

# ThreatQuotient



## Intel 471 Alerts CDF User Guide

**Version 1.2.3**

December 11, 2023

### **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        |
| Intel471 Alerts .....                       | 10        |
| actor .....                                 | 11        |
| report .....                                | 14        |
| post.....                                   | 15        |
| privateMessage.....                         | 18        |
| entity.....                                 | 21        |
| event.....                                  | 23        |
| indicator .....                             | 27        |
| cveReport.....                              | 29        |
| spotReport.....                             | 34        |
| instantMessage.....                         | 37        |
| credential.....                             | 39        |
| breachAlert.....                            | 41        |
| Get Report by ID (Supplemental).....        | 45        |
| Get Watcher Group Name (Supplemental) ..... | 58        |
| Indicator Type Mapping .....                | 59        |
| <b>Average Feed Run.....</b>                | <b>60</b> |
| Intel 471 Alerts .....                      | 60        |
| <b>Change Log .....</b>                     | <b>61</b> |

# 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 © 2023 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      | 1.2.3             |
| Compatible with ThreatQ Versions | >= 4.30.0         |
| Support Tier                     | ThreatQ Supported |

---

# Introduction

The Intel 471 Alerts CDF ingests events, indicators, reports, adversaries, vulnerabilities, malware and tags from Intel471 TITAN API.

The integration includes the following feeds:

- **Intel471 Alerts** - returns a list of Alerts and related information.
- **Intel471 Get Report by ID - supplemental** - returns threat data using the `.alerts[].report.id` from the Intel471 Alerts feed as the `reportId` parameter.
- **Intel471 Get Watcher Group Name - supplemental** - returns threat data using the `.alerts[].watcherGroupUid` from the Intel471 Alerts feed as the `groupId` parameter.

The integration ingests the following system objects:

- Indicators
- Events
- Reports
- Adversaries
- Tags
- Vulnerabilities
- Identities
- Malware

# 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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration 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.

6. If prompted, select the individual feeds to install and click **Install**. 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 **Commercial** 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                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Email Address  | Your Intel471 account email address.                                                                                          |
| API Key        | Your Intel471 Account API Key.                                                                                                |
| Ingest CVEs As | Select whether to ingest CVE IDs as indicators, vulnerabilities, or both. The Vulnerabilities option is selected by default.  |
| Count          | The maximum number of records to retrieve from the provider per request. The value range is 0-100. The default setting is 10. |

< Intel 471 Alerts



Disabled
☐
Enabled

Uninstall

**Additional Information**

Integration Type: Feed

Version:

Accepted Data Types:

Configuration
Activity Log

Email Address

API Key 👁

**Ingest CVEs As...**

Select the type of entity you want to ingest CVE IDs as

☐ Indicators

☒ Vulnerabilities

Count  
10

Maximum number of records to retrieve from the provider per request. Default value: 10. Size range: 0-100.

Set indicator status to...  
Active

Run Frequency

Every 24 Hours
▼

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

## Intel471 Alerts

The Intel471 Alerts endpoint returns a list of Alerts and related information.

GET – <https://api.intel471.com/v1/alerts>

Sample Response:

```
{
  "alertTotalCount": 133,
  "alerts": [
    {
      "uid": "6216e6d855075802a8c0a936",
      "status": "unread",
      "watcherUid": "d590d398ac5906d93428d6fd2e589f9f",
      "watcherGroupUid": "7892e0cb-8c1b-42b9-b91d-9f9e73593082",
      "foundTime": 1645668056389,
      ...
    }
  ]
}
```

An Alert event will be created for each item in the list and will be described below.

| FEED DATA PATH   | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE      | EXAMPLES                       | NOTES                                                       |
|------------------|-----------------|--------------------------------------|---------------------|--------------------------------|-------------------------------------------------------------|
| N/A              | event.title     | Alert                                | .alerts[].foundtime | Intel 471 Alert 1497446972076" | View title format below                                     |
| .alerts[].uid    | event.attribute | UID                                  | .alerts[].foundtime | 59413a3c441d6663bf8795bb"      | N/A                                                         |
| .alerts[].status | event.attribute | Status                               | .alerts[].foundtime | unread                         | N/A                                                         |
| .alerts[].uid    | event.attribute | Watcher Group Name                   | .alerts[].foundtime | testG                          | Details in Get Watcher Group Name supplemental feed section |

The Title is created by concatenating the following:

- Intel 471 Alert .uid
- ['Forum: ' + .post.links.forum.name] if .post and forum are present
- ['Type: Private Message'] if .privateMessage is present
- ['Type: Post'] if .post is present
- ['Type: Instant Message'] if .privateMessage is present
- ['Vulnerable Product: ' + value.cveReport.data.cve\_report.product\_name] if .cveReport is present
- ['Risk: ' + value.cveReport.data.cve\_report.risk\_level] if .cveReport is present
- ['Type: Spot Report'] if .spotReport is present

- ['Type: Breach Alert'] if .breachAlert is present

Each alert can contain one of the following objects, which will be detailed in the following sections:

- actor
- report
- post
- privateMessage
- entity
- event
- indicator
- cveReport
- spotReport
- instantMessage
- credential
- breachAlert

All entities created based of those objects will be detailed in the sections below.

