CyDefSIG: Cyber Defence Signature Sharing Platform, version: 1.1.1

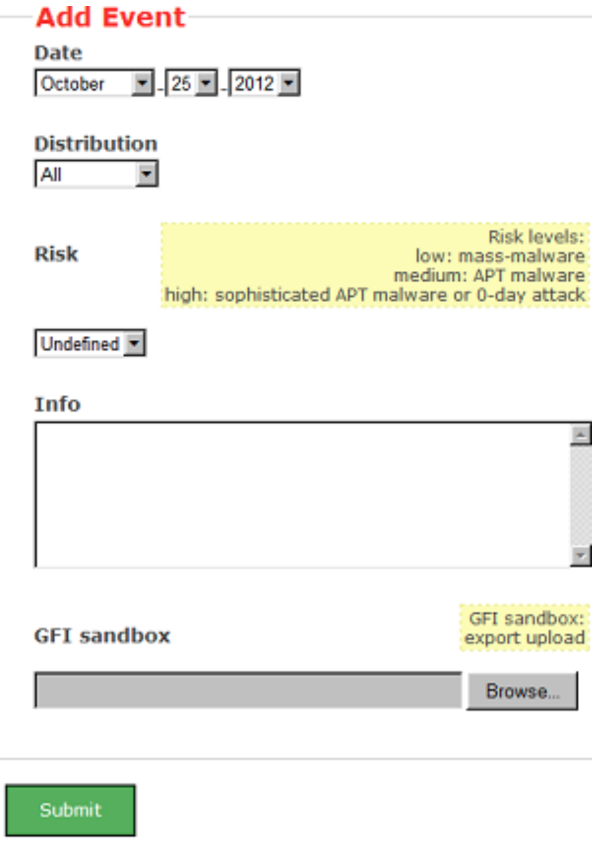
Table of contents

Using the system:

Creating an event:

The process of entering an event can be split into 3 phases, the creation of the event itself, populating it with attributes and attachments and finally publishing it.

During this first step, you will be create a basic event without any actual attributes, but storing general information such as a description, time and risk level of the incident. To start creating the event, click on the New Event button on the left and fill out the form you are presented with. The following fields need to be filled out:



Add Event

Date: October - 25 - 2012

Distribution: All

Risk: Undefined

Risk levels:
low: mass-malware
medium: APT malware
high: sophisticated APT malware or 0-day attack

Info:

GFI sandbox:

GFI sandbox: export upload

- ***Date:*** The date when the incident has happened.
- ***Distribution:*** This setting controls, who will be able to see this event once it becomes published. Apart from being able to set which users on this server are allowed to see the event, this also controls whether the event will be synchronised to other servers or not. The following options are available:
  - *Your organization only:* This setting will only allow members of your organisation on this server to see it.
  - *This server-only:* This setting will only allow members of any organisation on this server to see it.
  - *This Community-only:* Users that are part of your MISP community will be able to see the event. This includes your own organisation, organisations on your MISP server and organisations running MISP servers that synchronise with this server. Any other organisations connected to such linked servers will be restricted from seeing the event. Use this option if you are on the central hub of your community.

  - *Connected communities:* Users that are part of your MISP community will be able to see the event. This includes all organisations on your own MISP server, all organisations on MISP servers synchronising with this server and the hosting organisations of servers that connect to those afore mentioned servers (so basically any server that is 2 hops away from this one). Any other organisations connected to linked servers that are 2 hops away from this own will be restricted from seeing the event. Use this option if this server isn't the central MISP hub of the community but is connected to it.

  - *All communities:* This will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.

- ***Risk:*** This field indicates the risk level of the event. Incidents can be categorised into three different threat categories (low, medium, high). This field can alternatively be left as undefined. The 3 options are:

  - *Low:* General mass malware.

  - *Medium:* Advanced Persistent Threats (APT)

  - *High:* Sophisticated APTs and 0day attacks.

- ***Analysis:*** Indicates the current stage of the analysis for the event, with the following possible options:

  - *Initial:* The analysis is just beginning

  - *Ongoing:* The analysis is in progress

  - *Completed:* The analysis is complete

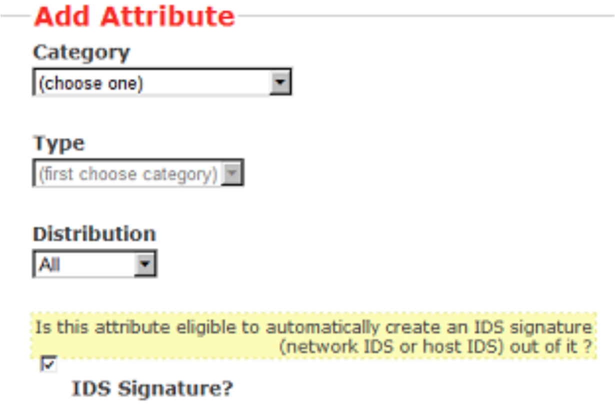
- ***Info:*** The info field, where the malware/incident can get a brief description starting with the internal reference. This field should be as brief and concise as possible, the more detailed description happens through attributes in the next stage of the event's creation. Keep in mind that the system will automatically replace detected text strings that match a regular expression entry set up by your server's administrator(s).

- ***GFI Sandbox:*** It is possible to upload the exported .zip file from GFI sandbox with the help of this tool. These will be dissected by the MISP and a list of attributes and attachments will automatically be generated from the .zip file. Whilst this does most of the work needed to be done in the second step of the event's creation, it is important to manually look over all the data that is being entered.

