

# ThreatQuotient

A Securonix Company



## Abnormal Security Threat Intel Blog CDF

Version 1.0.0

August 04, 2025

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Installation..... 7

Configuration ..... 8

ThreatQ Mapping..... 10

    Abnormal Security Threat Intel Blog ..... 10

Average Feed Run..... 19

Known Issues / Limitations ..... 20

Change Log ..... 21

# 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 © 2025 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:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.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 | >= 5.5.0          |
| Support Tier                     | ThreatQ Supported |

# Introduction

The Abnormal Security Threat Intel Blog CDF enables analysts to ingest the latest security news and research from the Abnormal Security team in the form of advisories, bulletins, and analyses posted on the Abnormal Security blog .

The integration provides the following feed:

- **Abnormal Security Threat Intel Blog** - ingests Abnormal Security Threat Intel blogs as ThreatQ reports and related CVEs.

The integration ingests the following object types:

- Indicators
- Reports
- Vulnerabilities

# 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



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 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:

| PARAMETER               | DESCRIPTION  |
|-------------------------|--|
| <b>Blog Types</b>       | <p>Select the blog types to fetch and ingest into ThreatQ. Options include:</p> <ul style="list-style-type: none"> <li>◦ Threat Intel <i>(default)</i></li> <li>◦ Attack Stories <i>(default)</i></li> <li>◦ Credential Phishing <i>(default)</i></li> <li>◦ Vendor Email Compromise</li> <li>◦ Business Email Compromise</li> <li>◦ Account Takeover</li> </ul> |
| <b>Parsed IOC Types</b> | <p>Select the IOC types you would like to automatically parse from the content. The only option available at this time is CVE.</p>   |
| <b>Ingest CVEs As</b>   | <p>Select the entity type to ingest CVE IDs as into the ThreatQ platform. Options include:</p> <ul style="list-style-type: none"> <li>◦ Vulnerabilities <i>(default)</i></li> <li>◦ Indicators</li> </ul>  |
|                         |  This parameter is only accessible if the CVE option is selected for the <b>Parsed IOC Types</b> parameter.   |



## PARAMETER

## DESCRIPTION

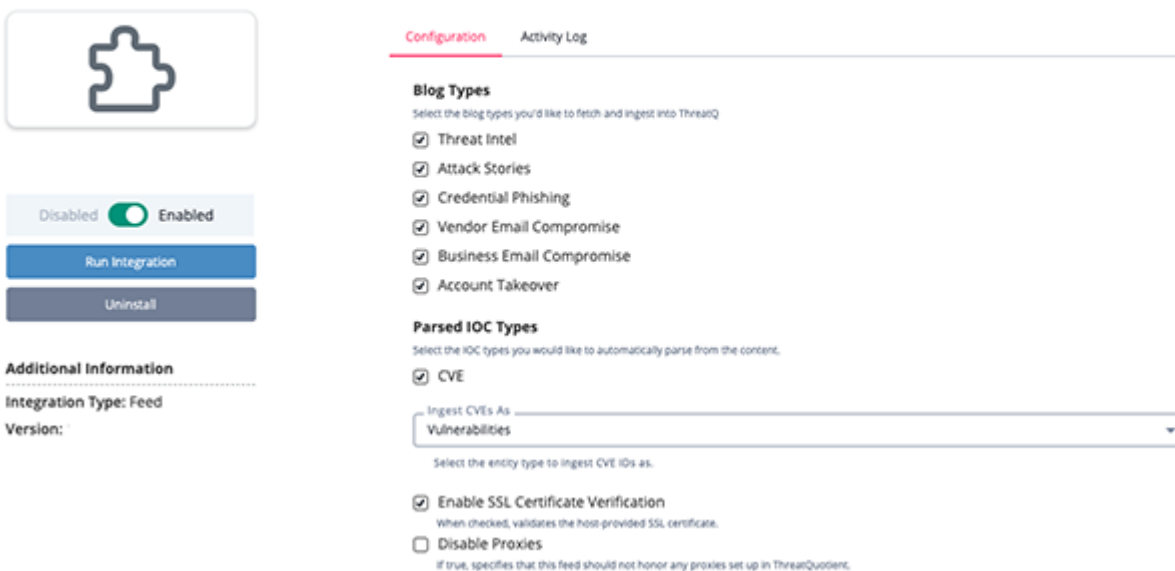
Enable SSL Certificate Verification

Enable this parameter if the feed should validate the host-provided SSL certificate.

