

# Collecting and analysing OSINT into MISP threat intelligence platform.

Collecting and analysing OSINT into MISP threat intelligence platform. ....	1
1. Cross-checking if the OSINT is already known .....	2
1.1. Search in public indexer if already reported in other blog posts, reports or any public sources. ....	3
2. Cross-checking if the OSINT already exists in one or more MISP communities (public or private) .....	3
2.1. If not create a new MISP event .....	3
2.2. If some events already exist and require an update, then make a MISP proposal. ....	3
3. Create one or more MISP events.....	3
3.1. Set a meaningful event info .....	4
3.2. Set a date in accordance with the event.....	5
3.3. Tag and classify information at event level (default tagging for the whole event) .....	5
3.4. Add attributes related to the OSINT source .....	5
3.4.1. Add "External analysis"/link to the original source.....	6
3.4.2. Add "External analysis"/text to the event .....	7
3.4.3. Classify and tags the OSINT source (with at least the osint namespace) .....	7
3.5. Add one or more galaxy/cluster to the event .....	8
3.5.1. If there is no related galaxy/cluster/value, add a new one. ....	9
3.6. Add attributes related to the indicators mentioned in the OSINT document.....	9
3.6.1. If there is any files mentioned in the OSINT information, add corresponding file object(s). ....	10
3.7. Add attributes related to the target groups mentioned in the OSINT document.....	10
3.7.1. If there is any target groups, pick the right attribute types in the "Targeting data" category. ....	10
3.8. Add and attach evidences.....	11
3.8.1. Evidence like screenshot or static report .....	11
3.8.2. Evidence like malicious sample files or malware .....	12
4. Update an existing MISP galaxy cluster .....	12
4.1. Adding a new value to an existing cluster (or fix an existing one).....	12
4.1.1. Open an issue.....	13
4.1.2. Update the JSON of the cluster and create a pull-request.....	13
5. Update an existing MISP taxonomy .....	13
5.1. Adding a new value to an existing taxonomy (or fix an existing one) .....	13
5.1.1. Open an issue.....	13
5.1.2. Update the JSON and create a pull-request.....	13




## Collecting and analysing OSINT into MISP threat intelligence platform.


Cross-checking if the OSINT is already known

Cross-checking if the OSINT already exists in one or more MISP communities (public or private)

Create one or more MISP events

 A MISP event is usually a semantic bundle of information...

Update an existing MISP galaxy cluster

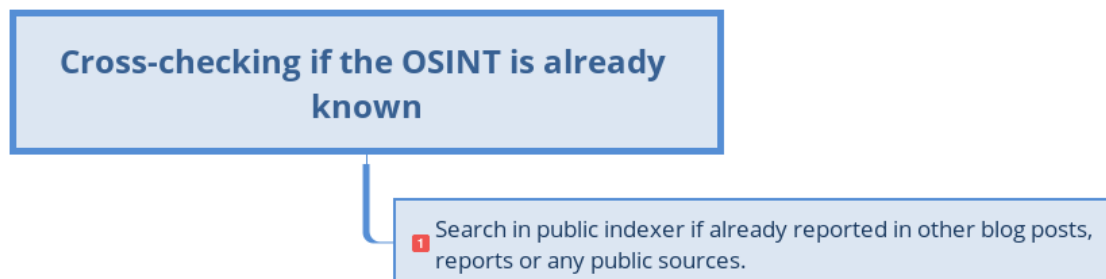
 <https://www.misp-project.org/galaxy.html>

Update an existing MISP taxonomy

 <https://www.misp-project.org/taxonomies.html>



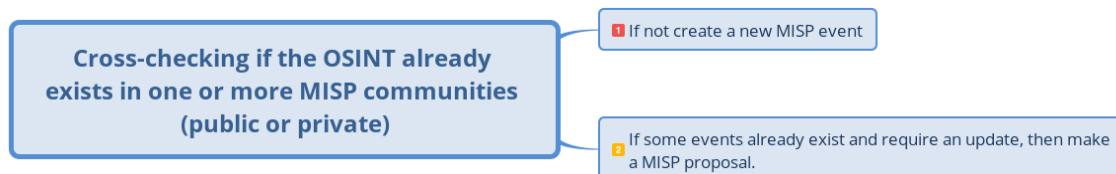
### 1. Cross-checking if the OSINT is already known



