



**THREAT
FABRIC**

Unweaving threats

MTI & ThreatConnect Feed User Guide



ThreatFabric B.V.

Naritaweg 132
1043 CA Amsterdam

E-mail: info@threatfabric.com

Web: www.threatfabric.com

The information in this document, including possible attachment(s), is confidential and solely intended for the addressee. Publication, multiplication, distribution, use, or viewing of this document is only permitted if the addressee explicitly granted permission to do so. ThreatFabric and ThreatFabric's logos are trademarks of ThreatFabric B.V. The trademarks, names, and illustrations of other organizations and products are the property of their respective owners. © ThreatFabric B.V.

Reviews

Date	Version	Description
June 24, 2020	v1	Initial release

About this document

This document is intended for ThreatFabric prospects, customers and registered partners, the content of the document is meant for use of such parties only. This document is strictly private and personal to its recipient(s) and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party. Shall information be lacking, or should you need additional details, please refer to your ThreatFabric contact point.

Table of Contents

REVIEWS	3
ABOUT THIS DOCUMENT.....	3
1. INTRODUCTION.....	5
2. DATA STRUCTURE AND CONTENT	6
2.1 STRUCTURE	6
2.2 CONTENT.....	7
3. CONFIGURATION	8
3.1 REQUIREMENTS.....	8
3.2 INSTALLATION	8
3.3 ATTRIBUTES CONFIGURATION	8
3.4 THREATCONNECT JOB CONFIGURATION.....	10
3.5 INDICATOR DEPRECATION CONFIGURATION	13
4. USING THE THREATFABRIC MTI DATA.....	14
4.1 FINDING CAMPAIGNS TARGETING YOUR MOBILE APPS	14
4.2 ACCESSING MALWARE INFORMATION RELATING TO A CAMPAIGN	15
4.3 ACCESSING C2 INFORMATION RELATING TO A CAMPAIGN	16
5. CONTACT AND SUPPORT	18
5.1 THREATFABRIC.....	18

1. Introduction

MTI, shortened for Mobile Threat Intelligence, is the Cyber Threat Intelligence solution provided by ThreatFabric. By subscribing to the MTI solution, you benefit from ThreatFabric's expertise and visibility on the mobile threat landscape. This expertise is paired with the analysis and classification solution built and used by the ThreatFabric analysts to track distribution campaigns, birth and evolution of each malware family and its variants.

By making use of ThreatFabric MTI, depending on the bundle you purchased, you can access the MTI portal. Through the MTI portal, you can access all tactical and operational intelligence related to the malware campaigns tracked by ThreatFabric, access the overview of activity on the threat landscape and details of the specific malware families and variants, submit malware samples for analysis and request help for investigations from the ThreatFabric experts.

