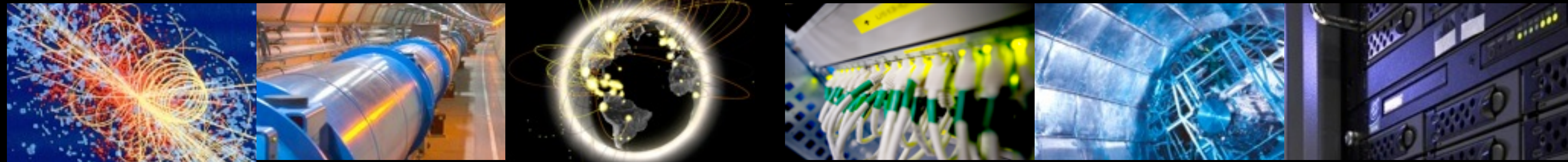


Creating a trust-group for security information sharing (in Asia Pacific?)



Romain Wartel, ISGC 2018, Taipei, 20 March 2018



Indicators of compromise

- Examples of indicators:
 - IP or domain names
 - May be shared and used for legitimate purposes or recycled
 - Easy to use
 - File names or file hashes
 - May be trivially changed
 - Easy to use
 - Yara rules, regular expression, etc.
 - Less chance of false positives
 - More costly to use
 - Email headers and fields



Threat intelligence

- Proposed definition – not universal
- Threat intelligence includes:
 - Indicators of compromise (IP addresses, hashes, etc.)
 - Contextual information
 - Tactics, Technique and Procedures for a malicious actor
- Goal: Enable the recipient to take action
 - As a preventive measure
 - As a remediation against ongoing or past attacks



Sourcing intelligence

- No shortage of sources!
- Public feeds, raw or filtered
- Paid-for feeds from security vendors
- Tailored blends of private and public feeds for sale
- “Black box” appliances
 - Intelligence data not available for review
 - Data is analysed by the system or appliance
 - Alert is raised upon positive match of a proprietary indicator
- But is this a good investment?
 - Catch more than low-risk threats and internet background noise?
 - How about the false positive rate?



Relevance

- Actors are continuously changing parameters
 - Change at least partially their infrastructure for each campaign
 - Fast-flux DNS infrastructures
 - Domain Name Generators for Command & Control
 - Randomised email content, mail headers (from field, subject. etc.)
 - Randomised malware payload (different filename and hash)
- Relevance
 - Is it relevant to my sector, local configuration and location?
 - Is it actionable?
 - Reasonable to expect a low or manageable false positive rate?



Quality

- Key aspects of threat intelligence quality

- Malicious

- Often malware contacts "8.8.8.8"
 - Behavior requires careful analysis before flagging as indicator

- Targeted

- Full URLs are better than domains or IPs
 - Multiple customer may use the same domain
 - *sharepoint.com* or

- https://supremeselfstorage-my.sharepoint.com/personal/andrew_supremeselfstorage_com_au/_layouts/15/guestaccess.aspx?guestaccesstoken=GTQPc%2brKLAsKHba4nXtvl0hXrBsUmCUxoYGuu9msk0U%3d&docid=0c4b96dfd3319496a8feb1a56d88de679&rev=1

- Timeliness

- Bad actors also read the news and at least public feeds
 - Domains and IP addresses get re-assigned quickly (especially IPv4)
 - Infected hosts are being cleaned

- Who can provide quality and relevant threat intelligence?



Back to the basics

- Research & Education is a viable market for cybercriminals
 - Ransomware, finance fraud, etc.
- Offers a favorable cost/benefit ratio for many bad actors
- Main attackers profile:
 - Cybercriminals (money) – less opportunistic, more targeted
 - Hacktivists (delay, disrupt, destroy)
 - Nation-states (data, strategy, tender info, technology, IP)



Back to the basics

- Most serious attack will be complex or sophisticated
 - *Can your organisation or project defend against a nation-state or an international criminal gang with a multi-million dollars budget for both its malware and distributed attacking computing infrastructure?*
 - As individual organisations, it is not affordable
 - But as a community, we are much better positioned!
 - **Sharing information, expertise... and threat intelligence is key**



