

New ZeroMQ functionality in MISP



CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

July 2, 2015

ZeroMQ?

- ZMQ is a high-performance asynchronous messaging library, aimed at use in scalable distributed or concurrent applications.
- CIRCL already uses ZMQ at various places:
 - AIL Analysis Information Leak Framework¹ is based on ZMQ.
 - IntelMQ² connectors rely on ZMQ too.
 - Datafeed exchange (Leak, malicious IP addresses,...).
- MISP used a push-pull model. The new ZMQ extension allow to have a pub-sub³ model on a message bus.

¹<https://github.com/CIRCL/AIL-framework>

²<https://github.com/certtools/intelmq>

³publisher-subscriber

MISP ZMQ publish-subscribe

- First version implemented⁴ and focus on the global events published.
- At each new publish, MISP pushes the event in JSON format into a Redis list.
- Then a Python-based service is dequeuing the Redis list and does the pub-sub.
- The pub-sub feed is limited to the administrator of the instance (TCP-based).
- External services subscribe to the feed to get all new or updated events from a MISP instance.

⁴<https://github.com/MISP/MISP/commit/3f215743f0cae97587d01d460c222d1c84765c18>

Future of pub-sub in MISP

- Integration with real-time and alert searches in SIEM (e.g. Splunk) or log analysis tools.
- Having a historical or audit view of MISP events (new, updated and published).
- Extending to other pub-sub systems like Apache Kafka to integrate with other systems.
- Improving the pub-sub distribution with dedicated channel per community.

MISP flows

