TNC'18 Networking Conference, Trondheim, Norway

An Indicator Scoring Method for MISP Platforms

A. Dulaunoy[♦], A. Iklody[♦], S. Mokkadem[♦], G. Wagener[♦] and <u>C. Wagner</u>[♣]

♦ Computer Incident Response Center Luxembourg – CIRCL
♣ Fondation RESTENA

Introduction

- New threats appear and disappear on daily base
  - Share information about actual threats and work collaboratively
  - Decrease resolution time
- Collaboration and information sharing are key element in CSIRT world
  - Sharing information is a critical point
    - Sensitive data it may include respectively the authenticity of information
    - Joint-efforts to handle a problem have direct impact on reaction time and resources.
  - The appearance of information sharing platforms confirms this trend
- Indicator Scoring model applied to the open source threat intelligence platform MISP
  - MISP permits private or public IT-communities to share their information, IoCs, malware and other existing threats.

Information sharing

- Successful cyber incident response is information sharing in its different forms
  - Trusted third parties, email lists of CERTs (Computer Emergency Response Teams), platforms….
- Case studies on information sharing on problems and legal aspects showed
  - Information sharing remains a group or community activity
  - Restricted access due to commercial service approaches
  - Need for accurate information sharing practices
  - Low false positive rates and correctness of data
- Information sharing is related to a lot of challenges
  - Added value of shared data to knowledge management
    - What kind of data - IP-addresses, protocols, timestamps, etc
  - Privacy
  - Quality control approaches
    - From Netflow to information
    - Reduction techniques, s.a. Aggregation , hashing....
  - Beside technical challenges , find volunteers to share data
    - For implementing the scoring method → MISP

Background information on MISP

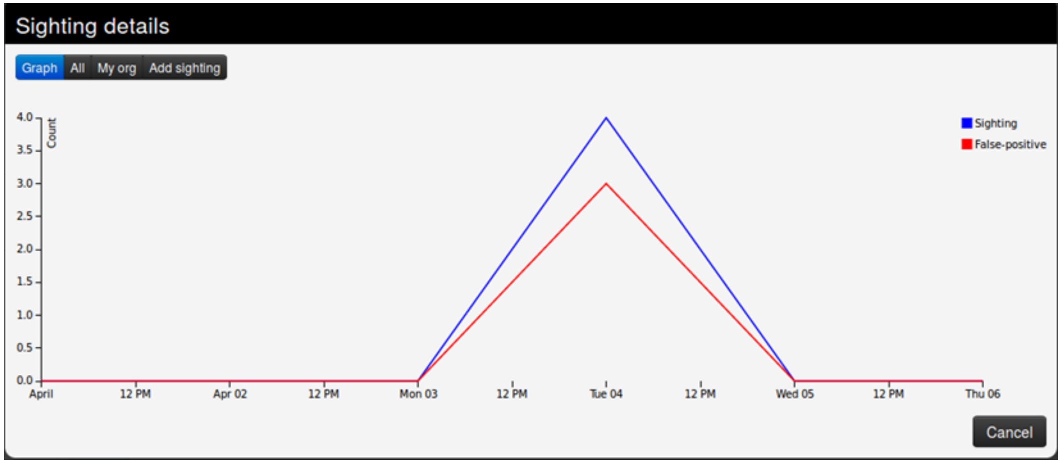
- MISP is a collaborative open-source project that continuously evolves by community-driven effort to share
  - All kind of threats and all kinds of indicators of compromise
  - But also others such as financial indicators as for example bank accounts of money mules, which were abused
- The data model implemented in MISP for sharing information is simple
  - User can decide on the granularity of information to
  - Set the sharing level (f. ex. organisation only, community only…)
- MISP is designed to be peer to peer, where multiple instances can exchange information with each other
  - The synchronization protocol in MISP resulted from a trial-and-error approach
  - Main criteria were efficiency, accuracy and scalability

Background information on MISP

- Sharing information in MISP
  - Shared information in MISP is called event
    - Having a list of attributes (destination IP addresses, file hashes)
    - Currently 140 types are available in MISP software
    - An attribute is tuple (category, type, value)
    - The more an event is also linked with contextual information s.a date, threat level, description, organisation…
  - To avoid time-consuming form filling it has integrated
    - Free text importer that allows users to copy and paste raw data into a single field and analysed to extract attributes
  - Taxonomies for the filtering of events (classification scheme)
    - Facilitate description of IoCs and other relevant information.
    - Machine-tag approach with triple-tags
    - 47 different taxonomies (law enforcement, CSIRT, intelligence…

