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

# 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.

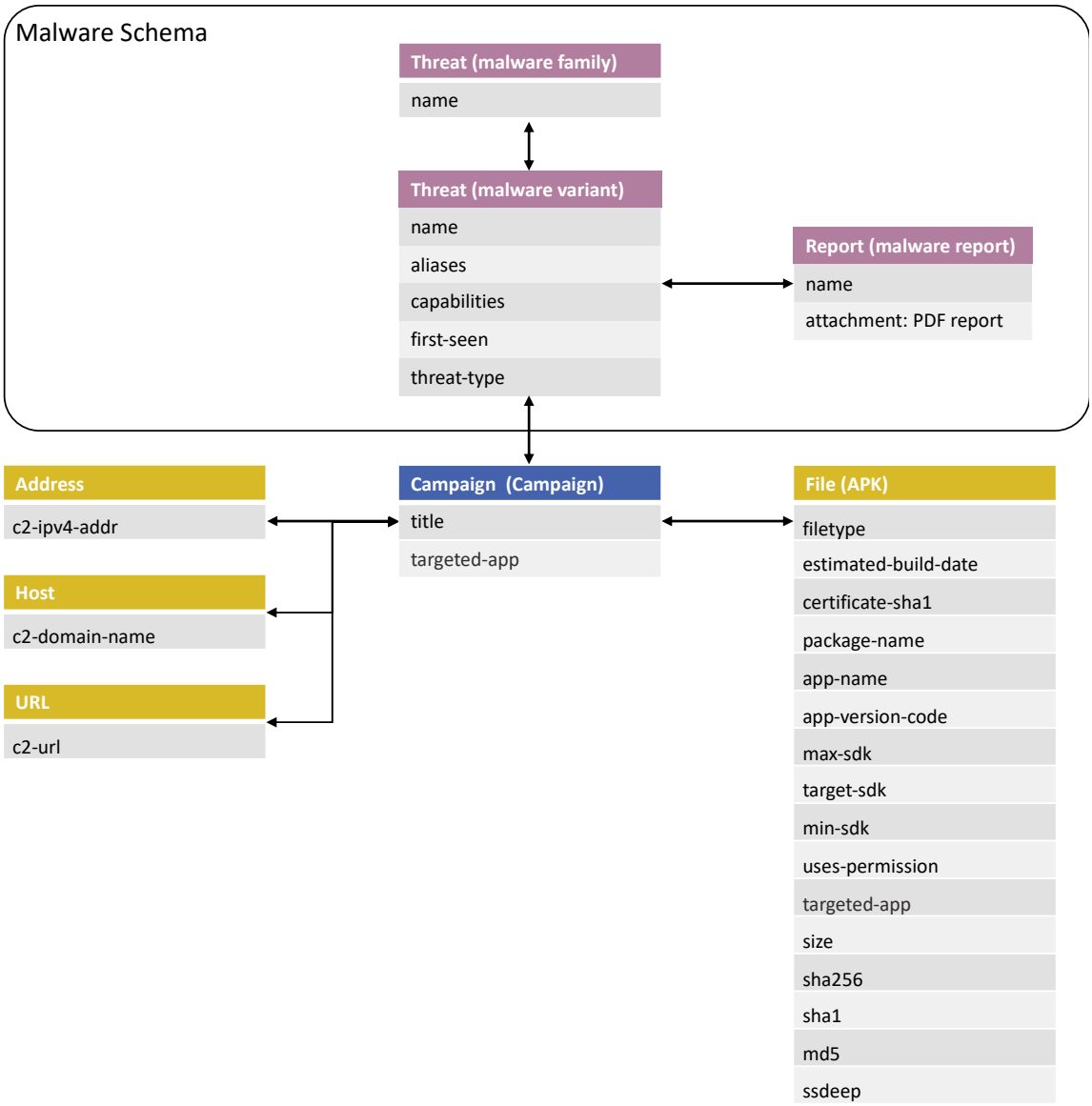
In order to simplify ingestion, correlation and consumption of the threat intelligence, MTI is available for ThreatConnect users that subscribed to the ThreatFabric MTI service, through the integration described in this document.