## actor

### Sample Response:

```
{
  "alertTotalCount": 112,
  "alerts": [
    {
      "uid": "014f7a860a14924b5cb74eeb",
      "status": "unread",
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "foundTime": 1649375878316,
      "actor": {
        "lastUpdated": 1649367894186,
        "handles": [
          "carter"
        ],
        "links": {
          "forumTotalCount": 0,
          "instantMessageChannelTotalCount": 3,
          "forumPrivateMessageTotalCount": 0,
          "reportTotalCount": 1,
          "reports": [
            {
              "subject": "Conti ransomware group's information technology team
examined",
              "released": 1649367885000,
              "actorHandle": "carter",
              "motivation": [
                "CC"
              ],
              "portalReportUrl": "https://titan.intel471.com/report/inforep/"
            }
          ]
        }
      }
    }
  ]
}
```

```

9d6d955d3e94c5a5b0aeb392c3f351ca",
    "uid":
    "b7e50f1bae213e247505c67f67689815e8e024dc11161e8f7a2eb5f03e9beb9f",
    "sourceCharacterization": "Information was derived from the Conti
ransomware gang\u2019s leaked data, our actors\u2019 database and open
sources.",
    "admiraltyCode": "F3",
    "dateOfInformation": 1648944000000
  }
],
  "instantMessageTotalCount": 0,
  "instantMessageServerTotalCount": 4,
  "forumPostTotalCount": 0
},
  "uid": "3ace6bad392acc4d295727017ac5583d"
},
  "highlights": []
}
]
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                           | THREATQ ENTITY      | THREATQ<br>OBJECT TYPE<br>OR<br>ATTRIBUTE<br>KEY | PUBLISHED DATE             | EXAMPLES | NOTES                                                                                                                                                                     |
|----------------------------------------------------------|---------------------|--------------------------------------------------|----------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .alerts[].actor.handles[]                                | Adversary.Name      | N/A                                              | .alerts[].actor.activeFrom | carter   | N/A                                                                                                                                                                       |
| .alerts[].actor.handles[]                                | Adversary.Attribute | Intel471<br>Actor Link                           | .alerts[].actor.activeFrom | carter   | Formatted as<br><a href="https://titan.intel471.com/search/Actor:{{.alerts[].actor.handles[]}}">https://titan.intel471.com/search/Actor:{{.alerts[].actor.handles[]}}</a> |
| .alerts[].actor.links.forum<br>TotalCount                | Adversary.Attribute | Linked<br>Forums<br>Count                        | .alerts[].actor.activeFrom | 2        | N/A                                                                                                                                                                       |
| .alerts[].actor.links.forum<br>PrivateMessageTotalCount  | Adversary.Attribute | Linked<br>Private<br>Messages<br>Count           | .alerts[].actor.activeFrom | 0        | N/A                                                                                                                                                                       |
| .alerts[].actor.links.forum<br>PostTotalCount            | Adversary.Attribute | Linked<br>Posts Count                            | .alerts[].actor.activeFrom | 2        | N/A                                                                                                                                                                       |
| .alerts[].actor.links.report<br>TotalCount               | Adversary.Attribute | Linked<br>Reports<br>Count                       | .alerts[].actor.activeFrom | 1        | N/A                                                                                                                                                                       |
| .alerts[].actor.links.instant<br>MessageServerTotalCount | Adversary.Attribute | Linked<br>Instant<br>Message<br>Server<br>Count  | .alerts[].actor.activeFrom | 2        | N/A                                                                                                                                                                       |

| FEED DATA PATH                                                                                              | THREATQ ENTITY              | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE             | EXAMPLES                         | NOTES                                                                                                       |
|-------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------------------------|----------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------|
| .alerts[].actor.links.instantMessageChannelTotalCount                                                       | Adversary.Attribute         | Linked Instant Message Channel Count | .alerts[].actor.activeFrom | 2                                | N/A                                                                                                         |
| .alerts[].actor.links.instantMessageTotalCount                                                              | Adversary.Attribute         | Linked Instant Message Count         | .alerts[].actor.activeFrom | 2                                | N/A                                                                                                         |
| .alerts[].actor.links.forumTotalCount                                                                       | Adversary.Attribute         | Linked Forums Count                  | .alerts[].actor.activeFrom | 4                                | N/A                                                                                                         |
| .alerts[].links.instantMessageServers[].serviceType<br>- .alerts[].actor.links.instantMessageServers[].name | Adversary.Attribute         | Instant Message Server               | .alerts[].actor.activeFrom | 2                                | N/A                                                                                                         |
| .alerts[].actor.reports[].uid                                                                               | Related Report              | N/A                                  | .alerts[].actor.activeFrom | 014f7a860a14924b5cb74eeb         | Used by Get Report by ID (Supplemental) Feed to load information about the report                           |
| .alerts[].actor.links.forums[].uid                                                                          | Adversary.Attribute         | Intel 471 Forum Link                 | .alerts[].actor.activeFrom | 37fb05bc65bf6a1435e06a98e4266bc7 | Formatted as <code>https://titan.intel471.com/forums/{{value.privateMessage.links.forum.uid}}/topics</code> |
| .alerts[].actor.links.forums[].name                                                                         | Adversary.Attribute         | Forum Name                           | .alerts[].actor.activeFrom | kepahoo                          | N/A                                                                                                         |
| .alerts[].actor.links.forums[].contactInfo.value                                                            | Adversary.Attribute         | Forum Contact                        | .alerts[].actor.activeFrom | Jabber                           | N/A                                                                                                         |
| .alerts[].actor.links.forums[].contactInfo.type                                                             | Adversary.Attribute         | Forum Contact Type                   | .alerts[].actor.activeFrom | Jabber                           | Type: EmailAddress, ICQ, Jabber, MSN, YahooIM, AIM, Skype, QQ, BitcoinAddress, etc                          |
| .alerts[].actor.links.forums[].actorHandle                                                                  | Related Adversary.name      | N/A                                  | .alerts[].actor.activeFrom | John                             | N/A                                                                                                         |
| N/A                                                                                                         | Related Adversary.Attribute | Actor Type                           | .alerts[].actor.activeFrom | Author                           | Hardcoded Attribute                                                                                         |

## report

### Sample Response:

```
{
  "alertTotalCount": 112,
  "alerts": [
    {
      "uid": "014f7a860a14924b5cb74eeb",
      "status": "unread",
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "foundTime": 1649375878316,
      "report": {
        "uid":
"3487f9fe27c23efb0086faa4b80984bcbf1803820db9a0350f8bb9b32b1ae652",
        "admiraltyCode": "F3",
        "motivation": [
          "CC"
        ],
        "subject": "Conti ransomware group's information technology team
examined",
        "dateOfInformation": 1648944000000,
        "sourceCharacterization": "Information was derived from the Conti
ransomware gang\u2019s leaked data, our actors\u2019 database and open
sources.",
        "portalReportUrl": "https://titan.intel471.com/report/inforep/
9d6d955d3e94c5a5b0aeb392c3f351ca",
        "released": 1649367885000
      },
      "highlights": []
    }
  ]
}
```



.alerts[].report.uid if used by [Get Report by ID \(Supplemental\)](#) feed in order to load detailed information about the report.

## post

### Sample Response:

```
{
  "alerts": [
    {
      "uid": "62044763cb0db71af2f8b1c8",
      "status": "read",
      "watcherUid": "8cfcff4d783bfed6d8d33a189956071d",
      "watcherGroupUid": "7892e0cb-8c1b-42b9-b91d-9f9e73593082",
      "foundTime": 1644447587028,
      "post": {
        "lastUpdated": 1644429977657,
        "links": {
          "forum": {
            "uid": "7e7757b1e12abcb736ab9a754ffb617a",
            "name": "wwh-club.co",
            "description": "WWH (aka WWHClub, WWH-Club) is a long-standing,
primarily Russian-language and mostly cybercrime-related underground forum that
was started about February 2014. Its membership stands at approximately 192,000
(November 2020), and consists of actors of average sophistication. The forum
has a low barrier of entry that only requires registration for a basic
(\"Observer\") profile type, however five paid profile tiers are also offered:
\"Project participant\" (US $50), \"Premium member\" (US $150), \"Gold
member\" (US $350), \"Platinum member\" (US $600) and \"WWH-Club\" (US $950).
Higher tiers provide additional privileges, which include access to a
restricted forum section, ability to view messages protected by \"hides\",
various profile customization options and other features.\r\n\r\nThe forum has
very active administration and moderation teams (administrator and founder the
actor W.W.H. and principal moderator the actor Makein are assisted by about 20
lower-level moderators), which regularly patrol the forum, provide
\"accreditation\" service and collect fees from actors wishing to offer
commodities and services at the forum. The forum's crew also offers an escrow
service, brokering and protecting deals between forum members, and regularly
organizes \"training courses\" for newbie forum members."
          },
          "thread": {
            "uid": "1c1dc13b50afd1fb7b902d1b4ab963e0",
            "topic": "Хакеры атаковали португальское подразделение Vodafone",
            "count": 1
          },
          "authorActor": {
            "uid": "c0a03d1193163fd9d4d4c64565d6a243",
            "handle": "el_cesar"
          }
        },
        "date": 1644395628000,
        "uid": "01fb60ab6a74e66e5e75322ae0bdeef8",
        "message": "<article class=\"forumPost\">\nVodafone Portugal ;.
```