**1.1. Search in public indexer if already reported in other blog posts, reports or any public sources.**

**1**

## **2. Cross-checking if the OSINT already exists in one or more MISP communities (public or private)**



**2.1. If not create a new MISP event**

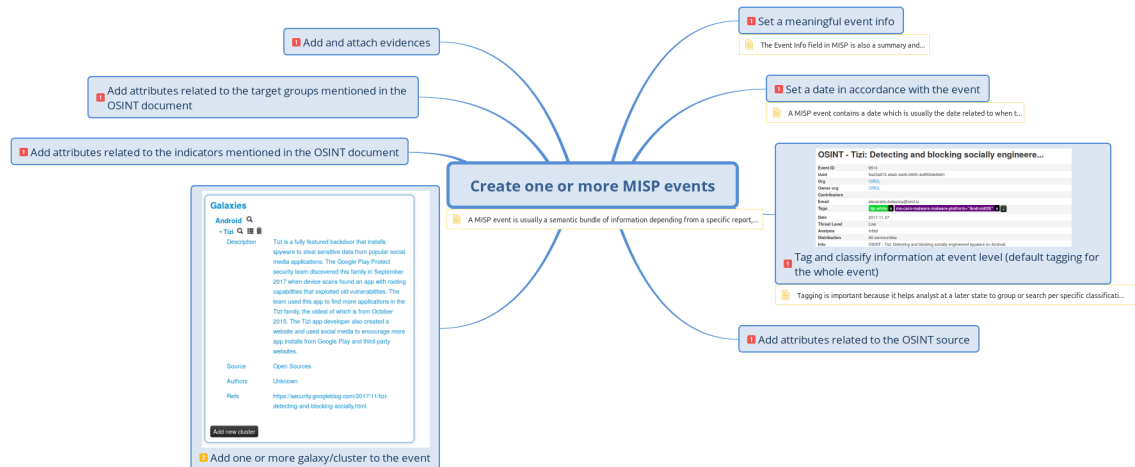
**1**

**See Also:** [Create one or more MISP events](#)

**2.2. If some events already exist and require an update, then make a MISP proposal.**

**2**

## **3. Create one or more MISP events**



**See Also:** [If not create a new MISP event](#)

A MISP event is usually a semantic bundle of information depending from a specific report, event, notes, blog posts or information.

As an example, the following blogpost can be considered as an event:

<https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html>

The above example will be used for the overall flow.

### 3.1. Set a meaningful event info

1

The Event Info field in MISP is also a summary and a title of the event. It's important to set a meaning and concise summary.

Based on the above example, the title of the blog post:

Tizi: Detecting and blocking socially engineered spyware on Android

It's meaningful and concise. Some analysts like to prefix immediately in the title that the information is OSINT and do the following title:

OSINT - Tizi: Detecting and blocking socially engineered spyware on Android

### 3.2. Set a date in accordance with the event

1

A MISP event contains a date which is usually the date related to when the activity happens or detected. It's often easier and clearer to set the publishing date of the OSINT information even if the event happened in the past.

For the above case, the date is  
November 27, 2017 as this is the date mentioned in the blog post.

### 3.3. Tag and classify information at event level (default tagging for the whole event)

1

#### OSINT - Tizi: Detecting and blocking socially engineere...

Event ID	9513
Uuid	5a23a972-e6a0-4a05-b505-4e8f02de0b81
Org	<a href="#">CIRCL</a>
Owner org	<a href="#">CIRCL</a>
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	<span>tlp:white</span> <span>x</span> <span>ms-caro-malware:malware-platform="AndroidOS"</span> <span>x</span> <span>+</span>
Date	2017-11-27
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	OSINT - Tizi: Detecting and blocking socially engineered spyware on Android

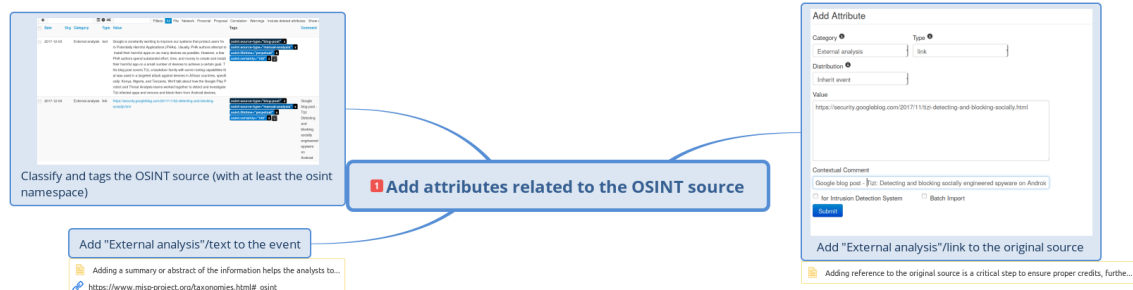
Tagging is important because it helps analyst at a later state to group or search per specific classification or categories.

We strongly recommend to tag as tlp:white classification for information collected from OSINT source and especially add a distribution to "All communities". This allows everyone to get your structured information via MISP sharing. And especially to benefit from correction, improvement or updates from other analysts.

