Data experts skeptical

An employee in the Norwegian National Security Authority runs private surveillance of suspicious computer users by using several thousands of fake computers. - Unethical and unacceptable, says computer experts.

Per Anders Johansen

Through a private organization the employee at the Norwegian National Security Authority (NSM) performs surveillance of people suspected for hacking. At least ten different networks with several thousands of fake computers have been placed around Norway. The networks are "honeypots" luring in - and then surveils - suspicious computer users and hackers.

The networks are owned by the volunteer non-profit organization The Norwegian HoneyNet Project, which was started and is lead by a security expert at NSM. The Norwegian Chapter is a part of the volunteer organization HoneyNet.

- We have to trick the hacker to visit our home, without the him knowing. This sounds like a difficult task, but this is some of what honeynets are about. Tricking a hacker into our systems, allowing us to monitor him without his knowledge. We are then able to see what he is typing on the keyboard, who he is attacking and what he is planning, it says in a presentation of the Norwegian HoneyNet Chapter.

Sponsored by Telenor. The private methods are clearly separated from what NSM is usually doing:

- The Norwegian HoneyNet Project has private sponsors such as Telenor, Lysenet, Phonet, Netpower and anonymous donations.
- The funds are used to buy computer hardware and software, which is then hooked into Internet as a "Honeypots" and "Honeynets".
- The honeytraps are luring in outsiders, e.g. hackers that try to hack the servers, and have several million visits.
- When an outsider enter the "honeypot", everything that person does, can be monitored down to a single click of the keyboard.
- The data is used to create profiles over hackers and their methodologies, computer files, IP-addresses and background.
- Information on suspicious computer users is then sent to internet providers such as Telenor and Lysenet.

Provides more info. HoneyNet is entirely open regarding what they do and have been praised by IT security companies and data journalists. The creator and leader of the Norwegian HoneyNet Project is Einar Oftedal. On his daily basis he is hired full time as a security advisor at the Norwegian National Security Authority and Computer Emergency Response Team (NorCERT). NorCERT handles serious IT-situations, but as of today they are not allowed to use honeypot based methods or run computer surveillance on private citizens.

NSM is governed by the Minister of Defense Anne-Grete Strøm-Erichsen and it is NSM's job to audit, monitor and control the security throughout the Norwegian government.

The honeypots can provide a lot more information than NSM's own official "alert and warning system for digital infrastructure" VDI, which is controlled and inspected by The Norwegian Parliamentary Intelligence Oversight Committee (EOS-utvalget).

NSM earlier raised alarms because the Defence security service (FOST) may have used methods they are not allowed to. This caused minister of defence Anne-Grete Strøm-Erichsen to press charges on suspicion of illegal surveillance of internet traffic in the government offices and the royal castle.

Aftenposten fact box

THE NORWEGIAN HONEYNET PROJECT

The international organization was started by former US Army tank driver Lance Spitzner, in 1999, to take on the battle against attackers on the internet.

Bush advisor. Spitzner has been a computer security advisor for the American defense and former president George W. Bush.

The Norwegian chapter is called The Norwegian HoneyNet Project and consists of 10 members, from research, NSM, and several companies including Telenor, Norman and Lysenet.

THIS IS A HOBBY

HoneyNet-leader and NSM-employee denotes the "honeypots" as a hobby and denies that this is surveillance.

- These computers are not used by anyone, and they are connected to the Internet to see what happens if anyone tries to attack them, says the security advisor at NSM and leader of the Norwegian HoneyNet Project Einar Oftedal.

- How far can you go with your surveillance? - Questions regarding my work at NSM, should go through the press contact at NSM.

- Are you leading the NHP as a private citizen or as NSM employee? - As a private citizen. This is a hobby project.

- Are you allowed to run this type of surveillance? - This is not surveillance.