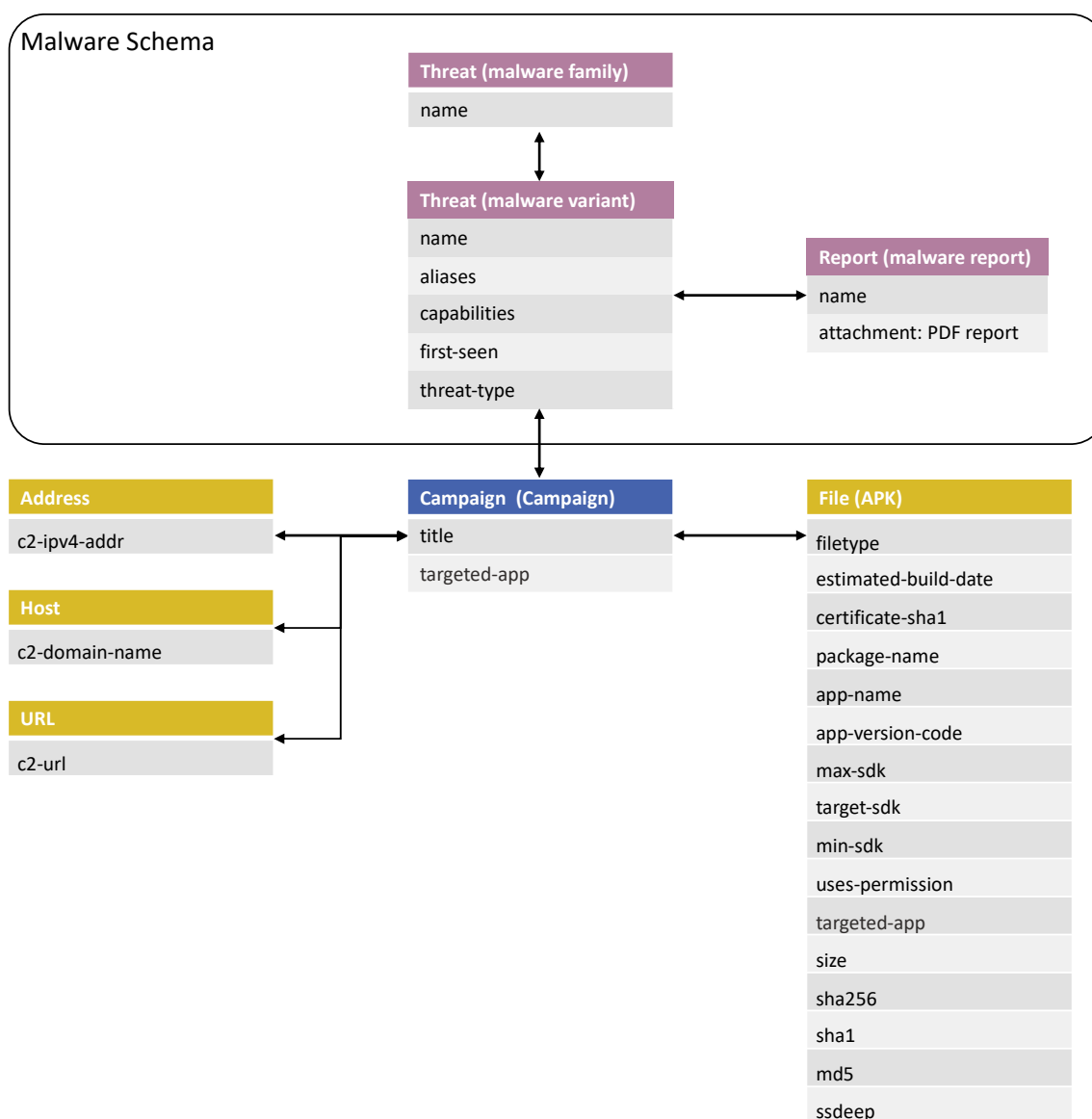
In order to simplify ingestion, correlation and consumption of the threat intelligence, MTI is available for ThreatConnect users that subscribed to the ThreatFabric MTI service, through the integration described in this document.

2. Data structure and content

2.1 Structure

The MTI feed includes both the operational data and technical indicators resulting from the malware analysis as well as the strategic threat reports about the malware families tracked by the ThreatFabric team.

The schema below shows the data structure as made available through the integration. The “Malware Schema” is composed of 2 “Threat” elements, respectively (i) the malware family and (ii) the malware variant. The malware variant contains all the details about the observed version of the malware, including a link to the relevant malware report (when available). Those elements are linked to a campaign object which, in its turn, makes the link between (i) the malware samples (payloads) observed in this campaign and (ii) information about the command and control infrastructure used by threat actors to control the malware on the infected devices.



2.2 Content

The fields used in the feed and their general structure are listed in the table below:

Field name	Format	Description
Threat: malware family		
Name	Text	The name of the malware
Type	Text	Information about what the malware type
Title	Text	The name of the specific malware instance
Threat: malware variant		
Name	Text	The name of the malware
Aliases	Text	The other names used to identify this variant
Capabilities	Text	The list of capabilities of this malware variant
First-seen	Date	The date at which this variant was first seen
Threat-type	Text	The type of malware
Report: Malware report		
Name	Text	The name of the specific malware report
Attachment	File	The malware report as a PDF file
File: APK_file		
filetype	Text	The type of file the indicators relate to
estimated-build-date	Date	Date in milliseconds at which the file was built
certificate-sha1	Hash	SHA-1 hash of the certificate signing the file
package-name	Text	Android package name given to the App
app-name	Text	Human friendly name given to the App
app-version-code	Number	Version code given to this specific App
max-sdk	Number	Newest Android SDK version App is made for
target-sdk	Number	Exact Android SDK version App is made for
min-sdk	Number	Oldest Android SDK version App is made for
uses-permission	Text	The permission(s) required by the App
component	Text	Specific components required by the App
Size_In_Bytes	Number	Size of the APK file (in bytes)
Magic_Number	Number	Constant numeric value to identify file format
SHA256	Hash	SHA-256 hash of the APK file
SHA1	Hash	SHA-1 hash of the APK file
MD5	Hash	MD5 hash of the APK file
SSDEEP	Hash	SSDEEP hash of the APK file
Address		
C2-ipv4-addr	IP	IPv4 address(es) of the C2 server
Host		
DomainName	Text	Domain name(s) of the C2 server
URL		
URL	Text	URL(s) of the C2 server
Campaign: Campaign		
Title	Text	Information on campaign and related malware
Targeted-app	Text	Android package name of the targeted App

3. Configuration

Following sections of the document contain all information on how to setup and configure the ThreatFabric MTI app to push the threat intelligence to the ThreatConnect Platform.

3.1 Requirements

In order to make use of the MTI app for ThreatConnect, you will need following:

- ThreatConnect paid subscription (you cannot use TCOpen)
- ThreatFabric MTI paid subscription
- At least one ThreatConnect API user
- ThreatFabric MTI API endpoint information and API key*
- ThreatFabric Custom Attributes (file)*

*This information can be retrieved from your account in the MTI portal. For additional assistance to access this information, you can also contact the ThreatFabric team as mentioned in the [Contact and support](#) section of this document.

3.2 Installation

In following steps, we consider that you have already downloaded the following files from the ThreatFabric MTI portal:

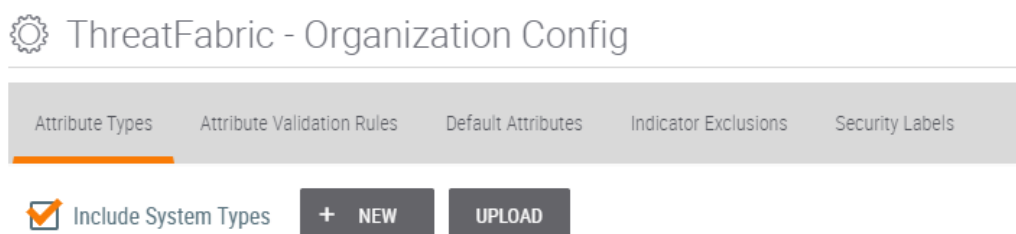
- ThreatFabric_-_Mobile_Threat_Intelligence_v1.tcx
- attributes.json

The steps required to install the app in your ThreatConnect instance are outlined in the ThreatConnect System Administration Guide (Install an App and Feed Deployer). Additionally, for more information you can contact your ThreatConnect Customer Success Engineer

3.3 Attributes configuration

Note: This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

In order to configure ThreatFabric custom attributes you need to access **Org Config > Attribute types** and click on the **Upload** button:



Once done, click the **Select File** button and upload the file “attributes.json” that you downloaded from the ThreatFabric MTI portal:

Upload Attributes

+ SELECT FILE

Upload any text file in the format:

Name, Description, Error Message, Length, Applicable Types

For example:

Report ID,My Report ID,Invalid report ID,50,Incident|Host|Url|Address
Report Type,My Report Type,Invalid Report Type,100,Incident|Document

Note that ',' is used as a column delimiter, but '|' is used to delimitate applicable types.