```
\n#160;\n</article>"
  },
  "highlights": [
    {
      "field": "data.post.message.escaped",
      "chunks": [
        {
          "text": "Португальское подразделение Vodafone стало жертвой
хакерской атаки, в результате которой была нарушена работа услуг компании. Как
заверили [https://www.vodafone.pt/press-releases/2022/2/"
        },
        {
          "hl": "vodafone-portugal"
        },
        {
          "text": "-alvo-de-ciberataque.html] представители "
        },
        {
          "hl": "Vodafone"
        },
        {
          "text": " "
        },
        {
          "hl": "Portugal"
        },
        {
          "text": ", персональные данные клиентов не были
скомпрометированы. В понедельник вечером, 7 февраля, система "
        }
      ]
    }
  ]
}
]
```

ThreatQ provides the following default mapping:

| FEED DATA PATH                 | THREATQ ENTITY  | THREATQ<br>OBJECT TYPE<br>OR ATTRIBUTE<br>KEY | PUBLISHED DATE      | EXAMPLES                                                       | NOTES                                                                                               |
|--------------------------------|-----------------|-----------------------------------------------|---------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| .alerts[].post.uid             | Event.Attribute | Post UID                                      | .alerts[].post.date | 6613f939099a5db1b7b627478c74f6e9                               | N/A                                                                                                 |
| .alerts[].post.message         | Event.Attribute | Post<br>Message                               | .alerts[].post.date | Dear, Волна!\r\n\r\nA virus alert was noticed on your computer | Stripped HTML tags                                                                                  |
| .alerts[].post.links.forum.uid | Event.Attribute | Intel471<br>Forum Link                        | .alerts[].post.date | 37fb05bc65bf6a1435e06a98e4266bc7                               | Formatted as<br><a href="https://titan.intel471.com/forums/">https://titan.intel471.com/forums/</a> |

| FEED DATA PATH                                       | THREATQ ENTITY      | THREATQ<br>OBJECT TYPE<br>OR ATTRIBUTE<br>KEY | PUBLISHED DATE                   | EXAMPLES                                                      | NOTES                                                                                                         |
|------------------------------------------------------|---------------------|-----------------------------------------------|----------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|                                                      |                     |                                               |                                  |                                                               | <code>{{.alerts[].post.links.forum.uid}}/topics</code>                                                        |
| <code>.alerts[].post.links.forum.name</code>         | Event.Attribute     | Forum Name                                    | <code>.alerts[].post.date</code> | carder.pro                                                    | N/A                                                                                                           |
| <code>.alerts[].post.links.forum.description</code>  | Event.Attribute     | Forum Description                             | <code>.alerts[].post.date</code> | carder.pro is a forum focused on carding (credit card fraud). | N/A                                                                                                           |
| <code>.alerts[].post.links.thread.uid</code>         | Event.Attribute     | Intel471 Thread Link                          | <code>.alerts[].post.date</code> | 41ca85374b5e87717a8474c6add09292                              | Formatted as <code>https://titan.intel471.com/post_thread/{{.alerts[].post.thread.uid}}/topics</code>         |
| <code>.alerts[].post.links.thread.topic</code>       | Event.Attribute     | Thread Topic                                  | <code>.alerts[].post.date</code> | Anonymous Surfing Kit 2010                                    | N/A                                                                                                           |
| <code>.alerts[].post.links.thread.count</code>       | Event.Attribute     | Thread Posts Count                            | <code>.alerts[].post.date</code> | 233                                                           | N/A                                                                                                           |
| <code>.alerts[].post.links.authorActor.handle</code> | Adversary.Name      | N/A                                           | <code>.alerts[].post.date</code> | BestForumTeam                                                 | N/A                                                                                                           |
| <code>.alerts[].post.links.authorActor.uid</code>    | Adversary.Attribute | Author UID                                    | <code>.alerts[].post.date</code> | 6613f939099a5db1b7b627478c74f6e9                              | N/A                                                                                                           |
| <code>.alerts[].post.links.authorActor.handle</code> | Adversary.Attribute | Intel471 Actor Link                           | <code>.alerts[].post.date</code> | <code>.alerts[].post.links.authorActor.handle</code>          | Formatted as <code>https://titan.intel471.com/search/Actor:{{.alerts[].post.links.authorActor.handle}}</code> |
| N/A                                                  | Adversary.Attribute | Actor Type                                    | <code>.alerts[].post.date</code> | Author                                                        | Hardcoded Attribute                                                                                           |

## privateMessage

### Sample Response:

```
{
  "alerts": [
    {
      "uid": "62044763cb0db71af2f8b1c8",
      "status": "read",
      "watcherUid": "8cfcff4d783bfed6d8d33a189956071d",
      "watcherGroupUid": "7892e0cb-8c1b-42b9-b91d-9f9e73593082",
      "foundTime": 1644447587028,
      "privateMessage": {
        "date": 1644395628000,
        "uid": "01aa60ab6a74e66e5e75322ae0bdeef8",
        "message": "Vodafone Portugal very important message",
        "subject": "Vodafone Portugal",
        "lastUpdated": 1644429977657,
        "links": {
          "forum": {
            "uid": "7e7757b1e12abcb736ab9a754ffb617a",
            "name": "wwh-club.co",
            "description": "WWH (aka WWHClub, WWH-Club) is a long-standing,
primarily Russian-language and mostly cybercrime-related underground forum that
was started about February 2014. Its membership stands at approximately 192,000
(November 2020), and consists of actors of average sophistication. The forum
has a low barrier of entry that only requires registration for a basic
(\"Observer\") profile type, however five paid profile tiers are also offered:
\"Project participant\" (US $50), \"Premium member\" (US $150), \"Gold
member\" (US $350), \"Platinum member\" (US $600) and \"WWH-Club\" (US $950).
Higher tiers provide additional privileges, which include access to a
restricted forum section, ability to view messages protected by \"hides\",
various profile customization options and other features.\r\n\r\nThe forum has
very active administration and moderation teams (administrator and founder the
actor W.W.H. and principal moderator the actor Makein are assisted by about 20
lower-level moderators), which regularly patrol the forum, provide
\"accreditation\" service and collect fees from actors wishing to offer
commodities and services at the forum. The forum's crew also offers an escrow
service, brokering and protecting deals between forum members, and regularly
organizes \"training courses\" for newbie forum members.\"
          },
          "thread": {
            "uid": "1c1dc13b50afd1fb7b902d1b4ab963e0",
            "topic": "Хакеры атаковали португальское подразделение Vodafone",
            "count": 1
          },
          "authorActor": {
            "uid": "c0a03d1193163fd9d4d4c64565d6a243",
            "handle": "el_cesar"
          }
        }
      }
    }
  ]
}
```

```

    "recipientActor": {
      "uid": "c0a03d1193163fd9d4d4c64565d6a243",
      "handle": "john"
    }
  },
  "highlights": [
  ]
}
]
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                    | THREATQ ENTITY      | THREATQ<br>OBJECT TYPE<br>OR<br>ATTRIBUTE<br>KEY | PUBLISHED DATE                | EXAMPLES                                                       | NOTES                                                                                                                                                                                                                  |
|---------------------------------------------------|---------------------|--------------------------------------------------|-------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .alerts[].privateMessage.subject                  | Indicator.value     | Email Subject                                    | .alerts[].privateMessage.date | Important message from the forum administration!               | N/A                                                                                                                                                                                                                    |
| .alerts[].privateMessage.uid                      | Indicator.Attribute | UID                                              | .alerts[].privateMessage.date | 6613f939099a5db1b7b627478c74f6e9                               | N/A                                                                                                                                                                                                                    |
| .alerts[].privateMessage.message                  | Indicator.Attribute | Message                                          | .alerts[].privateMessage.date | Dear, Волна!\r\n\r\nA virus alert was noticed on your computer | Stripped HTML tags                                                                                                                                                                                                     |
| .alerts[].privateMessage.links.forum.uid          | Event.Attribute     | Intel 471 Forum Link                             | .alerts[].privateMessage.date | 37fb05bc65bf6a1435e06a98e4266bc7                               | Formatted as <a href="https://titan.intel471.com/forums/{{.alerts[].privateMessage.links.forum.uid}}/topics">https://titan.intel471.com/forums/{{.alerts[].privateMessage.links.forum.uid}}/topics</a>                 |
| .alerts[].privateMessage.links.forum.name         | Event.Attribute     | Forum Name                                       | .alerts[].privateMessage.date | carder.pro                                                     | N/A                                                                                                                                                                                                                    |
| .alerts[].privateMessage.links.forum.description  | Event.Attribute     | Forum Description                                | .alerts[].privateMessage.date | carder.pro is a forum focused on carding (credit card fraud)   | N/A                                                                                                                                                                                                                    |
| .alerts[].privateMessage.links.authorActor.handle | Adversary.Name      | N/A                                              | .alerts[].privateMessage.date | BestForumTeam                                                  | N/A                                                                                                                                                                                                                    |
| N/A                                               | Adversary.Attribute | Actor Type                                       | .alerts[].privateMessage.date | Author                                                         | Hardcoded Attribute                                                                                                                                                                                                    |
| .alerts[].privateMessage.links.authorActor.uid    | Adversary.Attribute | UID                                              | .alerts[].privateMessage.date | 5328c3099dbc67b62cf7ee620ffee4c2                               | N/A                                                                                                                                                                                                                    |
| .alerts[].privateMessage.links.authorActor.handle | Adversary.Attribute | Intel 471 Actor Link                             | .alerts[].privateMessage.date | BestForumTeam                                                  | Formatted as <a href="https://titan.intel471.com/search/Actor:{{.alerts[].privateMessage.links.authorActor.handle}}">https://titan.intel471.com/search/Actor:{{.alerts[].privateMessage.links.authorActor.handle}}</a> |