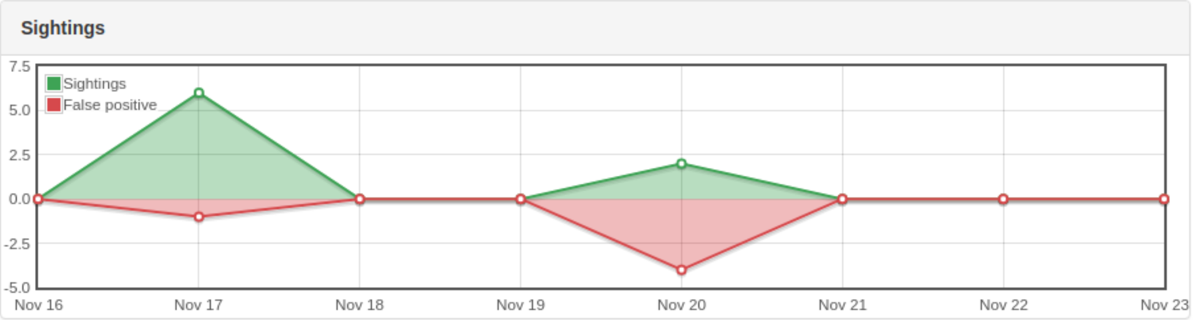
Sightings

- Sightings is a feature for users, scripts or IDS to share information about a attribute
  - Report information about presence , false positive, expiration dates…
  - Provide more credibility to an attribute and can be used for prioritizing or decaying attributes



Example

- Visual representation of the occurrences of sightings and false-positive for one week



- Observation
  - False positives were detected →spam campaign
  - Larger proportion of sightings than average
  - Informs security experts about actual threat
    - Indicates deeper investigation
- Sightings provide input for decaying attributes

Scoring IoCs

- Why scoring and decaying Indicators
  - Challenges:
    - Correctness of information and handling attributes
    - Get decay time for attribute/indicator
  - Example of MISP community for private sector
    - 1 531 users from 761 different organisations
    - 8 101 shared events
    - 1 003 908 attributes until early December 2017
  - User objectives change from user to user
    - Built of non-homogeneous crowd with different objectives
    - Unwanted false positives → data to be correct and reliable
    - Correlation of attributes with other threat actors

    => Need for a correct and reliable source of historical data

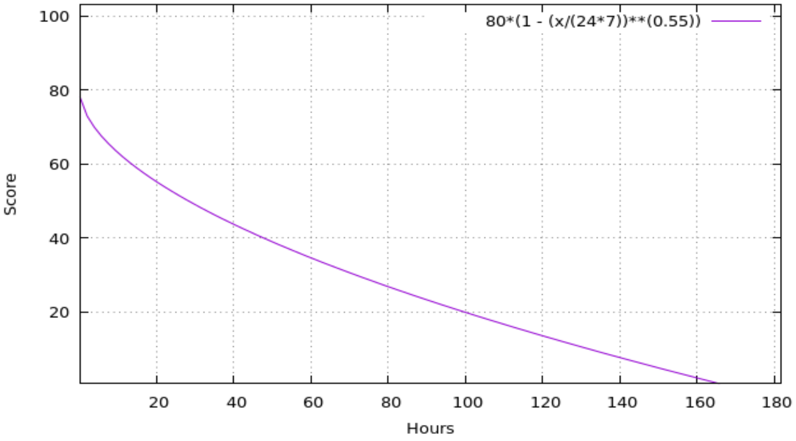
Scoring IoCs

- The lifetime of attributes is not homogeneous
  - Example: hosts of machines change, IP addresses changed or cleaned, domain names traded…
    - → each attribute has its own decay function
- The scoring of attributes over time considers factors like
  - Confidence of its source
  - The taxonomies attached to it
  - → Giving the initial value of an indicator's life cycle
- The decay rate represents
  - Speed at which the overall score is decreasing over time.
  - Example of an IP address
    - Decay rate of IP should be low for the first hours, but steadily increase since threat still ongoing
    - IP address is shared among a community targeted by the threat actor
    - → Members take measures, e.g. blocking IP address
    - →The attack becomes ineffective forcing threat actors to use other IP addresses

Scoring IoCs - Examples

Attribute for compromised IP address in botnet

- Destination IP of compromised webserver hosting exploit kit distributing malware
- Clean-up started
  - Grace time of ISP 1 week
- IP address added to blacklists
  - 48 hours generally
- Threat actor may notice detection
  - Move to another one



