

ReversingLabs Ransomware-Feed Integration for ThreatConnect

User Documentation

Author: ReversingLabs Integrations

Table of Contents

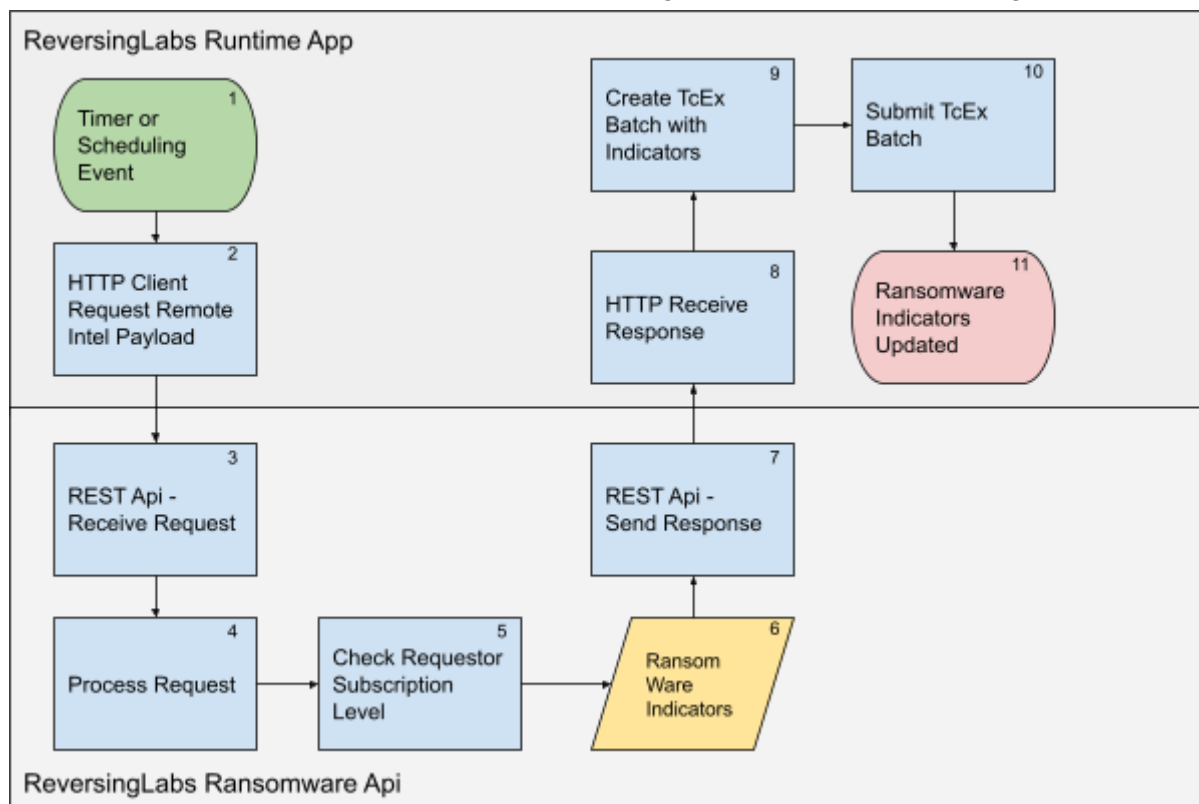
| | |
|--|----|
| Table of Contents | 1 |
| 1. Introduction | 2 |
| Integration Diagram | 2 |
| 2. Release notes | 3 |
| 3. Feed Data and Mapping | 3 |
| 3.1 Indicators | 3 |
| 3.2 Tags | 3 |
| 3.2.1 Mitre Tags | 3 |
| 3.2.2 TCP Port Tags | 4 |
| 3.2.3 MalwareFamily Tags | 4 |
| 3.2.4 MalwareFamily LifeCycle Tags | 4 |
| 3.2.5 Origin Tags | 4 |
| 3.3 Rating | 4 |
| 3.4 Confidence | 4 |
| 3.5 Data Mapping | 4 |
| 4. Configuration Requirements | 5 |
| 4.1 ReversingLabs Requirements | 5 |
| 4.2 ThreatConnect Requirements | 5 |
| 5. Job App Installation | 5 |
| 5.1 Obtaining the App | 5 |
| 5.2 Adding the App to ThreatConnect | 6 |
| 6. ThreatConnect Job App Configuration | 8 |
| 6.1 Org Settings | 9 |
| 6.2 Apps | 9 |
| 6.3 Name the job | 9 |
| 6.4 Parameters | 10 |
| 6.5 Schedule | 10 |
| 6.6 Output | 11 |
| 7. Using the Integration | 12 |
| 7.1 Browsing | 12 |
| 7.2 Indicator Details | 13 |
| 7.3 Cleaning up Indicators | 14 |
| 8. Support | 15 |

1. Introduction

The ReversingLabs Ransomware-Feed integration for ThreatConnect provides access to the ReversingLabs ransomware-feed api. This feed provides regular updates on threat indicators related to ransomware detected by ReversingLabs.

Integration Diagram

This section describes the function of the ReversingLabs TC Feed App at a high-level.



