The "Art" of Information Sharing

A Practical Approach

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

October 19, 2015

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the **private sector**, communes and non-governmental entities in Luxembourg.

Sharing indicators

- In order to improve sharing of Indicators of Compromise (IOCs), MISP was introduced in 2013:

- Sharing indicators about targeted attacks.
- Improve detection time of unknown malware.
- Avoid reversing similar malware (focusing on new analysis).

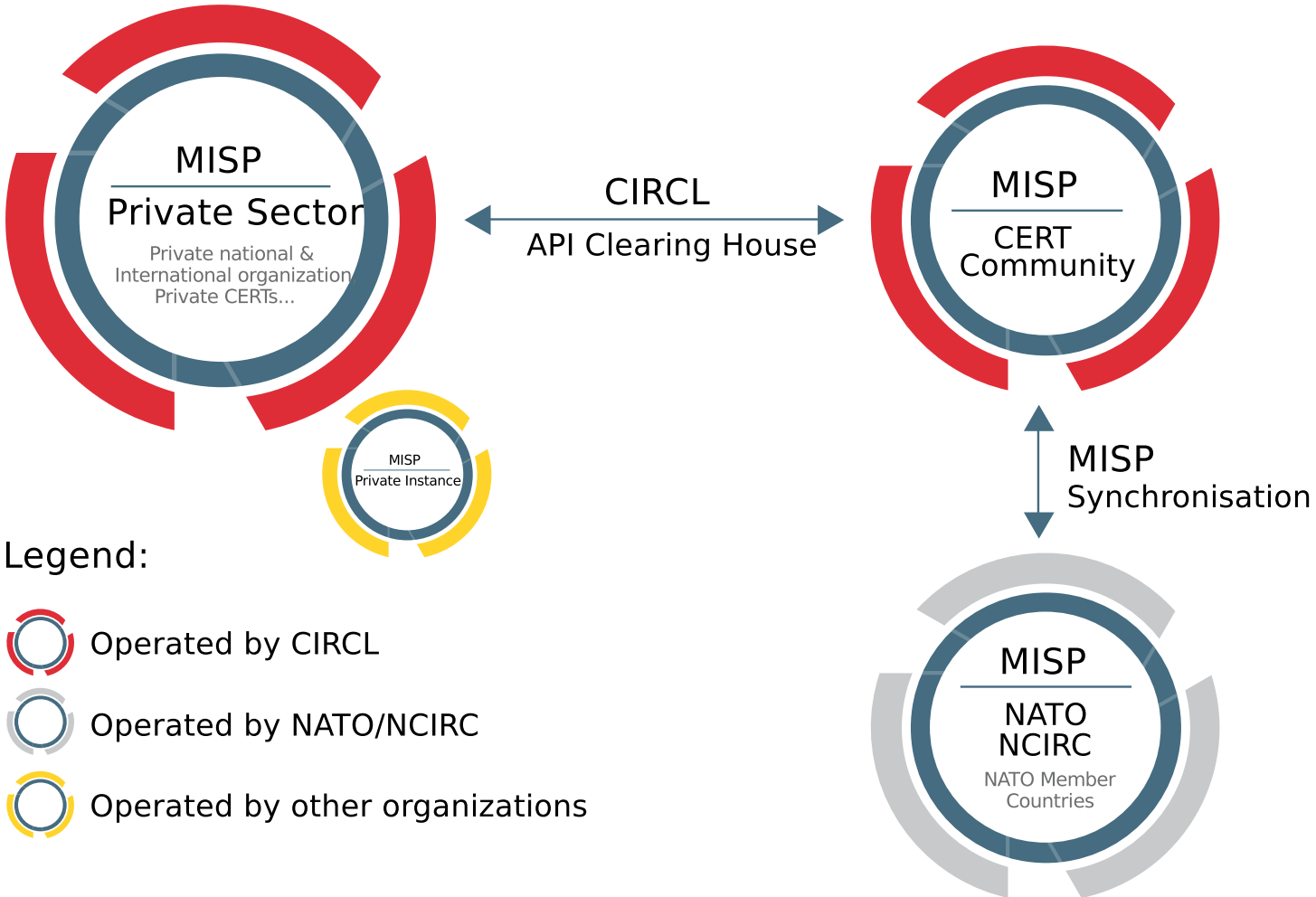
Challenges in threat sharing

3 years of trial-and-errors with some successes

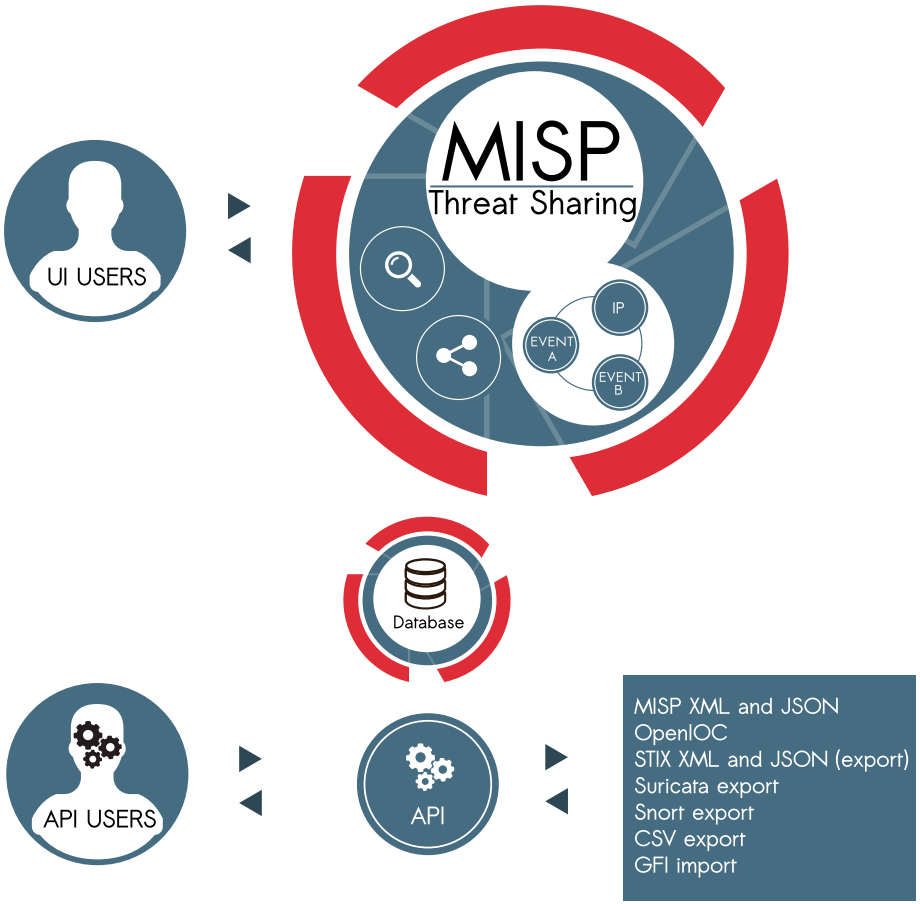
Threat Sharing - Different Objectives

- Sharing indicators for a detection matter.
  - Do I have infected systems in my infrastructure or the ones I operate?
- Sharing indicators to block.
  - I use the attributes to block, sinkhole or divert traffic.
- Sharing indicators to perform intel.
  - Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?
- $\rightarrow$ These objectives can be conflicting (e.g. False-positives have different impacts)

MISP overview



MISP technical overview



What kind of attributes are shared in MISP?

- Hashes of malware (MD5, SHA1, SHA256).
- IP addresses, ASN numbers.
- Hostnames and domain names.
- patterns in file, disk or memory.
- named pipes, mutexes,...

- These indicators can be used to search for potential compromised systems in network logs (proxy, firewall), system log.