| FEED DATA PATH                                           | THREATQ ENTITY      | THREATQ<br>OBJECT TYPE<br>OR<br>ATTRIBUTE<br>KEY | PUBLISHED DATE                | EXAMPLES                             | NOTES                                                                                                                                            |
|----------------------------------------------------------|---------------------|--------------------------------------------------|-------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                          |                     |                                                  |                               |                                      | .links.author<br>Actor.handle}<br>}                                                                                                              |
| .alerts[].privateMessage.<br>links.recipientActor.handle | Adversary.Name      | N/A                                              | .alerts[].privateMessage.date | Волн                                 | N/A                                                                                                                                              |
| N/A                                                      | Adversary.Attribute | Actor Type                                       | .alerts[].privateMessage.date | Recipient                            | Hardcoded<br>Attribute                                                                                                                           |
| .alerts[].privateMessage.<br>links.recipientActor.uid    | Adversary.Attribute | UID                                              | .alerts[].privateMessage.date | 37fb05bc65bf6a1435<br>e06a98e4266bc7 | N/A                                                                                                                                              |
| .alerts[].privateMessage.<br>links.recipientActor.handle | Adversary.Attribute | Intel 471<br>Actor Link                          | .alerts[].privateMessage.date | BestForumTeam                        | Formatted as<br>https://<br>titan.intel47<br>1.com/search/<br>Actor:<br>{{.alerts[].p<br>rivateMessage<br>.links.recipi<br>entActor.hand<br>le}} |

## entity

### Sample Response:

```
{
  "alertTotalCount": 112,
  "alerts": [
    {
      "uid": "064f7a860a14924b5cb74eeb",
      "status": "unread",
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "foundTime": 1649375878316,
      "entity": {
        "lastUpdated": 1600335702864,
        "links": {
          "actors": [
            {
              "uid": "064f7a860a14924b5cb74eeb",
              "handle": [
                "yalishanda"
              ]
            }
          ]
        },
        "reports": [
          {
            "subject": "Actor SyntaX advertises service to offer custom fraud websites",
            "released": 1432332472000,
            "motivation": [
              "CC"
            ],
            "portalReportUrl": "https://titan.intel471.com/report/inforep/6eb72aef7e1207f57b8c2e7084e86422",
            "uid": "fc7100d3297d3df804227937c41ff92b",
            "sourceCharacterization": "Information derived from the English speaking cyber crime forum AlphaBay hosted on TOR network and our actor database.",
            "admiraltyCode": "C3",
            "dateOfInformation": 1431561600000
          }
        ]
      },
      "uid": "0d613670b4b684ae79c797445112afe6",
      "type": "url",
      "value": "http://45.67.231.78:3214",
      "activeFrom": 1522874107000,
      "activeTill": 1522874107000
    }
  ]
}
```

```
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                          | THREATQ ENTITY         | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE              | EXAMPLES                         | NOTES                                                                                                                                                                                  |
|-----------------------------------------|------------------------|--------------------------------------|-----------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .alerts[].entity.value                  | Indicator.Value        | .alerts[].entity.type                | .alerts[].entity.activeFrom | http://45.67.231.78:3214         | View <a href="#">Indicator Type Map</a> table.                                                                                                                                         |
| .alerts[].entity.uid                    | Indicator.Attribute    | Indicator UID                        | .alerts[].entity.activeFrom | 3ace6bad392acc4d295727017ac5583d | N/A                                                                                                                                                                                    |
| .alerts[].entity.links.actorTotalCount  | Indicator.Attribute    | Actor Count                          | .alerts[].entity.activeFrom | 2                                | N/A                                                                                                                                                                                    |
| .alerts[].entity.links.reportTotalCount | Indicator.Attribute    | Report Count                         | .alerts[].entity.activeFrom | 3                                | N/A                                                                                                                                                                                    |
| .alerts[].entity.links.actors.handles[] | Related Adversary.Name | N/A                                  | .alerts[].entity.activeFrom | John                             | N/A                                                                                                                                                                                    |
| N/A                                     | Adversary.Attribute    | Actor Type                           | .alerts[].entity.activeFrom | Author                           | Hardcoded Attribute                                                                                                                                                                    |
| .alerts[].entity.links.actors[].uid     | Adversary.Attribute    | Actor UID                            | .alerts[].entity.activeFrom | 5328c3099dbc67b62cf7ee620ffee4c2 | N/A                                                                                                                                                                                    |
| .alerts[].entity.links.actors[].uid     | Adversary.Attribute    | Intel 471 Actor Link                 | .alerts[].entity.activeFrom | 3ace6bad392acc4d295727017ac5583d | Formatted as <a href="https://titan.intel471.com/search/Actor:{{.alerts[].entity.links.actors.uid}}">https://titan.intel471.com/search/Actor:{{.alerts[].entity.links.actors.uid}}</a> |
| .alerts[].entity.links.reports[].uid    | Related Report         | N/A                                  | .alerts[].entity.activeFrom | 014f7a860a14924b5cb74eeb         | Used by Get Report by ID (Supplemental) Feed to load information about the report                                                                                                      |

## event

### Sample Response:

```
{
  "alerts": [
    {
      "uid": "054f7a860a14924b5cb74eeb",
      "status": "unread",
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "foundTime": 1649375878316,
      "event": {
        "uid": "334f7a860a14924b5cb74eeb",
        "activity": {
          "first": 1648160173000,
          "last": 1648160173000
        },
        "data": {
          "event_data": {
            "settings": [
              {
                "plugin_location": "http://176.111.174.67/7Ndd3SnW/plugins/
cred.dll"
              },
              {
                "plugin_location": "http://176.111.174.67/7Ndd3SnW/plugins/
scr.dll"
              },
              {
                "bot_version": "2.11"
              },
              {
                "campaign_id": "c5c741"
              }
            ],
            "file": {
              "md5": "59d1f5846536ae9ef334b9aebd9e8e92",
              "sha1": "4acb7917cfc125e472db270f3743ff3cff64a3ab",
              "sha256":
"1fb6ed5ec4a03acd2e8a086058446e3fc19497fd3f3f53980b3bf3a2559bf24e",
              "type": "PEEXE_x86",
              "size": 344576,
              "download_url": "https://api.intel471.com/v1/download/
malwareIntel/
1fb6ed5ec4a03acd2e8a086058446e3fc19497fd3f3f53980b3bf3a2559bf24e.zip"
            },
            "controller": {
              "url": "http://176.111.174.68/7Ndd3SnW/index.php",
              "ipv4": "8.8.8.7",
              "geo_ip": {
```

