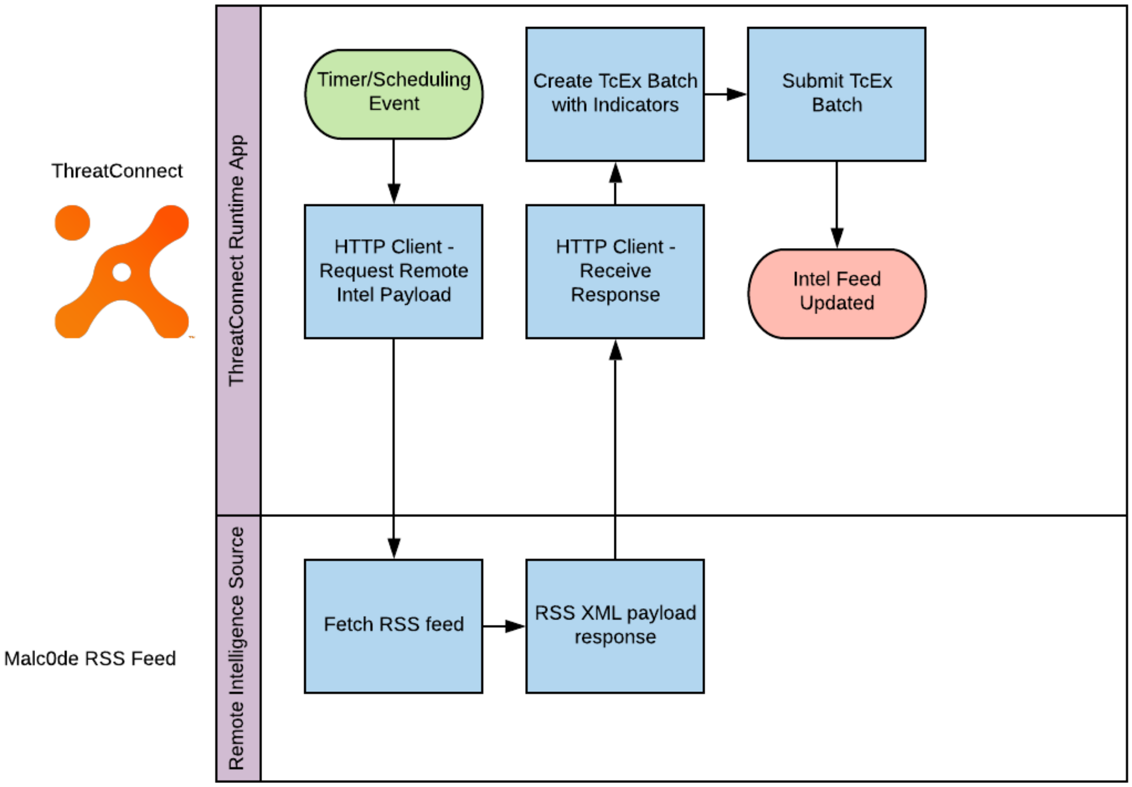
ThreatConnect Malc0de Threat Intelligence Integration v1.0.4 User Guide

Contents

1. Introduction

This integration consists of consuming the Malc0de database feed in RSS format and importing the data as threat groups with associated indicators into the ThreatConnect Platform as a Threat Intelligence feed. A high level run of the Malc0de Threat intelligence feed is shown below.


ThreatConnect
Malc0de RSS Feed
ThreatConnect Runtime App
Remote Intelligence Source
Timer/Scheduling Event
HTTP Client - Request Remote Intel Payload
Create TcEx Batch with Indicators
HTTP Client - Receive Response
Submit TcEx Batch
Intel Feed Updated
Fetch RSS feed
RSS XML payload response

2. Release Notes

App Version	Release Date	Details
1.0.3	3/9/2021	Initial Release
1.0.4	3/22/2021	Updated with threat rating and confidence parameters

