REVERSINGLABS

VERSION 1.0.0
September 2021

ReversingLabs Ransomware-Feed Integration for ThreatConnect

User Documentation

Author: ReversingLabs Integrations

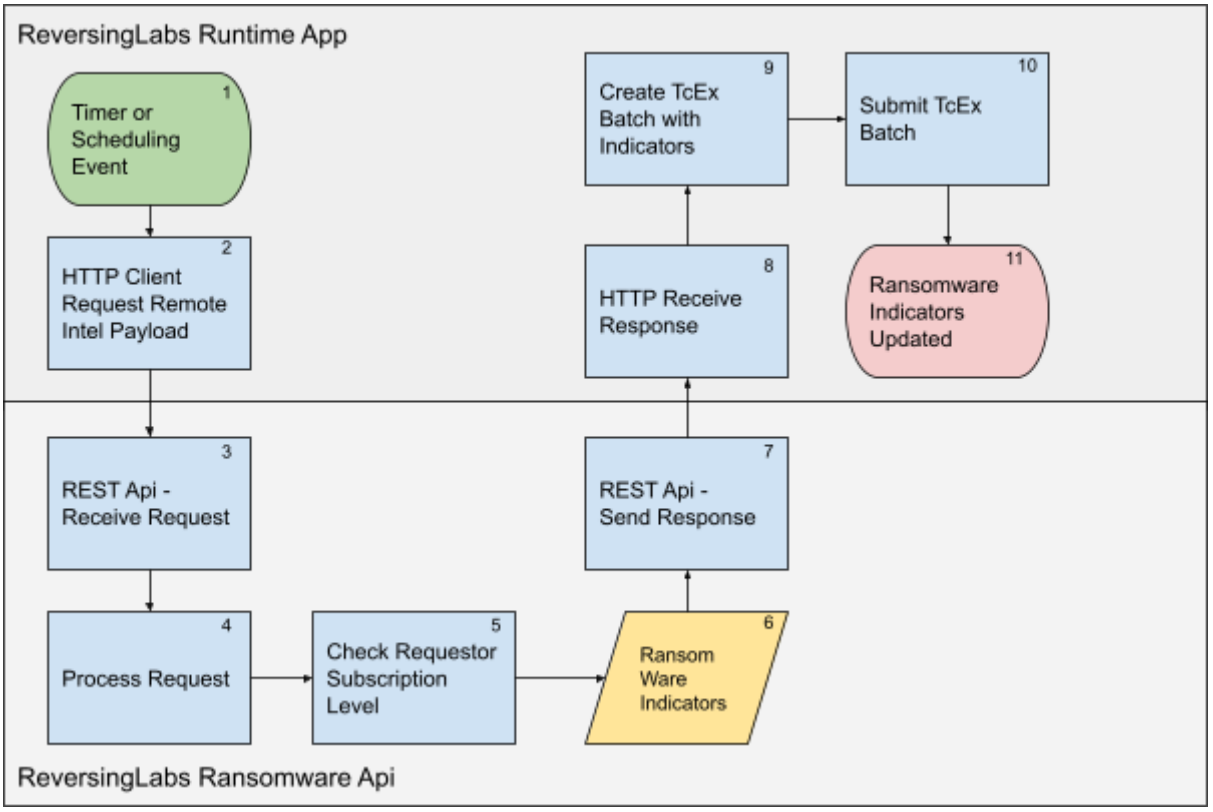
Table of Contents

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

Version 1.0.0

This is the initial version of this implementation.

App Version	Release Date	Details
1.0.0	2021-09-28	Initial User Document

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

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	The hash type is derived from the length of the value. The sha1 string has a length of 40
ipv4	Address	Any valid ipv4 address	
domain	Host	Any valid dns domain.	

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

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.

ThreatConnect Requirements

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

5. Job App Installation

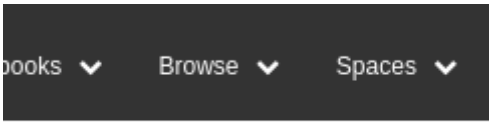
Installation instructions on how to install the integration on the ThreatConnect Platform, to be done when we have access to the TC testing environment.