Add attributes to the event:

The second step of creating an event is to populate it with attributes and attachments. In addition to being able to import the attributes and attachments from GFI, it is also possible to manually add attributes and attachments to an event, by using the two appropriate buttons on the event's page. Let's look at adding attributes first.
When clicking on the add attribute button, you will have to fill out a form with all the data about the attribute.

Keep in mind that the system searches for regular expressions in the value field of all attributes when entered, replacing detected strings within it as set up by the server's administrator (for example to enforce standardised capitalisation in paths for event correlation or to bring exact paths to a standardised format). The following fields need to be filled out:



Add Attribute

Category
(choose one)

Type
(first choose category)

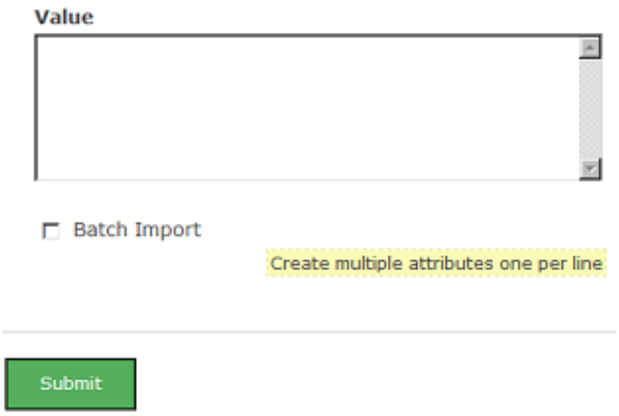
Distribution
All

Is this attribute eligible to automatically create an IDS signature (network IDS or host IDS) out of it ?

☑ IDS Signature?

- ***Category:*** This drop-down menu explains the category of the attribute, meaning what aspect of the malware this attribute is describing. This could mean the persistence mechanisms of the malware or network activity, etc. For a list of valid categories, **click here**

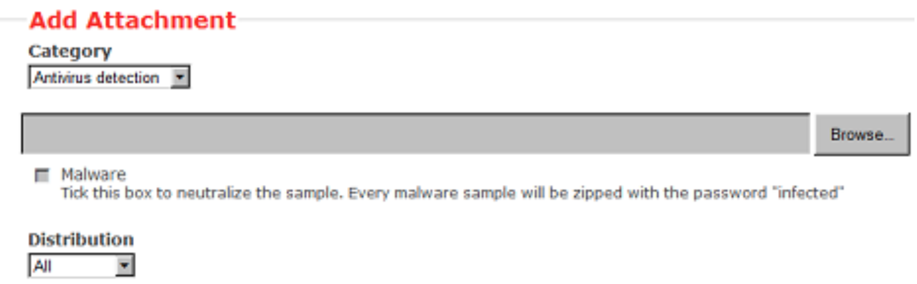
- ***Type:*** Whilst categories determine what aspect of an event they are describing, the Type explains by what means that aspect is being described. As an example, the source IP address of an attack, a source e-mail address or a file sent through an attachment can all describe the payload delivery of a malware. These would be the types of attributes with the category of payload deliver. For an explanation of what each of the types looks like together with the valid combinations of categories and types, **click here**.



- ***Distribution:*** This drop-down list allows you to control who will be able to see this attribute, independently from its event's distribution settings.
  - *Your organisation only:* This setting will only allow members of your organisation on your server to see it.
  - *This server-only:* This setting will only allow members of any organisation on your server to see it.
  - *This Community-only:* Users that are part of your MISP community will be able to see the attribute. This includes your own organisation, organisations on your MISP server and organisations running MISP servers that synchronise with your server. Any other organisations connected to such linked servers will be restricted from seeing the attribute. Use this option if you are on the central hub of your community.
  - *Connected communities:* Users that are part of your MISP community will be able to see the attribute. This includes all organisations on your own MISP server, all organisations on MISP servers synchronising with your server and the hosting organisations of servers that connect to those afore mentioned servers (so basically any server that is 2 hops away from your own). Any other organisations connected to linked servers that are 2 hops away from your own will be restricted from seeing the attribute. Use this option if your server isn't the central MISP hub of the community but is connected to it.
  - *All communities:* This will share the attribute with all MISP communities, allowing the attribute to be freely propagated from one server to the next.
- ***IDS Signature:*** This option allows the attribute to be used as an IDS signature when exporting the NIDS data, unless it is being overruled by the white-list. For more information about the whitelist, head over to the **administration** section.
- ***Value:*** The actual value of the attribute, enter data about the value based on what is valid for the chosen attribute type. For example, for an attribute of type ip-src (source IP address), 11.11.11.11 would be a valid value. For more information on types and values, **click here**.
- ***Batch import:*** If there are several attributes of the same type to enter (such as a list of IP addresses, it is possible to enter them all into the same value-field, separated by a line break between each line. This will allow the system to create separate lines for the each attribute.