In the diagram above, the following sequence of events takes place:

1. A timer/scheduling event takes place in the ThreatConnect Platform to initiate the ReversingLabs Runtime App.
2. An HTTP client requests the Ransomware Feed payload. This request will include the ReversingLabs API Key for identification.
3. The ReversingLabs systems receive this request via our REST API.
4. The ReversingLabs systems will process the request to determine what information is being requested.
5. The ReversingLabs systems will check the subscription level for the supplied ReversingLabs API Key to determine if this customer has a valid subscription.
6. The Ransomware Indicators are compiled together in a payload.
7. The ReversingLabs REST API responds with this payload.
8. The HTTP client in the ReversingLabs Runtime App receives the response.
9. The data is parsed and turned into a TcEx Batch.
10. The TcEx Batch is submitted into the platform to store the Ransomware Indicators.
11. The ReversingLabs Runtime App cycle is complete.

2. Release notes

| App Version | Release Date | Details |
|-------------|--------------|---------------------------------------|
| 1.0.0 | 2021-09-28 | Initial User Document |
| 1.0.1 | 2021-10-04 | Update doc ch 6 and ch 7 |
| 1.0.4 | 2021-11-16 | Add URL indicator types |
| 1.0.5 | 2021-11-20 | Add md5 and sha256 to File indicators |

3. Feed Data and Mapping

The ransomware feed provides indicators related to ransomware activities detected by ReversingLabs.

3.1 Indicators

Indicator types provided in the feed are (using ThreatConnect terminology):

- Files
- Addresses
- Hosts
- URL

3.2 Tags

All indicators are accompanied by a set of tags. The tags enhance the indicator with additional information related to the detected behaviour of the ransomware activity. The set of tags relate to various types of information that ReversingLabs detected on the indicator.

3.2.1 Mitre Tags

Mitre tags have the pattern `T####` or `T####.###` followed by a text string that can have spaces.

- `T####` is a MITRE ATT&CK Technique code with a string indicating technique name.
- `T####.###` is a MITRE ATT&CK Technique.SubTechnique code with a subtechnique name.

Examples:

- T1001 Data Obfuscation
- T1048 Exfiltration Over Alternative Protocol
- T1071 Application Layer Protocol
- T1090 Proxy
- T1090.003 Multi-hop Proxy
- T1095 Non-Application Layer Protocol
- T1102 Web Service
- T1105 Ingress Tool Transfer
- T1132 Data Encoding
- T1219 Remote Access Software
- T1571 Non-Standard Port
- T1573 Encrypted Channel

3.2.2 TCP Port Tags

Tcp port tags have the pattern TCP-<number>. The number is the tcp port number on which the ransomware contacted a remote partner.

Examples:

- TCP-995
- TCP-9781
- TCP-10004

3.2.3 MalwareFamily Tags

MalwareFamily tags indicate to what Malware Family this indicator belongs to.

Each indicator has only one MalwareFamily tag. If an indicator happens to belong to more than one malware family we select the malware family with the strongest impact and the latest life-cycle.

Examples:

- Bazar
- Icedid
- ZLoader

3.2.4 MalwareFamily LifeCycle Tags

LifeCycle tags show in what life cycle phase this ransomware family is.

The following tags are used for this tag.

- Early
- Middle
- Late

Each indicator has only one LifeCycle tag. If an indicator happens to belong to more than one LifeCycle we select the malware family with the strongest impact and the latest life-cycle.

3.2.5 Origin Tags

The origin tag shows the origin of the indicator.

There is only one tag like this:

- ReversingLabs

3.3 Rating

All values in the feed have a rating. The rating is based on the Malware Family Life Cycle:

- Early: 3.0
- Middle: 4.0
- Late: 5.0

3.4 Confidence

All values have a confidence expressed as a percentage.

100% is the highest confidence rating.

3.5 Data Mapping

The table below documents the data mapping that takes place between the ReversingLabs Ransomware Indicators data and the ThreatConnect Platform.

| ReversingLabs Field | ThreatConnect Field | Possible Values | Notes |
|---------------------|---------------------|------------------------|--|
| Hash | File | sha1 md5 sha256 | The hash type is derived from the length of the value. <ul style="list-style-type: none"> • The sha1 string has a length of 40 • The md5 string has a length of 32 • The sha256 string has a length of 64 |
| ipv4 | Address | Any valid ipv4 address | |
| domain | Host | Any valid dns domain. | |
| uri | URL | A network url | Max len is 500, domain part in lowercase |
| tag | Tag | A text string | The ReversingLabs tag is present on all indicators from this feed. |
| rating | rating | 1.0 -- 5.0 | The rating is currently based on the LifeCycle Tag. Early: 3.0, Middle: 4.0, Late: 5.0 |
| confidence | confidence | 0-100% | |

4. Configuration Requirements

4.1 ReversingLabs Requirements

The application is a self contained package but it will require an account on ReversingLabs TiCloud to fetch the Ransomware Feed data from the ReversingLabs Ransomware Feed API.

A request for a TiCloud account should be made to support@reversinglabs.com before installing the application. The request should mention that access is required to the Ransomware Feed API. You will receive a username and a password that will have to be entered when installing the app for the first time.

4.2 ThreatConnect Requirements

- As the app will run inside the ThreatConnect Platform you will need access to ThreatConnect.

5. Job App Installation

5.1 Obtaining the App

The app can be obtained from the ThreatConnect [marketplace](#). Click the download button and save the file in a location that will allow you to upload that file into the ThreatConnect web interface.