```

        "country": "some country",
        "city": "some city",
        "subdivision": [
            "some subdivision"
        ]
    },
    "encryption": [
        {
            "algorithm": "RC4",
            "key": "5eba991cccd123490699d79978f03f44",
            "context": "COMMUNICATION"
        }
    ],
    "intel_requirements": [
        "1.1.5",
        "1.1.6"
    ],
    "event_type": "artifact_extraction",
    "threat": {
        "type": "malware",
        "uid": "6e81e9acbfd4442ed5bb0dbde77436d5",
        "data": {
            "malware_family_profile_uid": "2ba5fdaf61b7499d50a525a9d9d3327c",
            "family": "amadey",
            "version": "2.11"
        }
    }
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                              | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES           | NOTES                                                                  |
|---------------------------------------------|-----------------|--------------------------------------|--------------------|------------------------------------------------------------------------|
| .alerts[].event.data.event_type             | Event.Attribute | Event Type                           | download_execute   | download_execute, start_ddos, execute_command, keylog, screenshot, etc |
| .alerts[].event.data.intel_requirements[]   | Event.Attribute | Intelligence Requirements            | 1.1.5              | N/A                                                                    |
| .alerts[].event.data.event_data.plugin_type | Event.Attribute | Plugin Type                          | CREDENTIAL_STEALER | Type of plugin. i.e. REMOTE_ACCESS, CREDENTIAL_STEALER, OTHER.         |
| .alerts[].event.data.event_data.plugin_name | Event.Attribute | Plugin Name                          | Contact Form       | N/A                                                                    |
| .alerts[].event.data.event_data.file.type   | Event.Attribute | File Type                            | TEXT               | N/A                                                                    |

| FEED DATA PATH                                                                                                                        | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                                                                                           | NOTES |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------|----------------------------------------------------------------------------------------------------|-------|
| .alerts[].event.data.<br>event_data.file.md5                                                                                          | Event.Attribute | File MD5 hash                        | 59d1f5846536ae9ef334<br>b9aebd9e8e92                                                               | N/A   |
| .alerts[].event.data.<br>event_data.file.sha1                                                                                         | Event.Attribute | File SHA1 hash                       | 4acb7917cfc125e472db<br>270f3743ff3cff64a3ab                                                       | N/A   |
| .alerts[].event.data.<br>event_data.file.sha256                                                                                       | Event.Attribute | File SHA256 hash                     | 1fb6ed5ec4a03acd2e8a<br>086058446e3fc19497fd<br>3f3f53980b3bf3a2559bf<br>24e                       | N/A   |
| .alerts[].event.data.<br>event_data.file.size                                                                                         | Event.Attribute | File Size                            | 344576                                                                                             | N/A   |
| .alerts[].event.data.<br>event_data.file.<br>download_url                                                                             | Event.Attribute | File Download URL                    | https://api.intel471.com<br>/v1/download/malwarel<br>ntel/<br>1fb6ed5ec4a03acbf<br>3a2559bf24e.zip | N/A   |
| .alerts[].event.data.<br>event_data.controllers<br>[].url                                                                             | Event.Attribute | Controller URL                       | http://176.111.174.67/<br>7Ndd3SnW/index.php                                                       | N/A   |
| .alerts[].event.data.<br>event_data.controller.<br>url                                                                                | Event.Attribute | Controller URL                       | http://176.111.174.67<br>/7Ndd3SnW/index.php                                                       | N/A   |
| .alerts[].event.data.<br>event_data.controller<br>.ipv4                                                                               | Event.Attribute | Controller IPV4                      | 103.150.68.124                                                                                     | N/A   |
| .alerts[].event.data.<br>event_data.controller.<br>geo_ip.country -<br>.alerts[].event.data.<br>event_data.controller.<br>geo_ip.city | Event.Attribute | Controller Geo IP<br>Location        | United States - New<br>York                                                                        | N/A   |
| .alerts[].event.data.<br>event_data.controller.<br>geo_ip.subdivision[]                                                               | Event.Attribute | Controller Geo IP<br>Subdivision     | n/a                                                                                                | N/A   |
| .alerts[].event.data.<br>event_data.encryption[].<br>algorithm                                                                        | Event.Attribute | Encryption Algorithm                 | RC4                                                                                                | N/A   |
| .alerts[].event.data.<br>event_data.encryption<br>[].key                                                                              | Event.Attribute | Encryption Key                       | 5eba991cccd123<br>490699d79978f0<br>3f44                                                           | N/A   |
| .alerts[].event.data.<br>event_data.encryption<br>[].context                                                                          | Event.Attribute | Encryption Context                   | COMMUNICATION                                                                                      | N/A   |
| .alerts[].event.data.<br>event_data.triggers[].<br>trigger                                                                            | Event.Attribute | Trigger Path                         | N/A                                                                                                | N/A   |
| .alerts[].event.data.<br>event_data.component_<br>type                                                                                | Event.Attribute | Component Type                       | CORE                                                                                               | N/A   |
| .alerts[].event.data.<br>event_data.location.url                                                                                      | Event.Attribute | Location URL                         | http://176.111.174.<br>67/7Ndd3SnW/plug<br>ins/cred.dll                                            | N/A   |

| FEED DATA PATH                                             | THREATQ ENTITY            | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                         | NOTES                       |
|------------------------------------------------------------|---------------------------|--------------------------------------|----------------------------------|-----------------------------|
| .alerts[].event.data.event_data.location.ipv4              | Event.Attribute           | Location IPV4                        | 103.150.68.124                   | N/A                         |
| .alerts[].event.data.event_data.inject_type                | Event.Attribute           | Inject Type                          | N/A                              | N/A                         |
| .alerts[].event.data.event_data.config_file                | Event.Attribute           | Config File                          | N/A                              | N/A                         |
| .alerts[].event.data.event_data.command                    | Event.Attribute           | Command                              | N/A                              | N/A                         |
| .alerts[].event.data.event_data.target_type                | Event.Attribute           | Target Type                          | N/A                              | N/A                         |
| .alerts[].event.data.event_data.senders[]                  | Event.Attribute           | Sender                               | John                             | N/A                         |
| .alerts[].event.data.event_data.recipient_domains[].domain | Event.Attribute           | Recipient Domain                     | domain.com                       | N/A                         |
| .alerts[].event.data.threat.uid                            | Event.Attribute           | Threat Type UID                      | 97eb1ec130425016f030886ea513dd48 | N/A                         |
| .alerts[].event.data.threat.type                           | Event.Attribute           | Threat Type                          | malware                          | malware, proxy_service etc. |
| .alerts[].event.data.threat.data.family                    | Related Malware.Value     | N/A                                  | smokeloader                      | for malware threat type     |
| .alerts[].event.data.threat.data.variant                   | Related Malware.Attribute | Threat variant                       | N/A                              | N/A                         |

## indicator

### Sample Response:

```
{
  "data": {
    "uid": "03966eb21fe3b33e026f3363b9f012af",
    "threat": {
      "type": "malware",
      "uid": "29f58ed4a99ee32fc64c25f9670e0f4e",
      "data": {
        "malware_family_profile_uid": "29f58ed4a99ee32fc64c25f9670e0f4e",
        "family": "redline"
      }
    },
    "expiration": 1617937719000,
    "confidence": "high",
    "context": {
      "description": "redline controller URL"
    },
    "mitre_tactics": "command_and_control",
    "indicator_type": "url",
    "indicator_data": {
      "url": "http://45.67.231.78:3214"
    },
    "intel_requirements": [
      "1.1.5",
      "1.1.6"
    ]
  },
  "meta": {
    "version": "0.1"
  },
  "last_updated": 1615345743440,
  "uid": "03966eb21fe3b33e026f3363b9f012af",
  "activity": {
    "first": 1615345265000,
    "last": 1615345719000
  }
}
```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                      | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY        | EXAMPLES                 | NOTES                                        |
|-----------------------------------------------------|-----------------|---------------------------------------------|--------------------------|----------------------------------------------|
| .alerts[].indicator.data.<br>indicator_data.url     | Indicator.Value | .alerts[].indicator.data.<br>indicator_type | http://45.67.231.78:3214 | View<br>Indicator<br>Type Map<br>table below |
| .alerts[].indicator.data.<br>indicator_data.address | Indicator.Value | .alerts[].indicator.data.<br>indicator_type | N/A                      | View<br>Indicator                            |