Add attachments to the event:

You can also upload attachments, such as the malware itself, report files from external analysis or simply artifacts dropped by the malware. Clicking on the add attachment button brings up a form that allows you to quickly attach a file to the event. The following fields need to be filled out:



Add Attachment

Category

Antivirus detection

□ Malware

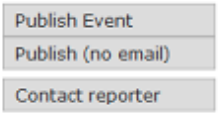
Tick this box to neutralize the sample. Every malware sample will be zipped with the password "infected"

Distribution

All

- ***Category:*** The category is the same as with the attributes, it answers the question of what the uploaded file is meant to describe.
- ***Upload field:*** By hitting browse, you can browse your file system and point the uploader to the file that you want to attach to the attribute. This will then be uploaded when the upload button is pushed.
- ***Malware:*** This check-box marks the file as malware and as such it will be zipped and passworded, to protect the users of the system from accidentally downloading and executing the file. Make sure to tick this if you suspect that the filed is infected, before uploading it.
- ***Private:*** This drop-down menu controls who the attachment will be shared as.
  - *Your organisation only:* This setting will only allow members of your organisation on your server to see it.
  - *This server only:* This setting will only allow members of any organisation on your server to see it.
  - *This community only:* Users that are part of your MISP community will be able to see the attachment. This includes your own organisation, organisations on your MISP server and organisations running MISP servers that synchronise with your server. Any other organisations connected to such linked servers will be restricted from seeing the attachment. Use this option if you are on the central hub of your community.
  - *Connected communities:* Users that are part of your MISP community will be able to see the attachment. This includes all organisations on your own MISP server, all organisations on MISP servers synchronising with your server and the hosting organisations of servers that connect to those afore mentioned servers (so basically any server that is 2 hops away from your own). Any other organisations connected to linked servers that are 2 hops away from your own will be restricted from seeing the attachment. Use this option if your server isn't the central MISP hub of the community but is connected to it.
  - *All:* This will share the attachment with all MISP communities, allowing the attachment to be freely propagated from one server to the next.

Publish an event:



Once all the attributes and attachments that you want to include with the event are uploaded / set, it is time to finalise its creation by publishing the event (click on publish event in the event view). This will alert the eligible users of it (based on the private-controls of the event and its attributes/attachments and whether they have auto-alert turned on), push the event to servers that your server connects to if allowed (private needs to be set to all) and readies the network related attributes for NIDS signature creation (through the NIDS signature export feature, for more information, go to the export section.).

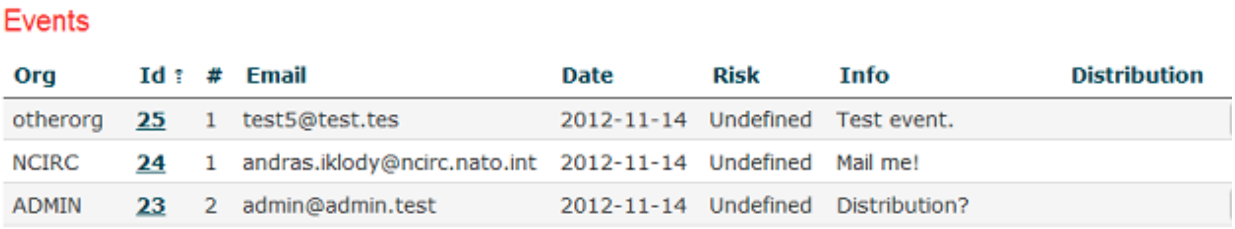
There is an alternate way of publishing an event without alerting any other users, by using the "publish (no email)" button. This should only be used for minor edits (such as correcting a typo).

Browsing past events:

The MISP interface allows the user to have an overview over or to search for events and attributes of events that are already stored in the system in various ways.

To list all events:

On the left menu bar, the option "List events" will generate a list of the last 60 events. While the attributes themselves aren't shown in this view, the following pieces of information can be seen:



Events

Org	Id	#	Email	Date	Risk	Info	Distribution
otherorg	25	1	test5@test.tes	2012-11-14	Undefined	Test event.	
NCIRC	24	1	andras.iklody@ncirc.nato.int	2012-11-14	Undefined	Mail me!	
ADMIN	23	2	admin@admin.test	2012-11-14	Undefined	Distribution?	

- ***Org:*** The organisation that uploaded the event.

- ***ID:*** The event's ID number, assigned by the system when the event was first entered (or in the case of an event that was synchronized, when it was first copied over - more on synchronisation in chapter xy)

- ***#:*** The number of attributes that the event has.

- ***Email:*** The e-mail address of the event's reporter.

- ***Date:*** The date of the attack.

- ***Risk:*** The risk level of the attack, the following levels are possible:

  - ***Low:*** General Malware
  - ***Medium:*** Advanced Persistent Threats (APTs)
  - ***High:*** Sophisticated APTs and 0day exploits
  - ***Undefined:*** This field can be left undefined and edited at a later date.

- ***Analysis:*** Indicates the current stage of the analysis for the event, with the following possible options:

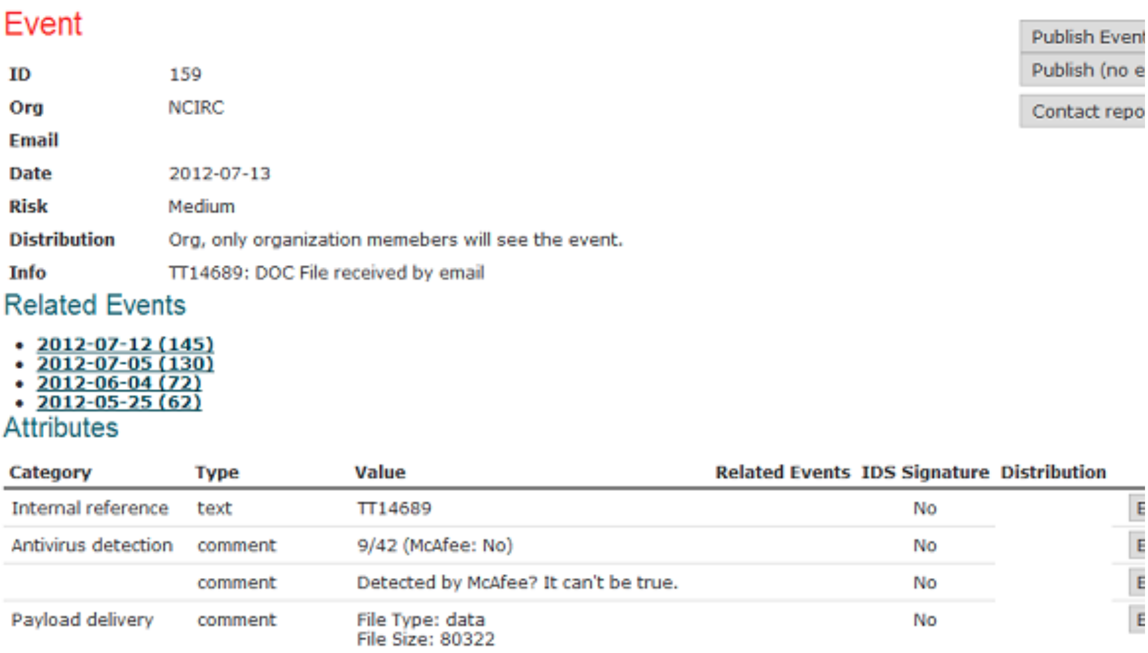
  - ***Initial:*** The analysis is just beginning
  - ***Ongoing:*** The analysis is in progress
  - ***Completed:*** The analysis is complete

- ***Info:*** A short description of the event, starting with an internal reference number.

- ***Distribution:*** This field indicates what the sharing privileges of the event are. The selectable options are "This organisation only", "This server only", "This community only", "Connected communities", "All". For a detailed description of these settings read the section on **creating a new event**.

- ***Actions:*** The controls that the user has to view or modify the event. The possible actions that are available (depending on user privileges - **click here** to find out more about privileges):

  - ***Publish:*** Publishing an event will have several effects: The system will e-mail all eligible users that have auto-alert turned on (and having the needed privileges for the event, depending on its private classification) with a description of your newly published event, it will be flagged as published and it will be pushed to all eligible servers (to read more about synchronisation between servers, have a look at the **section on connecting servers**).
  - ***Edit:*** Clicking on the edit button will bring up the same same screen as the one used for creating new events, with the exception that all fields come filled out with the data of the event that is being edited. For more information on this view, refer to the section on **creating an event**.
  - ***Delete:*** The system will prompt you before erasing the unwanted event.
  - ***View:*** Will bring up the event view, which besides the basic information contained in the event list, will also include the following:



Event

ID	159
Org	NCIRC
Email	
Date	2012-07-13
Risk	Medium
Distribution	Org, only organization memebers will see the event.
Info	TT14689: DOC File received by email

Related Events

- 2012-07-12 (145)
- 2012-07-05 (130)
- 2012-06-04 (72)
- 2012-05-25 (62)

Attributes

Category	Type	Value	Related Events	IDS Signature	Distribution	
Internal reference	text	TT14689		No		E
Antivirus detection	comment	9/42 (McAfee: No)		No		E
	comment	Detected by McAfee? It can't be true.		No		E
Payload delivery	comment	File Type: data File Size: 80322		No		E

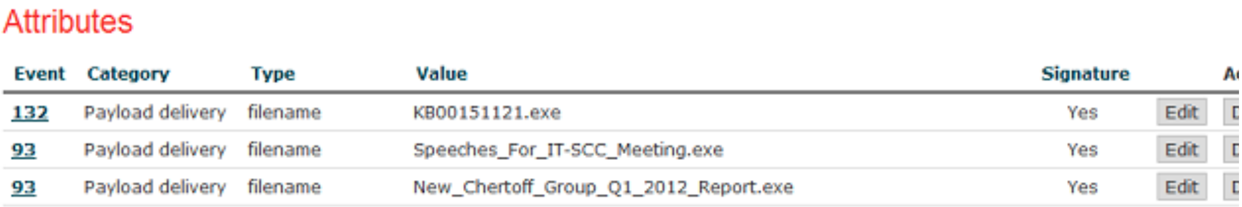
- ***List of related events:*** Events can be related by having one or more attributes that are exact matches. For example, if two events both contain a source IP attribute of 11.11.11.11 then they are related. The list of events that are related the currently shown one, are listed under "Related Events", as links (titled the related event's date and ID number) to the events themselves.

- ***Attributes:*** A list of all attributes attached to the event, including its category, type, value, whether the attribute in itself is related to another event, whether the flag signalling that the attribute can be turned into an IDS signature is on, and a field showing the current privacy setting of the attribute.Attributes can also be modified or deleted via the 3 buttons at the end of each line.

  Using the modify button will bring up the attribute creation view, with all data filled out with the attribute's currently stored data.

Listing all attributes:

Apart from having a list of all the events, it is also possible to get a list of all the stored attributes in the system by clicking on the list attributes button. The produced list of attributes will include the followings fields:



Attributes

Event	Category	Type	Value	Signature	A
132	Payload delivery	filename	KB00151121.exe	Yes	Edit D
93	Payload delivery	filename	Speeches_For_IT-SCC_Meeting.exe	Yes	Edit D
93	Payload delivery	filename	New_Chertoff_Group_Q1_2012_Report.exe	Yes	Edit D

- ***Event:*** This is the ID number of the event that the attribute is tied to.