3. Data Mapping

Malcode Types	**ThreatConnect Field**	**ThreatConnect Type**	**ThreatConnect Associated Group**	**Possible Values Example**	**Notes**
N/A	*Threat Group*	*Group*	*N/A*	*Name of malware binary and malware md5hash.* *zel.exe - 9323f1897112a5ff0affabc1829edf05*	*This is the base threat group that will contain the indicators in the RSS feed*
N/A	*First Seen*	*Attribute- Group*	*Threat*	*ISO8601 date with Z at the end.* *2020-11-25T15:51:00Z*	
N/A	*Last Seen*	*Attribute- Group*	*Threat*	*ISO8601 date with Z at the end.* *2020-11-25T15:51:00Z*	
N/A	*Description*	*Attribute-Group*	*Threat*	*Description of the malware including the binary name and md5sum.*	

<description> Country	Origin Country	Attribute- Group	Threat	Russian Federation	Country of Origin
<title >	Address	Associated Indicator	Threat	Ashleywalkerfuns.com Or 92.63.197.153	<title> can either be a host or address of the site containing the malicious executable
<description> URL	URL	Associated Indicator	Threat	ashleywalkerfuns.com/ama_orj_pr.exe	Direct link to the malicious executable
<description> IP	Address	Associated Indicator	Threat	92.63.197.153	IP of the host containing malicious executable
<description> ASN	ASN	Associated Indicator	Threat	29182	Autonomous System Number
<description> MD5	File	Associated Indicator	Threat	a267bf9e58726a34a91c365b61e1424a	MD5 Hash of the malicious executable
N/A	First Seen	Attribute - indicators	N/A	ISO8601 date with Z at the end. 2020-11-25T15:51:00Z	
N/A	Last Seen	Attribute - indicators	N/A	ISO8601 date with Z at the end. 2020-11-25T15:51:00Z	

4. Configuration Requirements

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

5. Job App Installation

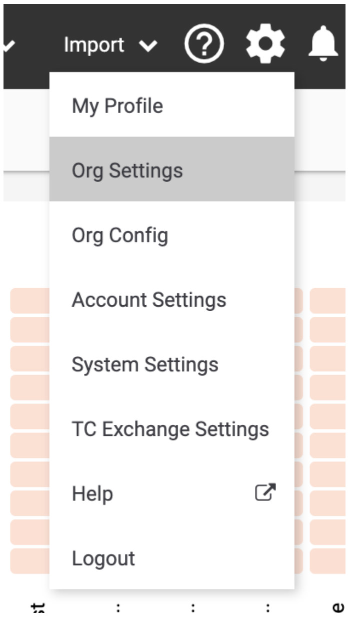
For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

6. ThreatConnect Job Configuration

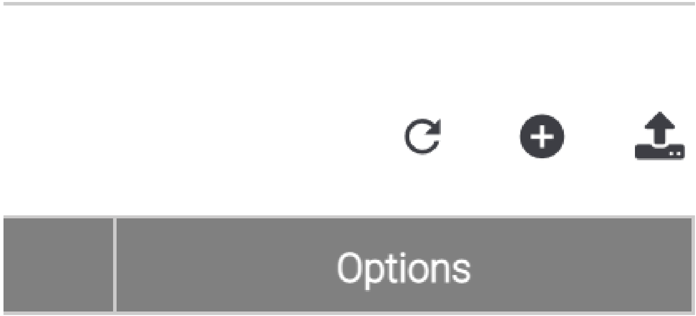
The ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer can run the Malc0de Threat Intelligence feed as frequently as they desire. The Malc0de RSS feed is quite small and so running the feed very frequently does not affect the performance of the ThreatConnect Platform.

**Note that these steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.

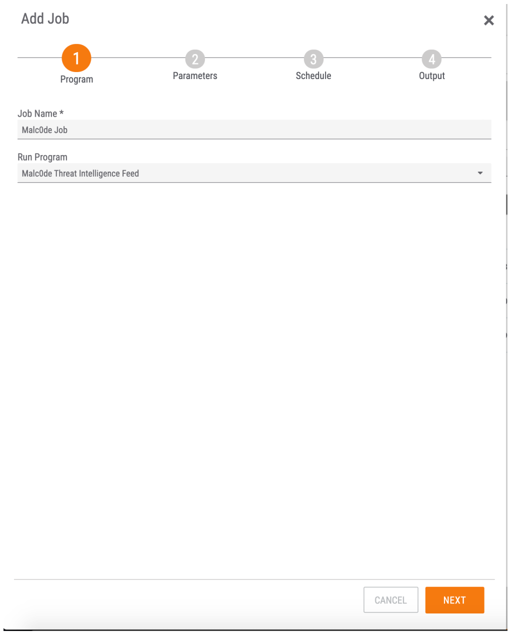
1. Login to the ThreatConnect Platform and Navigate to the Org Settings page.



