MISP and Decaying of Indicators

An indicator scoring method and ongoing imple-

info@circl.lu

February 6, 2019

Team CIRCL

Indicators - Problem Statement

- Various users and organisations can share data via MISP, multiple parties can be involved
  - Trust, data quality and time-to-live issues
  - Each user/organisation has different use-cases and interests
- Attributes can be shared in large quantities (more than 1.3 million on MISPPRIV)
  - Partial info about their validity (sightings)
  - Partial info about their freshness (last update)
  - Varius conflicting interests such as operational security, attribution, source reliability evaluation...

Sightings - Refresher

Sightings add temporal context to indicators. A user, script or an IDS can extend the information related to indicators by reporting back to MISP that an indicator has been `seen`, or that an indicator can be considered as a `false-positive`

- Sightings give more credibility/visibility to indicators
- This information can be used to **prioritise and decay indicators**

Organisations opt-in - setting a level of confidence

MISP is a peer-to-peer system, information passes through multiple instances.

- Producers can add context (such as tags from taxonomies, galaxies) about their asserted confidence or the reliability of the data
- Consumers can have different levels of trust in the producers and/or analysts themselves

Description	Value
Completely reliable	100
Usually reliable	75
Fairly reliable	50
Not usually reliable	25
Unreliable	0
Reliability cannot be judged	50
Deliberatly deceptive	0

Description	Value
Confirmed by other sources	100
Probably true	75
Possibly true	50
Doubtful	25
Improbable	0
Truth cannot be judged	50

Scoring Indicators 1/2

When scoring indicators[1], multiple parameters[2] can be taken into account. The **base score** is calculated with the following in mind:

- The reliability in the producer
- The trust in the data as signaled by the producer

$$base\_score = weigth_{tg} \cdot tags + \omega_{sc} \cdot source\_confidence$$

[1] Paper available: `https://arxiv.org/pdf/1803.11052`

[2] at a variable extent as required

Scoring Indicators 2/2

The weighted score is calculated using:

- The lifetime of the indicator (e.g. IP address vs hash value of a file)
  - The lifespan of the indicator (short for an IP - long for an hash): τ
  - The decay rate $\rightarrow$ Speed at which an attribute loses value: δ
  - Weigthed score is reset to its base score as new `sightings` are received

$$score = base\_score \cdot \left(1 - \left(\frac{t}{\tau_a}\right)^{\frac{1}{\delta a}}\right)$$

Ongoing Implementation in MISP

Setting thresholds and retrieving the information should be simple and straightforward for the user:

- Automatic scoring based on default values
- User-friendly UI to manually set lifetime parameters
- Interaction through the API