| FEED DATA PATH                                                                                                          | THREATQ ENTITY                                       | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                                                                                   | NOTES                |
|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------|----------------------|
|                                                                                                                         |                                                      |                                      |                                                                                            | Type Map table below |
| .alerts[].indicator.data.<br>indicator_data.file.type?                                                                  | Indicator.Attribute                                  | File Type                            | TEXT                                                                                       | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.file.md5?                                                                   | Indicator.Attribute                                  | File MD5 hash                        | 59d1f5846536ae9ef334b9<br>aebd9e8e92                                                       | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.file.sha1?                                                                  | Indicator.Attribute                                  | File SHA1 hash                       | 4acb7917cfc125e472db27<br>0f3743ff3cff64a3ab                                               | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.file.sha256 ?                                                               | Indicator.Attribute                                  | File SHA256 hash                     | 1fb6ed5ec4a03acd2e8a086<br>058446e3fc19497fd3f3f539<br>80b3bf3a2559bf24e                   | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.file.size?                                                                  | Indicator.Attribute                                  | File size                            | 700                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.file.download_url?                                                          | Indicator.Attribute                                  | File Download URL                    | https://api.intel471.com/v1/<br>download/malwareIntel/1fb<br>6ed5ec4a03acbf3a2559bf24e.zip | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.country<br>- .alerts[].indicator.data.<br>indicator_data.geo_ip.city | Indicator.Attribute                                  | Geo IP Location                      | United States - New York                                                                   | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.subdivision[]                                                        | Indicator.Attribute                                  | Geo IP Subdivision                   | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.isp.network                                                          | Indicator.Attribute                                  | ISP Network                          | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.<br>isp.autonomous_system                                            | Indicator.Attribute                                  | ISP Autonomous System                | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.isp.isp                                                              | Indicator.Attribute                                  | ISP Name                             | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>indicator_data.geo_ip.<br>isp.organization                                                 | Indicator.Attribute                                  | ISP organization                     | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.<br>threat.type                                                                                | Indicator.Attribute                                  | Threat Type                          | proxy_service                                                                              | N/A                  |
| .alerts[].indicator.data.<br>threat.data.family                                                                         | Related<br>Malware.Value                             | N/A                                  | smokeloader                                                                                | N/A                  |
| .alerts[].indicator.data.<br>threat.data.variant                                                                        | Indicator.Attribute,<br>Related<br>Malware.Attribute | N/A                                  | N/A                                                                                        | N/A                  |
| .alerts[].indicator.data.uid                                                                                            | Indicator.Attribute                                  | UID                                  | 29f58ed4a99ee32fc64c25f9670<br>e0f4e                                                       | N/A                  |
| .alerts[].indicator.data.<br>expiration                                                                                 | Indicator.Attribute                                  | Expiration Date                      | 1617937719000                                                                              | N/A                  |
| .alerts[].indicator.data.<br>confidence                                                                                 | Indicator.Attribute                                  | Confidence                           | high                                                                                       | N/A                  |
| .alerts[].indicator.data.<br>mitre_tactics                                                                              | Indicator.Attribute                                  | Mitre Tactics                        | command_and_control                                                                        | N/A                  |

| FEED DATA PATH                                | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES               | NOTES |
|-----------------------------------------------|---------------------|--------------------------------------|------------------------|-------|
| .alerts[].indicator.data.intel_requirements[] | Indicator.Attribute | Intelligence Requirements            | 1.1.3                  | N/A   |
| .alerts[].indicator.data.context.description  | Indicator.Attribute | Context                              | redline controller URL | N/A   |

## cveReport

### Sample Response:

```
{
  "alerts": [
    {
      "uid": "61ba31e66c54bd75836158ef",
      "status": "read",
      "watcherUid": "08022e2e4fe563abafb2ea15cd5047c1",
      "watcherGroupUid": "c68903fd-6f0e-4586-9eeb-0210b421af51",
      "foundTime": 1639592422960,
      "cveReport": {
        "data": {
          "cve_report": {
            "risk_level": "high",
            "name": "CVE-2021-45046",
            "activity_location": {
              "location_opensource": true,
              "location_underground": true,
              "location_private": false
            },
            "vendor_name": "Apache",
            "exploit_status": {
              "available": false,
              "weaponized": true,
              "productized": false
            },
            "titan_links": [
              {
                "title": "Для уязвимости в Log4j вышло второе исправление",
                "url": "https://titan.intel471.com/post_thread/7b887bdfb46e938e068721750154c3da?post_uid=a34b7e1eefe0e0dc2726553975d7dbb3"
              },
              {
                "title": "{warning} Log4Shell: RCE 0-day exploit found in log4j2,this is gonna be HUUUUUGE",
                "url": "https://titan.intel471.com/post_thread/b4e4a23d91e9a808b0416e75ac560509?post_uid=ee5faa6106cdad02731ceec7d7f16668"
              },
              {
                "title": "Apache Log4j (Java logging utility) major security flaw affects many systems across the world",

```

```

        "url": "https://titan.intel471.com/post_thread/
aacfb690e92324792ab1f6ae85853137?post_uid=30f61c614c5df54392f326767f0deab3"
    },
    ],
    "patch_status": "available",
    "poc": "not_observed",
    "counter_measures": "Apache addressed the vulnerability in Log4j
version 2.12.2 and Log4j version 2.16.0.",
    "interest_level": {
        "disclosed_publicly": true,
        "researched_publicly": true,
        "exploit_sought": false
    },
    "product_name": "Log4j",
    "cve_type": "Deserialization of untrusted data",
    "poc_links": [
        {
            "title": "Cloudflare: Protection against CVE-2021-45046, the
additional Log4j RCE vulnerability ",
            "url": " https://blog.cloudflare.com/protection-against-
cve-2021-45046-the-additional-log4j-rce-vulnerability/"
        }
    ],
    "cvss_score": {
        "v3": 9
    },
    "underground_activity_summary": "Intel 471 has not observed
weaponization or productization of CVE-2021-45046 in the underground. Several
actors shared information from open-source reporting.",
    "cve_status": "status_existing",
    "underground_activity": "observed",
    "patch_links": [
        {
            "title": "Apache Log4j version 2.16.0 ",
            "url": " https://logging.apache.org/log4j/2.x/download.html"
        },
        {
            "title": "Apache Log4j security update ",
            "url": " https://logging.apache.org/log4j/2.x/security.html"
        }
    ],
    "summary": "CVE-2021-45046 is a deserialization of untrusted data
vulnerability impacting Apache Log4j versions 2.0-beta9 through 2.12.1 and
2.13.0 through 2.15.0. A proof of concept (PoC) was not observed publicly or in
the underground. Security researchers claimed the vulnerability was being
actively exploited in the wild. This vulnerability exists because of an
incomplete fix for CVE-2021-44228."
    },
    },
    "last_updated": 1640270894000,