6. ThreatConnect Job App Configuration

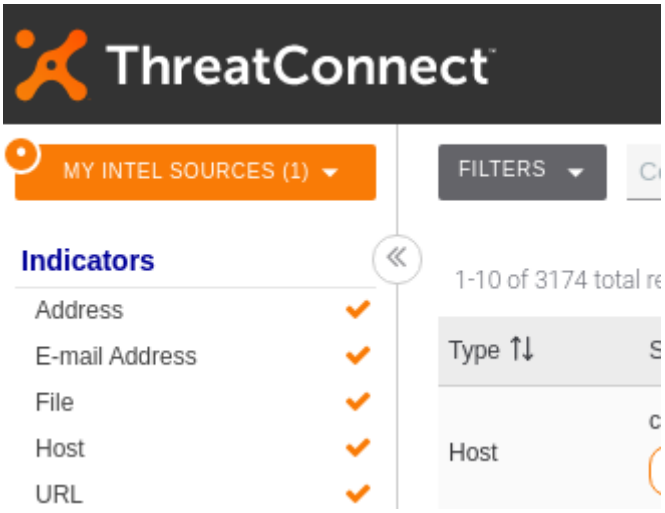
The app will need to be configured with credentials for **ReversingLabs TiCloud RansomwareFeed api.**
You will receive a TiCloud username and a password.

7. Using the Integration

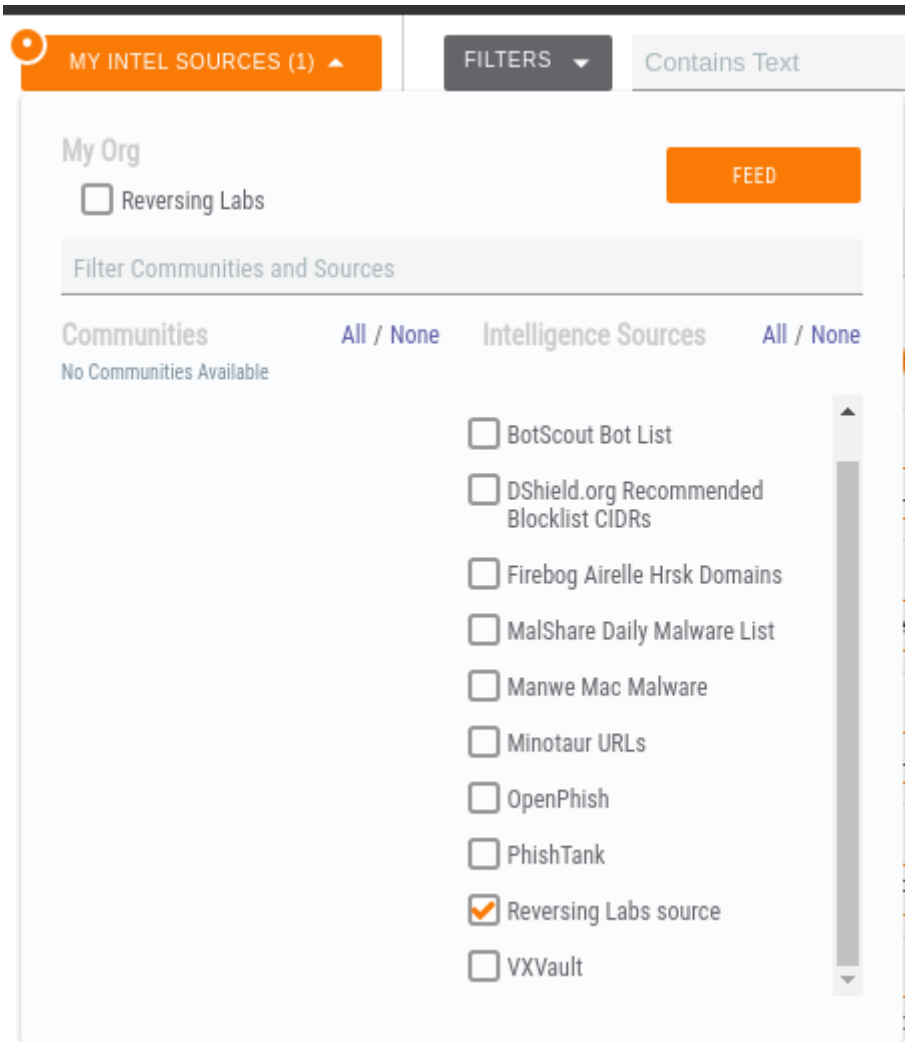
Browse Indicators:



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”



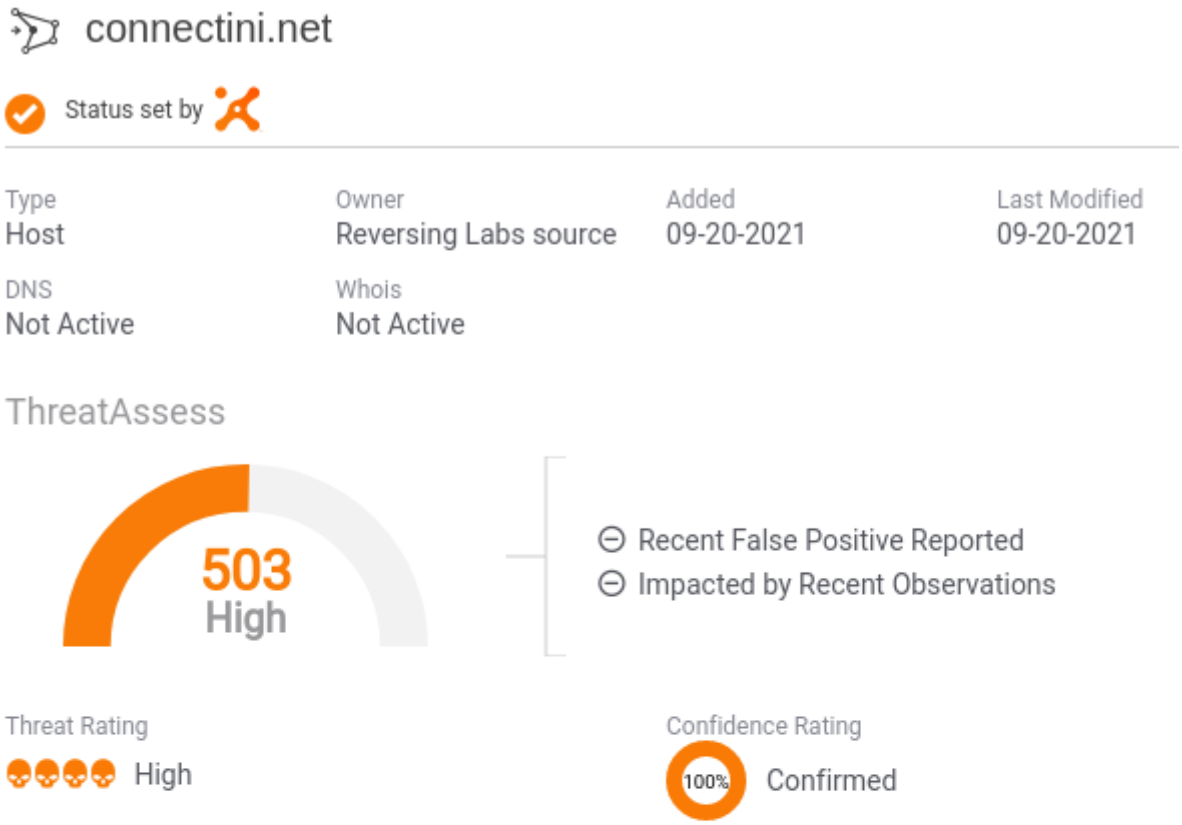
Select Feed:
To select explicitly only the ReversingLabs source, you can deselect all others and leave only the ReversingLabs source selected.



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	💀💀💀

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



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

8. Support

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