2. Click the Apps tab and click on the plus symbol on the right hand side above the options column.



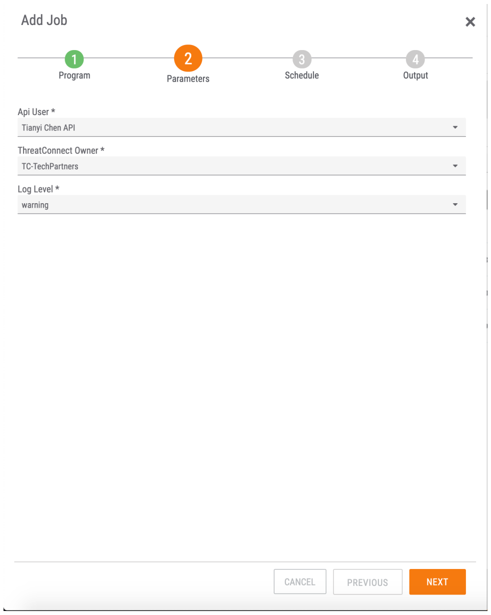
3. The add job screen will spear. Enter a name for the Job Name field and choose the Malc0de Threat Intelligence Feed to run.



Job Name *
Malc0de Job

Run Program
Malc0de Threat Intelligence Feed

4. Choose an API user to use, and the ThreatConnect Owner of the data.

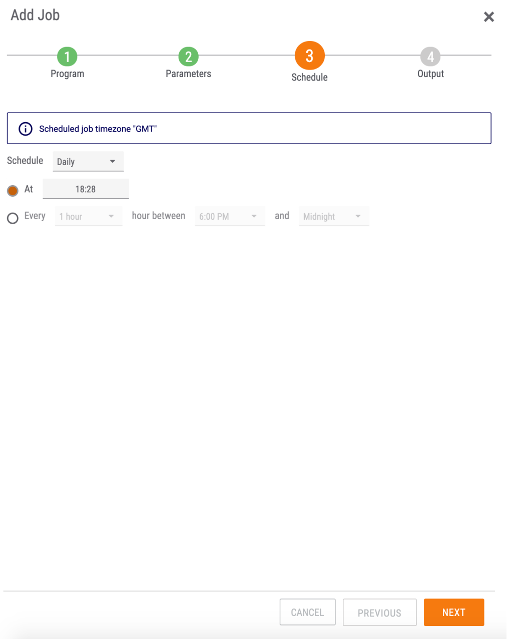


Api User *
Tianyi Chen API

ThreatConnect Owner *
TC-TechPartners

Log Level *
warning

5. Configure the scheduling for the app.



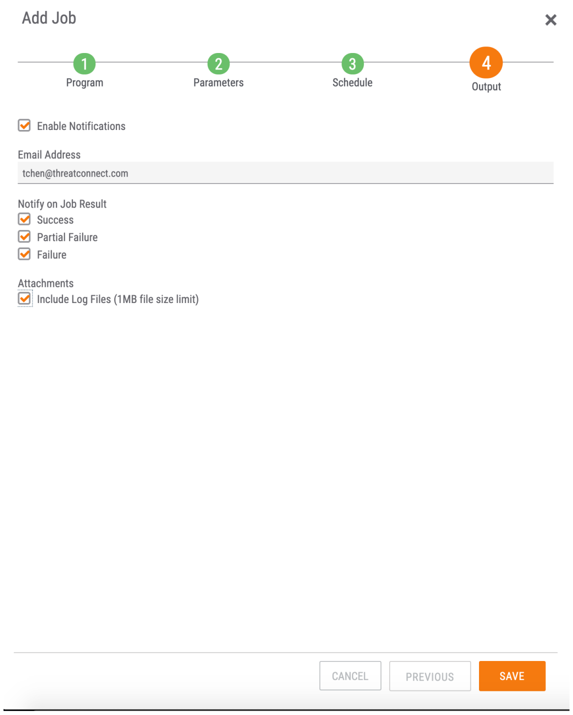
Scheduled job timezone "GMT"