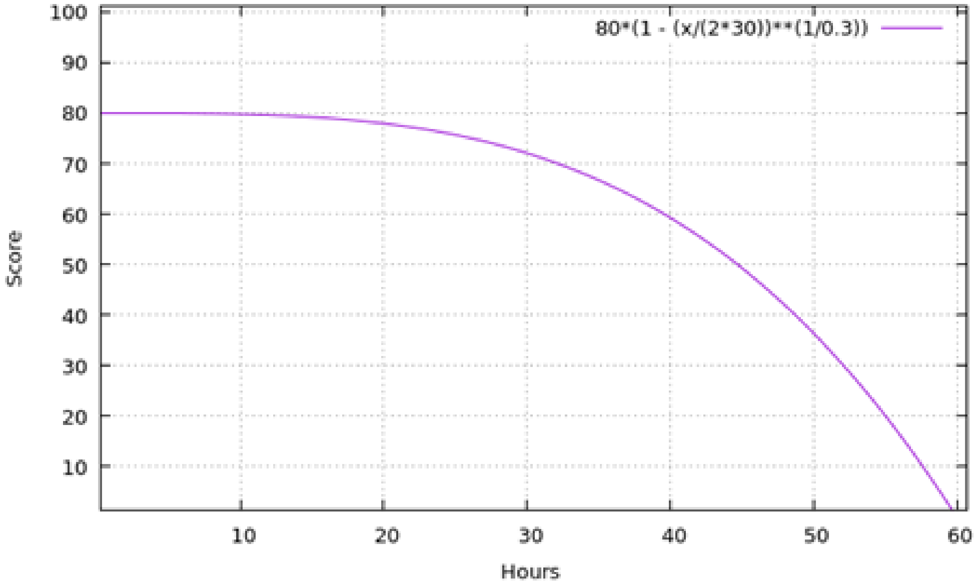
- By applying the model it can be observed that

→ Score halved after < 2 days

Scoring IoCs- Examples

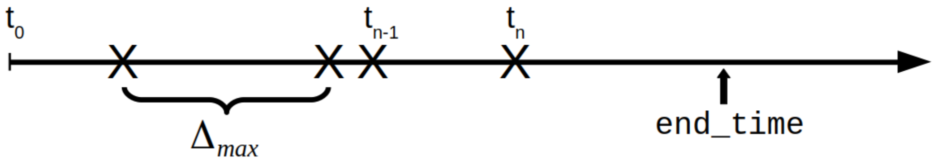
- Hash of Malware
  - Observation that score of a file-hash not as volatile as IP
  - The attribute is observed for 2 month

  → Slow decay only



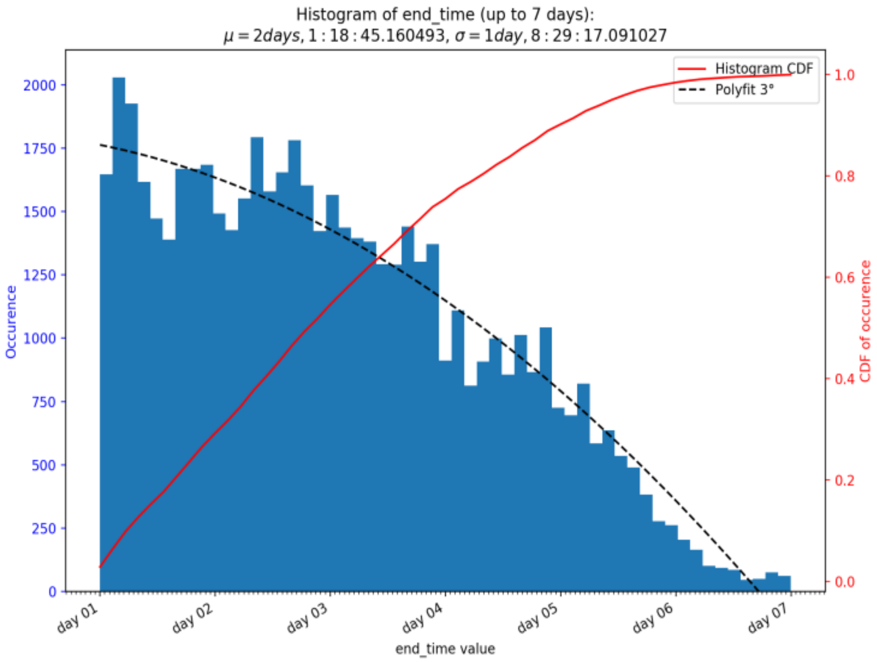
Experimental evalution

- Evaluations on time period and decay speed
  - Phishing dataset with short lived URLs from phishing campaigns
  - For CSIRT/CERTs it is critical to take down compromised server quickly
  - Interested in end-time of attribute by applying scoring model