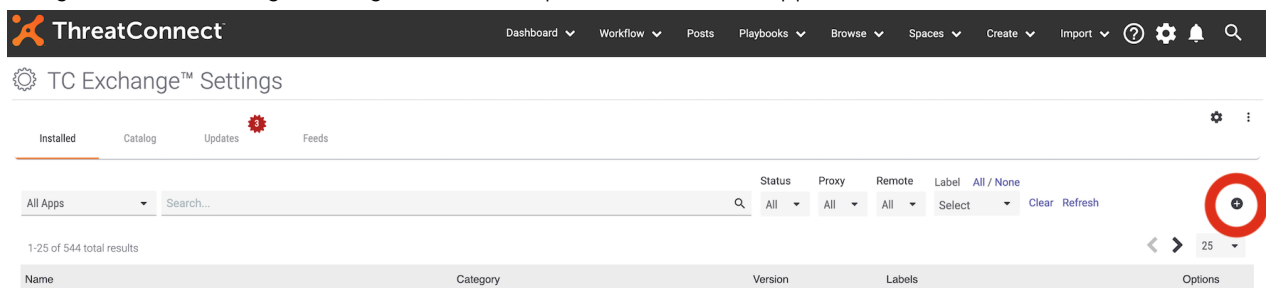
Download

Related Links

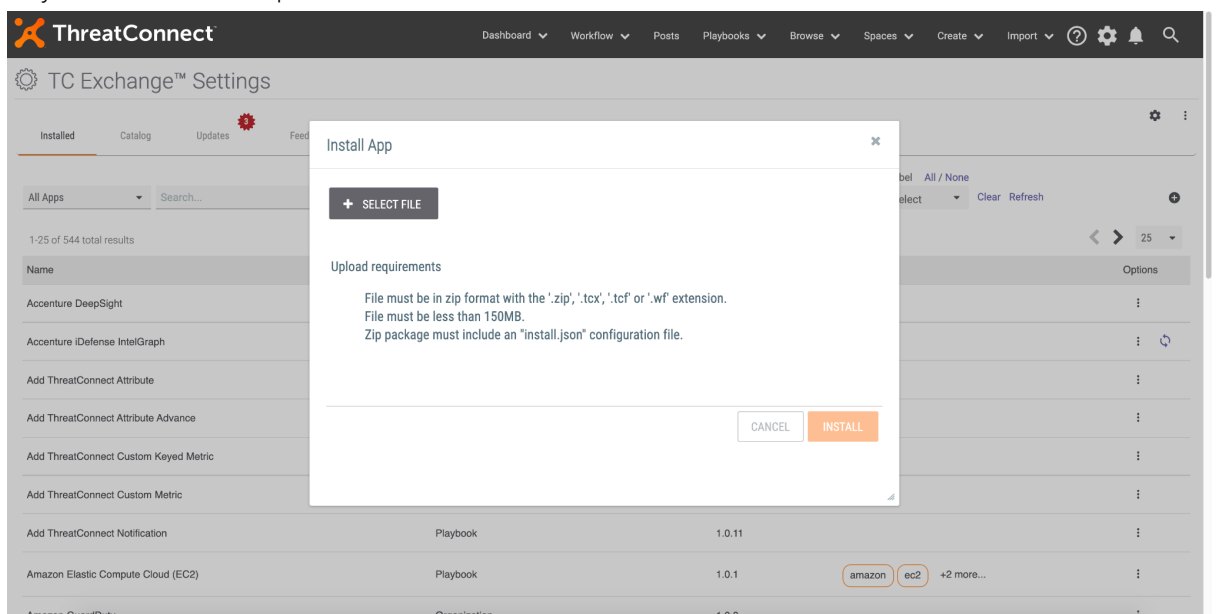
Installation and Configuration
Guide

5.2 Adding the App to ThreatConnect

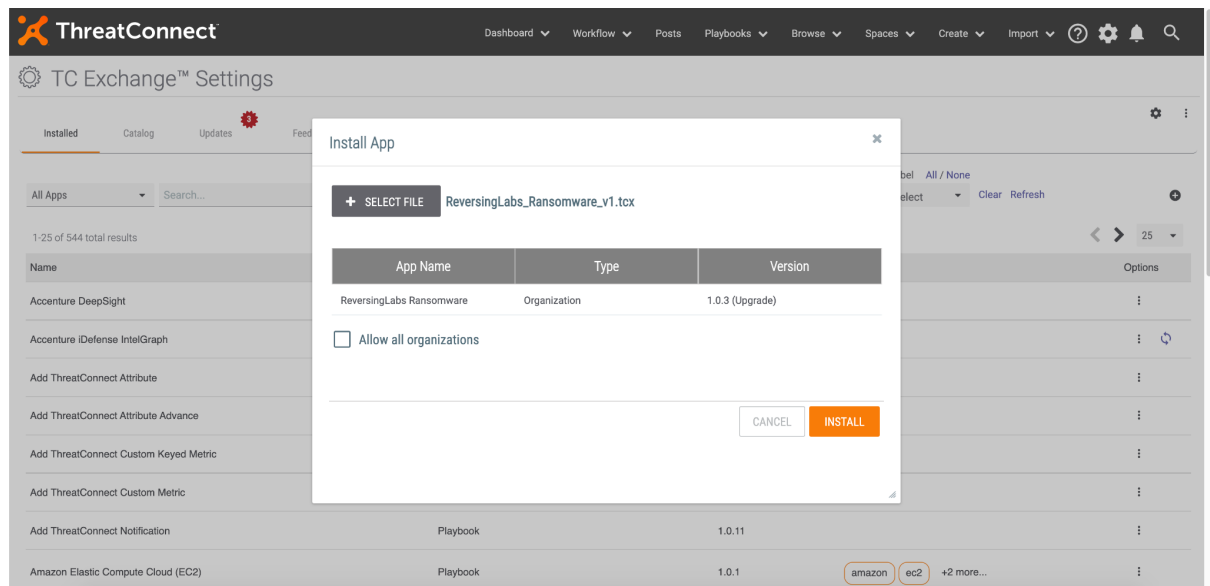
1. Navigate to TC Exchange Settings and select option to add a new app as shown in the screen.