Schedule Daily

● At 18:28

○ Every 1 hour hour between 6:00 PM and Midnight

6. Configure the output of the app. Notifications can be emailed to the user depending on their preferences.



Add Job

☑ Enable Notifications

Email Address

tchen@threatconnect.com

Notify on Job Result

☑ Success

☑ Partial Failure

☑ Failure

Attachments

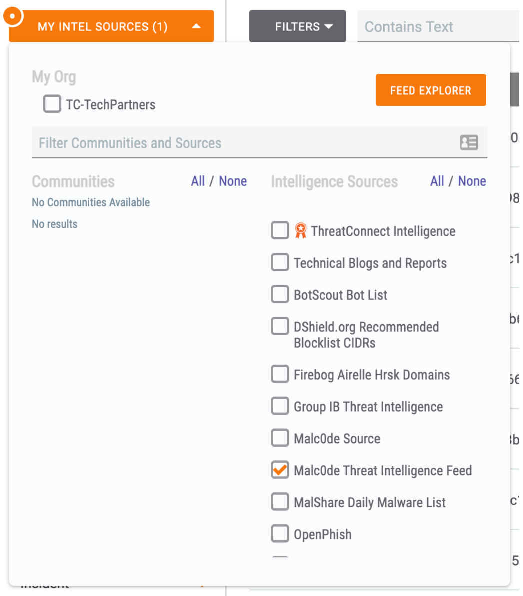
☑ Include Log Files (1MB file size limit)