```

```

    "uid": "f46441257a7d8ec08af42b1a30aa2e72",
    "classification": {
      "intel_requirements": [
        "2.1",
        "2.1.2",
        "2.2"
      ]
    },
    "activity": {
      "first": 1639572023000,
      "last": 1639572023000
    }
  },
  "highlights": []
}
]
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                                            | THREATQ ENTITY                    | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                          | NOTES |
|---------------------------------------------------------------------------|-----------------------------------|--------------------------------------|----------------------------------|-----------------------------------|-------|
| .alerts[].cveReport.data.cve_report.name                                  | Indicator/Vulnerability.Value     | CVE                                  | .alerts[].cveReport.last_updated | CVE-2021-44228                    | N/A   |
| .alerts[].cveReport.uid                                                   | Indicator/Vulnerability.Attribute | UID                                  | .alerts[].cveReport.last_updated | 61ba31e66c54bd75836158ef          | N/A   |
| .alerts[].cveReport.classification.intel_requirements[]                   | Indicator/Vulnerability.Attribute | Intelligence Requirements            | .alerts[].cveReport.last_updated | 1.1.3                             | N/A   |
| .alerts[].cveReport.data.cve_report.cve_type                              | Indicator/Vulnerability.Attribute | CVE Type                             | .alerts[].cveReport.last_updated | Deserialization of untrusted data | N/A   |
| .alerts[].cveReport.data.cve_report.risk_level                            | Indicator/Vulnerability.Attribute | Risk Level                           | .alerts[].cveReport.last_updated | high                              | N/A   |
| .alerts[].cveReport.data.cve_report.vendor_name                           | Indicator/Vulnerability.Attribute | Affected Vendor                      | .alerts[].cveReport.last_updated | Apache                            | N/A   |
| .alerts[].cveReport.data.cve_report.product_name                          | Indicator/Vulnerability.Attribute | Affected Product                     | .alerts[].cveReport.last_updated | Log4j                             | N/A   |
| .alerts[].cveReport.data.cve_report.cve_status                            | Indicator/Vulnerability.Attribute | CVE Status                           | .alerts[].cveReport.last_updated | status_existing                   | N/A   |
| .alerts[].cveReport.data.cve_report.interest_level.disclosed_publicly     | Indicator/Vulnerability.Attribute | Disclosed Publicly                   | .alerts[].cveReport.last_updated | True                              | N/A   |
| .alerts[].cveReport.data.cve_report.interest_level.researched_publicly    | Indicator/Vulnerability.Attribute | Researched Publicly                  | .alerts[].cveReport.last_updated | True                              | N/A   |
| .alerts[].cveReport.data.cve_report.interest_level.exploit_sought         | Indicator/Vulnerability.Attribute | Exploit Sought                       | .alerts[].cveReport.last_updated | True                              | N/A   |
| .alerts[].cveReport.data.cve_report.activity_location.location_opensource | Indicator/Vulnerability.Attribute | Location Opensource                  | .alerts[].cveReport.last_updated | True                              | N/A   |

| FEED DATA PATH                                                                                                  | THREATQ ENTITY                        | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                   | EXAMPLES                                                                                                            | NOTES                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------|---------------------------------------|--------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .alerts[].cveReport.data.cve_report.activity_location.location_underground                                      | Indicator/Vulnerability.Attribute     | Location Underground                 | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.activity_location.location_private                                          | Indicator/Vulnerability.Attribute     | Location Private                     | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.exploit_status.available                                                    | Indicator/Vulnerability.Attribute     | Exploit Available                    | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.exploit_status.weaponized                                                   | Indicator/Vulnerability.Attribute     | Exploit Weaponized                   | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.exploit_status.productized                                                  | Indicator/Vulnerability.Attribute     | Exploit Productized                  | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.exploit_status.not_observed                                                 | Indicator/Vulnerability.Attribute     | Exploit Not Observed                 | .alerts[].cveReport.last_updated | True                                                                                                                | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.cvss_score.v3                                                               | Indicator/Vulnerability.Attribute     | CVSSv3 Score                         | .alerts[].cveReport.last_updated | 10                                                                                                                  | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.cvss_score.v2                                                               | Indicator/Vulnerability.Attribute     | CVSSv2 Score                         | .alerts[].cveReport.last_updated | 10                                                                                                                  | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.patch_links[].title + .alerts[].cveReport.data.cve_report.patch_links[].URL | Indicator/Vulnerability.Attribute     | Patch Reference                      | .alerts[].cveReport.last_updated | <a href="https://logging.apache.org/log4j/2.x/security.html">https://logging.apache.org/log4j/2.x/security.html</a> | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.patch_status                                                                | Indicator/Vulnerability.Attribute     | Patch Status                         | .alerts[].cveReport.last_updated | available                                                                                                           | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.underground_activity                                                        | Indicator/Vulnerability.Attribute     | Underground Activity                 | .alerts[].cveReport.last_updated | not_observed                                                                                                        | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.underground_activity_summary                                                | Indicator/Vulnerability.Attribute     | Underground Activity Summary         | .alerts[].cveReport.last_updated | it was not observed                                                                                                 | N/A                                                                                                                                                                                               |
| .alerts[].cveReport.data.cve_report.summary                                                                     | indicator/vulnerability.description   | N/A                                  | .alerts[].cveReport.foundTime    | Summary-CVE-2021-44228 is a remote code execution..."                                                               | Formatted as a concatenation between .cveReport.data.cve_report.summary and .cveReport.data.cve_report.counter_measures if present and .cveReport.data.cve_report.underground_activity if present |
| .alerts[].cveReport.data.cve_report.summary                                                                     | Related Indicator/Vulnerability.Value | CVE                                  | N/A                              | CVE-2021-55555                                                                                                      | N/A                                                                                                                                                                                               |

| FEED DATA PATH                                                                                                               | THREATQ ENTITY                        | THREATQ OBJECT<br>TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE                       | EXAMPLES                                                                                                                  | NOTES |
|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|--------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------|
| + .counter_measures<br>+ .underground_activity                                                                               |                                       |                                            |                                      |                                                                                                                           |       |
| .alerts[].cveReport.data.cve_report.detection                                                                                | Indicator/<br>Vulnerability.Attribute | Available<br>Detection                     | .alerts[].cveReport.<br>last_updated | not_available                                                                                                             | N/A   |
| .alerts[].cveReport.data.cve_report.titan_links[].title<br>+ .alerts[].cveReport.data.cve_report.titan_links[].url           | Indicator/<br>Vulnerability.Attribute | Titan Reference                            | .alerts[].cveReport.<br>last_updated | <a href="https://titan.intel471.com/ims_thread/4e68...">https://<br/>titan.intel471.<br/>com/ims_thread/<br/>4e68..."</a> | N/A   |
| .alerts[].cveReport.data.cve_report.poc                                                                                      | Indicator/<br>Vulnerability.Attribute | Proof of Concept                           | .alerts[].cveReport.<br>last_updated | observed                                                                                                                  | N/A   |
| .alerts[].cveReport.data.cve_report.poc_links[].title + .alerts[].<br>cveReport.data.cve_report.poc_links[].url              | Indicator/<br>Vulnerability.Attribute | POC Reference                              | .alerts[].cveReport.<br>last_updated | <a href="https://titan.intel471.com/ims_thread/4e68...">https://<br/>titan.intel471.<br/>com/ims_thread/<br/>4e68..."</a> | N/A   |
| .alerts[].cveReport.data.cve_report.counter_measures[].title<br>+ .alerts[].cveReport.data.cve_report.counter_measures[].url | Indicator<br>/Vulnerability.Attribute | Countermeasure<br>Reference                | .alerts[].cveReport.<br>last_updated | Apache addressed<br>the vulnerability in<br>L..."                                                                         | N/A   |

## spotReport

### Sample Response:

```
{
  "alertTotalCount": 112,
  "alerts": [
    {
      "uid": "62056cb98d92075f6ebc1964",
      "status": "unread",
      "foundTime": 1649362530976,
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "spotReport": {
        "activity": {
          "first": 1644504121000,
          "last": 1644504643000
        },
        "last_updated": 1644504643000,
        "uid": "df0ebc265cae31c8de3b329dc210e5cb",
        "data": {
          "spot_report": {
            "uid": "df0ebc265cae31c8de3b329dc210e5cb",
            "spot_report_data": {
              "victims": [
                {
                  "name": "Vodafone Portugal - Comunicações Pessoais S.A.",
                  "urls": [
                    "https://vodafone.pt/"
                  ]
                }
              ]
            },
            "date_of_information": 1641686400000,
            "text": "[POSSIBLE BREACH ALERT] On Jan. 9, 2022, the threat
group LAPSUS$ used the team's Telegram channel to hint about its possible
involvement in a recent cyberattack against the ...",
            "intel_requirements": [
              "6.2.4.39",
              "4.2.5",
              "6.1.8.3"
            ],
            "version": "1",
            "links": [
              {
                "type": "internal",
                "url": "https://titan.intel471.com/ims_thread/
52ff52aa56d10a1287274ecf02dccb5f?message_uid=b9d5ca129cd4134109343620f2073f36",
                "title": "Telegram post #1"
              },
              {
                "type": "internal",
```

