Speakers:

- Matthias Vallentin, Tenzir
- Dominik Charousset, Tenzir

Adaptive and Automated Analysis with Broker

When it comes to analyzing massive amounts of network traffic, the cluster deployment of Bro enables full processing at line speed. Within a cluster, Bro nodes communicate to share state, perform computations, and export analysis results to downstream applications. Bro 2.6 comes with a major change: the legacy communication protocol that Bro nodes speak is replaced by Broker---a flexible new publish-subscribe messaging library third parties can nicely integrate with.

In this talk, we demonstrate how to communicate with Bro using the new C++ and Python interfaces of Broker. Specifically, we show how Broker enables (1) adaptively exporting Bro logs into our network forensics platform, that is, how Broker's back pressure mechanism avoids overloading downstream data consumers, (2) automated queries over historical log data with the intelligence framework, and (3) feed results of custom analysis back into Bro. This use case serves as an example of how users can build complex and fully automated applications in the Bro ecosystem. Our talk provides a use-case driven walkthrough with Bro scripts, Broker examples, and a performance analysis in terms of throughput and latency.