7. Browsing Malc0de Threat Intelligence Feed

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

- https://training.threatconnect.com/learn/article/browse-kb-article

1. Navigate to the browse page and check to make sure that the Malc0de Threat Intelligence Feed is checked.



My Org

☐ TC-TechPartners

Communities

No Communities Available

No results

Intelligence Sources

☐ ThreatConnect Intelligence

☐ Technical Blogs and Reports

☐ BotScout Bot List

☐ DShield.org Recommended Blocklist CIDRs

☐ Firebog Airelle Hrsk Domains

☐ Group IB Threat Intelligence

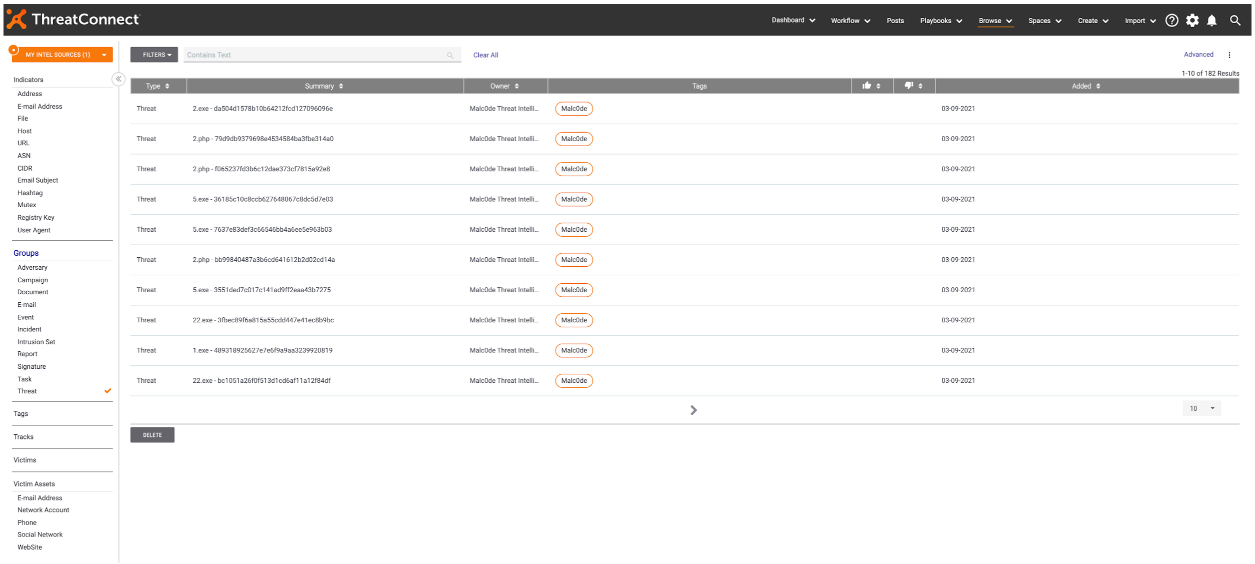
☐ Malc0de Source

☑ Malc0de Threat Intelligence Feed

☐ MalShare Daily Malware List

☐ OpenPhish

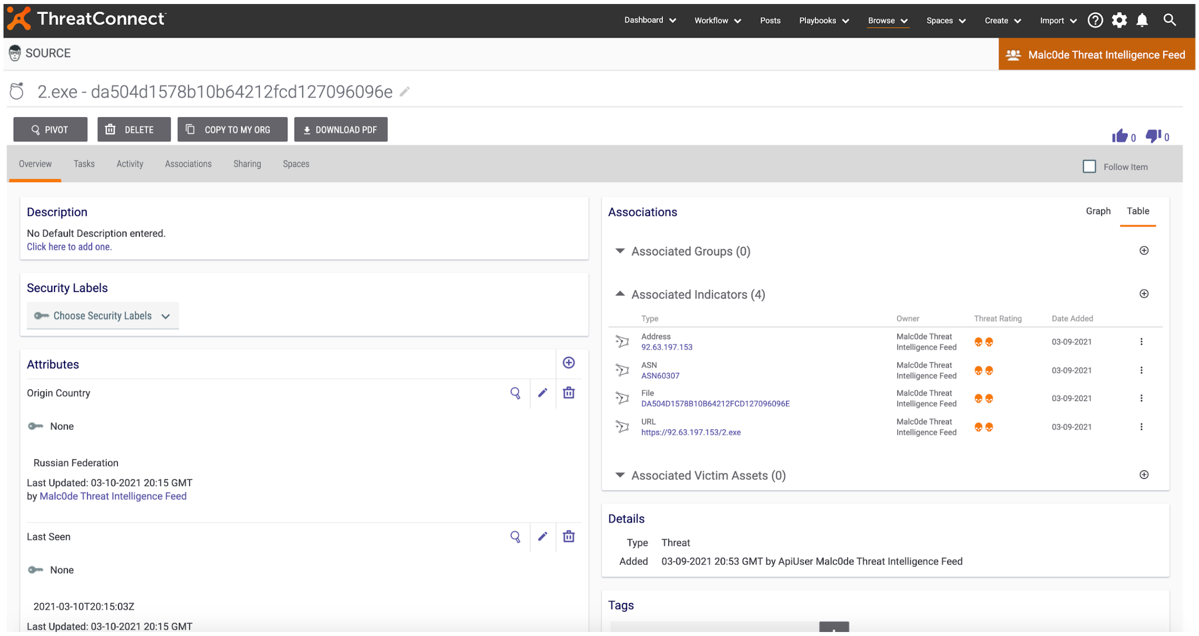
2. To browse malware threats from Malc0de, select to browse all groups or only the threat group.



1-10 of 182 Results

Type	Summary	Owner	Tags	👍	👎	Added
Threat	2.exe - da504d1578b10b64212fcd127096096e	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	2.php - 79d9db9379698e4534584ba3fbe314a0	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	2.php - f065237fd3b6c12dae373cf7815a92e8	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	5.exe - 36185c10c8ccb627648067c8dc5d7e03	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	5.exe - 7637e83def3c66546bb4a6ee5e963b03	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	2.php - bb99840487a3b6cd641612b2d02cd14a	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	5.exe - 3551ded7c017c141ad9ff2eaa43b7275	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	22.exe - 3fbec89f6a815a55cdd447e41ec8b9bc	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	1.exe - 489318925627e7e6f9a9aa3239920819	Malc0de Threat Intelli...	Malc0de			03-09-2021
Threat	22.exe - bc1051a26f0f513d1cd6af11a12f84df	Malc0de Threat Intelli...	Malc0de			03-09-2021

3. Threats will appear with the malware binary name and the md5 hash of that binary. Threats will also show the associated indicators from the Malc0de RSS feed.