Disable Proxies

Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

### ◀ Abnormal Security Threat Intel Blog



Configuration Activity Log

**Blog Types**  
Select the blog types you'd like to fetch and ingest into ThreatQ

- ☒ Threat Intel
- ☒ Attack Stories
- ☒ Credential Phishing
- ☒ Vendor Email Compromise
- ☒ Business Email Compromise
- ☒ Account Takeover

**Parsed IOC Types**  
Select the IOC types you would like to automatically parse from the content.

- ☒ CVE

Ingest CVEs As:

Select the entity type to ingest CVE IDs as.

- ☒ Enable SSL Certificate Verification  
When checked, validates the host-provided SSL certificate.
- ☐ Disable Proxies  
If true, specifies that this feed should not honor any proxies set up in ThreatQuotient.

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

## Abnormal Security Threat Intel Blog

The Abnormal Security Threat Intel Blog feed pulls blog posts from Abnormal Security's website and ingests them into ThreatQ as report objects.

GET <https://abnormalsecurity.com/blog>

The output of this request is HTML, which is parsed for a build ID that is used to fetch the blog posts.

GET [https://abnormalsecurity.com/\\_next/data/{{ build\\_id }}/blog/category/threat-intel.json](https://abnormalsecurity.com/_next/data/{{ build_id }}/blog/category/threat-intel.json)

For each of the posts returned, fetch the corresponding blog post.

GET [https://abnormalsecurity.com/\\_next/data/{{ build\\_id }}/blog/{{ uri }}.json](https://abnormalsecurity.com/_next/data/{{ build_id }}/blog/{{ uri }}.json)

### Sample Request:

```
{
  "pageProps": {
    "navigation": {
      "primaryNavigation": [],
      "primaryCallToActions": [],
      "footerPrimaryNavigation": []
    },
    "pageEntry": {},
    "persistentNav": {},
    "post": {
      "id": "129543",
      "title": "A Deep Dive into Active Ransomware Groups",
      "slug": "deep-dive-active-ransomware-groups",
      "uri": "blog/deep-dive-active-ransomware-groups",
      "url": "https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups",
      "sectionHandle": "blog",
      "typeHandle": "default",
      "image": [
        {
          "title": "B 05 27 22 Active Ransomware Groups",
          "entryThumb": [
            {
              "width": 760,
              "height": 760,
              "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/images/blog/B-05.27.22-Active-Ransomware-Groups.png?w=760&h=760&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-x=0.5&fp-y=0.5&dm=1675097662&s=d3a7f36f6877ea212f0a5f65fe9bee9e"
            },
            {
              "width": 10,
              "height": 10,
              "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/images/blog/B-05.27.22-Active-Ransomware-Groups.png?w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-x=0.5&fp-y=0.5&dm=1675097662&s=afdbe3ce983855e2b30378ce956f0137"
            },
            {
              "width": 90,
              "height": 90,
```

```

        "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/
images/blog/B-05.27.22-Active-Ransomware-Groups.png?
w=90&h=90&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-x=0.5&fp-
y=0.5&dm=1675097662&s=920e2d35be4021347e6819adeb070dc2"
    }
    ]
  },
  "postDate": "2022-05-27T10:30:00-07:00",
  "showSummary": true,
  "summary": "Here's an in-depth analysis of the 62 most prominent ransomware groups and
their activities since January 2020.",
  "blogCategory": [
    {
      "id": "5721",
      "title": "Threat Intel",
      "slug": "threat-intel",
      "uri": "blog/category/threat-intel",
      "groupId": 2,
      "groupHandle": "blogCategories",
      "order": 28
    }
  ],
  "postAuthors": [
    {
      "id": "43016",
      "title": "Crane Hassold",
      "slug": "crane-hassold",
      "uri": "blog/author/crane-hassold",
      "groupId": 1,
      "groupHandle": "postAuthors",
      "order": 20,
      "image": [
        {
          "id": "59848",
          "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/
images/blog/author-crane-hassold.png?
w=30&h=30&auto=compress%2Cformat&fit=crop&dm=1675097631&s=091b729bca6d4612409ad02fe571b190",
          "title": "Author crane hassold",
          "width": 30,
          "height": 30,
          "extension": "png",
          "size": "456806",
          "path": "blog/author-crane-hassold.png",
          "blur": [
            {
              "url": "https://optimise2.assets-servd.host/gifted-zorilla/
production/images/blog/author-crane-hassold.png?w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-
x=0.5&fp-y=0.5&dm=1675097631&s=a88e084f1249adc8880f02e79a4e9fa8"
            }
          ],
          "svgContent": ""
        }
      ]
    }
  ],
  "contentSections": [
    {
      "id": "181596",
      "typeId": 16,
      "typeHandle": "bodyText",
      "visibleAfterAccess": false,
      "bodyText": "<p dir=\"ltr\">Earlier this year, our threat intelligence team at
Abnormal published a report on the <a href=\"https://abnormalsecurity.com/resources/ransomware-