- Your web pages say you "surveil them without their knowledge, and that you are able to see what they are typing on their keyboards". If this is not surveillance, then what is it? - The Norwegian word for surveillance has a different meaning. This has been translated from English, says Oftedal. He refers Aftenposten to Sjur Eivind Usken, the product manager at Phonect, who handles "media communication" for the Norwegian HoneyNet.

- We do not provoke attacks. We are only looking at inbound traffic. The closest thing we do, is answer requests. If a person chooses to connect to one of these computers, then that person must have certain intentions. This is more like putting up a surveillance camera in your own house, says Usken. He points to the fact that HoneyNet is open about their findings.

- How many honeytraps are deployed? - This is not public knowledge. We are running a couple of tens of nets. But for an attacker it will look like several thousands of computers

Aftenposten fact box:

THE HONEYPOTS

Here are some of the methods used by The Norwegian HoneyNet Project to disclose hackers:

- Nepenthes is an interactive honeypot that collects information about potential attacks, emulates vulnerabilities that worms spread, and catches the worm.
- HoneyC and HoneyD are different honeypots that allows you to monitor malicious computer servers in a network.
- SSH-honeypots in different Norwegian ISP networks are used to monitor hackers who try to break codes and passwords.
- VoIP honeypots used through a larger company in Norway to make the trap even more attractive to hackers who try to exploit the VoIP equipment, ie equipment to talk together over the web.
- Capture HPC is a "high-interactive" honeypot that communicates with the hackers, and makes it possible to monitor the hackers data files
- Honeytrap is a tool that makes it possible to monitor the attack against a server.

NOT A PROBLEM

This is the response of Kjetil Nilsen, director of NSM. In an email from communications advisor Liv Nodeland at NSM, its noted that "employees at NSM have on their own initiative informed NSM about their role as participants in The Norwegian HoneyNet Project in their spare time", and this has been known since 2006.

- NSM stresses that they are not themselves using "Honeypots". Then what does NSM think about their own employees using these methods in their spare time? - NSM has not considered this to be a problem, replies the NSM-director through his communication advisor.

- Have NSM received any information collected from The Norwegian HoneyNet Project and their "honeypots"? - NSM have not received information from NHP. NHP is an independent research project creating and sharing information on computer security. It is all free and publicly available on the Internet, says Nilsen.

QUESTIONABLE METHODS

This is the same as if the cops would do private stakeouts in their spare time. No police department would have accepted that, says Professor of Law, Jon Bing.

This is far more serious than to set up a surveillance camera. It is more like building a new street and setting up surveillance cameras in the whole area, without the visitors knowing that the information is stored and analyzed, says Professor of Law Jon Bing, former head of Personvernemnda, PVN (committee on privacy).

While it is commendable to fight computer crime, it is still necessary to follow the rules and laws of the state. There are good reasons to monitor the hackers, but we can not do things we do not have permissions and legal mandate to do. I am very critical of the fact that this happens without legal regulation, and without public control and insight, says Bing.

He points out that the Norwegian HoneyNet Project collects personal information in the discovery of thousands of IP addresses.

Thus, the project do questionable activities, much like the hackers they are fighting. There is no doubt that the majority of data users who are monitored in honeypots, have not necessarily done anything criminal. Even if they go into a network that is not their own, it is not certain that they are criminals, says Bing.

How do you consider that NSM employees do this as a hobby?

It is not wrong to want to stop hackers, but this is ethically unacceptable, he says.

THE DATA INSPECTORATE: - NOT ACCEPTABLE

- Neither ethical or by law is it acceptable that someone mislead someone else into committing violations - be it a moral rule or government law. As an example the police should disclose and prevent offenses - not invite to them. I looks like the Honey-project in their eager may have tried to "expel Satan with Beelzebub", says director of the Data Inspectorate Georg Apenes.

- I assume just the administrative bodies who work with sensitive issues in the society set up clear criteria for what employees can engage in professionally - also in their spare time. Eventually we should have learned that just within control and surveillance business, for reasons of necessary measures legitimacy, they need to keep their things in order, says Apenes.