SOURCE

2.exe - da504d1578b10b64212fcd127096096e

Description

No Default Description entered.
Click here to add one.

Security Labels

Choose Security Labels

Attributes

Origin Country

None

Russian Federation

Last Updated: 03-10-2021 20:15 GMT
by Malc0de Threat Intelligence Feed

Last Seen

None

2021-03-10T20:15:03Z

Last Updated: 03-10-2021 20:15 GMT

Associations

Associated Groups (0)

Associated Indicators (4)

Type	Owner	Threat Rating	Date Added
Address 92.63.197.153	Malc0de Threat Intelligence Feed	●●	03-09-2021
ASN ASN60307	Malc0de Threat Intelligence Feed	●●	03-09-2021
File DA504D1578B10B64212FCD127096096E	Malc0de Threat Intelligence Feed	●●	03-09-2021
URL https://92.63.197.153/2.exe	Malc0de Threat Intelligence Feed	●●	03-09-2021

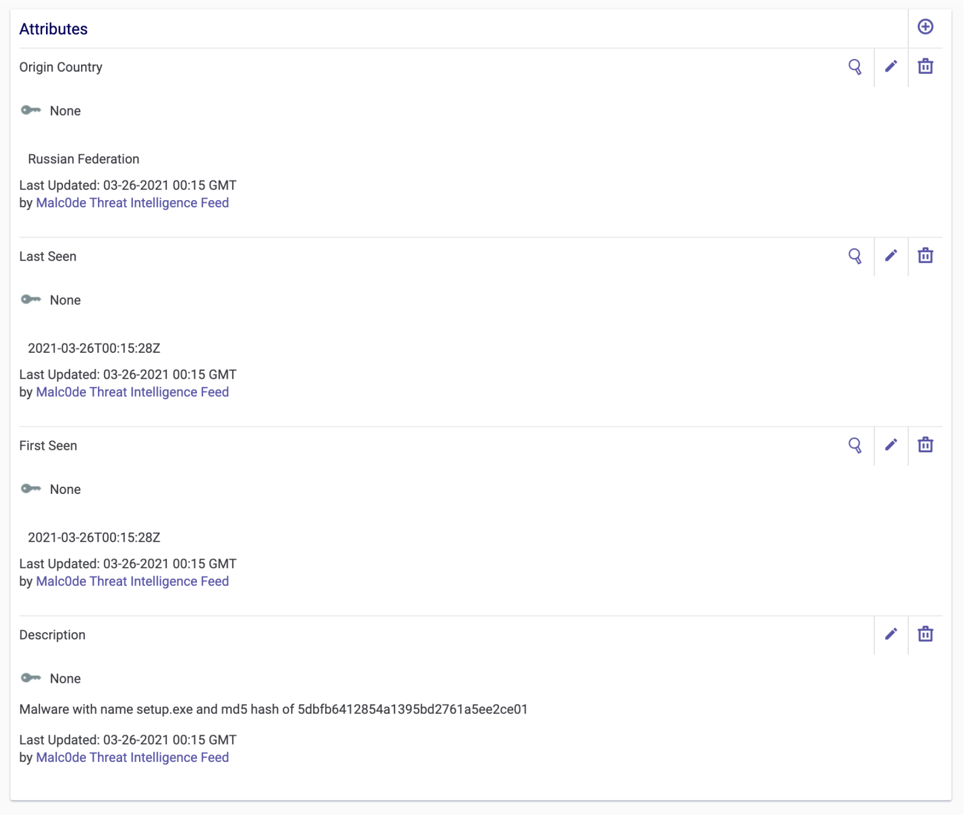
Associated Victim Assets (0)

Details

Type Threat
Added 03-09-2021 20:53 GMT by ApiUser Malc0de Threat Intelligence Feed