CANCEL

After clicking the **Save** button, the custom attributes will be configured for use with ThreatFabric's Mobile Threat Intelligence integration, as shown in following screenshot:

Upload Attributes

ThreatFabric Max SDK	Create
ThreatFabric Max SDK (Old)	Update
ThreatFabric Min SDK	Create
ThreatFabric Min SDK (Old)	Update
ThreatFabric Package Name	Create
ThreatFabric Package Name (Old)	Update
ThreatFabric Permission	Create
ThreatFabric Permission (Old)	Update
ThreatFabric Target SDK	Create
ThreatFabric Target SDK (Old)	Update
ThreatFabric Victim	Create
ThreatFabric Victim (Old)	Update

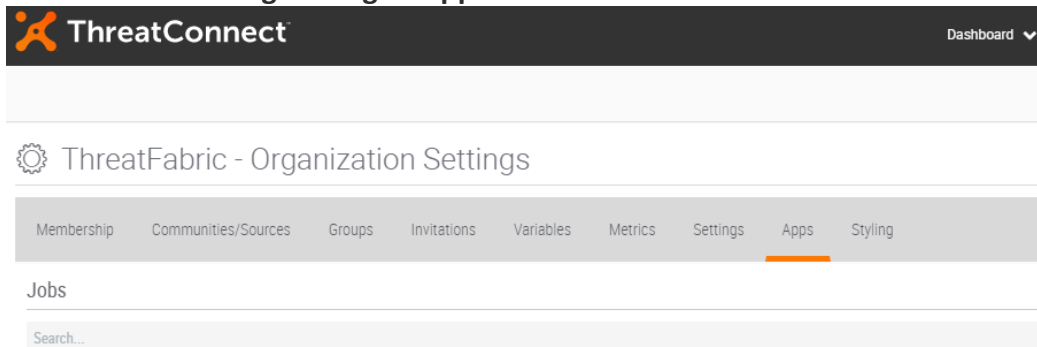
CANCEL

SAVE

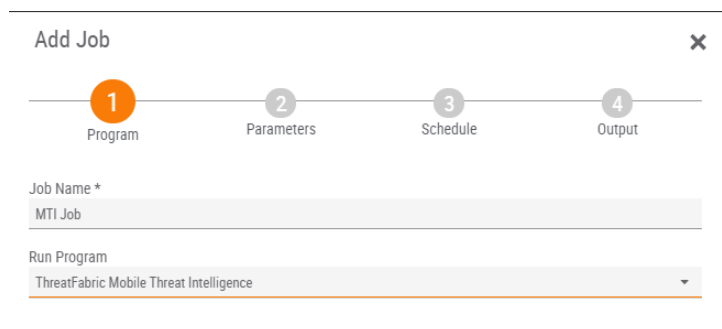
3.4 ThreatConnect Job configuration

Note: This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

You need to access the **Org Settings > Apps** and click on the **Add** button:



You then need to set the name of the job and select **“ThreatFabric Mobile Threat Intelligence”** as Run Program.



Configure the job using the ThreatFabric MTI API endpoint information and API key.

Note: the “last_run” parameter will be used as a starting date for which the threat intelligence feed will be ingested

Edit Job
×

1
Program
2
Parameters
3
Schedule
4
Output

ThreatConnect Owner *
ThreatFabric

Log Level *
info

ThreatFabric MTI API key *

ThreatFabric MTI API endpoint *
https://api.mti.threatfabric.net/

Threat Rating *
5

Last run
2020-06-24T13:16:05.965Z

You then need to configure the schedule for the job. We recommend using a frequency of “once every hour”.

Add Job
×

1
Program
2
Parameters
3
Schedule
4
Output

ⓘ Scheduled job timezone "GMT"

Schedule
Daily

At
17:21

Every
1 hour
hour between
5:00 PM
and
Midnight

As last step you can configure the job output if you wish to get notifications on the job.