# 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:

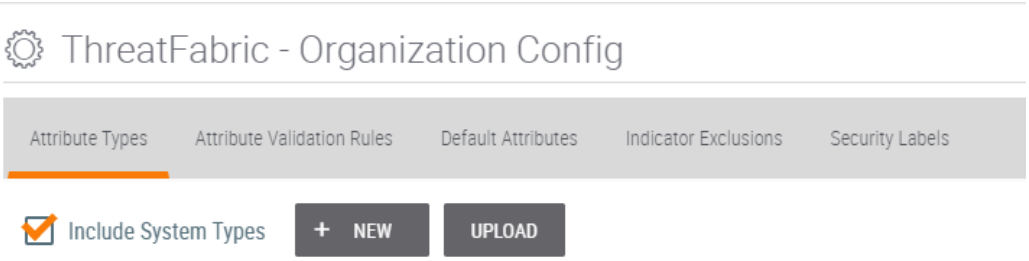
- ThreatFabric_-_Mobile_Threat_Intelligence_v1.tcx
- attributes.json

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

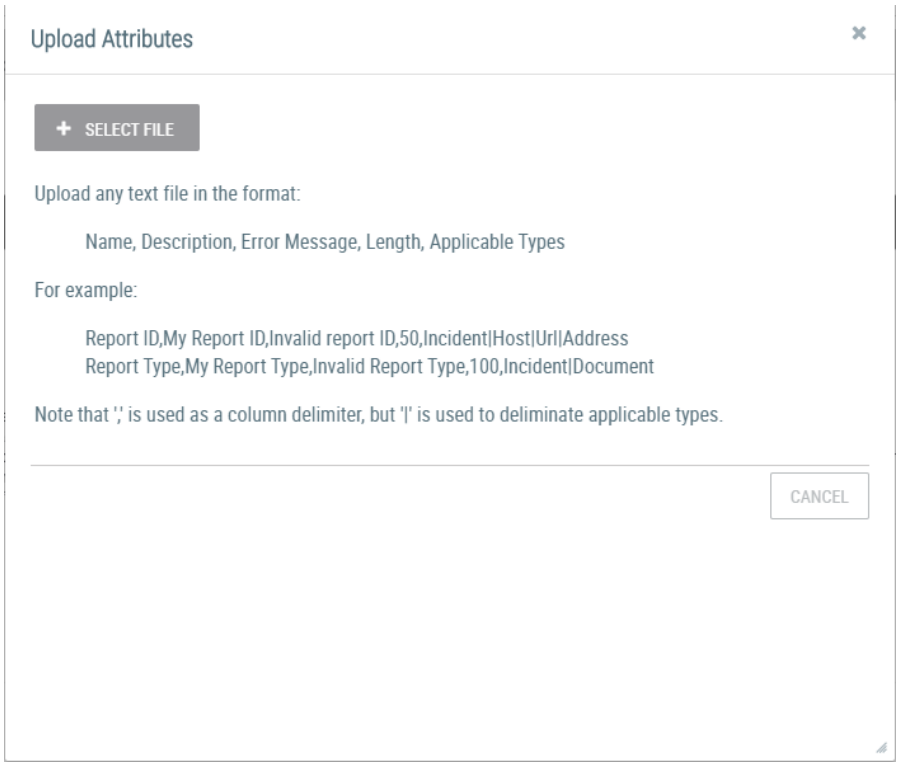
## 3.3 Attributes configuration

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

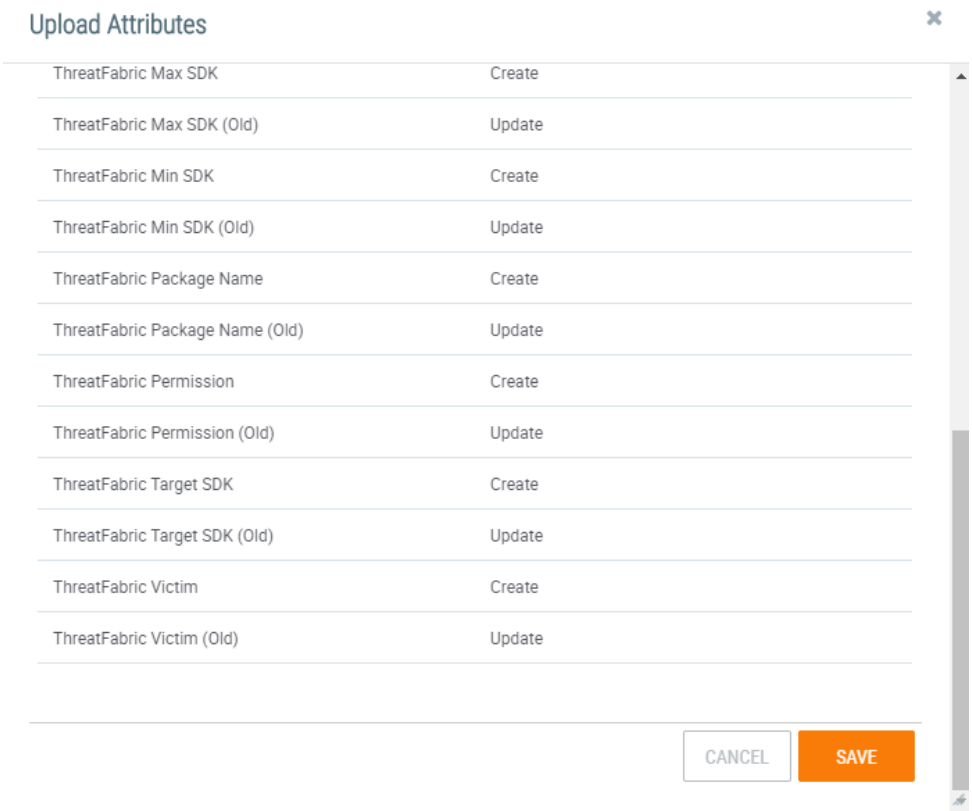
In order to configure ThreatFabric custom attributes you need to access **Org Config** > **Attribute types and** click on the **Upload** button:




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



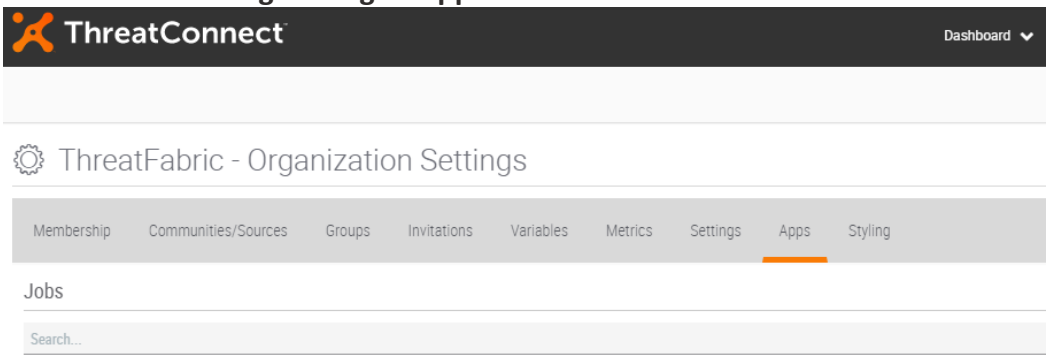

After clicking the **Save** button, the custom attributes will be configured for use with ThreatFabric's Mobile Threat Intelligence integration, as shown in following screenshot:



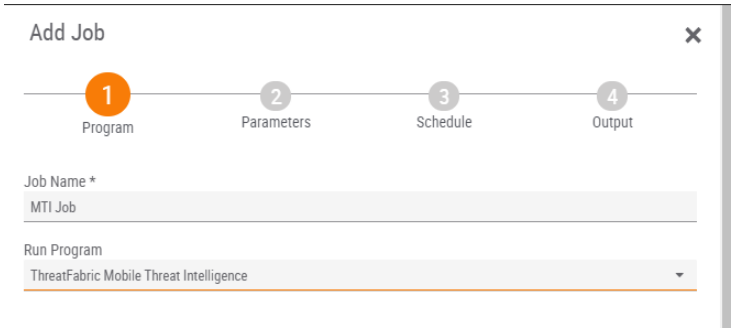
## 3.4 ThreatConnect Job configuration

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

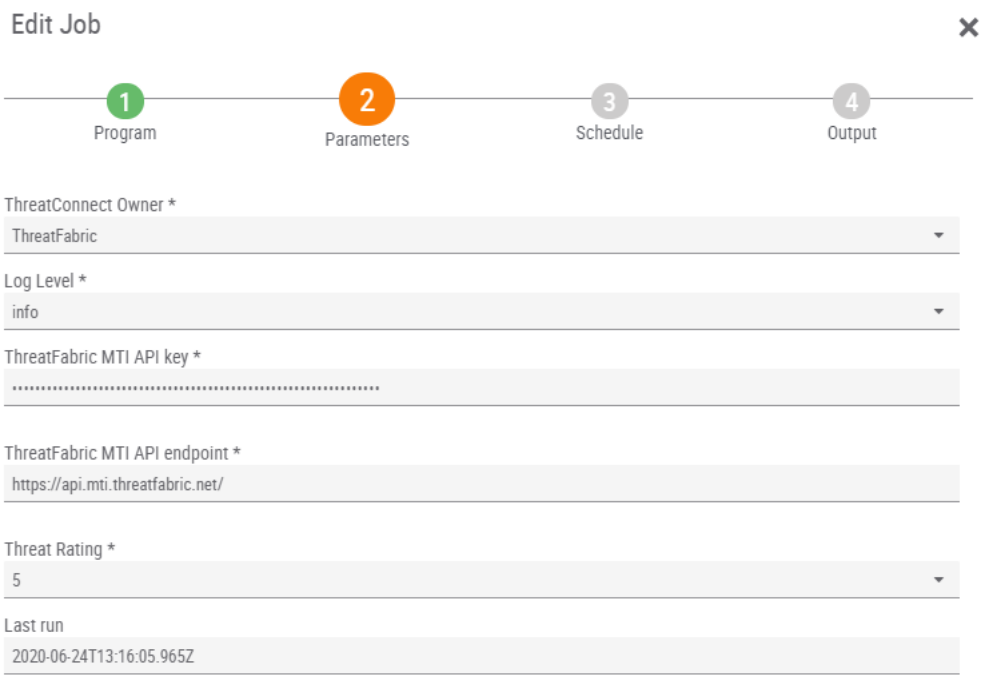
You need to access the **Org Settings** > **Apps** and click on the **Add** button:



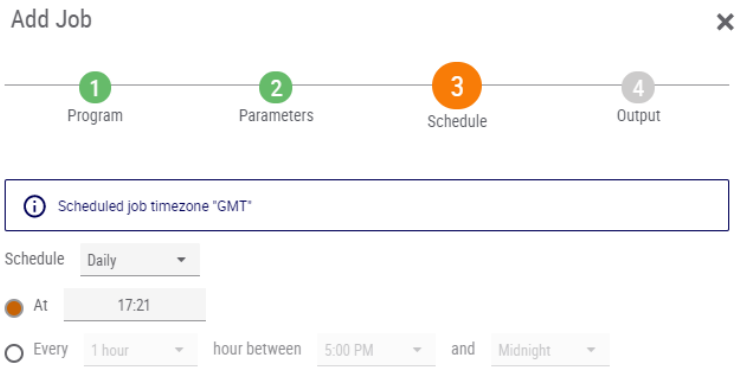

You then need to set the name of the job and select "**ThreatFabric Mobile Threat Intelligence**" as Run Program.



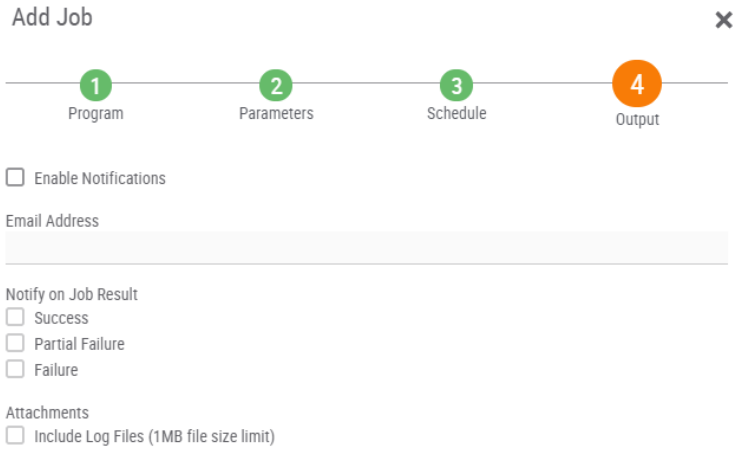

Configure the job using the ThreatFabric MTI API endpoint information and API key.
Note: *the "last_run" parameter will be used as a starting date for which the threat intelligence feed will be ingested*



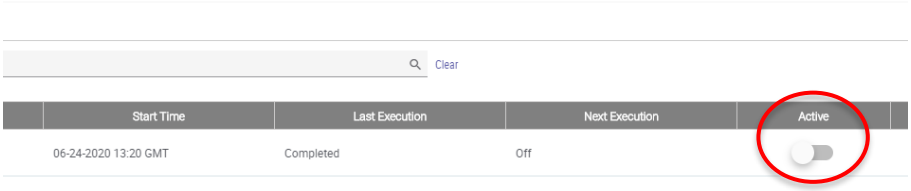

You then need to configure the schedule for the job. We recommend using a frequency of "once every hour".




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



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.



