Objective Reputation of Cyber Threat Intelligence (CTI) Sources

Project Description: In the recent past, CTI has received wide-spread popularity among the cyber defense community. The exponential increase in CTI mass can be attributed to the increased number of cyber threat sources. Owing to this phenomenon, it is becoming increasingly difficult for CTI consumers to identify well reputed threat sources that provide feeds suitable to their requirements. There are a number of problems that consumers face when subscribing to particular threat sources. **First**, the threat feeds received may contain noisy or irrelevant threat data that may be a result of blind aggregation of multiple threat feeds from other sources. Such a threat source cannot satisfy consumer requirements regarding the integrity, timeliness and relevance of threat information. **Second,** CTI sources may not be used as independent sources of evidence as they may share common sources. Ideally a dependency score for two sources, a number between 1 and 2, should be assigned with respect to a specific type of information (e.g. domains hosting malware). **Third**, due to bias or ulterior motives the threat data may be poisoned intentionally to mislead consumers from the real threats. **Forth**, some threat sources are limited in the threat data they provide for example they may provide specific threat events such as bad domains or IPs only as opposed to sophisticated APTs. Thus there is a strong need for an independent third party service that accurately determines and reports the reputation score and ranking of a threat source to the consumers who wish to opt for these services.

In light of the above mentioned problems this research proposes the design and development of an on-line service that will compute the rank and reputation of a wide-variety of threat sources and provide a comparative analysis of their rating based on multiple dimensions. Our reputation ranking technique will adopt a four pronged approach. First we will profile threat sources according to time the threat is reported and the analysis of threat information. Second we will perform multi-source correlation using clustering and visualization for threat feed inter-relationships and source inter-dependency analysis. Third, we will perform sentiment analysis via surveys and consumer reports. Fourth, we will integrate cyber intelligence to enrich the threat source reputation analysis. Finally we will define certain scores and metrics to represent the statistics of our reputation and ranking service.

We have identified a set of threat source features our reputation ranking service will consider: (1) signal to noise ratio, (2) accuracy and certainty of threat events (3) richness of contextual information, (4) relevance to the industry and or organization in question, (5) use of widely accepted standards for representation such as STIX or OpenIOC that could be used as direct input to the network firewall or IDS rule-engine, (6) update frequency (daily, hourly, real-time etc), (7) level of detail and coverage and (8) frequency of false positives. Value added services such as search based on application and features would also be considered. For instance the ranking service could suggest the consumer subscribe to multiple sources if no single source meets the requirement of the consumer.

The main objective of our research work is define a criteria that enables a consumer to objectively rank (both qualitatively and quantitatively) threat sources according to their reputation. Our proposed service will not only help consumers in the selection process but also create an environment of accountability among the threat sharing community so that individual sources automatically strive towards becoming better intelligence reporting citizens.