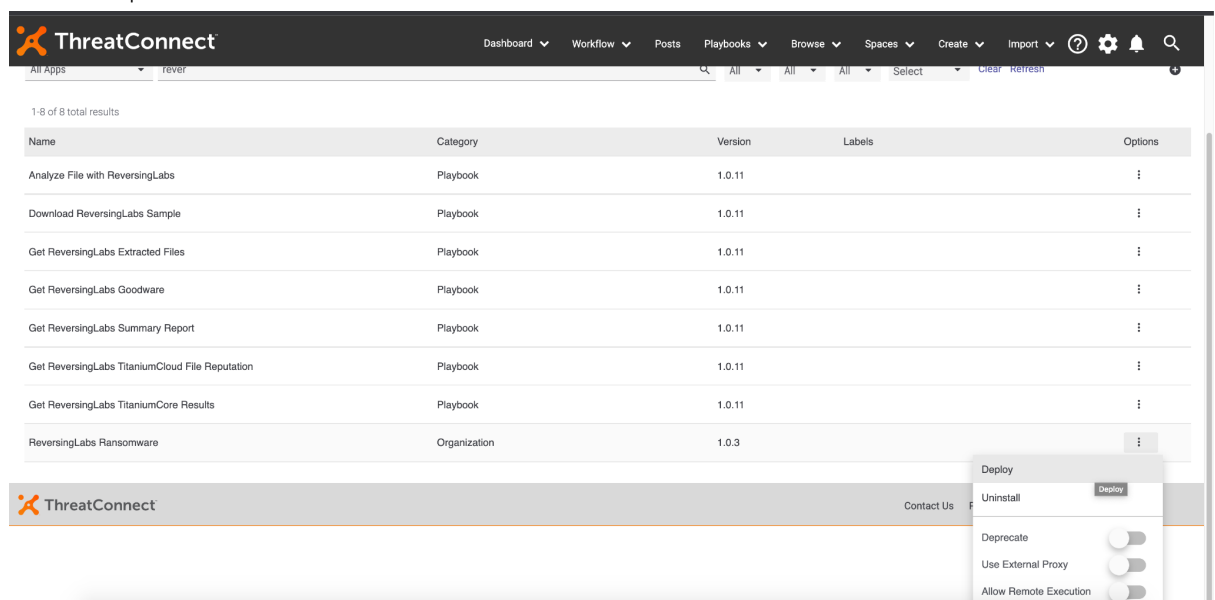
2. Select the file you downloaded in the previous step. The file gets unpacked at this stage so it may take some time to process.



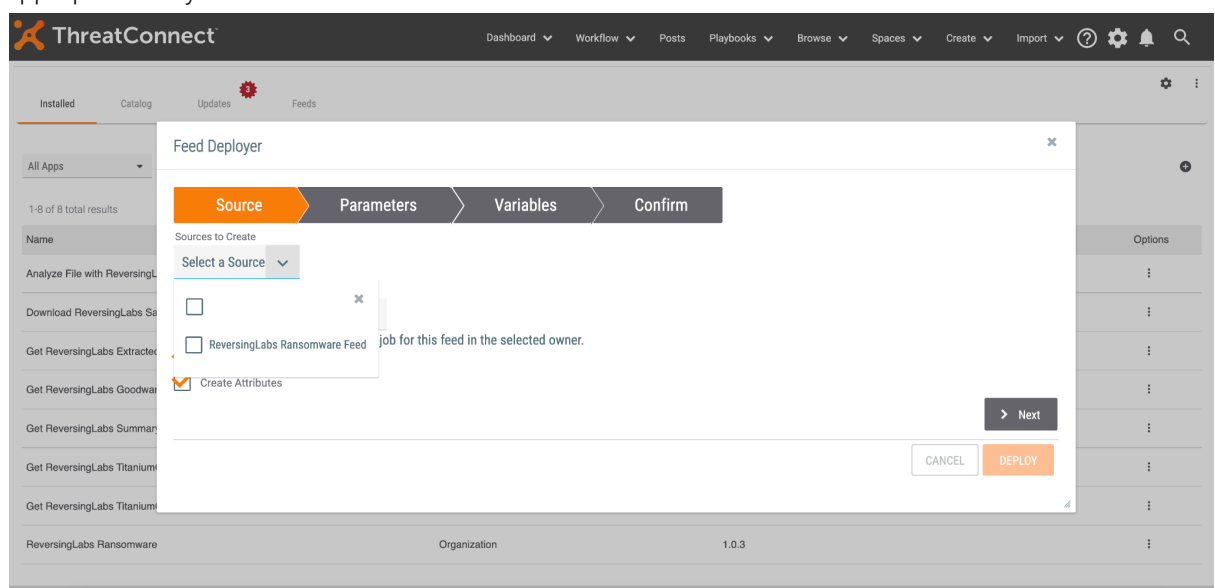
- Once the processing is complete choose the install button. The version you say may be different than in that screenshot below.