## 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:

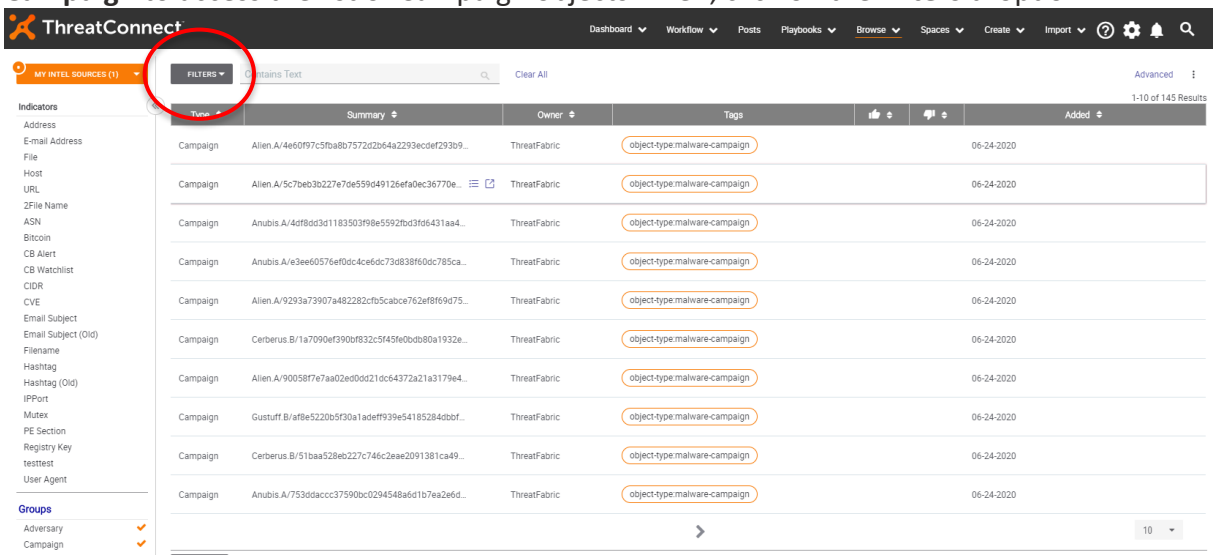
- Action at Minimum set to **Delete** so that indicators are deleted as soon as they reach minimum confidence
- **Percentage** checkbox checked which means that indicator confidence will be dropped as a percent of its previous value
- Confidence amount set to **1** so that 1% of an indicator's confidence 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).

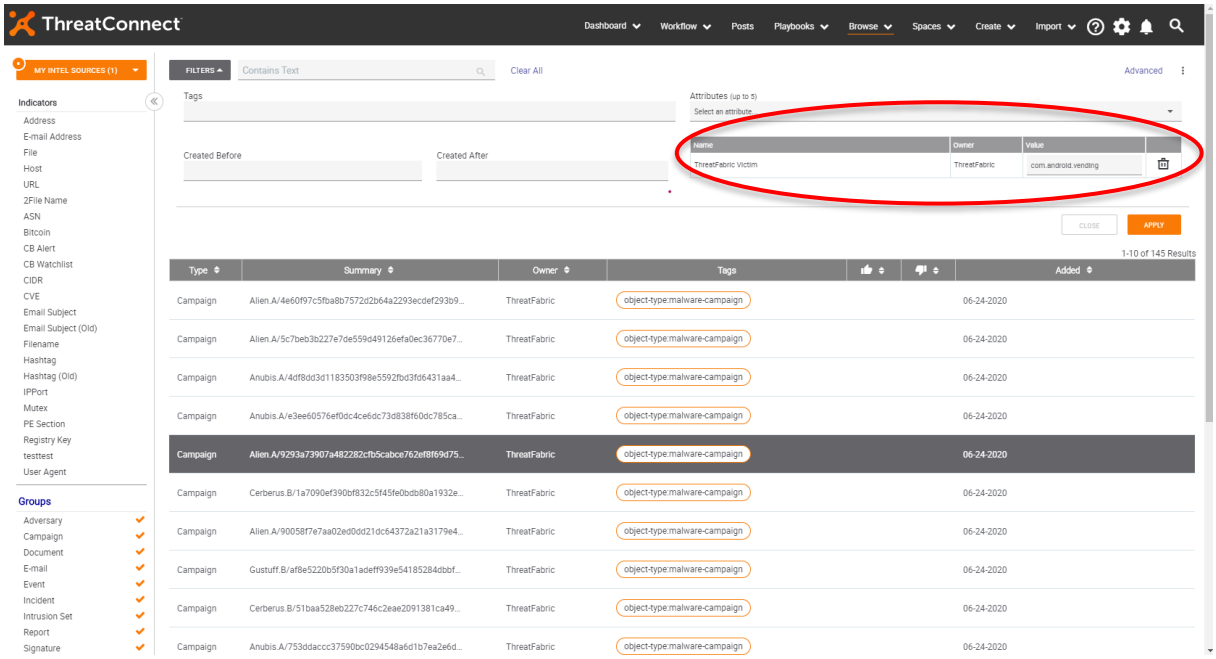
# 4. Using the ThreatFabric MTI data

## 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:




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**.

