

Building and designing MISP

A practical information-sharing tool for cybersecurity and fraud indicators



CIRCL

Computer Incident
Response Center
Luxembourg



MISP
Threat Sharing

Alexandre Dulaunoy @adulau
@MISPProject
TLP:WHITE

SHA2017

The bright side of information sharing

- CIRCL has a community of 750 organizations with more than 1500 users **sharing and updating daily cybersecurity indicators, financial indicators or threats in both ways.**
- To achieve this we actively maintain and support MISP (an open source threat sharing¹ platform).
- Beside the tools, **practices, standard formats and classifications** play an important role.
- These practices need to be shared among the communities to support efficient collaboration.

¹also called TIP, CTI platform. <https://www.misp-project.org>

How to be successful in building an information sharing community?

There was never a plan. There was just a series of mistakes.

Robert Caro, journalist.

MISP and starting from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work.**
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development.**

Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
 - **Malware reversers** willing to share indicators of analysis with respective colleagues.
 - **Security analysts** searching, validating and using indicators in operational security.
 - **Intelligence analysts** gathering information about specific adversary groups.
 - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
 - **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
 - **Fraud analysts** willing to share financial indicators to detect financial frauds.

Many objectives from different user-groups

- 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 these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
 - 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction
 - "Our legal framework doesn't allow us to share information."
 - "Risk of information leak is too high and it's too risky for our organization or partners."
- Practical restriction
 - "We don't have information to share."
 - "We don't have time to process or contribute indicators."
 - "Our model of classification doesn't fit your model."
 - "Tools for sharing information are tied to a specific format, we use a different one."

*The art of information sharing is
to share more (and smarter)
than your adversaries.*

MISP Project Overview



Galaxy



warning-lists



Taxonomies



modules (import, export, enrichment)

- The **core project**^a (PHP/Python) supports the backend, API and UI.
- Modules (Python) to expand MISP functionalities (import, export or enrich).
- Taxonomies (JSON) to add categories and global tagging.
- Warning-lists (JSON) to help analysts to detect potential false-positives.
- Galaxy (JSON) to add threat-actors, tools or "intelligence".

^a<https://github.com/MISP/>

MISP features

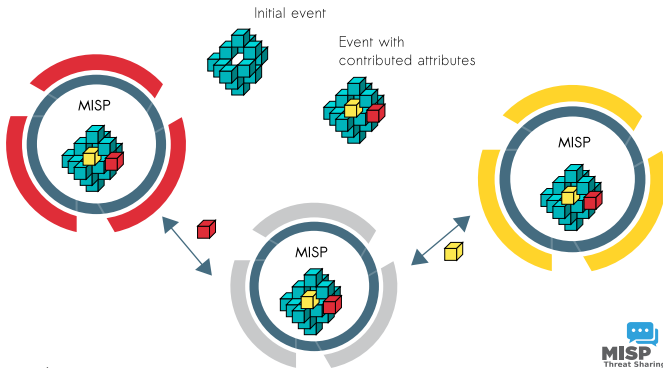


- MISP² is an IOC and threat indicators sharing free software.
- MISP has **many functionalities** e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution and collaboration.
- Many export formats which support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ)
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

²<https://github.com/MISP/MISP>

MISP core distributed sharing functionality

- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



Events and Attributes in MISP

- MISP attributes³ initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage and users (e.g. recent addition of the **financial indicators** in 2.4).
- In next release, MISP galaxy will be added to give the freedom to the **community to create new and combined attributes** and share them.

³attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information

Contributing data to MISP

- Offering a wide range of data creation possibilities
 - Various ways of contributing data via the MISP UI including a freetext parser and a dynamic templating system
 - Flexible APIs that ease automation
 - PyMISP Python library
 - Import tools and Python Import/Enrichment module system
 - Integration with external tools such as Viper, sandboxes such as Cuckoo, etc
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner or simply indicate a sighting.
- **Users should not be forced to use a single interface to contribute.**

Example: Freetext import in MISP

Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

This is a sample text to show how indicators can be extracted. Just paste your text including indicators such as 23.100.122.175, [host.microsoft.com](https://www.microsoft.com), or [b447c27a00e3a348881b0030177000cd](https://www.github.com/MISP/MISP) in here and the tool will automatically detect the indicators and save them as attributes - after allowing you to make some last minute changes. For more information, visit <https://www.github.com/MISP/MISP>

Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

| Value | Category | Type | IDS | Comment | Actions |
|---|------------------|----------|-------------------------------------|-----------------------------------|-------------------------------------|
| 23.100.122.175 | Network activity | ip-dst | <input checked="" type="checkbox"/> | Imported via the freetext import. | <input checked="" type="checkbox"/> |
| host.microsoft.com | Network activity | hostname | <input checked="" type="checkbox"/> | Imported via the freetext import. | <input checked="" type="checkbox"/> |
| b447c27a00e3a348881b0030177000cd | Payload delivery | md5 | <input checked="" type="checkbox"/> | Imported via the freetext import. | <input checked="" type="checkbox"/> |
| https://www.github.com/MISP/MISP | Network activity | url | <input checked="" type="checkbox"/> | Imported via the freetext import. | <input checked="" type="checkbox"/> |

ip-dst → ip-src

Update all comment fields

| + <input type="button" value="Filter"/> | | <input type="button" value="Reset"/> <input type="button" value="Save"/> | | Filters: All File Network Financial Proposal Correlation | | | | | |
|---|-----|--|----------|---|-----------------------------------|----------------|-----|--------------|--|
| Date | Org | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
| 2016-02-24 | | Network activity | hostname | host.microsoft.com | Imported via the freetext import. | | Yes | Inherit | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 2016-02-24 | | Network activity | ip-dst | 23.100.122.175 | Imported via the freetext import. | 298 | Yes | Inherit | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 2016-02-24 | | Network activity | url | https://www.github.com/MISP/MISP | Imported via the freetext import. | | Yes | Inherit | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 2016-02-24 | | Payload delivery | md5 | b447c27a00e3a348881b0030177000cd | Imported via the freetext import. | | Yes | Inherit | <input checked="" type="checkbox"/> <input type="checkbox"/> |

Supporting Sharing in MISP

- Delegate event publication to another organization (introduced in MISP 2.4.18).
 - The other organization can take over the ownership of an event and provide **pseudo-anonymity for the initial organization**.
- Sharing groups allow custom sharing (introduced in MISP 2.4) per event or even at attribute level.
 - Sharing communities can be used locally or even across MISP instances.
 - **Sharing groups** can be done at **event level or attribute level** (e.g. financial indicators shared to a financial sharing group and cyber security indicators to CSIRT community).

Sightings support

The screenshot displays the MISP 'Events' table with three rows. The first row is selected, and a 'Sightings' modal is open over it. The modal shows 'Sightings' in blue, followed by 'CIRCL: 2 (2017-03-19 16:17:59)'. Below the table, the 'Sighting Details' section is expanded, showing 'MISP: 2' and 'CIRCL: 2'. The 'Discussion' button is visible at the bottom of the modal.

| Events | | | |
|-------------------------------------|----|---------|--|
| <input checked="" type="checkbox"/> | No | | |
| <input checked="" type="checkbox"/> | No | | |
| <input checked="" type="checkbox"/> | No | Inherit | |

Tags: +

Date: 2016-02-24

Threat Level: High

Analysis: Initial

Distribution: Connected communities

freetext test

Sighting Details

No

MISP: 2

CIRCL: 2

Discussion

- Sightings allow users to notify the community about the activities related to an indicator.
- In recent MISP version, sighting supports negative sighting (FP) and expiration sighting.
- Sightings can be performed via API, and UI including import of STIX sighting documents.
- Many use-cases opportunities in scoring indicators based on users sighting.