Add Job
×

1
Program
2
Parameters
3
Schedule
4
Output

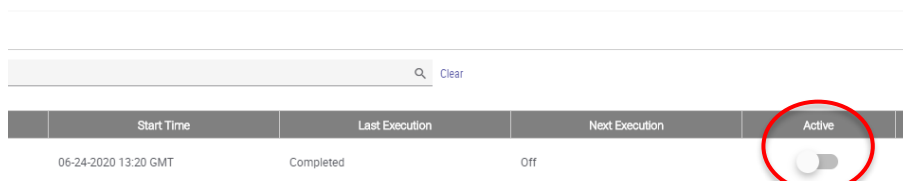
☐ Enable Notifications

Email Address

Notify on Job Result
☐ Success
☐ Partial Failure
☐ Failure

Attachments
☐ Include Log Files (1MB file size limit)

When done and having clicked on **Save**, the job to pull ThreatFabric's Mobile Threat Intelligence is setup, but not yet activated. To do so, you need to visualize the list of jobs and click on the **Active** button in order to activate the job.



The screenshot shows a web interface for managing jobs. At the top, there is a search bar with a magnifying glass icon and a 'Clear' button. Below the search bar is a table with the following columns: 'Start Time', 'Last Execution', 'Next Execution', and 'Active'. The 'Active' column contains a toggle switch. The first row of data shows a job with a start time of '06-24-2020 13:20 GMT', a last execution status of 'Completed', and a next execution status of 'Off'. The toggle switch in the 'Active' column is currently in the 'Off' position and is circled in red.

Start Time	Last Execution	Next Execution	Active
06-24-2020 13:20 GMT	Completed	Off	<input type="checkbox"/>

3.5 Indicator deprecation configuration

After some time, malware samples, command and control servers, or even threat actors, are no longer active. Therefore, related indicators previously ingested into the ThreatConnect Platform should also be deleted accordingly to avoid potential false positives. ThreatConnect provides the ability for users to configure an indicator deprecation policy to allow ThreatConnect indicators to drop in confidence rating if their confidence rating is not being maintained and updated. Once the indicator rating reaches a minimum value (i.e. 0%), it can either be set to inactive or be deleted.

To configure an indicator deprecation policy depending upon the type of your ThreatConnect instance, please refer to the detailed knowledge-base article from [ThreatConnect](#) (See section Configuring Indicator Confidence Deprecation for an Organization and Configuring Indicator Confidence Deprecation for a Community or Source)

The recommended indicator deprecation rule settings for ThreatFabric threat feed are as follows:

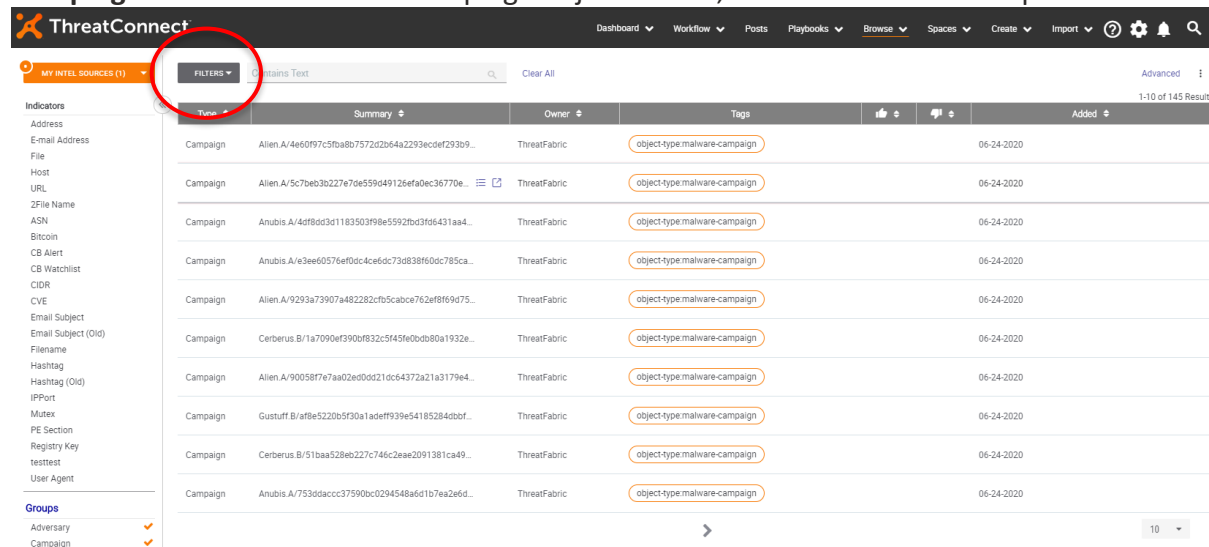
- Action at Minimum set to **Delete** so that indicators are deleted as soon as they reach minimum confidence
- **Percentage** checkbox checked which means that indicator confidence will be dropped as a percent of its previous value
- Confidence amount set to **1** so that 1% of an indicator's confidence is dropped
- Interval value set to **1 day** which is the period after which the confidence will be dropped
- Recurring checkbox also selected so that deprecation is performed on a recurring basis