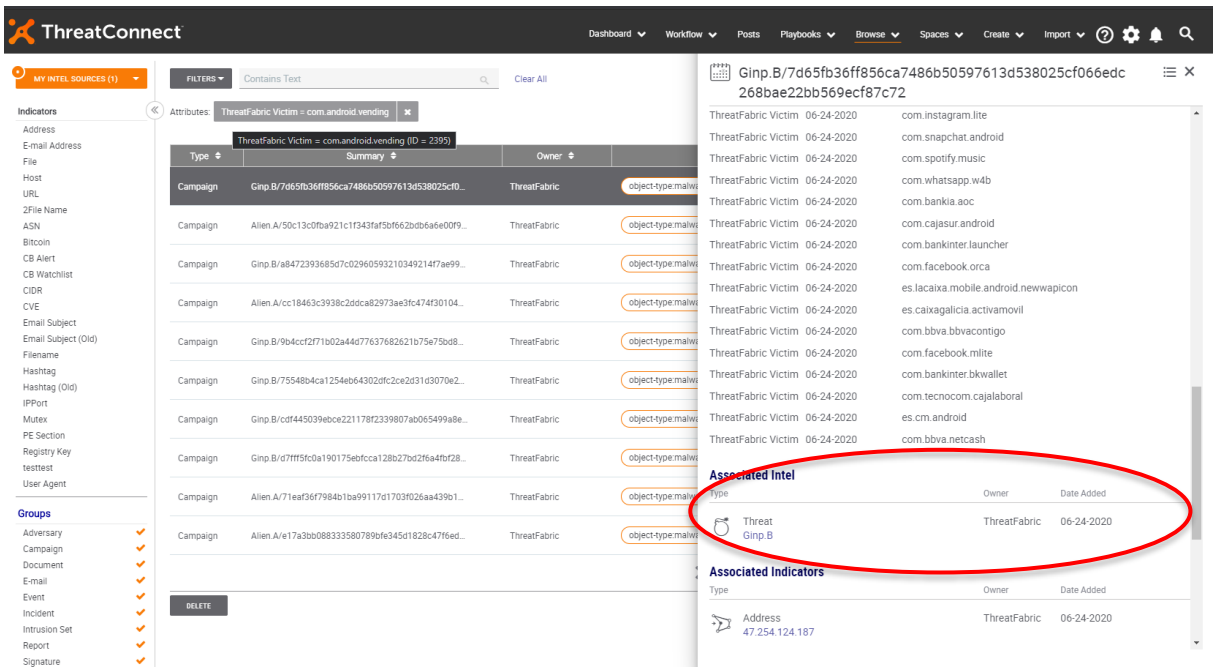



Resulting list of Campaigns will contain only Campaigns that are targeting the application bearing the package name that you provided.

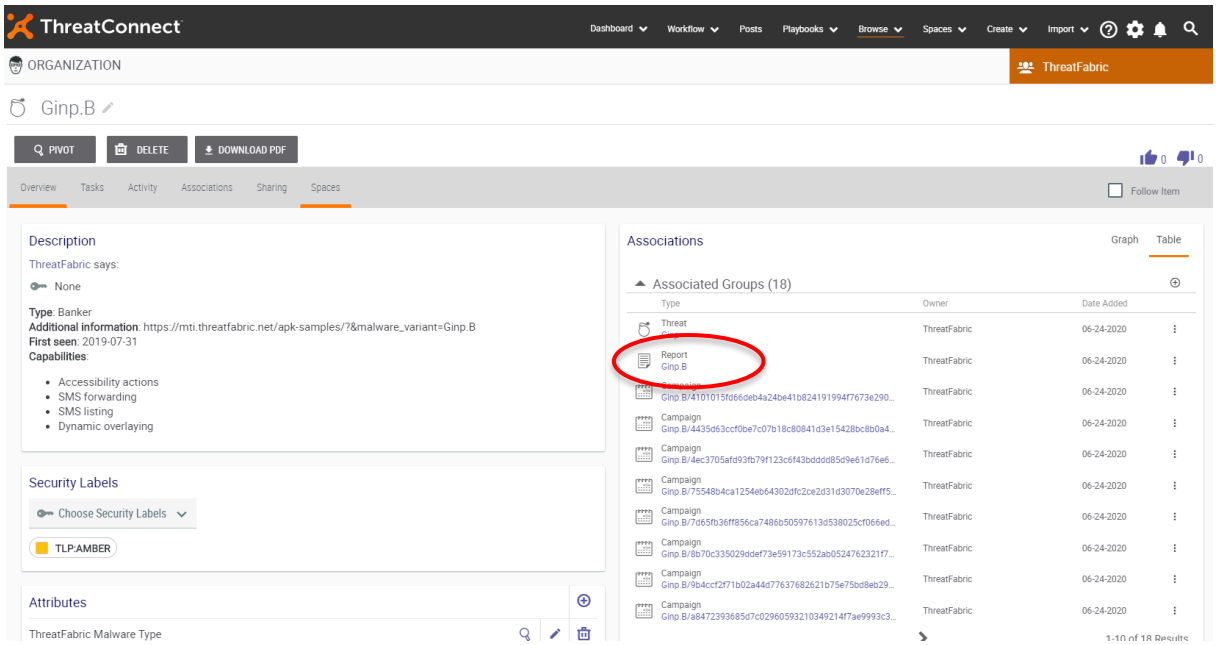
## 4.2 Access malware information relating to a campaign

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](#).