Machine Tags

- Triple tag (or machine tag) was introduced in 2004 to extend geotagging on images.

| | | |
|--|--|---|
| admiralty-scale:source-reliability="c" | | |
|  |  |  |
| namespace | predicate | value |

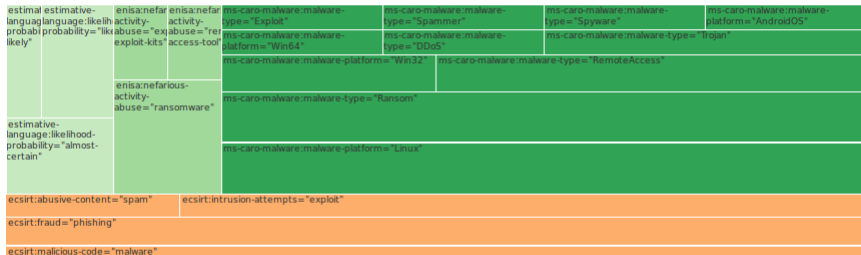
- A machine tag is just a tag expressed in way that allows systems to parse and interpret it.
- Still have a human-readable version:
 - admiralty-scale:Source Reliability="Fairly reliable"

MISP taxonomy statistics and overview

Statistics

Usage data Organisations **Tags** Attribute histogram

A treemap of the currently used event tags. Click on any of the taxonomies to hide it and click it again to show it.



34+ taxonomies available

- NATO - **Admiralty Scale**
- CIRCL Taxonomy - **Schemes of Classification in Incident Response and Detection**
- eCSIRT and IntelMQ incident classification
- EUCI **EU classified information marking**
- NATO Classification Marking
- OSINT **Open Source Intelligence - Classification**
- TLP - **Traffic Light Protocol**
- Vocabulary for Event Recording and Incident Sharing - **VERIS**
- and many more like **ENISA**, **Europol**, or the FIRST SIG Information Exchange Policy.

MISP taxonomy in use


















LOCKY Ransomware via .doc/.docm/.xls/.zip(.js) files (c...

| | |
|--------------|--|
| Event ID | 3142 |
| Uuid | 56c2ff95-bd44-4677-8de9-3dec950d210f |
| Org | CIRCL |
| Owner org | CIRCL |
| Contributors | CERT |
| Email | sascha.rommelfangen@circl.lu |
| Tags | circl:incident-classification="malware" x tlp:white x ecsiirt:malicious-code="ransomware" x veris:action:malware:variety="Ransomware" x ms-caro-malware:malware-type="Ransom" x enisa:nefarious-activity-abuse="ransomware" x + |
| Date | 2016-02-16 |
| Threat Level | Medium |
| Analysis | Completed |
| Distribution | All communities |
| Info | LOCKY Ransomware via .doc/.docm/.xls/.zip(.js) files (constantly updated) |
| Published | Yes |
| Sightings | 0 (0) |

- **Classification must be globally used to be efficient.**
- Tagging can be combined following the needs of the organizations.

Feed system

- Make MISP the tool to **consolidate** threat intel data from any source
- Ingest data from MISP style, CSV or freetext parsed feed source
- Preview and cherry pick the data to ingest

