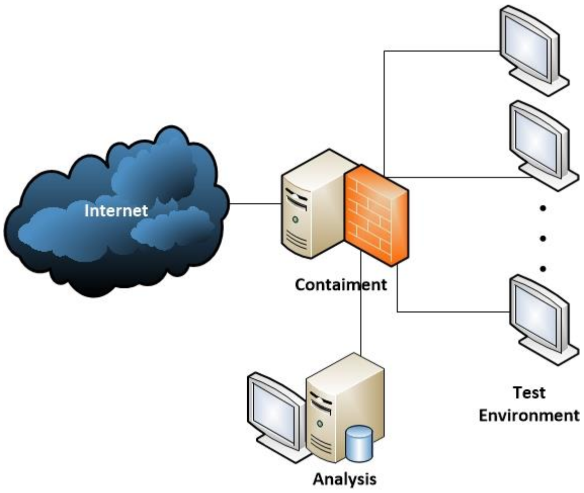
Project title: **Honeypot and Sandbox for malware studies**

Number of students (minimum 2)**: No limit**
Project duration (1-6 months): **No limit (ideally within Feb 1 – June 30)**
Project frame (Bachelor/Master, small project): **Can be any of these**

Background:



- AAU Honeyjar was established around 5 years ago as a platform for running malware in a controlled environment. The platform is currently being rebuild on brand new hardware – two powerful servers with plenty of CPU cores, memory and disk space – and a dedicated Fiber connection to the Danish research network.
- The platform has three main components: (1) The Test Environment, where large numbers of virtual machines can be installed, run, infected, and reset/wiped. This is also where emulated infrastructure exists, to make the environment as realistic as possible. (2) The containment, which filters out any harmful traffic, but allows for some Internet connectivity necessary for the malware to run. It is also used for monitoring traffic. (3) The analysis part, which receives traffic and other information that is monitored, and can be used for analysis of everything observed.
- The platform can accessed through a VPN channel, so no physical presence in Aalborg is necessary (in fact it is just two powerful servers).
-

The challenge:

- The platform is expected to be fully operational by February 1, but some of the components are very lightweight in their implementations – providing just the most basic functionality. Therefore, one option is to focus on one of these parts, and provide useful plugins. Two examples could be (a) Defining a more sophisticated emulated environment, that makes malware believe it is in a real operating network, (b) improving the containment so it can allow more nonharmful traffic through (we are quite conservative, and prefer to stop all traffic unless we are sure it is malicious).

- Another option is to use the platform for running actual experiments for analysis. There are many possibilities, but one would be to study large amount of malware, and see how they behave (in the old setup we ran 300.000 pieces of malware for two minutes each – now we can do much more). It could also focus on running on mobile devices, such as Android.
- Aalborg University has a strong focus on analysis of DNS traffic. An interesting project along these lines could be to study the DNS behaviour of a large number of malware samples, possibly including a better emulation of the DNS infrastructure within the testing environment.

The company:

- Projects might be carried out in collaboration with companies and/or as a research project including researchers from AAU. The relevant company would depend on the setting,
- One company could be the Danish Registrar DK-Hostmaster (www.dk-hostmaster.dk), who is responsible for the .DK Domain, and who has a good collaboration already in terms of DNS traffic analysis. The company is able to provide lots of valuable data for the research.

Supervisor:

- Jens Myrup Pedersen, Aalborg University, jens@es.aau.dk
- Jens Myrup Pedersen is Associate Professor at Aalborg University, Denmark. After finishing his M.Sc. in Mathematics and Computer science he did his PhD in the field of network planning, and through close collaboration with Danish ISPs the work developed into focusing on cyber security. Today his research is focusing mainly on security from a network point of view, and includes network-based detection of malicious activity using e.g. machine learning and DNS traffic analysis - still carried out in close collaboration with industrial partners. Together with his students he has been exploring the security weaknesses of a number of embedded and IoT devices, including demonstration of poor security in state-of-the art Industry 4.0 production lines
-

Candidate background:

- The project can be tailored to students of any background, as long as they are interested in cyber security and malware analysis. Basic knowledge of TCP/IP is a clear advantage through (but can be achieved through e-learning if needed).

References and complementary description:

- List of references used in the description of the project proposal