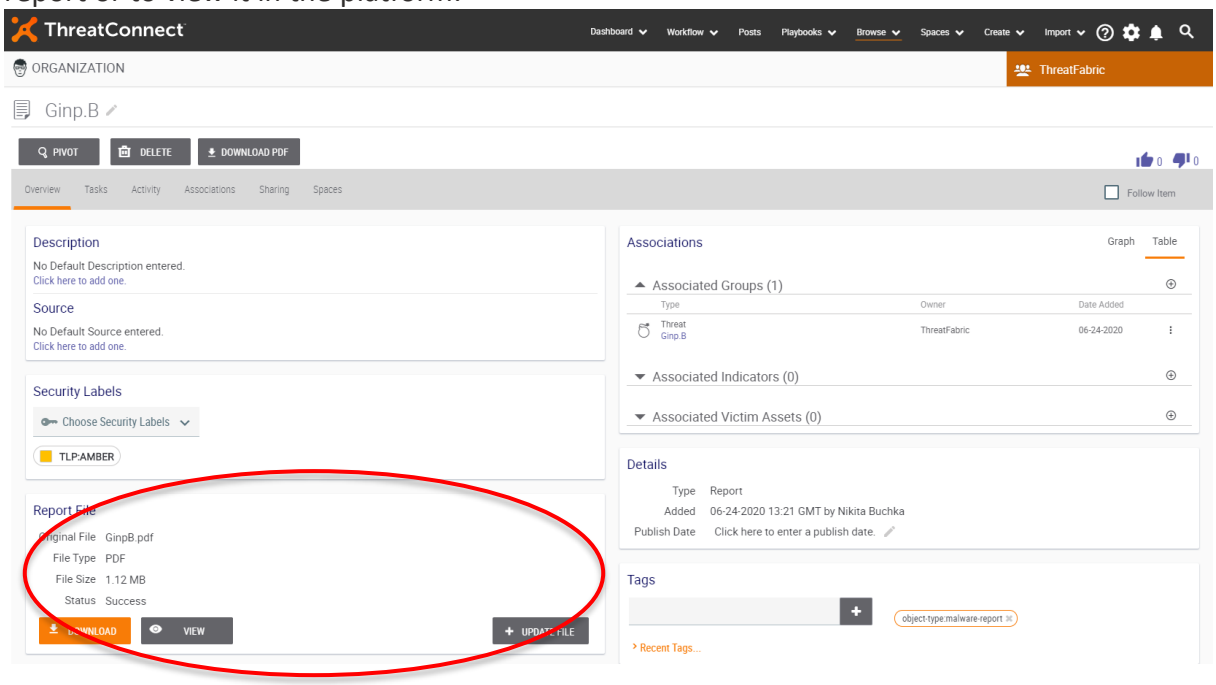
Once the campaign object is opened, scroll down to the **Associated Intel** section. There, click on the **Threat** object, linked to the Campaign. You will then be redirected to the details page.




