Malware Workshop

NTNU Malware lab will on during DFRWS 2019 host a malware workshop. The workshop is aimed at people in the forensics community that have seen malware analysis from the sideline or used results from a malware report and wondered how it is done. This is an introductory level workshop if you want to be guided through the analysis and get your hands dirty by trying it yourself. This will be a crash course and provide a taste of what malware analysis and reverse engineering is about. You will be guided through one sample, as we will employ all steps to the same sample. That way you can see how the different approaches complement each other.

This includes:

- Basic Static Analysis: How to retrieve information without executing the malware and form a quick hypothesis about what it is doing.
- Basic Dynamic Analysis: What happens to our filesystem and registry if we run the malware. Can we detect any network traffic?
- Advanced Static Analysis: How can we use a disassembler (IDA Pro free) to learn more about the malware's functionality?
- Advanced Dynamic Analysis: How can a controlled execution of the malware in a debugger can increase your understanding?

You will get the most out of this workshop, if you actively participate. In order to do so, you will have to bring your own computer with a preinstalled analysis platform.

We will provide detailed instructions on how to create your analysis platform prior to the workshop.

The workshop will be held by associate professor Geir Olav Dyrkolbotn and PhD candidate Sergii Banin. They both do research on malware analysis and teach a course in Reverse Engineering and Malware Analysis at NTNU