Tags

4. Threats will contain the attributes shown below such as First Seen, Last Seen, Origin Country, and Description.



Attributes

Origin Country

None

Russian Federation

Last Updated: 03-26-2021 00:15 GMT
by Malc0de Threat Intelligence Feed

Last Seen

None

2021-03-26T00:15:28Z

Last Updated: 03-26-2021 00:15 GMT
by Malc0de Threat Intelligence Feed

First Seen

None

2021-03-26T00:15:28Z

Last Updated: 03-26-2021 00:15 GMT
by Malc0de Threat Intelligence Feed

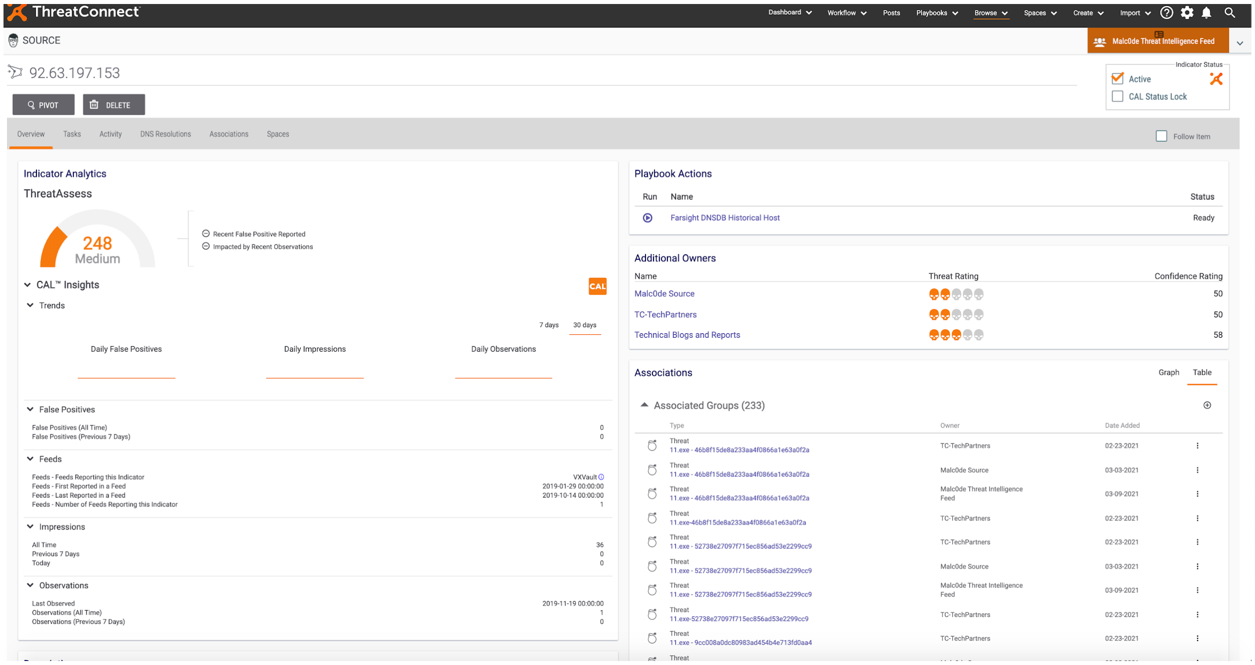
Description

None

Malware with name setup.exe and md5 hash of 5dbfb6412854a1395bd2761a5ee2ce01

Last Updated: 03-26-2021 00:15 GMT
by Malc0de Threat Intelligence Feed

5. Associated Indicators can also be browsed from the browse page or from the Threat group.



92.63.197.153

Indicator Status

☑ Active

□ CAL Status Lock

□ Follow Item

Indicator Analytics

ThreatAssess

248 Medium

⊖ Recent False Positive Reported

⊖ Impacted by Recent Observations

CAL™ Insights

Trends

7 days 30 days

Daily False Positives | Daily Impressions | Daily Observations

False Positives

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

Feeds

Feeds - Feeds Reporting this Indicator	VXVault
Feeds - First Reported in a Feed	2019-01-29 00:00:00
Feeds - Last Reported in a Feed	2019-10-14 00:00:00
Feeds - Number of Feeds Reporting this Indicator	1

Impressions

All Time	36
Previous 7 Days	0
Today	0

Observations

Last Observed	2019-11-19 00:00:00
Observations (All Time)	1
Observations (Previous 7 Days)	0

Playbook Actions

Run	Name	Status
▶	Farsight DNSDB Historical Host	Ready

Additional Owners

Name	Threat Rating	Confidence Rating
Malc0de Source	●●○○○	50
TC-TechPartners	●●○○○	50
Technical Blogs and Reports	●●●○○	58

