

Malware Information Sharing Platform or How to Share Efficiently IOCs Within a Country



CIRCL

Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

info@circl.lu

July 29, 2013

Automatic exchange of IOCs

- Improve counter-measures to targeted attacks.
- Improve detection ratio and reducing false positive.
- Avoid reversing similar malware (or validating analysis).
- A test was recently conducted with MISP¹.
 - The software works well as long as the CERTs are contributing.
 - Automatic notification using PGP per member is efficient.
 - Structured messages export (Snort rules or XML) works well but events synchronization/merging is under improvement.

¹<https://github.com/MISP>

Red October/Sputnik malware example

View Event

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from IOC

Populate from ThreatConnect

Contact Reporter

Download as XML

Download as IOC

Download as CSV

List Events







Add Event

Event

CIRCL

ID	43
Uuid	50f4ff9d-6438-4ec2-8099-35650a000b01
Org	CIRCL
Email	alexandre.dulaunoy@circl.lu
Date	2013-01-15
Risk	Undefined
Analysis	Completed
Distribution	All communities, this will share the event with all MSP communities, allowing the event to be freely propagated from one server to the next.
Info	Metadata from http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation
Published	Yes

Attributes

Category	Type	Value	Related Events	IDS	Distribution	Actions
Payload installation	filename md5	svchost.exe f4110f6e9212cb7897ee1f88f8bc27d9	3 3 3	Yes	All	 
	filename md5	svchost.exe 6e798c189f5b0c2d5e670023fb2ccd5a	3 3 3	No	All	 
	filename md5	dump.unp 318a90fb474ab1960fe1aae0f828a18a		Yes	All	 



















Related Events

2013-02-18 (3) 2013-01-18 (4) 2012-07-05 (60)

- This event includes all known artefacts from Red October/Sputnik malware.
- We see directly the relationship with previous events having similar artefacts.

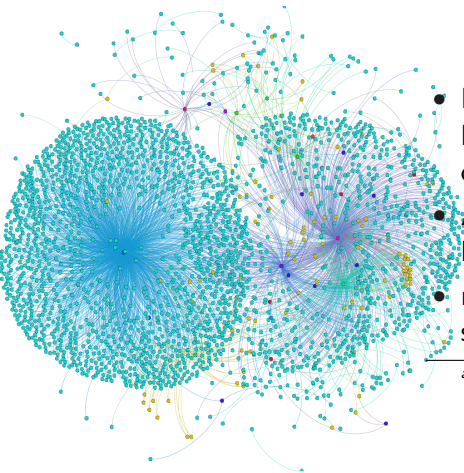
Data representation

Attributes

Category	Type	Value	Related Events	IDS	Distribution	Actions
Payload delivery	malware-sample	pdf-set.zip 81c6e9b4745cc11e0b6cc4fd45779c21		Yes	All	 
	md5	113e6fc85317fdd135e3f5f19e6c7a58		Yes	All	 
	md5	c786a4cdfc08dbe7c64972a14669c4d1		Yes	All	 
Network activity	domain	eamtm.com		Yes	All	 
	domain	arabooks.ch		Yes	All	 
	domain	artas.org		Yes	All	 
	domain	tsoftonline.com		Yes	All	 
	ip-dst	194.38.160.153		Yes	All	 
	ip-dst	95.128.72.24		Yes	All	 

- Type and data interpretation is critical for operators and systems.
- Some data might be confusing or used in different context (e.g. domain name versus hostname).
- Standardization of IOC is useful but should avoid confusion of interpretation.

Data representation - MISP Graph



- Example of relationships between event and related IOCs of APT1.
- A dot is an IOC or an event, a link means the dots are related
- `misp-grapha` is released as a free software.

^a<https://github.com/MISP/misp-graph>

Data Exchange

- Privacy or classification matter. How to share IOCs without giving the dataset?
- Bloomfilter (a kind of hash table) where you can lookup values if they are presents or not.
- `misp-bloomfilter2` is an implementation getting the XML from MISP and building bloomfilter databases.
- The bloomfilter can be safely shared within your constituency (e.g. Suricata NIDS, log files lookup...).

²<https://github.com/MISP/misp-bloomfilter>

Conclusion

- Malware Information Sharing Platform (MISP) is released as free software:
 - <https://github.com/MISP/>
- Overcome legal challenges limiting IOCs sharing, by creating innovative solutions.
- Export of events via TAXII or others automatic event streaming are under development.
- If you want to get access to the CIRCL MISP, contact us at info@circl.lu