Real Time Threat Detection Through Network Analysis

At Intermax Cloudsourcing B.V.

Final presentation: Tuesday July 2, 15:00h

Keywords: SSL, Neural Network, Network Security, Command and Control

Project abstract

Intermax Cloudsourcing B.V. designs, implements and manages critical IT-infrastructures for Dutch clients from the medical, public and financial sectors. In order to analyse the data from the IT-infrastructures to detect security incidents, Intermax is developing a Security Operations Center (SOC).
In this project, this SOC has been extended with a REST API to analyse network data and classify it. In addition, Neural Network Framework has been created to produce, train and test models that can be used by the REST API.

Within the scope of the project, the Neural Network Framework has been used to create a model for classifying SSL certificates which are used in command and control communication. When being used by the REST API, the model is able to detect such SSL-certificates which are passing through the SOC at high rates.

This proof of concept is able to analyse a SSL certificate within 1 millisecond and has an accuracy of 95%. The SOC is able to spawn multiple instances of the REST API, making this a scalable, accurate and fast solution for detecting malicious SSL certificates.

Team members:

1. **Name:** Kabilan Gnanavarothayan
   Email: k.gnanavarothayan@student.tudelft.nl

2. **Name:** Pravesh Moelchand
   Email: p.p.a.moelchand@student.tudelft.nl

3. **Name:** Just van Stam
   Email: j.a.vanstam@student.tudelft.nl

4. **Name:** Jim Verheijde
   Email: j.l.verheijde@student.tudelft.nl

Supervisor: René Kalff (Lead Security Engineer at Intermax)
Coach: Harm Griffioen (Focus Area: Network Security)