| | | | | | | | | | | | |
|---|--|--|--|--------------------|--------|-----------------|------------------------|-----|---------|--|--|
| ##### ## Feed of current IPs of ramnit C&Cs with 180 minute lookback ## | | | | : activity | ip-dst | 176.32.230.24 | 1 | Yes | Inherit |   |  |
| ## Feed generated at: 2017-06-21 05:03 ## | | | | : activity | ip-dst | 209.99.40.225 | 13 27 | | | | |
| ## Feed Provided By: John Bambenek of Bambenek Consulting ## jcb@bambenekconsulting.com // http://bambenekconsulting.com ## Use of this feed is governed by the licen- ## http://osint.bambenekconsulting.com/licen- ## | | | | : activity | ip-dst | 68.178.232.99 | 931 933 968 1176 | 1 | | | |
| ## For more information on this feed go to: ## http://osint.bambenekconsulting.com/manua ## | | | | : activity | ip-dst | 209.99.40.220 | 1310 27 | 13 | Yes | Inherit |   |
| ## All times are in UTC ## | | | | : activity | ip-dst | 208.73.210.29 | 1 | Yes | Inherit |   | |
| ## False Positive Risk: Low ##### | | | | : activity | ip-dst | | | | | | |
| 34.199.76.50,IP used by ramnit C&C,2017-06-21-05:24-172.250.129,IP used by ramnit C&C,2017-06-21-05:29-250.129,IP used by ramnit C&C,2017-06-21-05:52-9.172.230,IP used by ramnit C&C,2017-06-21-05:52-9.250.234,IP used by ramnit C&C,2017-06-21-05:59-195.129.75,IP used by ramnit C&C,2017-06-21-05:59-64.147.10,IP used by ramnit C&C,2017-06-21-05:59-223.109.60,IP used by ramnit C&C,2017-06-21-05:142.4.204.195,IP used by ramnit C&C,2017-06-21-05:173.230.158.166,IP used by ramnit C&C,2017-06-21-05:185.49.69.153,IP used by ramnit C&C,2017-06-21-05:209.99.40.219,IP used by ramnit C&C,2017-06-21-05:209.99.40.220,IP used by ramnit C&C,2017-06-21-05:209.99.40.222,IP used by ramnit C&C,2017-06-21-05:209.99.40.225,IP used by ramnit C&C,2017-06-21-05:213.247.47.190,IP used by ramnit C&C,2017-06-21-05: | | | | : Network activity | ip-dst | 52.9.250.234 | | | |  | AI |
| | | | | : Network activity | ip-dst | 69.195.129.75 | | | |  | AI |
| | | | | : Network activity | ip-dst | 69.64.147.10 | | | |  | AI |
| | | | | : Network activity | ip-dst | 89.223.109.60 | | | |  | AI |
| | | | | : Network activity | ip-dst | 142.4.204.195 | | | |  | AI |
| | | | | : Network activity | ip-dst | 173.230.158.166 | | | |  | AI |
| | | | | : Network activity | ip-dst | 185.49.69.153 | | | |  | AI |
| | | | | : Network activity | ip-dst | 209.99.40.219 | | | |  | 694 686 684 436 AI |
| | | | | : Network activity | ip-dst | 209.99.40.220 | | | |  | 4549 686 AI |
| | | | | : Network activity | ip-dst | 209.99.40.222 | | | |  | 4838 4674 3069 3335 2531 1190 686 684 AI |

Feed caching

- New caching system allows **correlations to uningested feeds**
- Wide range of default OSINT feeds
- Immediately benefit from correlations
- Build your own feed **overlap analysis matrix**
- Idea came after seeing MLSec's presentation on the TIQ test
- Feed providers just selling repackaged OSINT feeds: We're sorry...

