

Incident Response and Information Sharing

A Practical Approach



CIRCL

Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:GREEN*

May 22, 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.

CIRCL Services

- Incident ticket creation for reported **ICT incidents** via different media (e.g. international CSIRT channels, national incident reports,...)
- Incident identification and **triage**
- **Technical investigation** including information correlation (e.g. security vulnerability/incidents matching, similar incident resolution, malware reversing, system and network forensic...)
- Incident coordination might also include **vulnerability handling**, responsible vulnerability disclosure (e.g. the software originating the incident) or incident response training
- Services availability to organizations/citizen incorporated in Luxembourg

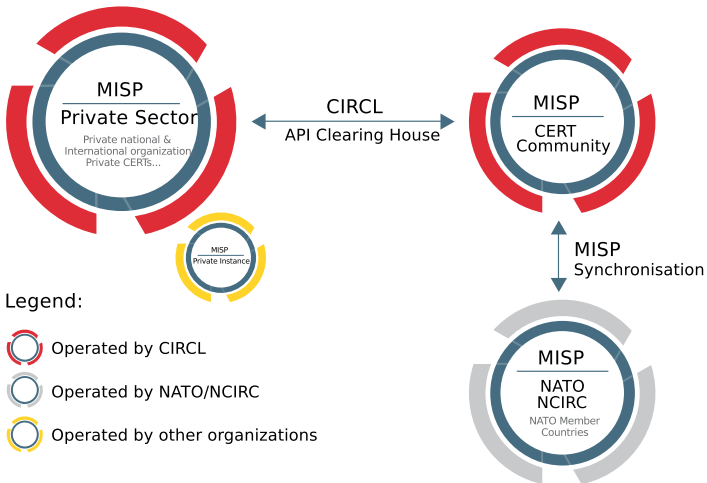
Sharing indicators

- 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).

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
- Malware family
- Vulnerability related (CVE Numbers)
- These indicators can be used to search for potential compromised systems in network logs (proxy, firewall), system log.

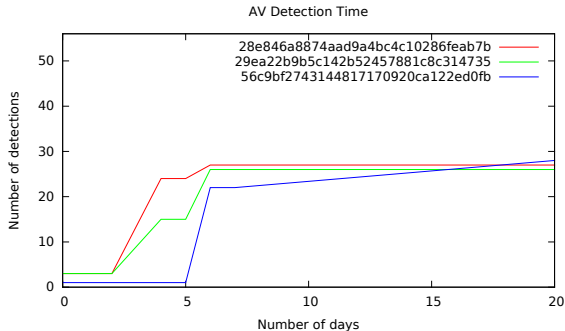
What are other benefits?

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

domain	icanihazip.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	109.86.178.37	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

- 145732 attributes in MISP for private sector.
- 27920 correlated attributes (at least shared between two events).
- 117 international companies and organizations are on the MISP platform.

Future

- Pseudonymity
- STIX Import
- TAXII for sharing between instances
- Improvements in the API
- Request Policy Zone Configuration export
- VirusTotal integration
- SMIME
- New attributes
- What else do *you* need?
- For bugs or features requests:
<https://github.com/MISP/MISP/issues>

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".
- All the CERTs can request an access to the platform
- Sharing of indicators can be also done anonymously via CIRCL if required.

Contact

- info@circl.lu
- <https://www.circl.lu/>
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2
CD49 44E6 CBCD