Trust and threat intelligence

- Threat intelligence is not necessarily a service
- Threat intelligence is an expression of a trust relationship
- Response to threats as a community
 - Best mean to fight sophisticated adversaries at acceptable costs



Building a cohesive community

1. Identify like-minded organisations
2. Identify security or technical experts within them, or anyone willing to collaborate
3. Build trust relationships between participants
(physical meeting, sharing war stories, etc.)
4. Establish common goals, needs and issues
5. Enable participants to share sensitive information (tools, mailing list)
6. Enable participants to act on intelligence... and share back!
7. Add value by pooling resources/effort (extra expertise for forensics, tools, etc.)
8. Establish strong external links with the of the security community
(cross-membership, etc.)



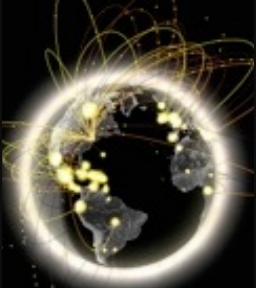
How to encourage new members to join?

- The community can provide:
 - Free expertise, help, tools, tutorials, etc.
 - Indicators of compromise, experience from attacks
- New members can provide with no security expertise:
 - Contact points
 - Access to compromised machines
 - Data, log files
- As a new member, the bar is very low. But the benefits are high!
- Similar strategy when small trust groups aim at participating in global groups
 - Be pro-active, share what you have/can, build trust relationship, profit.







Conclusion

- Best way to defend is to do it as a community
- Threat intelligence is an output of a community response
- Essential to support communities in:
 - Building trust
 - Creating and sharing value
 - Provide support on technical issues
 - Connect to other Internet security trust groups
- How can we (WLCG) help?
- Maybe a new operational security trust group could emerge from:
 - Asia Tier Forum? APGRIDPMA? APAN Security Working Group? PRAGMA?



Confidentiality

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.



Subject: [CERNCERT-2016-12-24] HEADS-UP: Multiple identities compromised at Acme Corporation [TLP:AMBER]
 -----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA256

Dear affected eduGAIN participants,

TLP:AMBER

SUMMARY

The CERN CERT has detected multiple identities being compromised at the Acme Corporation IdP. CERN is investigating the case and has reported the abuse to Acme Corporation (no reply yet). Early forensics findings highlighted several eduGAIN participants (all recipients of this email) are likely affected and should urgently check their security status.

This is an ongoing investigation and more details will be shared as they become available.

INTRUSION TIMELINE

2016-12-24 06:01: Will. E sends an abuse complaint to the CERN CERT.
 2016-12-24 08:31: CERN CERT confirms abuse and reports it to the Acme Corporation.
 2016-12-24 09:40: CERN CERT discovers other affected parties.
 2016-12-24 10:50: SWITCH Federation Security contact is informed and its is agreed CERN CERT will act as the incident coordinator for now



Don't Share

Share only with your team

Share with community but not public

Share with anyone



Mattermost or Slack

The image displays two overlapping screenshots of team communication tools. The background screenshot is Mattermost, showing a channel named 'Website Discussion' with a Python code snippet for activity tracking. The foreground screenshot is Slack, showing a channel named '#culture' with a discussion about tweets and a meeting announcement.

Mattermost Screenshot:

- Channel: Website Discussion
- User: Eric Vanderlin (7:56 PM)
- Code Snippet:


```

from time import localtime

activities = {8: 'Sleeping',
             9: 'Commuting',
             18: 'Commuting',
             22: 'Resting' }

time_now = localtime()
hour = time_now.tm_hour

for activity_time in sorted(activities.keys()):
    if hour < activity_time:
        print activities[activity_time]
        break
else:
    print 'Unknown, AFK or sleeping!'
      
```
- User: Stacy Walkin (8:00 PM)

So, should I update our marketing screenshot with a portion of this
- User: Eric Vanderlin (8:00 PM)

Yeah I think that would be great.
- User: Eric Vanderlin (8:01 PM)

Also @stacey, when would you be available to have a call? Need to c
- User: Stacy Walkin (8:01 PM)

I would be available in an hour if you'd like to talk.
- User: Eric Vanderlin (8:02 PM)

Cool, see you then!

