

ThreatQuotient

A Securonix Company



Ransomware.live CDF

Version 1.0.0

October 19, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Ransomware.live Victims Parameters.....	9
Ransomware.live Groups Parameters.....	10
ThreatQ Mapping	12
Ransomware.live Victims.....	12
Ransomware.live Groups.....	15
Average Feed Run	19
Ransomware.live Victims.....	19
Ransomware.live Groups.....	19
Known Issues / Limitations	21
Change Log	22

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein.

ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com

Support Web: <https://ts.securonix.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version 1.0.0

Compatible with ThreatQ Versions $\geq 6.5.0$

Support Tier ThreatQ Supported

Introduction

The Ransomware.live integration provides threat intelligence on ransomware victims and groups, helping teams monitor ongoing campaigns and understand threat actors' tools, tactics, techniques, and ransom notes. It ingests victim sightings and group profiles from Ransomware.live into ThreatQ.

The integration provides the following feeds:

- **Ransomware.live Victims** - ingests ransomware victim sightings as Events and, optionally, victim Identities.
- **Ransomware.live Groups** - ingests ransomware group profiles and related tools, ATT&CK techniques, YARA rules, and ransom notes.

The integration ingests the following system object types:

- Adversaries
- Attack Patterns
- Events
- Identities
- Malware
- Notes
- Signatures
- Tools

Prerequisites

The following is required to run the integration:

- A Ransomware.live API Key. A Ransomware.live account is required to access the API.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the file on your local machine
6. Select the individual feeds to install, when prompted and click **Install**.



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed(s) will be added to the integrations page. You will still need to [configure and then enable](#) the feed.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Ransomware.live Victims Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Ransomware.live API key. You can obtain an API key by creating an account on Ransomware.live.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Country Code Filter	Enter a line-separated list of country codes to filter victims. Each line should contain a single two-digit country code. The feed returns results matching at least one specified country code. Leave this field blank to ingest victims from all countries. When used with the Industry Filter, the feed returns results matching at least one specified country code or at least one specified industry.
Industry Filter	Enter a line-separated list of industries to filter victims. Each line should contain a single industry name. The feed returns results matching at least one specified industry. Leave this field blank to ingest victims from all industries. Refer to the documentation for a list of available industry names. When

PARAMETER	DESCRIPTION
	used with the Country Code Filter, the feed returns results matching at least one specified industry or at least one specified country code.
Ingest Victims As	Select how victim names are ingested into ThreatQ: ◦ Identities (default) — Aligns victim names with the STIX data model and allows context to be assigned to each victim in the Identity object or profile. ◦ Attributes — Makes victim names available in attribute-based dashboard widgets. When victims are ingested only as attributes, their context is stored in the ransomware activity event description.

Ransomware.live Groups Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Ransomware.live API key. You can obtain an API key by creating an account on Ransomware.live.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Skip Groups Without Victims	Check this box to skip groups without victims. Enabling this option reduces the number of API requests made by the feed. <i>Default: true</i>
Fetch YARA Rules	Check this box to fetch YARA rules related to each group. Enabling this option adds one API request for each group. <i>Default: false</i>
Fetch Ransom Notes	Check this box to fetch ransom notes related to each group. Enabling this option adds one API request for each group, plus requests for each ransom note associated with the group. <i>Default: false</i>

-
5. Review any additional settings, make any changes if needed, and click on **Save**.
 6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Ransomware.live Victims

The Ransomware.live Victims feed ingests ransomware victims sightings from the Ransomware.live API. Each sighting will be ingested as an Event object with the Ransomware Victim type. Events will receive a rich description containing details about the ransomware attack, as well as attribution relating to the ransomware group, target victim's industry, and country.