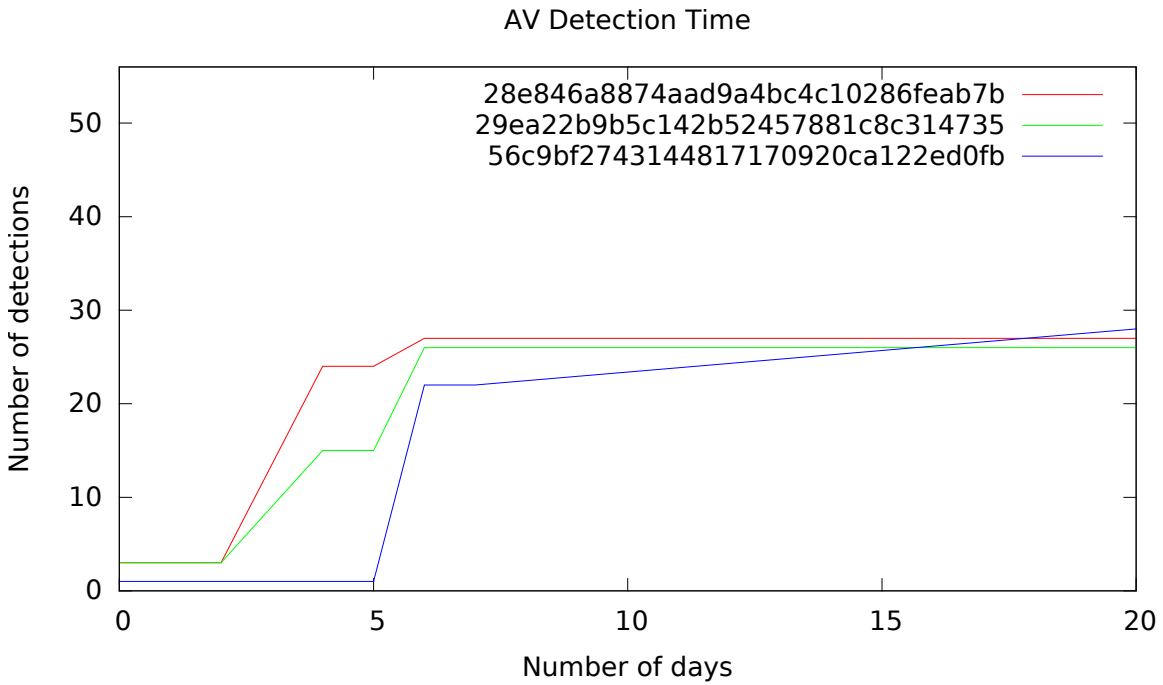
What are other benefits?

- Attackers and adversaries can be lazy. They reuse infrastructures and techniques.
- You can find relationships between the attackers' campaigns and the indicators.

domain	icanhazip.com		497 429
ip-dst	188.123.34.203	C&C	
ip-dst	5.44.15.70	C&C	
ip-dst	188.255.212.27	C&C	
ip-dst	217.23.194.237		
ip-dst	31.42.170.198		
ip-dst	93.184.71.88		
ip-dst	194.28.190.84		
ip-dst	195.34.206.204		
ip-dst	46.180.147.50		
ip-dst	91.187.75.75		
ip-dst	109.86.176.37		1132
ip-dst	31.28.115.88		

Sharing indicators not detected by AntiViruses

- Indicators are often shared before they are detected by A/V.
- Dridex malware sample in April 2015:



Statistics

- 265330 attributes in CIRCL MISP for private sector.
- 75506 correlated attributes (at least shared between two events).
- 184 (433 users) national and international companies/organizations are on the MISP platform.
- What about the API?
  - 35% of the users are using the API (outside MISP sync).
  - The main software to access the API is curl then PHP, Python, wget, MS API, Java.
  - The most commonly used export format is CSV then JSON, NIDS, XML.

Conclusion

- Fetching indicators from MISP and searching internally is already a quick win.
- Contributing is not required but it's enhancing the global view on who already seen/worked on such attack.
- Small incidents can be the origin of "complex targeted attacks".
- Sharing of indicators can be also done anonymously[1] via CIRCL if required.
- Ease of importing indicators/event is a key factor to ease sharing.

[1] MISP will include a delegation of sharing to ask a third-party to share an event

Contact

- info@circl.lu
- `https://www.circl.lu/`
- MISP - `https://www.circl.lu/services/misp-malware-information-sharing-platform/`
- OpenPGP fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5