- ***Category:*** The category of the attribute, showing what the attribute describes (for example the malware's payload). For more information on categories, go to section xy

- ***Type:*** The type of the value contained in the attribute (for example a source IP address). For more information on types, go to section xy

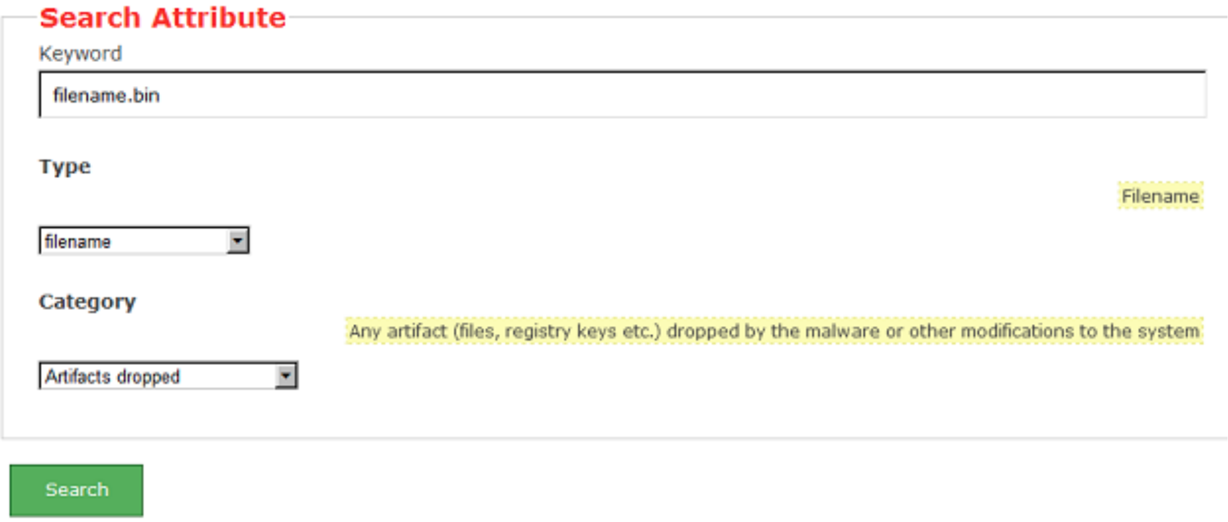
- ***Value:*** The actual value of the attribute, describing an aspect, defined by the category and type fields of the malware (for example 11.11.11.11).

- ***Signature:*** Shows whether the attribute has been flagged for NIDS signature generation or not.

- ***Actions:*** A set of buttons that allow you to view the event that the attribute is tied to, to edit the attribute (using the same view as what is used to set up attributes, but filled out with the attribute's current data) and a delete button.

Searching for attributes:

Apart from being able to list all events, it is also possible to search for data contained in the value field of an attribute, by clicking on the "Search Attributes" button.



Search Attribute

Keyword

filename.bin

Type

Filename

filename

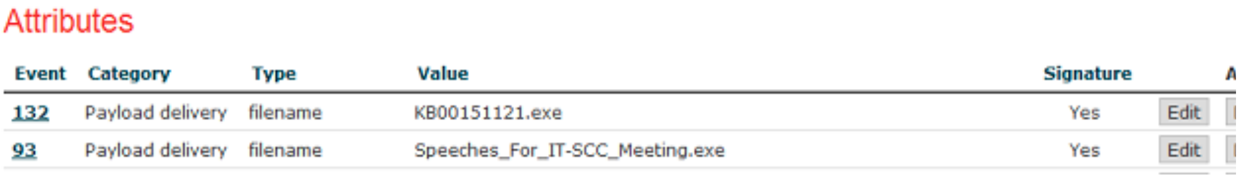
Category

Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system

Artifacts dropped

This will bring up a form that lets you enter a search string that will be compared to the values of all attributes, along with options to narrow down the search based on category and type. The entered search string has to be an exact match with (the sub-string of) a value.

The list generated by the search will look exactly the same as listing all attributes, except that only the attributes that matched the search criteria will be listed (to find out more about the list attributes view, **click here**.).



Attributes

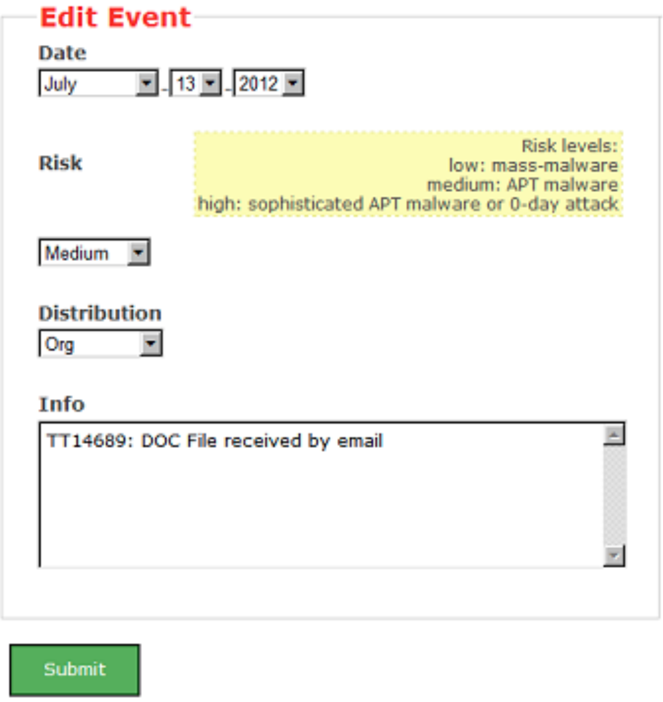
Event	Category	Type	Value	Signature	A
132	Payload delivery	filename	KB00151121.exe	Yes	Edit
93	Payload delivery	filename	Speeches_For_IT-SCC_Meeting.exe	Yes	Edit

Updating and modifying events and attributes:

Every event and attribute can easily be edited. First of all it is important to find the event or attribute that is to be edited, using any of the methods mentioned in the section on **browsing past events**.