```

victims-threat-actors?PS=organic%20website\" target=\"\_blank\" rel=\"noreferrer noopener\">evolution of ransomware</a>. The report explored the growing threat of ransomware, including the primary factors influencing the ransomware landscape, with insight into who is being <a href=\"https://abnormalsecurity.com/blog/ransomware-victims\" target=\"\_blank\" rel=\"noreferrer noopener\">targeted across various industries and locations</a>.</p>\n<p dir=\"ltr\">The report also included a deep dive into the threat actors themselves, their activities, and a few reasons why we've seen a 600% increase in the number of active groups since January 2020.<br /></p>"

```
    },
    {
      "id": "181597",
      "typeId": 15,
      "typeHandle": "heading",
      "visibleAfterAccess": false,
      "heading": "Pros and Cons of the Centralized Ransomware Ecosystem",
      "headingTag": "h2",
      "headingSize": "lg"
    }
  ],
  {
    "id": "181598",
    "typeId": 16,
    "typeHandle": "bodyText",
    "visibleAfterAccess": false,
    "bodyText": "<p dir=\"ltr\">Similar to what we saw in 2016 when ransomware saw
```

its initial global explosion, a growing number of minor threat groups have entered the scene—piggybacking on the success of the more established groups.</p>\n<p dir=\"ltr\">We tracked 62 different ransomware groups and their activities starting in January 2020. While some of these were merely rebranded variations of previous ransomware strains (such as Maze rebranding to Eggregor or DarkSide renaming itself BlackMatter), most of these groups are unique threats that have emerged for a few months at a time in smaller volumes.</p>\n<p dir=\"ltr\">The number of active ransomware groups each month has increased dramatically, growing from just three in February 2020 to a peak of 28 in November 2021.<br /></p>"

```
    },
    {
      "id": "181599",
      "typeId": 14,
      "typeHandle": "image",
      "visibleAfterAccess": false,
      "image": [
        {
          "id": "129822",
          "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/
```

images/blog/Monthly-Active-Ransomware-Groups.png?  
w=1536&h=812&auto=compress%2Cformat&fit=crop&dm=1675097662&s=45961ce07ef33174b0c839bfb680a033",  
"title": "Monthly Active Ransomware Groups",  
"width": 1536,  
"height": 812,  
"extension": "png",  
"size": "45997",  
"path": "blog/Monthly-Active-Ransomware-Groups.png",  
"blur": [  
 {  
 "url": "https://optimise2.assets-servd.host/gifted-zorilla/  
production/images/blog/Monthly-Active-Ransomware-Groups.png?  
w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-x=0.5&fp-  
y=0.5&dm=1675097662&s=fbf4a6de7e93e9cd4728bdf8b1959d5f"

```
  }
],
"svgContent": ""
},
"imageBlur": [
  {
    "url": ""
  }
],