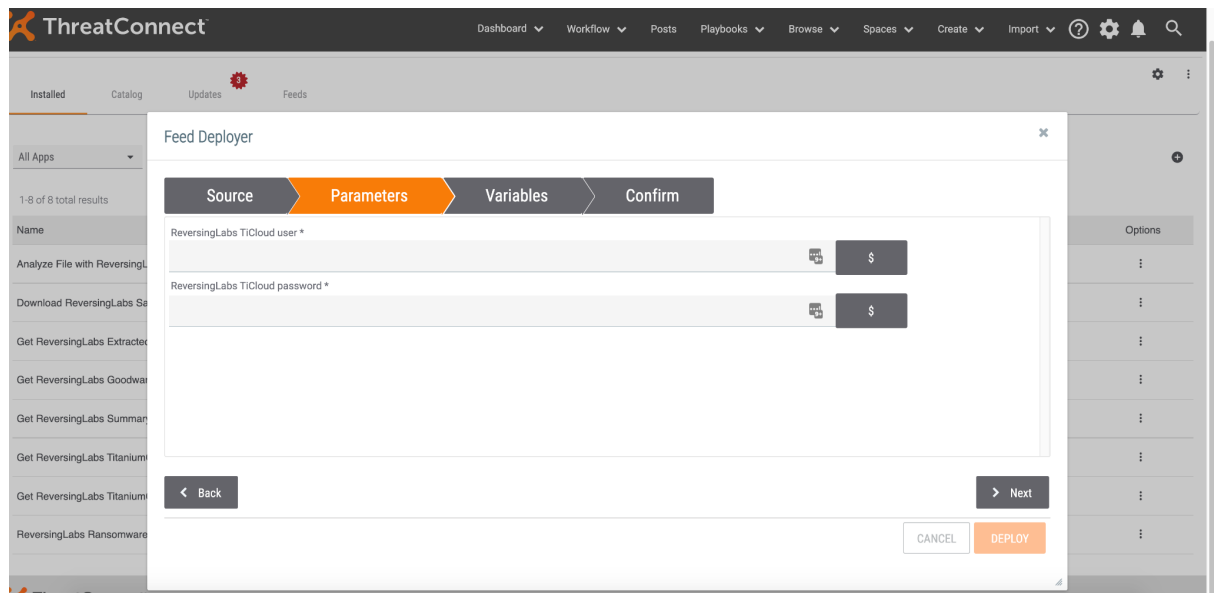
- The application is now installed. Find the ReversingLabs application in the list and select deploy from the Options column.



- You will then be presented with an install wizard. Step through the sections and select options appropriate for your environment.

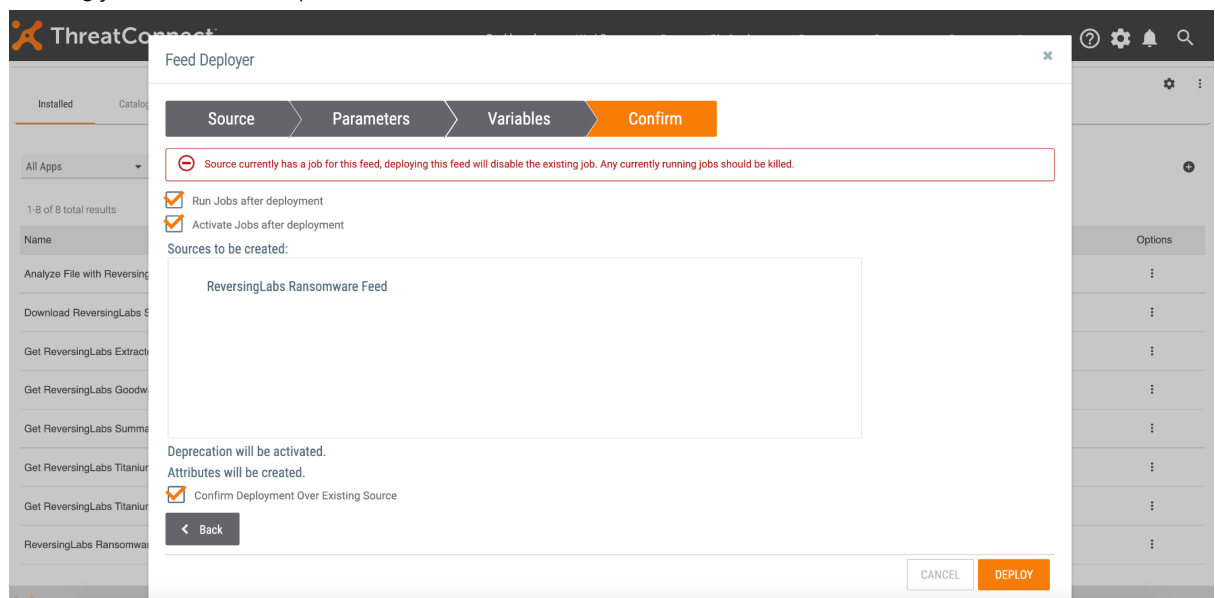


- The parameters section will prompt you for TiCloud credentials. These are obtained from ReversingLabs.