Slack Screenshot:

- Channel: #culture
- User: Lane Collins (12:50 PM)

Really need to give some Kudos to @julie for helping out with the new influx of Tweets yesterday. People are really, really excited about yesterday's announcements.
- User: Kiné Camara (12:55 PM)

No! It was my pleasure! People are very excited. ⚡
- User: Jason Stewart (2:14 PM)

What are our policies in regards to pets in the office? I'm assuming it's a no-go, but thought I would ask here just to make sure what was the case.
- Event: Acme Culture Meeting (2:15 PM)

Event starting in 15 minutes:

Culture Weekly Meeting
Today from 2:30 PM to 3:00 PM
- User: Johnny Rodgers (2:18 PM)

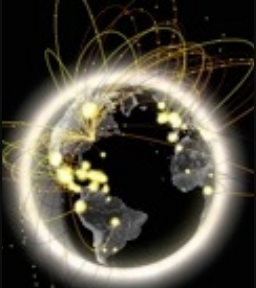
shared a post

Building Policies & Procedures
Last edited 2 months ago

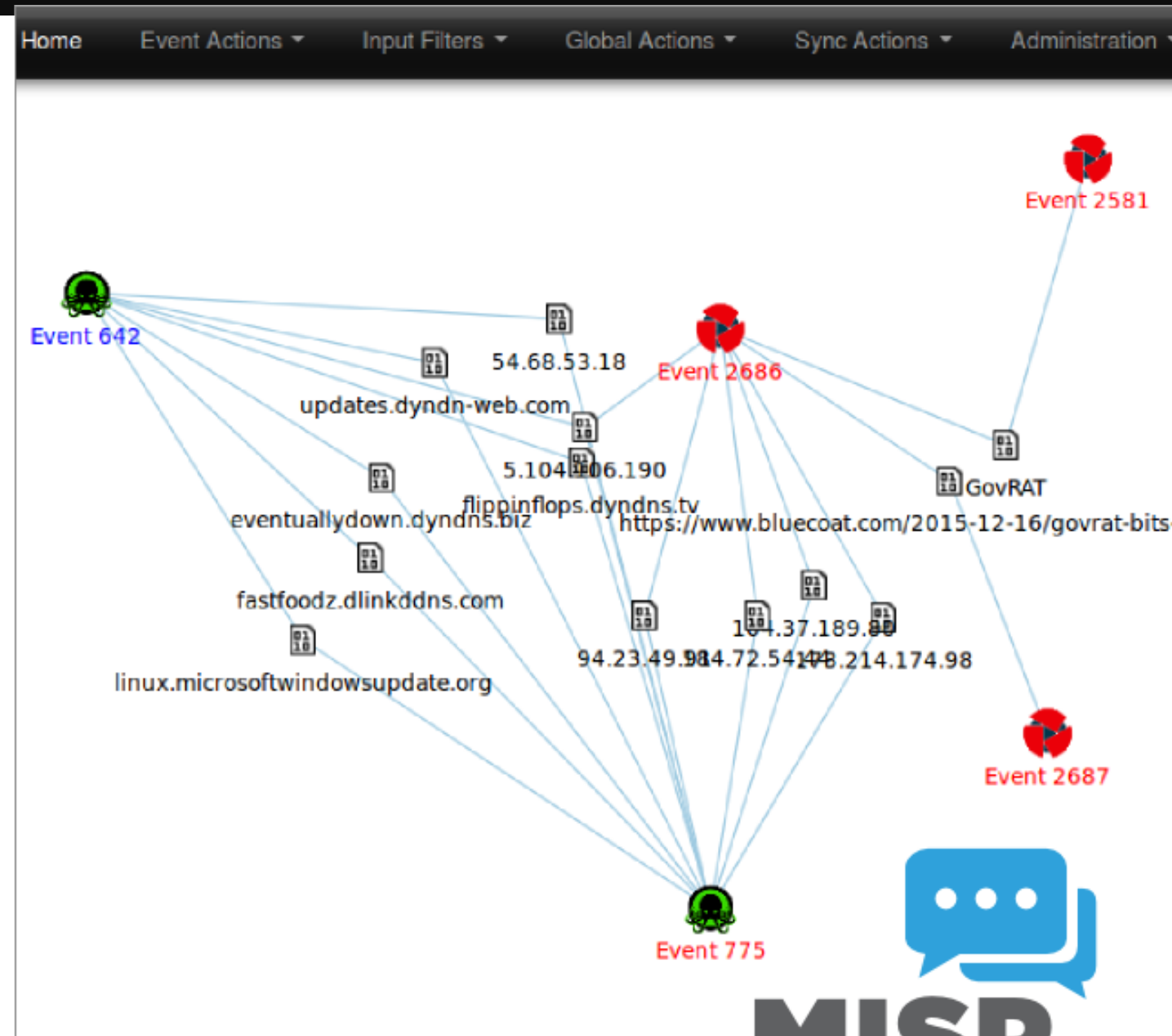
SECURITY POLICIES

 - All guests and visitors must sign in
- User: Jason Stewart (2:22 PM)

Thanks Johnny!



MISP



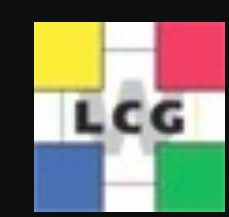
TLP Taxonomy Library

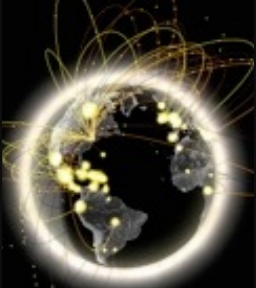
Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

← previous next →

<input type="checkbox"/> Tag	Expanded	Events	Tag	Action
<input type="checkbox"/>	tip:red (TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	🔄
<input type="checkbox"/>	tip:amber (TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	🔄
<input type="checkbox"/>	tip:green (TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	🔄