```



```

        "caption": null,
        "captionPosition": "center"
    },
    {
        "id": "181600",
        "typeId": 16,
        "typeHandle": "bodyText",
        "visibleAfterAccess": false,
        "bodyText": "<p dir=\"ltr\">Five groups—Conti, LockBit, Pysa, REvil, and Maze/
Egregor—were responsible for more than half of all ransomware attacks over the past two years. Two
of those groups (Conti and LockBit) are still active today, and, as of Q1 2022, they make up almost
50% of the present <a href=\"https://abnormalsecurity.com/blog/ransomware-volume-drops-q1-2022\"
target=\"_blank\" rel=\"noreferrer noopener\">ransomware attack volume</a>.</p>\n<p dir=\"ltr\">This
demonstrates the centralized nature of the ransomware landscape, where a very small number of threat
groups drive most of the malicious activity.</p>\n<p dir=\"ltr\">The silver lining to this top-heavy
ecosystem is that disruptive actions against one of these primary groups, such as law enforcement
takedowns, can have a significant impact on the overall landscape. This is different from a threat
like <a href=\"https://abnormalsecurity.com/solutions/business-email-compromise\" target=\"_blank\"
rel=\"noreferrer noopener\">business email compromise</a>, where targeted disruptive actions are
generally less impactful to overall attack volume due to the decentralized structure of the threat
landscape.</p>"
    },
    {
        "id": "181601",
        "typeId": 14,
        "typeHandle": "image",
        "visibleAfterAccess": false,
        "image": [
            {
                "id": "129823",
                "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/
images/blog/Number-of-Victims-for-Top-15-Ransomware-Groups.png?
w=1536&h=987&auto=compress%2Cformat&fit=crop&dm=1675097662&s=954987cfa5f941fa97ba1d40914a2981",
                "title": "Number of Victims for Top 15 Ransomware Groups",
                "width": 1536,
                "height": 987,
                "extension": "png",
                "size": "37519",
                "path": "blog/Number-of-Victims-for-Top-15-Ransomware-Groups.png",
                "blur": [
                    {
                        "url": "https://optimise2.assets-servd.host/gifted-zorilla/
production/images/blog/Number-of-Victims-for-Top-15-Ransomware-Groups.png?
w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-x=0.5&fp-
y=0.5&dm=1675097662&s=5556855b755561fc308e75314b9cf9a4"
                    }
                ],
                "svgContent": ""
            }
        ],
        "imageBlur": [
            {
                "url": ""
            }
        ],
        "caption": "<p><em>Number of victims in all of 2020 and 2021</em></p>",
        "captionPosition": "center"
    },
    {
        "id": "181602",
        "typeId": 16,
        "typeHandle": "bodyText",
        "visibleAfterAccess": false,
        "bodyText": "<p dir=\"ltr\">One of the biggest challenges to disrupting the <a

```

$$\left. \begin{array}{l} \} \\ \{ \end{array} \right\}$$

when selecting their targets, preferring to settle for easy victims rather than consciously singling out specific companies to attack. Individually, however, some groups have solicited access to companies that meet certain criteria on underground forums.