The screenshot shows the ThreatConnect interface with the 'Feed Deployer' modal open. The 'Parameters' tab is selected, showing two input fields: 'ReversingLabs TiCloud user *' and 'ReversingLabs TiCloud password *'. Both fields have a password icon and a dollar sign icon. The modal has a progress bar at the top with four steps: Source, Parameters (active), Variables, and Confirm. At the bottom, there are 'Back', 'Next', 'Cancel', and 'Deploy' buttons.

- When you reach the end choose deploy. If this is an upgrade you may see a warning about existing jobs. It is safe to proceed.

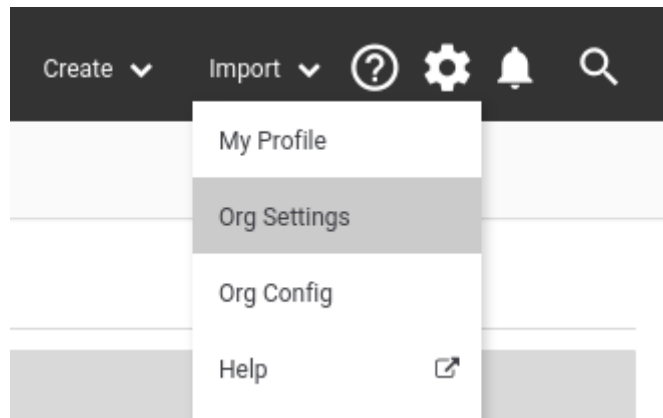


The screenshot shows the ThreatConnect interface with the 'Feed Deployer' modal open. The 'Confirm' tab is selected, showing a warning message: 'Source currently has a job for this feed, deploying this feed will disable the existing job. Any currently running jobs should be killed.' Below the warning, there are two checked checkboxes: 'Run Jobs after deployment' and 'Activate Jobs after deployment'. Under 'Sources to be created:', there is a list box containing 'ReversingLabs Ransomware Feed'. At the bottom, there are 'Back', 'Cancel', and 'Deploy' buttons.

6. ThreatConnect Job App Configuration

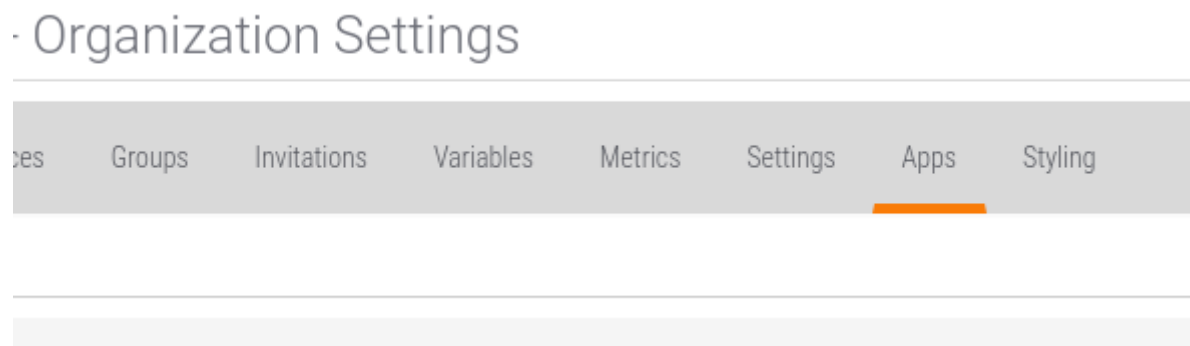
The app will need to be configured with credentials for **ReversingLabs TiCloud RansomwareFeed api**. You will receive a TiCloud username and a password.

6.1 Org Settings

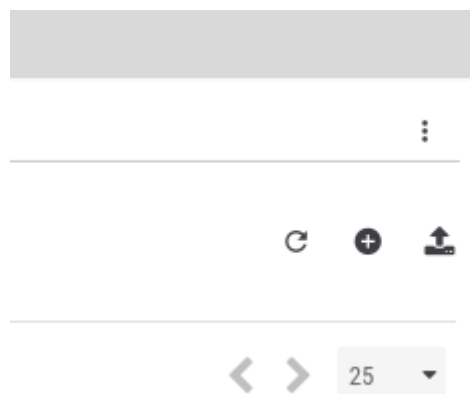


6.2 Apps

Select the Apps section on the "organisation settings" menu bar.



Select the plus sign on the right side of the screen.



6.3 Name the job

1. In our case we name the job "Fetch ReversingLabs Ransomware Hourly", but any name you prefer will do.
2. In the drop down "Run Program" find the program: "reversinglabs-ransomware-feed-for-threatconnect"
3. Press the Next button on the bottom of the window

Add Job

1

Program

2

Parameters

Job Name *

Fetch ReversingLabs Ransomware Hourly

Run Program

reversinglabs-ransomware-feed-for-threatconnect

6.4 Parameters

1

Program

2

Parameters

Api User *

ReversingLabs ApiTesting

ThreatConnect Owner *

Reversing Labs

ReversingLabs TiCloud user *

ReversingLabs TiCloud password *

6.5 Schedule

We schedule hourly at every hour precisely

1

2

3

Program

Parameters

Schedule

i

Advanced schedule timezone is UTC

Schedule

Advanced

Custom cron expression

0 0 * * * ?