Once it is found, the edit button (whether it be under actions when events/attributes get listed or simply on the event view) will bring up the same screen as what is used to create the entry of the same type (for an event it would be the event screen as **seen here**, for an attribute the attribute screen as **described here**).

Keep in mind that editing any event (either directly or indirectly through an attribute) will unpublish it, meaning that you'll have to publish it (through the event view) again once you are done.



Edit Event

Date July 13 2012

Risk

Risk levels:
low: mass-malware
medium: APT malware
high: sophisticated APT malware or 0-day attack

Medium

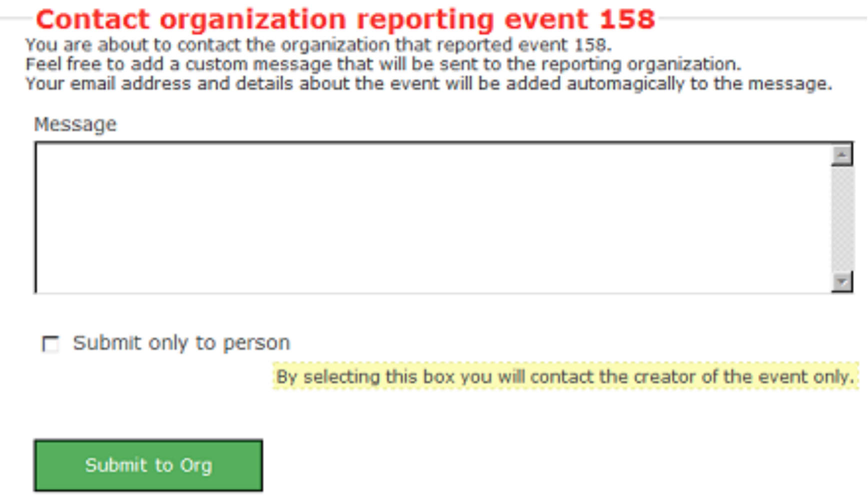
Distribution
Org

Info
TT14689: DOC File received by email

Contacting the publisher:

To get in touch with the reporter of a previously registered event, just find the event for which you would like to contact the reporter by either finding it on the list of events, by finding it through one of its attributes or by finding it through a related event.

Once the event is found and the event view opened, click the button titled "Contact Reporter". This will bring up a view where you can enter your message that is to be e-mailed to the reporting organisation or the reporter himself. Along with your message, the detailed information about the event in question will be included in the e-mail.



Contact organization reporting event 158

You are about to contact the organization that reported event 158.
Feel free to add a custom message that will be sent to the reporting organization.
Your email address and details about the event will be added automagically to the message.

Message

□ Submit only to person

By selecting this box you will contact the creator of the event only.

By default, the message will be sent to every member of the organisation that posted the event in the first place, but if you tick the check-box below the message field before sending the mail, only the person that reported the event will get e-mailed.

Exporting data:

It is possible to quickly and conveniently export the data contained within the system using the export features located in the main menu on the left. There are various sets of data that can be exported, by using the authentication key provided by the system (also shown on the export page). If for whatever reason you would need to invalidate your current key and get a new one instead (for example due to the old one becoming compromise) just hit the reset link next to the authentication key in the export view or in your "my profile" view.

The following types of export are possible:

XML export:

Exports all attributes and the event data of every single event in the database in the XML format. The usage is:

<server>/events/xml/<authentication_key>

In order to export the data about a single event and its attributes, use the following syntax:

<server>/events/xml/<authentication_key>/<EventID>

NIDS export:

This allows the user to export all network related attributes under the Snort format. The attributes have to belong to a published event and they have to have IDS signature generation enabled. The types that will be used when creating the export are: email-dst, ip-src, ip-dst, snort, url, domain. The usage is as follows:

<server>/events/nids/<authentication_key>

Hash database export:

There are two hash formats (sha1 and md5) in which all filenames stored in the system can be exported. Events need to be published and the IDS Signature field needs to be turned on for this export. The usage is as follows:

For MD5: *<server>events/hids_md5/<authentication_key>*

For SHA1: *<server>events/hids_sha1/<authentication_key>*

Text export:

It is also possible to export a list of all attributes that match a specific type into a plain text file. The format to do this is:

<server>/events/text/<authentication_key>/<type>

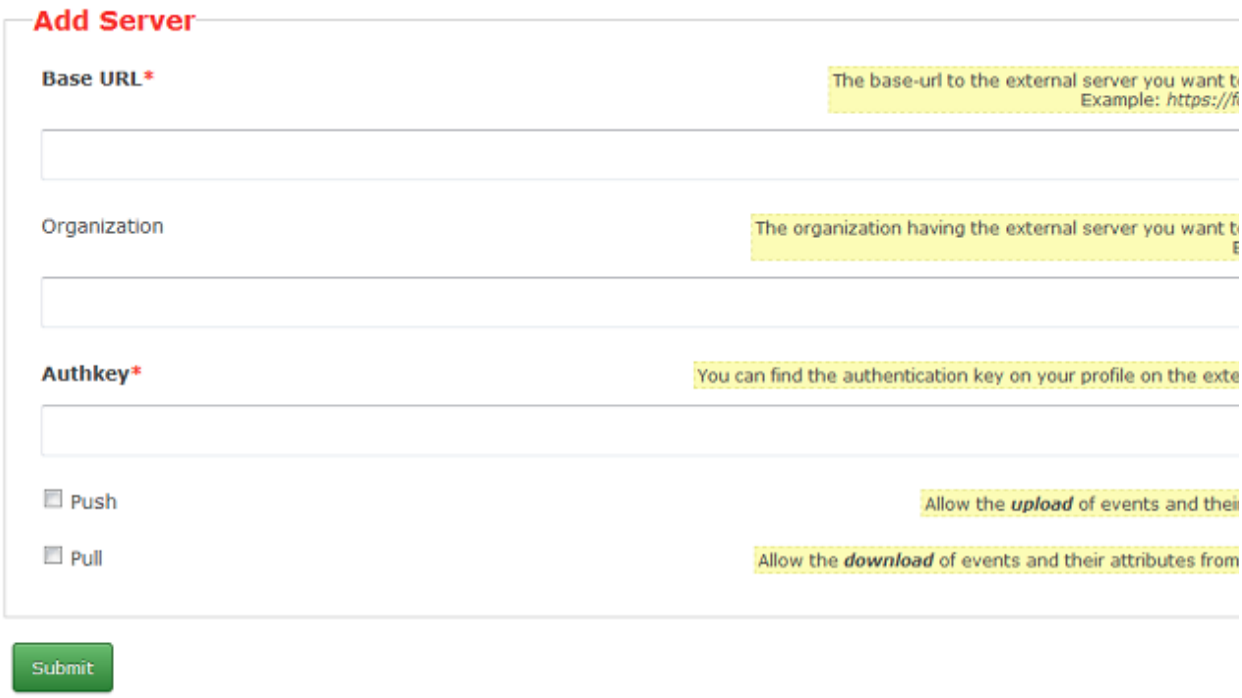
Type could be any valid type (as according to section 10), for example md5, ip-src or comment.

Connecting to other servers:

Apart from being a self contained repository of attacks/malware, one of the main features of MISP is its ability to connect to other instances of the server and share (parts of) its information. The following options allow you to set up and maintain such connections.

Setting up a connection to another server:

In order to share data with a remote server via pushes and pulls, you need to create an account on the remote server, note down the authentication key and use that to add the server on the home server. When clicking on List Servers and then on New Server, a form comes up that needs to be filled out in order for your server to connect to it. The following fields need to be filled out:



Add Server

Base URL* — The base-url to the external server you want t
Example: *https://f*

Organization — The organization having the external server you want t
E

Authkey* — You can find the authentication key on your profile on the exte

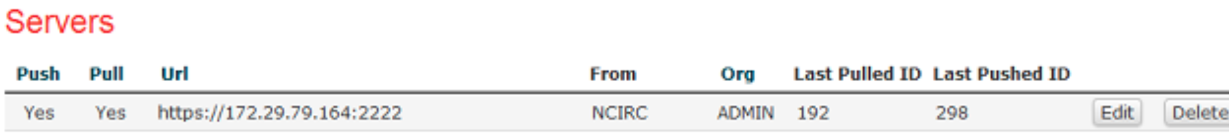
□ Push — Allow the ***upload*** of events and thei

□ Pull — Allow the ***download*** of events and their attributes from

- ***Base URL:*** The URL of the remote server.
- ***Organization:*** The organisation that runs the remote server.
- ***Authkey:*** The authentication key that you have received on the remote server.
- ***Push:*** This check-box controls whether your server is allowed to push to the remote server.
- ***Pull:*** This check-box controls whether your server can request to pull all data from the request server.

Browsing the currently set up server connections and interacting with them:

If you ever need to change the data about the linked servers or remove any connections, you have the following options to view and manipulate the server connections, when clicking on List Servers: (you will be able to see a list of all servers that your server connects to, including the base address, the organisation running the server the last pushed and pulled event IDs and the control buttons.).



Servers

Push	Pull	Url	From	Org	Last Pulled ID	Last Pushed ID		
Yes	Yes	https://172.29.79.164:2222	NCIRC	ADMIN	192	298	Edit	Delete

- ***Editing the server data:*** By clicking edit a view, that is identical to the new server view, is loaded, with all the current information on the server pre-entered.
- ***Deleting the server:*** Clicking the delete button will delete the link to your server.
- ***Push all:*** By clicking this button, all events that are eligible to be pushed on your server will start to be pushed to the remote server.
- ***Pull all:*** By clicking this button, all events that are set to be pull-able or full access on the remote server will be copied to your server.

Rest API:

The platform is also RESTfull, so this means you can use structured format (XML) to access

Events data.

Requests

Use any HTTP compliant library to perform requests. However to make clear you are doing a REST request you need to either specify the Accept type to application/xml, or append .xml to the ur

The following table shows the relation of the request type and the resulting action:

HTTP format	URL	Controller action invoked
GET	/events	EventsController::index() (1)
GET	/events/123	EventsController::view(123) (2)
POST	/events	EventsController::add()
PUT	/events/123	EventsController::edit(123)
DELETE	/events/123	EventsController::delete(123)
POST	/events/123	EventsController::edit(123)

(1) Warning, there's a limit on the number of results when you call `index`.
(2) Attachments are included using base64 encoding below the `data` tag.