For example, in July 2021, an actor associated with the BlackMatter ransomware group (the successor to DarkSide) posted on the Exploit forum that the group was looking for access to corporate networks of companies meeting specific location, revenue, and industry specifications.

$$\left. \begin{array}{l} \} \\ \{ \end{array} \right\}$$

```
{
  "id": "129824",
  "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/Forum-Post.png?"
```

w=1536&h=1304&auto=compress%2Cformat&fit=crop&dm=1675097662&s=4f26356a5f67b797080448a1ef85e4e8",

```
"title": "Black Matter Forum Post",
"width": 1536,
"height": 1304,
"extension": ".png",
"size": "207509",
"path": "blog/BlackMatter-Forum-Post.png",
"blur": [
```

```
{
  "url": "https://optimise2.assets-servd.host/gifted-zorilla/ter-Forum-Post.png?w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-cd10431638b44b38b0552ffb2dadf17d"
}
```

```
],
"svgContent": ""
```

```
    },
  ],
  "imageBlur": [
    {
      "url": ""
    }
  ]
}
```

```

    ],
    "caption": null,
    "captionPosition": "center"
  },
  {
    "id": "181606",
    "typeId": 16,
    "typeHandle": "bodyText",
    "visibleAfterAccess": false,
    "bodyText": "<p dir=\"ltr\">We can also see evidence of this preferred targeting
in our data. Some groups significantly deviate from the overall baseline characteristics of <a
href=\"https://abnormalsecurity.com/blog/ransomware-victims\" target=\"_blank\" rel=\"noreferrer
noopener\">ransomware victims</a>, indicating that while these groups may not be targeting specific
companies, they seem to have a preferred target profile.<br /></p>"
  },
  {
    "id": "181607",
    "typeId": 15,
    "typeHandle": "heading",
    "visibleAfterAccess": false,
    "heading": "Threat Groups by Target Revenue",
    "headingTag": "h2",
    "headingSize": "lg"
  },
  {
    "id": "181608",
    "typeId": 16,
    "typeHandle": "bodyText",
    "visibleAfterAccess": false,
    "bodyText": "<p dir=\"ltr\">While the median annual revenue for a ransomware
victim is $27 million, our data shows that a few ransomware groups aim for bigger targets than
others. The group that is most prevalently involved in big game hunting is CL0P, whose victims had a
median annual revenue of $111 million—more than four times higher than the average. Although not as
drastic, the median revenue for victims of Conti ransomware attacks was almost two times higher than
average at $48 million.</p>\n<p dir=\"ltr\">On the other end of the spectrum, a few groups seem to
prefer smaller prey. Avaddon's victims had a median annual revenue of $10 million, while the revenue
for LockBit victims was even lower at only $8 million.<br /></p>"
  },
  {
    "id": "181609",
    "typeId": 15,
    "typeHandle": "heading",
    "visibleAfterAccess": false,
    "heading": "Threat Groups by Target Location",
    "headingTag": "h2",
    "headingSize": "lg"
  },
  {
    "id": "181610",
    "typeId": 16,
    "typeHandle": "bodyText",
    "visibleAfterAccess": false,
    "bodyText": "<p dir=\"ltr\">While most ransomware victims over the last two
years have been located in North America or Western Europe, some groups have made these two regions
their almost exclusive hunting grounds.</p>\n<p dir=\"ltr\">Nearly all of Conti's almost 700 targets
(94%) were located in one of these two regions. Similarly, Grief ransomware and its predecessor
DoppelPaymer both almost exclusively targeted North American and Western European companies, with
92% of their victims in those areas.</p>\n<p dir=\"ltr\">Other groups have focused their efforts on
other parts of the world. Ragnarok, which was active between December 2020 and August 2021, was the
only group we observed where a majority (61%) of their targets were based in Europe. In fact, none
of Ragnarok's corporate victims in 2021 were located in North America—a definite outlier in the
ransomware world.</p>\n<p dir=\"ltr\">Prometheus, which was active between March 2021 and July 2021
before rebranding as Spook, was the only group where a plurality (37%) of its targets were located
in South America. And while companies in the Asia-Pacific region are generally lower down on a