GET <https://api-pro.ransomware.live/victims?year=2026&month=06>

Sample Response:

```
{
  "client": "acme@gmail.com",
  "filters": {
    "group": null,
    "sector": null,
    "country": null,
    "year": "2026",
    "month": "05",
    "date": "discovered"
  },
  "count": 789,
  "victims": [
    {
      "id": "R3J1cG8gTWF1w6FAYnJhdm94",
      "discovered": "2026-05-31T22:20:55.989247+00:00",
      "website": "www.grupomaua.com.br",
      "country": "BR",
      "activity": "Manufacturing",
      "description": "Operates in the construction, real
estate, energy, and infrastructure sectors.",
      "post_url": "http://
bravoxxcwcfz5qk43ychgveprpd5mw5hvxfs4a2uz2okx7mumiht4fzyd.onion/blog/
2979a59a-c02f-4a3b-804f-2b1d8cabefd8",
      "ransom": null,
      "data_size": null,
      "screenshot": "https://images.ransomware.live/victims/
f0f951bb1e69d286d1f7ce05b1cfeaf7.png",
      "infostealer": "",

```

```

        "press": null,
        "permalink": "https://www.ransomware.live/id/
R3J1cG8gTWF1w6FAYnJhdm94",
        "attackdate": "2026-05-31T22:20:42.870095+00:00",
        "victim": "Grupo Mauá",
        "group": "bravox"
    },
    {
        "id":
"TGFrZSBXYXNoaW5ndG9uIFNjaG9vbCBEaXN0cm1jdEBjbWRvcmdhbm16YXRpb24=",
        "discovered": "2026-05-31T10:50:12.167640+00:00",
        "website": "lwsd.wednet.edu",
        "country": "US",
        "activity": "Education",
        "description": "Founded in 1914, Lake Washington School
District is the administrative body responsible for planning and
managing public education for 33 elementary, 14 middle, and 9 high
schools. It serves communities of Kirkland, Redmond and about half of
Sammamish. The company is headquartered in Redmond, Washington.",
        "post_url": "",
        "ransom": null,
        "data_size": null,
        "screenshot": "",
        "infostealer": {
            "update": "2026-05-31T10:50:10",
            "employees": 0,
            "users": 0,
            "thirdparties": 29,
            "employees_url": 0,
            "users_url": 0,
            "last_employee_compromised": null,
            "last_user_compromised": null,
            "infostealer_stats": {}
        },
        "press": null,
        "permalink": "https://www.ransomware.live/id/
TGFrZSBXYXNoaW5ndG9uIFNjaG9vbCBEaXN0cm1jdEBjbWRvcmdhbm16YXRpb24=",
        "attackdate": "2026-05-31T10:50:10.639173+00:00",
        "victim": "Lake Washington School District",
        "group": "cmdorganization"
    }
]

```

```
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's `.victims` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.victim, .activity, .group, .country</code>	Event Title	Ransomware Victim	<code>.attackdate</code>	Victim: Tecfi SpA \\\ Business Services/IT \\\ Group: dragonforce	Fields are concatenated together and will only be included if they are present and an allowed value.
<code>.victim</code>	Event Attribute	Victim	<code>.discovered</code>	Lake Washington School District	Added when the user-selects to ingest victims as attributes
<code>.attackdate</code>	Event Attribute	Attack Date	<code>.discovered</code>	March 05, 2026	Converted from an ISO 8601 date format
<code>.discovered</code>	Event Attribute	Discovered Date	<code>.discovered</code>	March 07, 2026	Converted from an ISO 8601 date format
<code>.country</code>	Event Attribute	Target Country Code	<code>.discovered</code>	US	N/A
<code>.country</code>	Identity Attribute	Country Code	<code>.discovered</code>	US	Added when ingesting victims as Identity objects
<code>.activity</code>	Event Attribute	Target Industry	<code>.discovered</code>	Education	N/A
<code>.website</code>	Event Attribute	Victim Website	<code>.discovered</code>	N/A	N/A

Ransomware.live Groups

The Ransomware.live Groups feed ingests information pertaining to the ransomware groups responsible for the attacks on the victims tracked in the Ransomware.live Victims feed. Groups will be ingested as Adversary objects and will be linked to relevant tools, ransom notes, and MITRE ATT&CK techniques.

The first request to Ransomware.live's API will be to fetch the list of ransomware groups:

GET `https://api-pro.ransomware.live/groups`

Sample Response:

```
{
  "client": "acme@gmail.com",
  "count": 349,
  "groups": [
    {
      "group": "0apt",
      "altname": null,
      "victims": 0
    },
    {
      "group": "0day syndicate",
      "altname": null,
      "victims": 5
    },
    {
      "group": "0mega",
      "altname": null,
      "victims": 7
    }
  ]
}
```

For each group returned by the above request, the feed will then make a request to get the full group details:

GET `https://api-pro.ransomware.live/group/{{ group_name }}`

Sample Response:

```
{
  "client": "acme@gmail.com",
  "group": "0day Syndicate",
  "description": null,
  "added_date": null,
  "victims": 5,
  "firstseen": "2026-05-28T09:03:51.344156+00:00",
  "lastseen": "2026-05-29T13:50:02.458830+00:00",
  "ttps": [],
  "vulnerabilities": [],
  "tools": {},
  "locations": [
    {
      "fqdn":
"odaygplp3zhyx7zl45egetl6dzc4reduisnoyym34rjdmaryfaz5doqd.onion",
      "title": "0day | Command Ops",
      "slug": "http://
odaygplp3zhyx7zl45egetl6dzc4reduisnoyym34rjdmaryfaz5doqd.onion",
      "type": "DLS",
      "available": true
    }
  ],
  "has_negotiations": false,
  "negotiation_count": 0,
  "has_ransomnote": false,
  "ransomnotes_count": 0,
  "url": "https://www.ransomware.live/group/0daysyndicate"
}
```

When Fetch Ransom Notes is enabled and a group has ransom notes, the feed retrieves the note names:

GET `https://api-pro.ransomware.live/ransomnotes/{{ group_name }}`

Sample Response:

```
{
  "client": "acme@gmail.com",
  "group": "blackbyte",
  "count": 4,
  "ransomnotes": [
    "BB_Readme",
    "BB_Readme2",
    "BB_Readme_[rand]",
  ]
}
```

```

    "blackbyte_v2"
  ]
}

```

For each ransom note, the feed will then make a request to get the full ransom note details:

```
GET https://api-pro.ransomware.live/ransomnotes/{{ group_name }}/{{ ransomnote_name }}
```

When Fetch YARA Rules is enabled and a group has YARA rules, the feed retrieves them with this request:

```
GET https://api-pro.ransomware.live/yara/{{ group_name }}
```

Sample Response:

```

{
  "client": "acme@gmail.com",
  "group": "lockbit",
  "count": 1,
  "rules": [
    {
      "filename": "lockbit.yar",
      "content": "{{ YARA file content }}"
    }
  ]
}

```

ThreatQ provides the following default mapping for this feed:



Paths refer to the corresponding endpoint response or the group detail response. Related YARA rules and ransom notes are optional and are fetched only when enabled in the feed configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
groups[].group	Adversary Name	N/A	.added_date	lockbit	N/A
group.tools[key]	Tool Value	N/A	.added_date	Hydra	N/A
group.ttps[key].techniques[].technique_id	Attack Pattern Value	N/A	.added_date	T1024 - Technique Name	TID mapped to corresponding ThreatQ object
group.*	Adversary Description	N/A	N/A	N/A	Various fields concatenated to build a rich text description

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
yara.rules[].content	Signature Name/Value	YARA	.added_date	N/A	Rule is parsed for name, value, and supporting context
ransomnotes[].content	Note Value	N/A	.added_date	N/A	N/A

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Ransomware.live Victims

METRIC	RESULT
Run Time	1 minute
Adversaries	13
Events	21
Event Attributes	78
Identities	21
Identity Attributes	46
Malware	14

Ransomware.live Groups

METRIC	RESULT
Run Time	6 minutes
Adversaries	277
Attack Patterns	276

METRIC	RESULT
Malware	1
Notes	206
Signatures	251
Signature Attributes	1,265
Tools	274
Tool Attributes	275

Known Issues / Limitations

- The **Ransomware.live Groups** feed defaults to a 14-day schedule. Because the API does not support filtering groups by date, each run checks all eligible groups. Fetching optional YARA rules and ransom notes can generate many additional API requests, so do not schedule the feed more frequently than once a week.

Change Log

- **Version 1.0.0**
 - Initial release