In simple words the recommended deprecation rule can be stated as, "Each day, drop the confidence of each indicator by 1% of its previous value and when any indicator's confidence reaches the minimum value, delete it from ThreatConnect", therefore the indicators expire after approximatively 3 months (100 days).

4. Using the ThreatFabric MTI data

4.1 Find campaigns targeting your mobile apps

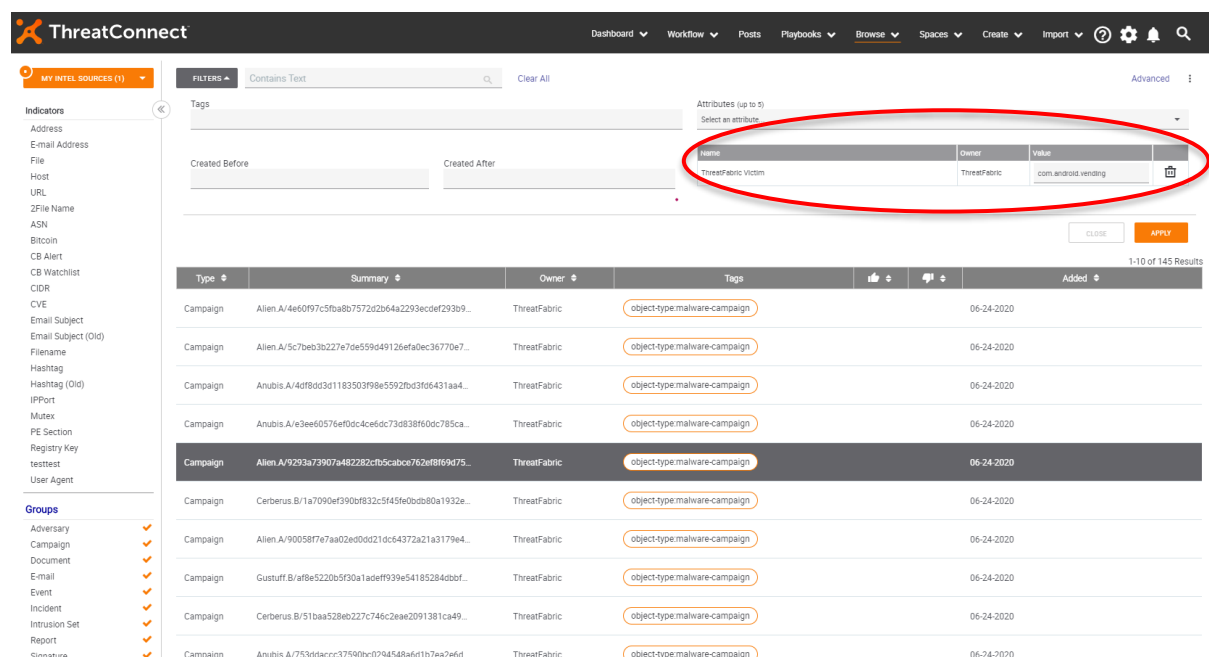
In order to find ThreatFabric's campaigns targeting your apps, proceed to **Browse > Groups > Campaign** to access the list of Campaign objects. Then, click on the **Filters** dropdown:



The screenshot shows the ThreatConnect interface with the 'Campaigns' list. The 'Filters' dropdown is circled in red. The list displays various campaign objects with columns for Type, Summary, Owner, Tags, and Added. The 'Tags' column shows 'object-type:malware-campaign' for all entries.