```

ransomware group's list of targets, two groups—LV and LockBit—targeted organizations in the region at a significantly higher rate.<br /></p>"

```

    },
    {
      "id": "181611",
      "typeId": 15,
      "typeHandle": "heading",
      "visibleAfterAccess": false,
      "heading": "Protecting Your Organization From Ransomware",
      "headingTag": "h2",
      "headingSize": "lg"
    },
    {
      "id": "181612",
      "typeId": 16,
      "typeHandle": "bodyText",
      "visibleAfterAccess": false,
      "bodyText": "<p dir=\"ltr\">Ransomware continues to be a significant threat
vector across all industries, all company sizes, and all countries. Ransomware actors have proven
that they are focused on one thing: making money in whatever way possible.</p>\n<p dir=\"ltr\"><a
href=\"https://abnormalsecurity.com/solutions/malware-ransomware\" target=\"_blank\"
rel=\"noreferrer noopener\">Malware delivered via email</a> continues to be the initial foothold for
ransomware. Once this first payload has been delivered, threat actors can deploy additional malware
to gain access to the company network and hold your information for ransom. Now is the time to
secure your environment and protect your end users from these malicious emails—before the next
ransomware attack impacts you.<br /></p>\n\n<p dir=\"ltr\"><a href=\"https://abnormalsecurity.com/
resources/ransomware-victims-threat-actors?PS=organic%20website\" target=\"_blank\" rel=\"noreferrer
noopener\"><strong><em>Download the full report</em></strong></a><strong><em> for a comprehensive
look at the ransomware landscape.</em></strong><br /></p>"
    },
  ],
  "legacyBlogContent": null,
  "heroImage": [
    {
      "id": "109526",
      "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/images/
abstract/Abstract-Seafoam-Corner.png?
w=2400&h=1350&auto=compress%2Cformat&fit=crop&dm=1675097613&s=aeaac2c29037907aa3d439f27c2eef9e",
      "title": "Abstract Seafoam Corner",
      "width": 2400,
      "height": 1350,
      "extension": "png",
      "size": "1389821",
      "path": "abstract/Abstract-Seafoam-Corner.png",
      "blur": [
        {
          "url": "https://optimise2.assets-servd.host/gifted-zorilla/production/
images/abstract/Abstract-Seafoam-Corner.png?w=10&h=10&q=80&fm=jpg&fit=crop&crop=focalpoint&fp-
x=0.5&fp-y=0.5&dm=1675097613&s=4398b19d6cf147a37407b0642fb383ee"
        }
      ],
      "svgContent": ""
    },
  ],
  "heroImageBlur": [
    {
      "url": ""
    },
  ],
  "overlayTextTheme": "dark",
  "mobileHeroImage": [],
  "mobileHeroImageBlur": [],
  "seomatic": {
    "metaTitleContainer": "{\"title\":{\"title\":\"A Deep Dive into Active Ransomware
Groups | Abnormal Security\"}}",