6.6 Output

If you wish you can be notified of failure, the email is just an example use one that is valid for your functionality.

Add Job

1

2

3

4

Program

Parameters

Schedule

Output

checkbox

Enable Notifications

Email Address

nobody@nowhere.in.space

Notify on Job Result

checkbox

Success

checkbox

Partial Failure

checkbox

Failure

Attachments

checkbox

Include Log Files (1MB file size limit)

Activate

By default after creating a job it is not yet activated. To activate, move the activate button to the active position. After activating you will see the next Execution has been set.

| Start Time | Last Execution | Next Execution | Active |
|------------|----------------|----------------|--------------------------------------|
| N/A | N/A | Off | <div> <div></div> <div></div> </div> |

Activated now:

| Start Time | Last Execution | Next Execution | Active |
|------------|----------------|-----------------------|-------------------------------------|
| N/A | N/A | 10-01-2021 11:00 CEST | <input checked="" type="checkbox"/> |

You can schedule a immediate run with the button:



| Start Time | Last Execution | Next Execution | Active | |
|-----------------------|----------------|-----------------------|-------------------------------------|-------|
| 10-01-2021 10:16 CEST | Running | 10-01-2021 11:00 CEST | <input checked="" type="checkbox"/> | ⏸ ✎ ⋮ |

⏪ ⏩

After pressing the immediate run you will see the Running on the Last Execution.

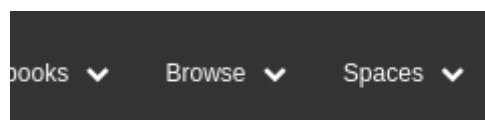
Afterwards you will see Completed in the Last Execution.

| Start Time | Last Execution | Next Execution | Active | |
|-----------------------|----------------|-----------------------|-------------------------------------|-------|
| 10-01-2021 10:16 CEST | Completed | 10-01-2021 11:00 CEST | <input checked="" type="checkbox"/> | ⏸ ✎ ⋮ |

7. Using the Integration

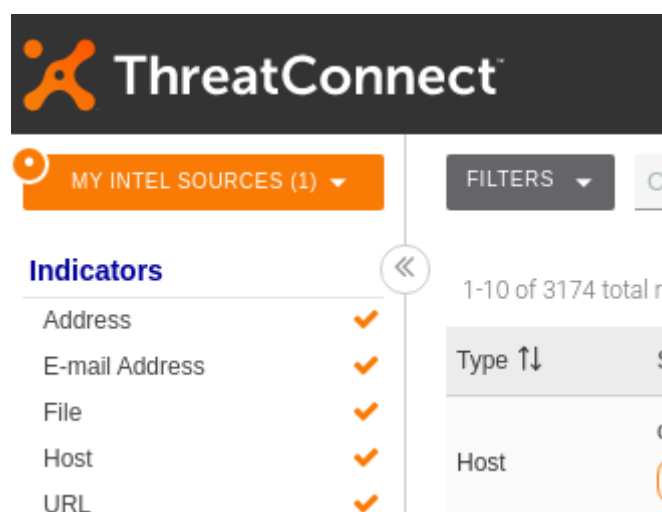
7.1 Browsing

Browse Indicators:



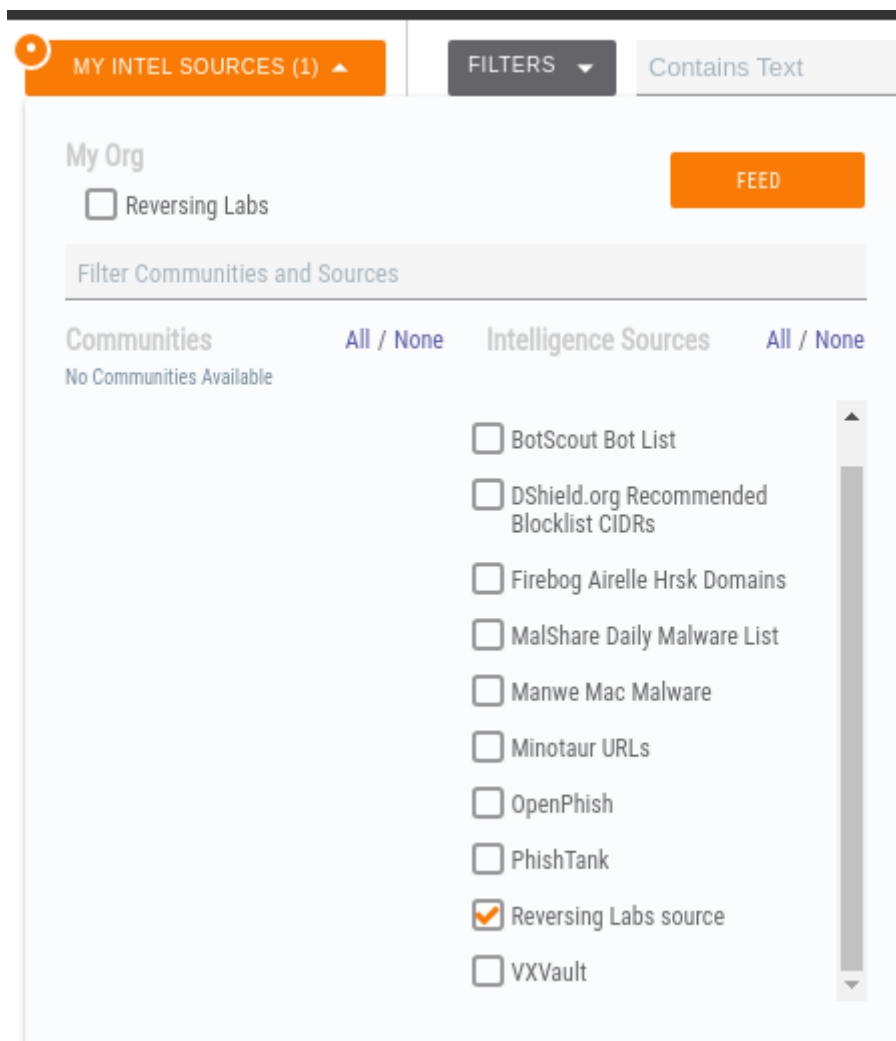
Select Browse and then Indicators, you will be redirected to the Indicators screen.