Authentication

REST being stateless you need to authenticate your request by using your **authkey/apikey**. Simply set the `Authorization` HTTP header.

Example - Get single Event

In this example we fetch the details of a single Event (and thus also his Attributes).
The request should be:

```
GET http://localhost:8888/events/123
```

And with the HTTP Headers:

```
Accept: application/xml
Authorization: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

The response you're going to get is the following data:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<response>
        <Event>
                <id>57</id>
                <date>2012-11-19</date>
                <risk>Undefined</risk>
                <info>Test</info>
                <user_id>1</user_id>
                <published>0</published>
                <uuid>50aa54aa-f7a0-4d74-910d-10f0ff32448e</uuid>
                <revision>0</revision>
                <private>0</private>
                <attribute_count>0</attribute_count>
                <communitie>0</communitie>
                <distribution>This Community-only</distribution>
                <Attribute>
                        <id>9577</id>
                        <event_id>123</event_id>
                        <category>Artifacts dropped</category>
                        <type>other</type>
                        <to_ids>1</to_ids>
                        <uuid>50aa54bd-adec-4544-b494-10f0ff32448e</uuid>
                        <revision>1</revision>
                        <private>0</private>
                        <cluster>0</cluster>
                        <communitie>0</communitie>
                        <value>0</value>
                        <distribution>0</distribution>
                </Attribute>
        </Event>
</response>
```

Example - Add new Event

In this example we want to add a single Event.
The request should be:

```
POST http://localhost:8888/events
Accept: application/xml
Authorization: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

And the request body:

```
<Event>
        <id>14</id>
        <org>ORG</org>
        <date>2012-11-26</date>
        <risk>Undefined</risk>
        <info>Event information</info>
        <user_id>1</user_id>
        <alerted>0</alerted>
        <uuid>4f8c2c4e-00dc-42c9-83ad-76e9ff32448e</uuid>
        <private>0</private>
        <published>0</published>
        <Attribute>
                <id>116</id>
                <event_id>14</event_id>
                <type>ip-dst</type>
                <category>Network activity</category>
                <to_ids>1</to_ids>
                <uuid>4f8c2cc3-0410-4bf0-8559-5b9dff32448e</uuid>
                <revision>1</revision>
                <private>0</private>
                <value>1.1.1.111</value>
                <category_order>g</category_order>
        </Attribute>
        <Attribute>
                <id>117</id>
                <event_id>14</event_id>
                <type>malware-sample</type>
                <category>Payload delivery</category>
                <to_ids>0</to_ids>
                <uuid>4f8c2d08-7e6c-4648-8730-50a7ff32448e</uuid>
                <revision>1</revision>
                <private>0</private>
                <value>.doc|3f6f1aaab6171925c81de9b34a8fcf8e</value>
                <category_order>c</category_order>
                <data />
        </Attribute>
</Event>
```

The response you're going to get is the following data:

```
HTTP/1.1 100 Continue
HTTP/1.1 200 Continue
Date: Mon, 26 Nov 2012 14:17:11 GMT
Server: Apache/2.2.13 (Win32) PHP/5.2.10
X-Powered-By: PHP/5.2.10
Set-Cookie: CAKEPHP=deleted; expires=Sun, 27-Nov-2012 14:17:11 GMT; path=/
Set-Cookie: CAKEPHP=a4ok3lr5p9n5drqj27025i41e3; expires Mon, 26-Nov-2012 18:17:11 GMT; path=/; HttpOnly
Content-Length: 1466
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8">
<response>
        <Event>
                <id>14</id>
                <org>ORG</org>
                <date>2012-11-26</date>
                <risk>Undefined</risk>
                <info>Event information</info>
                <user_id>1</user_id>
                <published>0</published>
                <uuid>4f8c2c4e-00dc-42c9-83ad-76e9ff32448e</uuid>
                <revision>0</revision>
                <private>0</private>
                <attribute_count>0</attribute_count>
                <communitie>0</communitie>
                <distribution>All communities</distribution>
                <Attribute>
                        <id>116</id>
                        <event_id>14</event_id>
                        <category>Network activity</category>
                        <type>ip-dst</type>
                        <to_ids>1</to_ids>
                        <uuid>4f8c2cc3-0410-4bf0-8559-5b9dff32448e</uuid>
                        <revision>1</revision>
                        <private>0</private>
                        <cluster>0</cluster>
                        <communitie>0</communitie>
                        <value>1.1.1.111</value>
                        <distribution>All communities</distribution>
                        <category_order>g</category_order>
                </Attribute>
                <Attribute>
                        <id>117</id>
                        <event_id>14</event_id>
                        <category>Payload delivery</category>
                        <type>malware-sample</type>
                        <to_ids>0</to_ids>
                        <uuid>4f8c2d08-7e6c-4648-8730-50a7ff32448e</uuid>
                        <revision>1</revision>
                        <private>0</private>
                        <cluster>0</cluster>
                        <communitie>0</communitie
                        <value>.doc|3f6f1aaab6171925c81de9b34a8fcf8e</value>
                        <distribution>All communities</distribution>
                        <category_order>c</category_order>
                </Attribute>
        </Event>
</response>
```

The respone from requesting an invalid page

```
<?xml version = "1.0" encoding = "UTF-8"?>
<response>
        <name>Not Found</name>
        <url>/Waldo/</url>
</response>
```