```



```

        "metaTagContainer": "{ \"generator\": [], \"keywords\": { \"content\": \"analysis, prominent, ransomware, groups, activities, in-depth, january, here's, 2020\", \"name\": \"keywords\" }, \"description\": { \"content\": \"Here's an in-depth analysis of the 62 most prominent ransomware groups and their activities since January 2020.\", \"name\": \"description\" }, \"referrer\": { \"content\": \"no-referrer-when-downgrade\", \"name\": \"referrer\" }, \"robots\": { \"content\": \"all\", \"name\": \"robots\" }, \"fb:profile_id\": [], \"fb:app_id\": [], \"og:locale\": { \"content\": \"en_US\", \"property\": \"og:locale\" }, \"og:locale:alternate\": [], \"og:site_name\": { \"content\": \"Abnormal Security\", \"property\": \"og:site_name\" }, \"og:type\": { \"content\": \"website\", \"property\": \"og:type\" }, \"og:url\": { \"content\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\\n\\n/deep-dive-active-ransomware-groups/\", \"property\": \"og:url\" }, \"og:title\": { \"content\": \"A Deep Dive into Active Ransomware Groups\", \"property\": \"og:title\" }, \"og:description\": { \"content\": \"Here's an in-depth analysis of the 62 most prominent ransomware groups and their activities since January 2020.\", \"property\": \"og:description\" }, \"og:image\": { \"content\": \"https://\\n\\n\\n/optimise2.assets-servd.host/\\n\\n/gifted-zorilla/\\n\\n/production/\\n\\n/images/\\n\\n/blog/\\n\\n/L-05.27.22-Active-Ransomware-Groups.png?w=1200&h=630&q=82&auto=format&fit=crop&dm=1675097662&s=d488aa82b3b5872de5af2b630e8f0ac8\", \"property\": \"og:image\" }, \"og:image:width\": { \"content\": \"1200\", \"property\": \"og:image:width\" }, \"og:image:height\": { \"content\": \"630\", \"property\": \"og:image:height\" }, \"og:image:alt\": [], \"og:see_also\": [], \"facebook-site-verification\": [], \"twitter:card\": { \"content\": \"summary_large_image\", \"name\": \"twitter:card\" }, \"twitter:site\": { \"content\": \"@AbnoramlSec\", \"name\": \"twitter:site\" }, \"twitter:creator\": { \"content\": \"@AbnoramlSec\", \"name\": \"twitter:creator\" }, \"twitter:title\": { \"content\": \"A Deep Dive into Active Ransomware Groups\", \"name\": \"twitter:title\" }, \"twitter:description\": { \"content\": \"Here's an in-depth analysis of the 62 most prominent ransomware groups and their activities since January 2020.\", \"name\": \"twitter:description\" }, \"twitter:image\": { \"content\": \"https://\\n\\n\\n/optimise2.assets-servd.host/\\n\\n/gifted-zorilla/\\n\\n/production/\\n\\n/images/\\n\\n/blog/\\n\\n/T-05.27.22-Active-Ransomware-Groups.png?w=800&h=418&q=82&auto=format&fit=crop&dm=1675097662&s=c0a4308175ad1f3bece0126cfd501bb\", \"name\": \"twitter:image\" }, \"twitter:image:width\": { \"content\": \"800\", \"name\": \"twitter:image:width\" }, \"twitter:image:height\": { \"content\": \"418\", \"name\": \"twitter:image:height\" }, \"twitter:image:alt\": [], \"google-site-verification\": [], \"bing-site-verification\": [], \"pinterest-site-verification\": [] }",
        "metaLinkContainer": "{ \"canonical\": { \"href\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\\n\\n/deep-dive-active-ransomware-groups/\", \"rel\": \"canonical\" }, \"home\": { \"href\": \"https://\\n\\n\\n/abnormalsecurity.com/\", \"rel\": \"home\" }, \"author\": { \"href\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/humans.txt\", \"rel\": \"author\", \"type\": \"text/plain\" }, \"publisher\": [] },
        "metaScriptContainer": "[]",
        "metaJsonLdContainer": "{ \"mainEntityOfPage\": { \"@context\": \"http://\\n\\n\\n/schema.org/\", \"@type\": \"BlogPosting\", \"author\": { \"id\": \"#identity\" }, \"copyrightHolder\": { \"id\": \"#identity\" }, \"copyrightYear\": \"2022\", \"creator\": { \"id\": \"#creator\" }, \"dateModified\": \"2022-08-12T15:04:11-07:00\", \"datePublished\": \"2022-05-27T10:30:00-07:00\", \"description\": \"Here's an in-depth analysis of the 62 most prominent ransomware groups and their activities since January 2020.\", \"headline\": \"A Deep Dive into Active Ransomware Groups\", \"image\": { \"@type\": \"ImageObject\", \"url\": \"https://\\n\\n\\n/optimise2.assets-servd.host/\\n\\n/gifted-zorilla/\\n\\n/production/\\n\\n/images/\\n\\n/blog/\\n\\n/B-05.27.22-Active-Ransomware-Groups.png?w=1200&h=630&q=82&auto=format&fit=crop&dm=1675097662&s=628ffae2a045ded225dd8fb8ca0de6ba\" }, \"inLanguage\": \"en-us\", \"mainEntityOfPage\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\\n\\n/deep-dive-active-ransomware-groups/\", \"name\": \"A Deep Dive into Active Ransomware Groups\", \"publisher\": { \"id\": \"#creator\" }, \"url\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\\n\\n/deep-dive-active-ransomware-groups/\", \"identity\": { \"@context\": \"http://\\n\\n\\n/schema.org/\", \"id\": \"#identity\", \"@type\": \"Organization\", \"creator\": { \"@context\": \"http://\\n\\n\\n/schema.org/\", \"id\": \"#creator\", \"@type\": \"Organization\" }, \"breadcrumbList\": { \"@context\": \"http://\\n\\n\\n/schema.org/\", \"@type\": \"BreadcrumbList\", \"description\": \"Breadcrumbs list\", \"itemListElement\": [ { \"@type\": \"ListItem\", \"item\": \"https://\\n\\n\\n/abnormalsecurity.com/\", \"name\": \"Homepage\", \"position\": 1 }, { \"@type\": \"ListItem\", \"item\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\", \"name\": \"Abnormal Blog\", \"position\": 2 }, { \"@type\": \"ListItem\", \"item\": \"https://\\n\\n\\n/abnormalsecurity.com/\\n\\n/blog/\\n\\n/deep-dive-active-ransomware-groups/\", \"name\": \"A Deep Dive into Active Ransomware Groups\", \"position\": 3 } ], \"name\": \"Breadcrumbs\" } }",
    },
    "faqSchema": [],
  },
  "posts": [],
},
"_N_SSG": true
}

