Information Sharing

Cornerstone in Incident Detection and Handling

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

DBIR 2014 - Paris, France

May 14, 2014

Luxembourg - CERT collaborative landscape

CIRCL, national CERT of Luxembourg

- CIRCL[1] is composed of 6 full-time incident handlers + 2 FTE backup operators.
- The team is operating as an autonomous technical team relying on its own infrastructure.
  - Operators competencies include reverse engineering, malware analysis, network and system forensic, software engineering and data mining.
- CIRCL, the national CERT, is part of SMILE[2] gie (a publicly funded organization to promote information security in Luxembourg).
- In 2013, CIRCL handled 35958 security events and conducted more than 1006 technical investigations.

[1] `http://www.circl.lu/`

[2] `http://www.smile.public.lu/`

Incident Handling and Trust

- Each sector of activity has its own sensibility regarding incident handling (e.g. financial sector versus industrial sector)
- Incident handling can only be performed if trust is present between the CERT and the victim(s)
- Trust can be built from previous cases or pro-active information security services
- The roots of trust can be also due to the non-direct depencies of the CERT with the victim(s) (e.g. the structure is not automatically reporting the incident to law enforcement)

There are no small incidents

- Every single incident needs to be handled even if they seem insignificant:
  - Major targeted attacks are usually detected from minor security incidents (e.g. you came for a suspicious phishing email and then you ended up with successful targeted on an internal network)
  - Software or infrastructure exploitation is still too easy and the high-profile attacker can benefit from multicompromised infrastructure (e.g. MiniDuke case)
  - We don't look blindly at our constituency (e.g. an incident in another country won't be limited to that country)
- Staged automatization[3] is a MUST to process all events/incidents:
  - To track down small events to better understand potential new attacks
  - To avoid boredom of your incident handling team with the minor events

[3] Depending of human evaluation. Machine versus human for analysis.

Sharing is key, and DBIR is vital

- Statistical analysis like the DBIR report need comparable datasets.
- Sharing is an element to ensure coherent detection within various organizations.
- The DBIR exchange processes with Verizon helps to:
  - Ensure that you are collecting the right information for statistics.
  - Review your classification process and ensuring adequate protection of the victims.
  - Improve information data exchange among partners.

Automatic exchange of IOCs with MISP

- Improve counter-measures to targeted attacks.
- Improve detection ratio and reducing false positive.
- Avoid reversing similar malware (or validating analysis).
- Malware Information Sharing Platform (MISP) in production with 15 private companies
- The software works well as long as the members are contributing.
- Automatic notification using PGP per member is efficient.

PoisonIvy via CN/HK example

2013-09-19		mutex	2SF#@R@#!	289	Yes	All	
2013-09-19	Network activity	ip-dst	219.76.208.163	289	Yes	All	
2013-09-19		ip-dst	113.10.246.30	289	Yes	All	
2013-09-19		ip-dst	219.90.112.203	289	Yes	All	
2013-09-19		ip-dst	202.65.220.64	289 177	Yes	All	
2013-09-19		ip-dst	75.126.95.138	289	Yes	All	
2013-09-19		ip-dst	219.90.112.197	289	Yes	All	
2013-09-19		ip-dst	202.65.222.45	289	Yes	All	
2013-09-19		ip-dst	98.126.148.114	289	Yes	All	
2013-09-19		ip-dst	180.210.206.96	289	Yes	All	
2013-09-19		ip-dst	101.78.151.179	289	Yes	All	
2013-09-19		ip-dst	60.10.1.120	289	Yes	All	
2013-09-19		ip-dst	60.10.1.115	289 248	Yes	All	

- This event includes known artefacts from a report of Fireeye in an ordened manner.
- We see directly the relationship with previous events having similar artefacts.

Conclusion

- Malware Information Sharing Platform (MISP) is released as free software:
  - `https://github.com/MISP/`
- All private companies interested by the project can contact us to get an acces to our MISP platform...
- ... as long as they contribute in the future.
- The platform is maintained by a strong community of CERTs and private companies.

Contact

- raphael.vinot@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: 8647 F5A7 FFD3 50AE 38B6 E22F 32E4 E1C1 33B3 792F

- Or come to talk to me after the presentations!

Hack.lu 2014 - 21-23 October