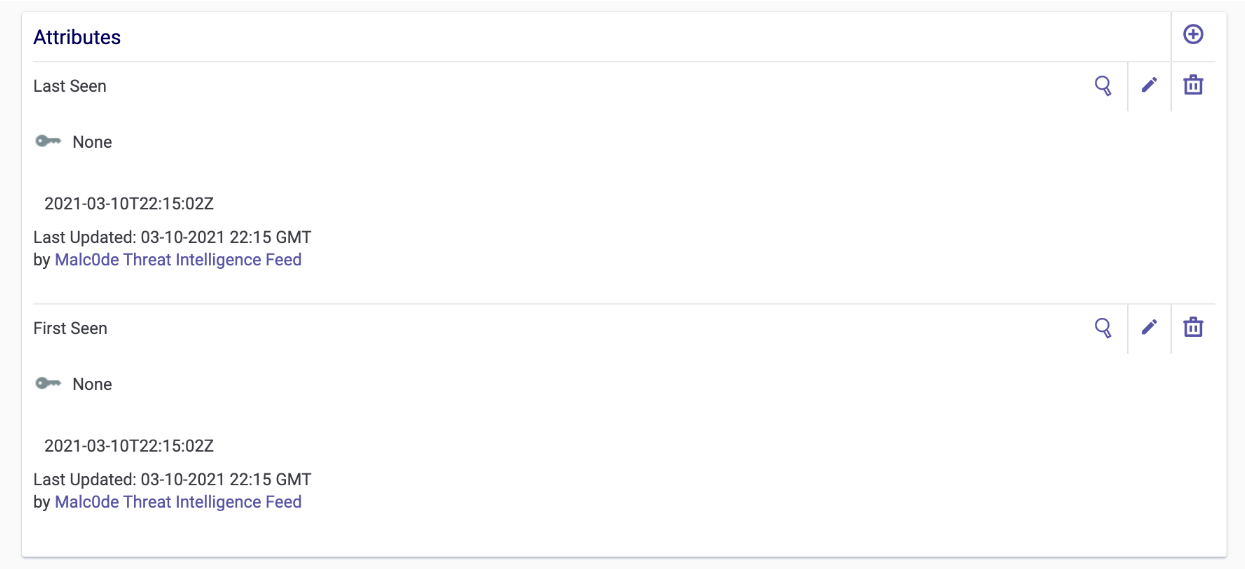
Associations

Graph Table

Associated Groups (233)

Type	Owner	Date Added
Threat 11.exe - 46b8f15de8a233aa4f0866a1e63a0f2a	TC-TechPartners	02-23-2021
Threat 11.exe - 46b8f15de8a233aa4f0866a1e63a0f2a	Malc0de Source	03-03-2021
Threat 11.exe - 46b8f15de8a233aa4f0866a1e63a0f2a	Malc0de Threat Intelligence Feed	03-09-2021
Threat 11.exe-46b8f15de8a233aa4f0866a1e63a0f2a	TC-TechPartners	02-23-2021
Threat 11.exe - 52738e27097f715ec856ad53e2299cc9	TC-TechPartners	02-23-2021
Threat 11.exe - 52738e27097f715ec856ad53e2299cc9	Malc0de Source	03-03-2021
Threat 11.exe - 52738e27097f715ec856ad53e2299cc9	Malc0de Threat Intelligence Feed	03-09-2021
Threat 11.exe-52738e27097f715ec856ad53e2299cc9	TC-TechPartners	02-23-2021
Threat 11.exe - 9cc008a0dc80983ad454b4e713fd0aa4	TC-TechPartners	02-23-2021
Threat		

6. Associated Indicators will contain attributes such as First Seen and Last Seen.



Attributes

Last Seen

None

2021-03-10T22:15:02Z

Last Updated: 03-10-2021 22:15 GMT
by Malc0de Threat Intelligence Feed

First Seen

None

2021-03-10T22:15:02Z

Last Updated: 03-10-2021 22:15 GMT
by Malc0de Threat Intelligence Feed

8. Support

Please contact techpartnersupport@threatconnect.com for any support related inquiries regarding the Malc0de Threat Intelligence ThreatConnect Integration.