If you create or share your event in MISP CIRCL communities, feel free to add circl:osint-feed to add your event in the default OSINT export available in default MISP installation. This allows a larger diffusion of your work within MISP communities.

### 3.4. Add attributes related to the OSINT source

1



### 3.4.1. Add "External analysis"/link to the original source

#### Add Attribute

Category ⓘ

External analysis

Type ⓘ

link

Distribution ⓘ

Inherit event

Value

https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html

Contextual Comment

Google blog post - Tizi: Detecting and blocking socially engineered spyware on Android

☐ for Intrusion Detection System
 ☐ Batch Import

Submit

Adding reference to the original source is a critical step to ensure proper credits, further analysis or set a confidence/credibility level of the OSINT source.

An additional benefit of adding a source is the ability to track existing one with the built-in correlation in MISP.

### 3.4.2. Add "External analysis"/text to the event

Adding a summary or abstract of the information helps the analysts to find back later information without the need to check external resources.

### 3.4.3. Classify and tags the OSINT source (with at least the osint namespace)



+

Filters:

All

File

Network

Financial

Proposal

Correlation

Warnings

Include deleted attributes

Show c

Date

Org

Category

Type

Value

Tags

Comment

2017-12-03

External analysis

text

Google is constantly working to improve our systems that protect users from Potentially Harmful Applications (PHAs). Usually, PHA authors attempt to install their harmful apps on as many devices as possible. However, a few PHA authors spend substantial effort, time, and money to create and install their harmful app on a small number of devices to achieve a certain goal. This blog post covers Tizi, a backdoor family with some rooting capabilities that was used in a targeted attack against devices in African countries, specifically: Kenya, Nigeria, and Tanzania. We'll talk about how the Google Play Protect and Threat Analysis teams worked together to detect and investigate Tizi-infected apps and remove and block them from Android devices.

osint:source-type="blog-post" x

osint:source-type="manual-analysis" x

osint:lifetime="perpetual" x

osint:certainty="100" x

+

2017-12-03

External analysis

link

<https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html>

osint:source-type="blog-post" x

osint:source-type="manual-analysis" x

osint:lifetime="perpetual" x

osint:certainty="100" x

+

Google blog post - Tizi: Detecting and blocking socially engineered spyware on Android

If there is a missing value in an existing taxonomy or a new one have to be created.

2

See Also: [Update an existing MISP taxonomy](#)

### 3.5. Add one or more galaxy/cluster to the event

2

Galaxies

Android

-Tizi

Description

Tizi is a fully featured backdoor that installs spyware to steal sensitive data from popular social media applications. The Google Play Protect security team discovered this family in September 2017 when device scans found an app with rooting capabilities that exploited old vulnerabilities. The team used this app to find more applications in the Tizi family, the oldest of which is from October 2015. The Tizi app developer also created a website and used social media to encourage more app installs from Google Play and third-party websites.

Source

Open Sources

Authors

Unknown

Refs

<https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html>

Add new cluster

2 If there is no related galaxy/cluster/value, add a new one.

2 Add one or more galaxy/cluster to the event

8



## Galaxies

Android

- Tizi

Description

Tizi is a fully featured backdoor that installs spyware to steal sensitive data from popular social media applications. The Google Play Protect security team discovered this family in September 2017 when device scans found an app with rooting capabilities that exploited old vulnerabilities. The team used this app to find more applications in the Tizi family, the oldest of which is from October 2015. The Tizi app developer also created a website and used social media to encourage more app installs from Google Play and third-party websites.

Source

Open Sources

Authors

Unknown

Refs

<https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html>

Add new cluster

**3.5.1. If there is no related galaxy/cluster/value, add a new one.**

**2**

**See Also:** [Update an existing MISP galaxy cluster](#)

**3.6. Add attributes related to the indicators mentioned in the OSINT document**

**1**

1 Add attributes related to the indicators mentioned in the OSINT document

1 If there is any files mentioned in the OSINT information, add corresponding file object(s).

### 3.6.1. If there is any files mentioned in the OSINT information, add corresponding file object(s).

1

#### Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

Name	file
Meta-category	file
Distribution	Inherit event
Comment	

Attribute	Category	Type	Value	To IDS	Comment	UUID	Distribution
filename	Payload delivery	filename	com.press.nasa.com.tanofresh	Yes		5a23d49c-7248-4a34-8ed5-420402de0b81	Inherit event
sha256	Payload delivery	sha256	4d780a6fc18458311250d4d1edc750468fdb9b3e4c950dce5b35d4567b47d4a7	Yes		5a23d49c-a5fc-4147-b92e-4d8502de0b81	Inherit event
certificate	Payload delivery	x509-fingerprint-sha1	816bbe3cab5eed00b8bd16df56032a96e243201	Yes		5a23d49c-28a8-4e89-81e5-456702de0b81	Inherit event
state	Other	text	Malicious	No		5a23d49c-8bd4-42ea-ab63-478402de0b81	Inherit event

