Incident Handling of Targeted Attacks

NorCERT was established as a national CERT in 2006. NorCERTs history is dating back to 2000 when the national Early Warning System for Digital Infrastructure (VDI) was started as a cooperation project between the Norwegian Police Secret Service, the Norwegian Intelligence Service and the Norwegian Millitary Security Departement. In 2003 the VDI became a permanent section within the Norwegian National Security Authority (NSM). When NorCERT was created, VDI was integrated with NorCERT as a department in NSM.

With this background NorCERT has from the beginning had a strong focus on protection of national critical infrastructure, and less focus on the more traditional CERT work like abuse handling. The priorities of NorCERTs work has over the past few years been to use an increasing amount of resources on handling incidents that fall into the category of Advanced Persistent Threats (APT).

Several examples of incidents that we have been handling are indicating that Norway, as any other modern society that has a high technology industry (with R&D), is victim for intensive espionage. Cybercrime such as efraud and hacktivism are still important aspects to deal with as a national CERT, but this presentation will focus on incidents where we are suspecting that threat actors are using the Internet to spy on nations, governments and industry.

We handle such incidents in 3 phases:
1. Detection
Detection could be done by user awareness, a person may be receiving an email that make him or her suspect something is wrong. The social engineering skills of the attacker is however often so good, that we cannot expect the best APT-operations to be detected this way.
Further – international networks with security researchers and fellow experts see incidents connected with Norwegian IPs and therefore contacts NorCERT. We see that intelligence communities are also increasingly doing this.
A third way of detection is Norway's own intrusion detection system – the VDI. Here different private and public businesses have signed up for a membership saying that they will volunteerly purchase sensors and push data to NorCERT. In addition they contribute with a small sum of money, making it an exciting private public cooperation. Members pay 50 000 Euro plus the expenses for sensors. In return they are warned about incidents that NorCERT detects, they get invited to technical workshops, forums and courses and exercises.

2. Analysis
Handling APT is very much about handling something new, we often see custom made malware for each case. To fully understand the attackers techniques, intensions and capacities, both to report on the case, but also to detect similar cases in the future – Malware analysis has been one of the cornerstone successes for NorCERTs increased focus on APT.

3. Reporting and experience
The better you are- the more you understeand – the more you detect.
A talented NorCERT engineer realized in the summer of 2011, that several of the big APT cases handled the last few years had some similarities. Working more on this he could document that even though the operations were different in many ways, there were proof that the same actor was behind all.

The questions then is Who? And this is the last problem with working with APT. As a national CERT you want to create awareness in the media – but the stories are not quite as exciting when you have to anonymize the victim, what was taken and who is behind it.
These questions are however very important, and opens the door for CERTs to increasly work close with Intelligence and security services. In Norway we have a coordination group

being a great success in playing ball both with intelligence and counter intelligence organisations.

Seeing into the future – an increased role related to handling national crisis in Cyberspace will be natural. We are certain national CERTs have a role in crisis and war.