Malicious network activity data analysis

Goal : Analyse NetFlow history data on suspicious behaviour

Approach : The Malware Intelligence Team is interested in pragmatic students and graduates willing to explore new grounds in analysing stored NetFlow network traffic for detecting malicious behaviour. **Excellent statistical and mathematical or BI skills** and a good knowledge and understanding of internet and internet related network traffic is required:

- Research existing statistical malicious behaviour detection methods applicable to NetFlow history analysis
- Developing new statistical behaviour detection algorithms applicable to NetFlow history analysis on a conceptual level, using techniques like dimensionality reductions, feature extractions, Bayesian probabilities and probabilistic classifiers
- Select a subset of malicious behaviour on relevance and implementation feasibility
- Create a detailed presentation for implementing the subset
- Present the result to the Malware Intelligence Team
- Realize a proof of concept implementations of approved subset members in Python/SQL/XML/R/BI
- Test the individual implementations on effectiveness in a lab-environment

Result : The result is a report on effectiveness and relevance based on lab results, recommendation on applicability of the individual implementations and recommendations for future research.

Working environment : The Malware Intelligence Team is offering a pleasant, spacious working environment. Our lab environment is located on walking distance of a main train station. Skilful and experienced team members are responsive and supportive, the working environment is open, informal and relaxed. Work is goal oriented and not stringently office bound. Exceptions are working with confidential material and work with lab resources.

RS-contacts : dennis.kuit@redsocks.nl; pepijn.janssen@redsocks.nl Website : www.redsocks.nl