Submit Cancel

### 3.7. Add attributes related to the target groups mentioned in the OSINT document

1

1 Add attributes related to the target groups mentioned in the OSINT document

Add Attribute

Category
Targeting data
Type
target-location
Distribution
Inherit event
Value
Kenya  
Nigeria  
Tanzania
Contextual Comment
for Intrusion Detection System
Batch Import
Warning: You are about to share data that is of a classified nature. Make sure that you are authorized to share this.
Submit

1 If there is any target groups, pick the right attribute types in the "Targeting data" category.

### 3.7.1. If there is any target groups, pick the right attribute types in the "Targeting data" category.

1

## Add Attribute

Category ⓘ      Type ⓘ

Targeting data      target-location

Distribution ⓘ

Inherit event

Value

Kenya  
Nigeria  
Tanzania

Contextual Comment

☐ for Intrusion Detection System      ☒ Batch Import

**Warning: You are about to share data that is of a classified nature. Make sure that you are authorised to share this.**

Submit

### 3.8. Add and attach evidences

**1**

**1** Add and attach evidences

**1** Evidence like malicious sample files or malware

Add attachment in MISP allows to include malicious or non-malicious file to the pl...

**Add Attachment**

Category ⓘ

Payload delivery

Distribution ⓘ

Inherit event

Contextual Comment

Here is an example social media post promoting a T22-infected app

Browse... ts21.png

☐ IDS (encrypt and hash)

☐ Advanced extraction (if installed)

Upload

**1** Evidence like screenshot or static report

#### 3.8.1. Evidence like screenshot or static report

**1**

## Add Attachment

Category <sup>i</sup>

Payload delivery

Distribution <sup>i</sup>

Inherit event

Contextual Comment

Here is an example social media post promoting a Tizi-infected app

Browse... tizi1.png

☐ IDS (encrypt and hash)

☐ Advanced extraction (if installed)

Upload

### 3.8.2. Evidence like malicious sample files or malware

1

Add attachment in MISP allows to include malicious or non-malicious file to the platform. The difference is a matter of flag "IDS (encrypt and hash" where the evidence will be encrypted with a default password "infected" to avoid any human-error to execute malicious binaries.

## 4. Update an existing MISP galaxy cluster



**See Also:** [If there is no related galaxy/cluster/value, add a new one.](#)

### 4.1. Adding a new value to an existing cluster (or fix an existing one)

2



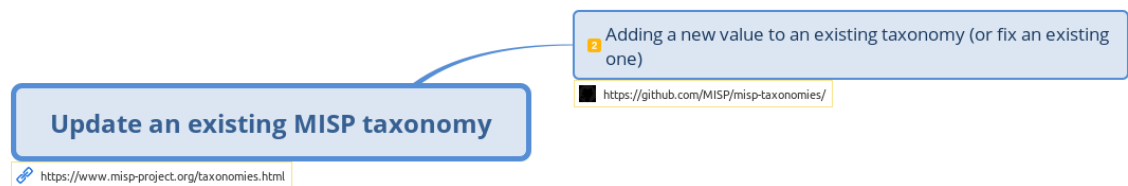
#### 4.1.1. [Open an issue](#)

3

#### 4.1.2. Update the JSON of the cluster and create a pull-request

2

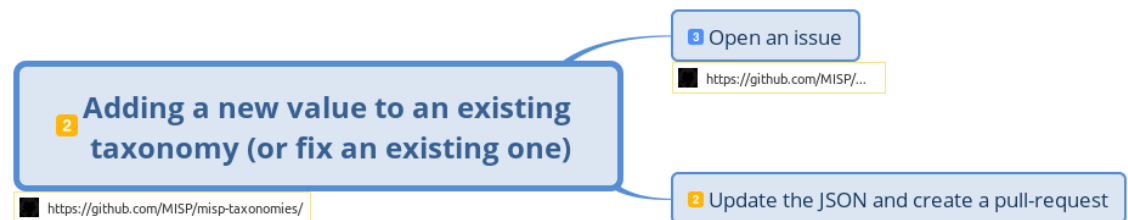
### 5. [Update an existing MISP taxonomy](#)



**See Also:** [If there is a missing value in an existing taxonomy or a new one have to be created.](#)

#### 5.1. [Adding a new value to an existing taxonomy \(or fix an existing one\)](#)

2



#### 5.1.1. [Open an issue](#)

3

#### 5.1.2. Update the JSON and create a pull-request

2