Master thesis proposal: Analysis of Cyber Threat Intelligence Feeds

Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch
Dr. David Gugelmann, dg@exeon.ch
Dr. Vincent Lenders, vincent.lenders@armasuisse.ch

Description

Threat intelligence feeds provide information for the identification of IT threats. This information is typically used by security monitoring and alerting systems to detected compromised hosts in the internal network of an organization. A large number of different intelligence feeds[1] is freely available on the Internet. We are continously collecting these data and have a growing archive of more than 20 publicly available intelligence feeds. However, it is difficult to assess the quality of the provided information.

The goals of this master thesis are to analyze and compare these data in detail, develop metrics to assess the quality of the different cyber intelligence feeds and correlate the intelligence feeds with real network traffic. The developed quality metrics should incorporate aspects like:

- How up-to-date is a cyber intelligence feed, that is, how often are indicators of compromise (IOC) updated?
- Is a feed just copying information from other feeds or does the feed indeed provide new information?
- How reliable is an intelligence feed?
- Is a feed focusing on a specific geographical region?
- What kind of threats are listed by a feed, are the provided threat labels accurate and and what is an approriate threat level for a listed IOC?
- How can the number of false alerts be reduced?

More in detail, the tasks of this thesis are to:

- Review the literature on studies comparing intelligence feeds.
- Get an overview of available feeds and add new feeds to our collection infrastructure.
- Compare the different intelligence feeds in detail.
- Develop metrics to assess the quality of an intelligence feed and assign threat levels.
- Correlate the feeds with real network traffic and analyze the reasons for false positives.
- Document the findings in a report.
- Present the findings.

More information

This is an external master thesis that will be conducted in collaboration with armasuisse W+T and the ETH Spin-off company Exeon Analytics.

For more information contact Dr. David Gugelmann at dg@exeon.ch.

[1] see `https://github.com/hslatman/awesome-threat-intelligence` for an overview