Time span	May 29, 2017 → May 3, 2018
Number of attributes	437027
Number of sightings	5338535
Mean (μ) of sighting / attribute	12
Stdev (σ) of sighting / attribute	58

Experimental evaluation



- One week representation
  - CDF indicates ~90% falls within 5 days
  - Consider end-time 5 days

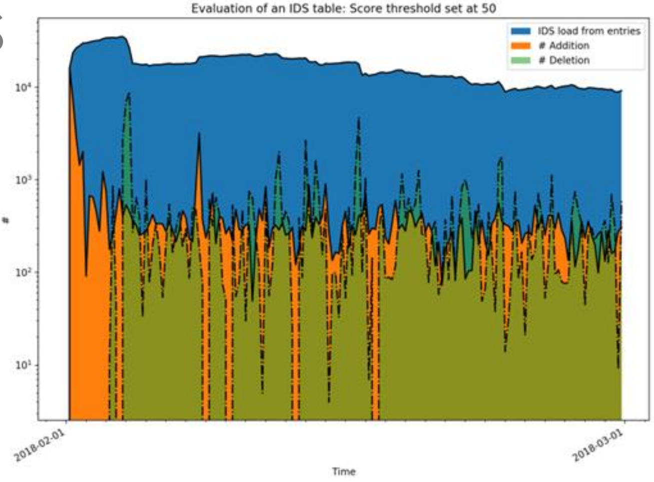
This information can be used in IDS to select rules

Experimental evaluation

- Evaluation with IDS table supporting the model
  - A subset of the dataset reused on IDS
  - Check evolution of its table
    - At start

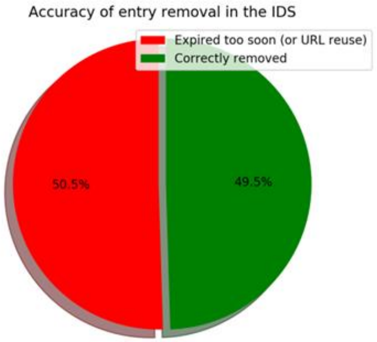
      Load of table is higher than average
      - No IOC expired yet
    - Later

      Deletions reduce load to balanced



  - Accuracy of entry removal in IDS
    - 50% removed correctly

    →Motivation to further develop the scoring model



Conclusion

- Information sharing has become an integrated part in the resolution of incidents
- MISP not only allows the sharing of information but also
  - Contribute useful add-ons by the community
  - Trusted environment
- Early work on scoring mechanisms for attributes only
  - Base score defined to combine these trust aspects
  - Scoring apporach to reflect lifetimes of attributes
- Demonstrated that decaying IoCs is a challenging task
- Future work includes
  - Evaluation and application of machine learning techniques
  - Exploration of game theoretical models in context of distributed information sharing.

QUESTIONS?

THANK YOU!

Hack.lu is an open convention/conference where people can discuss about computer security, privacy, information technology and its cultural/technical implication on society.
Hack.lu Conference 16-18 October 2018 in Luxembourg

The model

score of an attribute before taking into account its decay

$$base\_score_a = weight_{tg} \cdot tags \quad + \omega_{sc} \cdot source\_confidence$$

The score derived from the taxonomies is defined in equation (2), where **G** is the number of defined taxonomy groups and **T** the number of used taxonomy per group

$$tags = \frac{\sum_{j=1}^{j=G} \sum_{i=1}^{i=T} taxonomy_i * weight_i}{\sum_{j=1}^{j=G} \sum_{i=1}^{i=T} 100 \cdot weight_i}$$

The idea is to decrease the *base_score* over time. When it reaches zero, the related indicator can be discarded

$$score_a = base\_score_a - \delta_a(T_t + T_{t-1})$$

$$score_a = base\_score_a \cdot e^{-\delta_a t}$$

Final score

$$score_a = base\_score_a \cdot \left(1 - \left(\frac{t}{\tau_a}\right)^{\frac{1}{\delta_a}}\right)$$