Type	Summary	Owner	Tags	Added
Campaign	Alien.A/4e60f97c5ba8b7572d2b64a2293ecdef293b9...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/5c7beb3b227e7de559d49126efa0ec36770e...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/4df8dd3d1183503f98e5592fbd3f06431aa4...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/e3ee60576ef0dc4e6dc73d838f0dc785ca...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/9293a73907a482282cf05cabce762ef8f9d75...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Cerberus.B/1a7090ef390bf832c545fe0b0db0a1932e...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/90058f7e7aa02e0dd21dc64372a21a3179e4...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Gustuff.B/af8e5220b5f30a1adeff939e54185284dbf...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Cerberus.B/51baa528eb227c746c2eae2091381ca49...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/753ddaccc37590bc0294548a6d1b7ea2e6d...	ThreatFabric	object-type:malware-campaign	06-24-2020

In the **Filters** area, select the **Attributes** dropdown and choose **ThreatFabric Victim**. Provide the package name of your application e.g. "com.android.vending" and click on **Apply**.



The screenshot shows the ThreatConnect interface with the 'Campaigns' list. The 'Attributes' dropdown is circled in red. The list displays various campaign objects with columns for Type, Summary, Owner, Tags, and Added. The 'Tags' column shows 'object-type:malware-campaign' for all entries.

Type	Summary	Owner	Tags	Added
Campaign	Alien.A/4e60f97c5ba8b7572d2b64a2293ecdef293b9...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/5c7beb3b227e7de559d49126efa0ec36770e...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/4df8dd3d1183503f98e5592fbd3f06431aa4...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/e3ee60576ef0dc4e6dc73d838f0dc785ca...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/9293a73907a482282cf05cabce762ef8f9d75...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Cerberus.B/1a7090ef390bf832c545fe0b0db0a1932e...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Alien.A/90058f7e7aa02e0dd21dc64372a21a3179e4...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Gustuff.B/af8e5220b5f30a1adeff939e54185284dbf...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Cerberus.B/51baa528eb227c746c2eae2091381ca49...	ThreatFabric	object-type:malware-campaign	06-24-2020
Campaign	Anubis.A/753ddaccc37590bc0294548a6d1b7ea2e6d...	ThreatFabric	object-type:malware-campaign	06-24-2020

Resulting list of Campaigns will contain only Campaigns that are targeting the application bearing the package name that you provided.

4.2 Access malware information relating to a campaign

In order to access ThreatFabric's malware report about the malware variant used in a specific campaign, click on the Campaign object. Such campaign can be found in **Browse > Groups > Campaign** or by identifying specific campaigns as explained in [Finding campaigns targeting your mobile apps](#).

Once the campaign object is opened, scroll down to the **Associated Intel** section. There, click on the **Threat** object, linked to the Campaign. You will then be redirected to the details page.

The screenshot shows the ThreatConnect interface. On the left, there's a sidebar with 'Indicators' and 'Groups'. The main area displays a list of campaigns. One campaign is selected, and its details are shown on the right. The 'Associated Intel' section is highlighted with a red circle, showing a list of intel items. The 'Threat' object is selected, and its details are shown on the right.

Type	Summary	Owner	Object Type
Campaign	Ginp.B/7d65fb36ff856ca7486b50597613d538025cf066edc268bae22bb569ecf87c72	ThreatFabric	object-type:malware
Campaign	Alien.A/50c13c0fba921c11343af5b662b0b6a6e009...	ThreatFabric	object-type:malware
Campaign	Ginp.B/a8472393685d7c02960593210349214f7ae99...	ThreatFabric	object-type:malware
Campaign	Alien.A/cc18463c3938c2dca82973ae3fc474f30104...	ThreatFabric	object-type:malware
Campaign	Ginp.B/9b4ccf2f71b02a44d77637682621b75e7b0d8...	ThreatFabric	object-type:malware
Campaign	Ginp.B/75548b4ca1254eb64302dfc2ce2d31d3070e2...	ThreatFabric	object-type:malware
Campaign	Ginp.B/cdf445039ebce221178f2339807ab065499a9e...	ThreatFabric	object-type:malware
Campaign	Ginp.B/d7fff5fcd0a190175ebfca128b27b02f6a4fbf28...	ThreatFabric	object-type:malware
Campaign	Alien.A/71eaf36f784b1ba99117d1703f026aa439e1...	ThreatFabric	object-type:malware
Campaign	Alien.A/e17a3b0883339807890fe345d1828c47f6ed...	ThreatFabric	object-type:malware