You will see the accumulated Indicators and can select individual feeds via: "MY INTEL SOURCES"



Select Feed:

To select explicitly only the ReversingLabs source, you can deselect all others and leave only the ReversingLabs source selected.



ReversingLabs indicators will be shown:

| Type ↑↓ | Summary ↑↓ | Owner ↑↓ | Threat Rating ↑↓ |
|---------|---|-----------------------|------------------|
| Host | connectini.net AgentTesla DNS-Lookup DROPS-AgentTesla +9 more... | Reversing Labs source | 🔴🔴🔴🔴 |
| Host | eafuebdbedbedggr.ws DNS-Lookup Early HTTP +6 more... | Reversing Labs source | 🔴🔴🔴 |
| Host | cleaner-partners.biz DNS-Lookup DROPS-AgentTesla DROPS-Meterpreter +14 more... | Reversing Labs source | 🔴🔴🔴🔴🔴 |
| Host | coll.chinajcsc.com DNS-Lookup HTTP Middle +8 more... | Reversing Labs source | 🔴🔴🔴🔴 |
| Host | d2t3rnn2b8b6w3.cloudfront.net CobaltStrike DNS-Lookup Late +2 more... | Reversing Labs source | 🔴🔴🔴🔴🔴 |
| Host | alaricapps.com AgentTesla DNS-Lookup Middle +1 more... | Reversing Labs source | 🔴🔴🔴🔴 |

7.2 Indicator Details

When selecting a individual indicator you will be shown its full Tag list and other relevant data:

| | | | |
|------------|-----------------------|------------|---------------|
| Type | Owner | Added | Last Modified |
| Host | Reversing Labs source | 09-20-2021 | 09-20-2021 |
| DNS | Whois | | |
| Not Active | Not Active | | |

ThreatAssess



- ⊖ Recent False Positive Reported
- ⊖ Impacted by Recent Observations

Threat Rating

 High

Confidence Rating

 Confirmed

Tags

T1105 Ingress Tool Transfer
 Suspicious Domain
 DROPS-AgentTesla
 ReversingLabs
 AgentTesla
 T1095 Non-Application Layer Protocol
 T1571 Non-Standard Port
 Middle
 DNS-Lookup
 T1001 Data Obfuscation
 T1071 Application Layer Protocol
 T1573 Encrypted Channel

7.3 Cleaning up Indicators

Using depreciation rules you can schedule indicators to become less confident over time as they get older and are not updated again from the feed source.

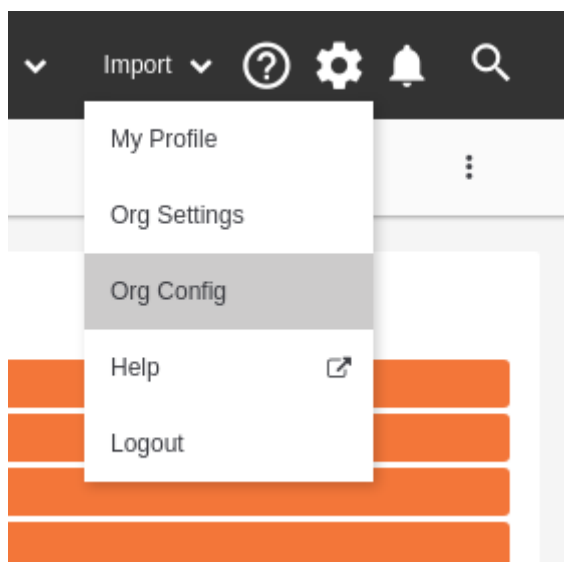
Installing cleanup rules that lower the confidence level of each indicator every day with 3 points results in the desired behaviour of deleting any indicator in 33 days that was not updated in the 33 day window.

You will have to create one rule per indicator type like:

| + NEW | | | | | |
|----------------|----------|--------|--------------------------|-------------------------------------|-----------------------|
| Indicator Type | Interval | Amount | Percentage | Recurring | Action At Minimum |
| Address | 1 day | 3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Delete ▼ |
| Host | 1 day | 3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Delete ▼ |
| File | 1 day | 3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Delete ▼ |



The rules can be configured via: and then Org Config as in:



Select the tab "Deprecation Rules" to configure and maintain your desired rules.



8. Support

For questions about this integration or the data feed contact: Support@ReversingLabs.com