<input type="checkbox"/>	tip:white (TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	🔄
<input type="checkbox"/>	tip:ex:chr (TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	🔄

Id	Exportable	Name ↓	Taxonomy	Tagged events	Actions
6	✗	APT		31	🔄 🗑️
7	✗	Actionable:NO		5	🔄 🗑️
3	✗	TLP:AMBER	tlp	131	🔄 🗑️
8	✗	TLP:EX:CHR	tlp	11	🔄 🗑️
5	✗	TLP:GREEN	tlp	550	🔄 🗑️
4	✗	TLP:RED	tlp	3	🔄 🗑️
2	✗	TLP:WHITE	tlp	531	🔄 🗑️
10	✗	TO:HIDE		2	🔄 🗑️
9	✗	TODO		9	🔄 🗑️
11	✗	TODO:VT-ENRICHMENT		8	🔄 🗑️
1	✗	Type:OSINT		832	🔄 🗑️
18	✓	admiralty-scale:information-credibility="1"	admiralty-scale	0	🔄 🗑️
19	✓	admiralty-scale:information-credibility="2"	admiralty-scale	0	🔄 🗑️
20	✓	admiralty-scale:information-credibility="3"	admiralty-scale	0	🔄 🗑️
21	✓	admiralty-scale:information-credibility="4"	admiralty-scale	0	🔄 🗑️
22	✓	admiralty-scale:information-credibility="5"	admiralty-scale	0	🔄 🗑️
23	✓	admiralty-scale:information-credibility="6"	admiralty-scale	0	🔄 🗑️





MISP

File Edit View History Bookmarks Tools Help

MISP/MISP: MISP - ... x Events - MISP x +

https://misppriv.circl.lu/events/view/5279

Home Event Actions Input Filters Global Actions Sync Actions Administration Audit Discussions MISP Alexandre Dulaunoy Log out

View Event

- View Correlation Graph
- View Event History
- Edit Event
- Delete Event
- Add Attribute
- Add Attachment
- Populate from...
- Merge attributes from...
- Contact Reporter
- Download as...
- List Events
- Add Event