Type	Owner	Date Added
Threat	ThreatFabric	06-24-2020

Type	Owner	Date Added
Address	ThreatFabric	06-24-2020

If the malware report is available for the specific malware variant, you will be able to find it in the **Associated Groups** section:

The screenshot shows the ThreatConnect interface. The main area displays the details of a specific malware variant, 'Ginp.B'. The 'Associated Groups' section is highlighted with a red circle, showing a list of groups. The 'Report' object is selected, and its details are shown on the right.

Type	Owner	Date Added
Threat	ThreatFabric	06-24-2020
Report	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020

After accessing the Report's page, user will be able either to download the PDF file for the report or to view it in the platform:

The screenshot shows the ThreatConnect interface for a report named 'Ginp.B'. The 'Report File' section is highlighted with a red circle, showing the file 'Ginp.B.pdf' (PDF, 1.12 MB) with a 'Success' status and a 'Download' button. Other sections include 'Description', 'Source', 'Security Labels' (set to TLP:AMBER), 'Associations' (showing one associated group, 'Threat Ginp.B'), 'Details' (report type, added date, and publish date), and 'Tags' (with a tag 'object type: malware-report').

4.3 Access C2 information relating to a campaign

In order to access ThreatFabric's C2 information related to a specific campaign, click on the Campaign object. Such campaign can be found in **Browse > Groups > Campaign** or by identifying specific campaigns as explained in [Finding campaigns targeting your mobile apps](#). Once the campaign object is shown, scroll down to the **Associated Indicators** section. There, click on the **Threat** object linked to the Campaign. You will then be redirected to the details page.

The screenshot shows the ThreatConnect interface for a campaign object. The 'Associated Indicators' section is expanded, showing 11 indicators. The 'Description' section shows the ThreatFabric URL for the campaign. The 'Security Labels' section shows 'TLP:AMBER'. The 'Associations' section shows one associated group, 'Threat Ginp.B'.

Type	Owner	Threat Rating	Date Added
Address	ThreatFabric	5/5	06-24-2020
Host	ThreatFabric	5/5	06-24-2020
File	ThreatFabric	5/5	06-24-2020
URL	ThreatFabric	5/5	06-24-2020

In that section, the objects **Host**, **URL** and **Address** will provide you information about domain names, URLs and IP addresses used by the C2 of the specific campaign. By clicking on the specific value, you can access the information about the Indicator and get further details:

The screenshot displays the ThreatConnect interface for an indicator with the value 47.254.124.187. The top navigation bar includes the ThreatConnect logo and various menu items like Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, and a search icon. The main header shows the organization name 'ThreatFabric' and the indicator status 'Active' with a 'CAL Status Lock' option.

The left sidebar contains tabs for Overview, Tasks, Activity, Associations, and Spaces. The main content area is divided into two sections: Indicator Analytics and Associations.

Indicator Analytics

ThreatAssess

A gauge shows a rating of 384 Medium. A legend indicates that the rating is impacted by recent observations.

CAL™ Insights

Trends

Three line charts show Daily False Positives, Daily Impressions, and Daily Observations over a 30-day period. The x-axis is labeled with 7 days and 30 days.

Classification

Classifiers

A button labeled 'DNSHosts.HistoricalResolutions' is visible.

False Positives

False Positives (All Time) 0
False Positives (Previous 7 Days) 0

Associations

Graph Table

Associated Groups (15)

Type	Owner	Date Added
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020
Campaign	ThreatFabric	06-24-2020

1-10 of 15 Results

5. Contact and support

5.1 ThreatFabric

You can get support about ThreatFabric Mobile Threat Intelligence related topics by contacting the MTI team at: mti@threatfabric.com.