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

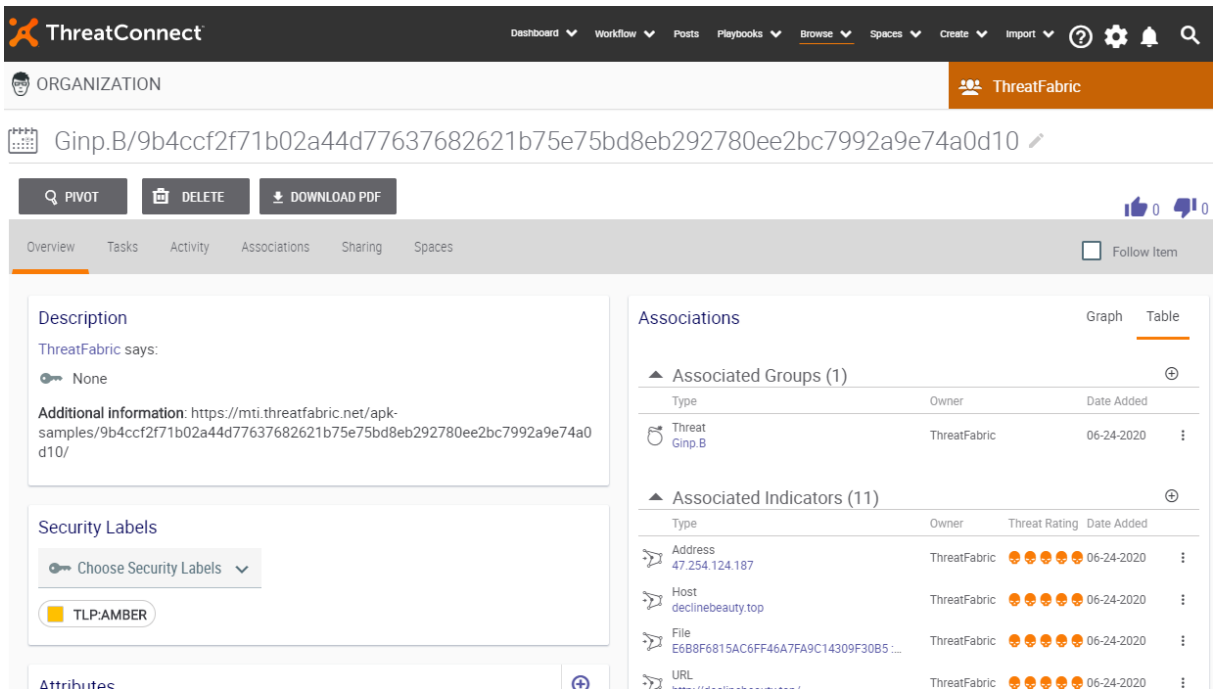


After accessing the Report's page, user will be able either to download the PDF file for the report or to view it in the platform:

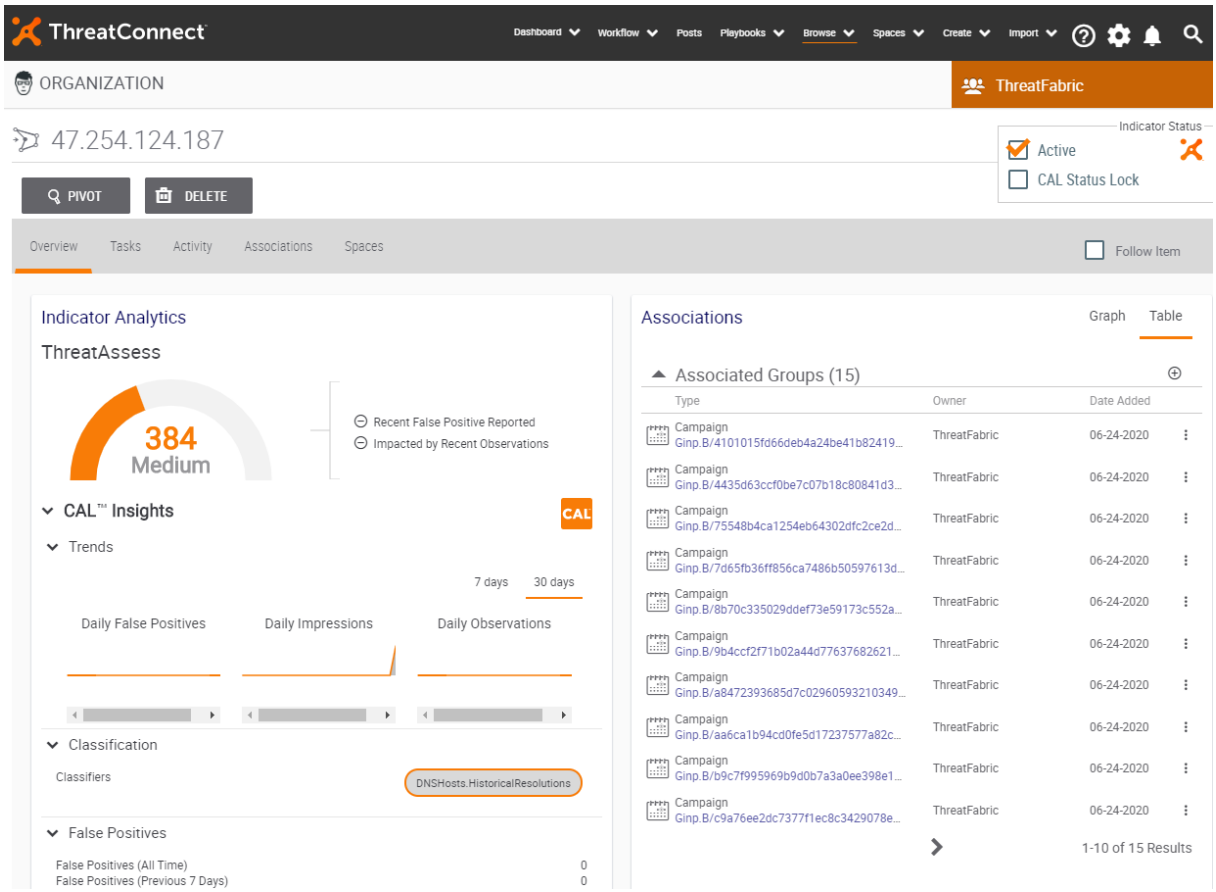



## 4.3 Access C2 information relating to a campaign

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.



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:



# 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.