OSINT - Octopus-Rex. Evolution of a multi task Botnet

Event ID: 5279
 Uuid: 5813ad13-c2fc-427d-b284-44cd02de0b81
 Org: CIRCL
 Owner org: CIRCL
 Contributors: alexandre.dulaunoy@circl.lu
 Email: alexandre.dulaunoy@circl.lu
 Tags: tlp:white x ms-caro-malware:malware-platform="Linux" x circl:incident-classification="malware" x circl:osint-feed x osint:source-type="blog-post" x +
 Date: 2016-10-28
 Threat Level: Low
 Analysis: Completed
 Distribution: All communities
 Info: OSINT - Octopus-Rex. Evolution of a multi task Botnet
 Published: Yes
 Sightings: 0 (0)

Related Event: 2016-09-16 (4925)
 Org: CIRCL
 Date: 2016-09-16
 Info: OSINT - ELF.Rex

5279: OSINT ...

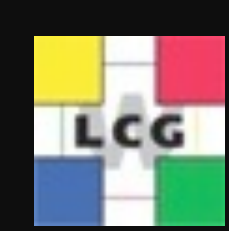
« previous 1 2 3 4 5 6 7 8 next » view all

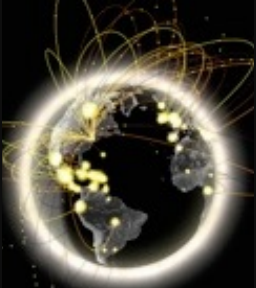
Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Sightings	Actions
2016-10-28		Artifacts dropped	md5	1b9b87630049af66d3ce27d022dcad0a	List of hashes (unpacked version only) - Xchecked via VT: ac36c87cacbe1b8327fae3084ebd1740a3a5c6c6f208c1c77da56932a9ca3be6	4694	Yes	Inherit	0 (0)	🗑️ 🗑️ 🗑️
2016-10-28		Artifacts dropped	md5	a22dfa9e4dfe97b9ede4d677de74a1b1	List of hashes (unpacked version only) - Xchecked via VT: 0e8be50f0ad59239599eaceb7a6e30cc5909d401b2ff784e670ddecca1bc29d0		Yes	Inherit	0 (0)	🗑️ 🗑️ 🗑️
2016-10-28		Artifacts dropped	md5	140720cf5ab52b22c36f04782d877ee1	List of hashes (unpacked version only) - Xchecked via VT: bf1f82ee300fa15a07ca02da78b1ed649877e38a613651377642b86dd0dbb40a		Yes	Inherit	0 (0)	🗑️ 🗑️ 🗑️

https://misppriv.circl.lu/events/view/4925/1/5279

Powered by MISP 2.4.53 operated by Computer Incident Response Center Luxembourg (CIRCL)





MISP

Example: Freetext import in MISP

Discussion

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

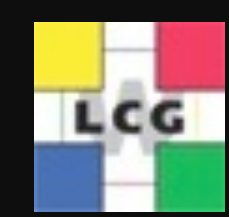
ip-dst → ip-src

Update all comment fields

+ [Icons]

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 type="button" value="✕"/> <input type="button" value="🔗"/> <input type="button" value="🗑️"/>
2016-02-24		Network activity	ip-dst	23.100.122.175	Imported via the freetext import.	298	Yes	Inherit	<input type="button" value="🔗"/> <input type="button" value="🗑️"/>
2016-02-24		Network activity	url	https://www.github.com/MISP/MISP	Imported via the freetext import.		Yes	Inherit	<input type="button" value="🔗"/> <input type="button" value="🗑️"/>
2016-02-24		Payload delivery	md5	b447c27a00e3a348881b0030177000cd	Imported via the freetext import.		Yes	Inherit	<input type="button" value="🔗"/> <input type="button" value="🗑️"/>





Acting on threat intelligence

- Sadly, sharing great threat intelligence is not sufficient
- Acting on indicators is a significant challenge!
- Each participant must:
 1. Collect enough information locally
 - Network flows, local logs, emails headers, etc.
 2. Accumulate, parse and incorporate incoming threat intelligence
 3. Correlate local information and indicators
 4. Take appropriate action & manage false positives
- Not only a technical challenge
 - Security teams “already busy” with other things
 - Not all data (step 1) may be within (legal, technical) reach
 - Need cooperation between different teams