```

ThreatQuotient provides the following default mapping for this feed based on the `pageProps.post` JSON keys:

| FEED DATA PATH                    | THREATQ ENTITY     | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE         | EXAMPLES  | NOTES                      |
|-----------------------------------|--------------------|--------------------------------------|------------------------|---|----------------------------|
| <code>.title</code>               | Report.Title       | N/A                                  | <code>.postDate</code> | A Deep Dive into Active Ransomware Groups   | N/A                        |
| <code>.contentSections[]</code>   | Report.Description | N/A                                  | N/A                    | N/A   | Items are parsed into HTML |
| <code>.url</code>                 | Report.Attribute   | External Reference                   | <code>.postDate</code> | <a href="https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups">https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups</a> | N/A                        |
| <code>.postDate</code>            | Report.Attribute   | Published At                         | <code>.postDate</code> | 2022-05-27T10:30:00-07:00   | N/A                        |
| <code>.blogCategory[].slug</code> | Report.Tag         | N/A                                  | <code>.postDate</code> | threat-intel  | N/A                        |
| <code>.postAuthors[].title</code> | Report.Attribute   | Author                               | <code>.postDate</code> | threat-intel  | N/A                        |
| N/A                               | Report.Indicator   | CVE                                  | <code>.postDate</code> | CVE-2023-41232  | Parsed from HTML           |

# 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.

| METRIC            | RESULT   |
|-------------------|----------|
| Run Time          | 1 minute |
| Reports           | 3        |
| Report Attributes | 9        |
| Vulnerabilities   | 1        |

## Known Issues / Limitations

- The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
- If you need to ingest historical blog posts, run the feed manually by setting the **since** date back.
- The feed will only return at maximum, the most recent 24 pots.
- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the site.

# Change Log

- **Version 1.0.1**
  - Resolved an issue where an error would occur when an author could not be found/parsed.
- **Version 1.0.0**
  - Initial release