Feed overlap analysis

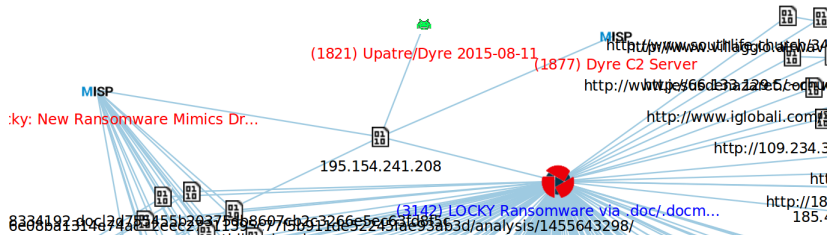
Feed overlap analysis matrix

| | 1 | 2 | 3 | 4 | 5 | 7 | 8 | 10 | 11 | 12 | 15 | 16 | 18 | 19 | 20 | 21 | 24 | 25 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 |
|---|-----|----|----|----|----|----|----|----|----|----|----|-----|-----|----|----|----|----|----|------|-----|----|----|-----|----|-----|-----|
| 1 CIRCL OSINT Feed | - | 1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 2% | 1% | 0% | 0% | 1% | 0% | 0% |
| 2 The Botvrij.eu Data | 48% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 7% | 0% | 0% | 0% | 1% | 0% | 0% |
| 3 ZeuS IP blacklist (Standard) | 1% | 1% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 1% | 99% | 2% | 0% | 0% | 0% | 0% | 76% |
| 4 ZeuS compromised URL blacklist | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 5 blockrules of rules.emergingthreats.net | 1% | 0% | 0% | 0% | - | 0% | 2% | 0% | 0% | 0% | 1% | 10% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 98% | 0% | 0% | 0% | 0% | 0% | 0% |
| 7 malwaredomainlist | 2% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 97% | 2% | 0% | 0% | 0% | 0% | 0% |
| 8 Tor exit nodes | 19% | 0% | 0% | 0% | 3% | 0% | - | 0% | 0% | 0% | 0% | 7% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 99% | 0% | 0% | 0% | 0% | 0% | 0% |
| 10 cybercrime-tracker.net - all | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 11 Phishtank online valid phishing | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 39% | 0% | 0% | 0% | 0% | 1% | 0% |
| 12 listdynamic dns providers | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 1% | 0% | 0% | 0% | 1% | 0% | 0% | 0% |
| 15 longtail.it.marist.edu | 2% | 0% | 0% | 0% | 7% | 0% | 1% | 0% | 0% | 0% | - | 37% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 77% | 0% | 0% | 0% | 0% | 0% | 0% |
| 16 longtail.it.marist.edu 7 days | 1% | 0% | 0% | 0% | 6% | 0% | 3% | 0% | 0% | 0% | 2% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 78% | 0% | 0% | 0% | 0% | 0% | 0% |
| 18 diamondfox_panels | 46% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 19 Mirai-only-dec2016 | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 9% | 0% | 0% | 0% | 0% | 2% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 20 Mirai-only-jan2017 | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 12% | - | 0% | 0% | 0% | 0% | 2% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 21 CIRCL - honeybot | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 38% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 24 booterblacklist.com Latest | 0% | 0% | 0% | 0% | 0% | 0% | 1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 8% | 0% | 0% |
| 25 openbl.org base | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 27 pop3gropers | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 9% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 28 inthreat test | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 1% | 0% | 0% | 0% | 0% | 1% | 0% |
| 29 Ransomware Tracker CSV Feed | 9% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 41% | - | 0% | 0% | 24% | 0% | 1% | 0% |
| 30 Feodo IP Blacklist | 11% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% | - | 0% | 0% | 0% | 99% | 0% |
| 31 hosts-file.net - hphost - malwarebytes | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | - | 0% | 0% | 0% | 0% |
| 32 hosts-file.net - hphost - malwarebytes - EMD classification ONLY | 1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 1% | 4% | 0% | 0% | - | 0% | 0% | 0% |
| 33 OpenPhish url list | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 9% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 86% | 0% | 0% | 0% | 0% | - | 0% | 0% |
| 34 firehol_level1 | 1% | 0% | 1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 85% | 1% | 5% | 0% | 0% | 0% | - | 0% |

Where Information Sharing Helped

- Suspicious executables which require shared analysis or evaluation (**pre-investigation** stage).
- Tracking financial malware including related cash out bank accounts (mixed events (IoC and financial indicators) with different sharing groups).
- Fake invoicing fraud bank details shared to discover the same mule acquisition network.
- Finding stable infrastructure of adversaries (malware targeting financial sector) by **sharing regularly**.

Practical Example: Benefit of Sharing



Conclusion

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support your internal practices.
- Enable users to customize threat intelligence platform to meet their community's use-cases or **mimic the sharing practices of the adversaries**.
- With adequate automation, **information overflow can become an advantage** (e.g. automated take-down request).

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- <https://github.com/MISP/> -
<https://www.misp-project.org/>
- MISP Summit before hack.lu (16th October 2017) - MISP Core Team will be at Open Source Security Hackathon
<https://hackathon.hack.lu/>