```
{
  "url": "https://titan.intel471.com/ims_thread/76444b3132fda0e2aca778051d776f1c?message_uid=1a6c2dc8a7a725224d15c28b04efeac1",
  "title": "Telegram post #2"
},
{
  "type": "external",
  "url": "https://apnews.com/article/technology-business-europe-hacking-telecommunications-24b6daae9237b1d394f781b7e6497b04",
  "title": "Associated Press article"
}
],
"released_at": 1644504121000,
"title": "Threat group LAPSUS$ suggests possible involvement in cyberattack against Vodafone Portugal"
}
},
"entities": [
  {
    "type": "Handle",
    "value": "LAPSUS$"
  }
]
}
}
```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                               | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                                                     | EXAMPLES                 | NOTES                                                                                                                                                        |
|--------------------------------------------------------------|-----------------|--------------------------------------|--------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .alerts[].spotReport.data.spot_report.spot_report_data.title | Event.Value     | N/A                                  | .alerts[].spotReport.data.spot_report.spot_report_data.released_at | Tokyo                    | If .alerts[].spotReport.data.spot_report.spot_report_data.title exists in the response                                                                       |
| .alerts[].spotReport.uid                                     | Event.Value     | N/A                                  | alerts[].spotReport.data.spot_report.spot_report_data.released_at  | 014f7a860a14924b5cb74eeb | Formatted as Intel 471 Spot Report - 014f7a860a14924b5cb74eeb if .alerts[].spotReport.data.spot_report.spot_report_data.title does not exist in the response |
| N/A                                                          | Event.Attribute | Report Type                          | alerts[].spotReport.data.spot_report.spot_report_data.released_at  | Spot                     | Hardcoded attribute                                                                                                                                          |
| .alerts[].spotReport.uid                                     | Event.Attribute | Intel 471 Spot Report Link           | alerts[].spotReport.data.spot_report.spot_report_data.released_at  | 014f7a860a14924b5cb74eeb | Formatted as `https://titan.intel471.com/`                                                                                                                   |

| FEED DATA PATH                                                                                                                                                    | THREATQ ENTITY             | THREATQ OBJECT TYPE OR ATTRIBUTE KEY          | PUBLISHED DATE                                                                | EXAMPLES                                                                                                          | NOTES                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
|                                                                                                                                                                   |                            |                                               | spot_report_data.<br>released_at                                              |                                                                                                                   | spotReports/<br>{{.alerts[].spotReport.uid}} |
| .alerts[].spotReport.<br>data.spot_report.spot<br>_report_data.victims[].<br>name                                                                                 | Event.Attribute            | Victim                                        | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | N/A                                                                                                               | N/A                                          |
| .alerts[].spotReport.<br>data.spot_report.spot<br>_report_data.victims[].<br>urls[]                                                                               | Event.Attribute            | Victim URL                                    | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | N/A                                                                                                               | N/A                                          |
| .alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>sensitive_source                                                                               | Event.Attribute            | Sensitive Source                              | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | True                                                                                                              | N/A                                          |
| .alerts[].spotReport.<br>data.spot_report.spot<br>_report_data.intel_<br>requirements[]                                                                           | Event.Attribute            | Intelligence<br>Requirements                  | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | 1.1.3                                                                                                             | N/A                                          |
| .alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.links<br>[].title + .alerts[].<br>spotReport.data.spot_<br>report.spot_report_<br>data.links[].url | Event.Attribute            | Linked Entity                                 | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | Forum thread -<br>https://<br>titan.intel471.<br>com/post_<br>thread/<br>a6bff640bf0c<br>8d0ea3154<br>4878935e3a6 | N/A                                          |
| .alerts[].spotReport.<br>data.entities[].value                                                                                                                    | Related<br>Adversary.Value | N/A                                           | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | LAPSUS\$                                                                                                          | If `` is Handl e                             |
| .alerts[].spotReport.<br>data.entities[].value                                                                                                                    | Related<br>Indicator.Value | .alerts[].spotReport.<br>data.entities[].type | alerts[].spotReport.<br>data.spot_report.<br>spot_report_data.<br>released_at | 72.217.16.46                                                                                                      | View Indicator Type Map<br>table bellow      |

## instantMessage

### Sample Response:

```
{
  "alerts": [
    {
      "uid": "61ba31e66c54bd75836158ef",
      "status": "read",
      "watcherUid": "08022e2e4fe563abafb2ea15cd5047c1",
      "watcherGroupUid": "c68903fd-6f0e-4586-9eeb-0210b421af51",
      "foundTime": 1639592422960,
      "instantMessage": {
        "data": {
          "message": {
            "uid": "88ea4933296e7c159bdf3d104720ba98",
            "text": "<article class=\"chatMessage\">...</article>",
            "attachments": [
              {
                "size": 38475,
                "uid": "telegram/media/9345/434819",
                "type": "image/jpeg",
                "original_url": "https://www.securitylab.ru/news/529621.php"
              }
            ]
          },
          "channel": {
            "name": "LAPSUS$ Chat",
            "url": "https://t.me/saudechat",
            "registration_date": 1639580760000,
            "uid": "76444b3132fda0e2aca778051d776f1c"
          },
          "server": {
            "uid": "70efdf2ec9b086079795c442636b55fb",
            "service_type": "Telegram"
          },
          "actor": {
            "uid": "fc90deed16ed5814f5b43c26299db325",
            "handle": "CARDANNA"
          }
        },
        "last_updated": 1644647086702,
        "activity": {
          "first": 1644647078000,
          "last": 1644647078000
        }
      }
    }
  ]
}
```

```
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                                                                                                 | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                        | EXAMPLES                                                                                                                                                                                | NOTES                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------------------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| .alerts[].instantMessage.data.message.text                                                                                     | Event.Attribute     | Message Text                         | .alerts[].instantMessage.last_updated | Message Instant                                                                                                                                                                         | Stripped HTML tags                                                                                                      |
| .alerts[].instantMessage.data.message.attachments[].type<br>- .alerts[].instantMessage.data.message.attachments[].original_url | Event.Attribute     | Message Attachment                   | .alerts[].instantMessage.last_updated | <a href="https://api.telegram.org/tg-photo/474992438154472501/-7907434886400454512-image/jpeg">https://api.telegram.org/tg-photo/474992438154472501/-7907434886400454512-image/jpeg</a> | Stripped HTML tags                                                                                                      |
| .alerts[].instantMessage.data.channel.name                                                                                     | Event.Attribute     | Channel Name                         | .alerts[].instantMessage.last_updated | LAPSUS\$ Chat                                                                                                                                                                           | Stripped HTML tags                                                                                                      |
| .alerts[].instantMessage.data.channel.url                                                                                      | Event.Attribute     | Channel URL                          | .alerts[].instantMessage.last_updated | <a href="https://t.me/saudechat">https://t.me/saudechat</a>                                                                                                                             | N/A                                                                                                                     |
| .alerts[].instantMessage.data.channel.topic                                                                                    | Event.Attribute     | Channel Topic                        | .alerts[].instantMessage.last_updated | Vodafone                                                                                                                                                                                | N/A                                                                                                                     |
| .alerts[].instantMessage.data.server.service_type                                                                              | Event.Attribute     | Service Type                         | .alerts[].instantMessage.last_updated | Telegram                                                                                                                                                                                | N/A                                                                                                                     |
| .alerts[].instantMessage.data.server.name                                                                                      | Event.Attribute     | Service Name                         | .alerts[].instantMessage.last_updated | N/A                                                                                                                                                                                     | N/A                                                                                                                     |
| .alerts[].instantMessage.data.server.uid                                                                                       | Event.Attribute     | Service UID                          | .alerts[].instantMessage.last_updated | 70efdf2ec9b086079795c442636b55fb                                                                                                                                                        | N/A                                                                                                                     |
| N/A                                                                                                                            | Adversary.Attribute | Actor Type                           | .alerts[].instantMessage.last_updated | Recipient                                                                                                                                                                               | N/A                                                                                                                     |
| .alerts[].instantMessage.data.actor.handle                                                                                     | Adversary.Name      | N/A                                  | .alerts[].instantMessage.last_updated | carter                                                                                                                                                                                  | Hardcoded Attribute                                                                                                     |
| .alerts[].instantMessage.data.actor.handle                                                                                     | Adversary.Attribute | Intel471 Actor Link                  | .alerts[].instantMessage.last_updated | <a href="https://titan.intel471.com/search/Actor:carter">https://titan.intel471.com/search/Actor:carter</a>                                                                             | Formatted as <code>https://titan.intel471.com/search/Actor:{{.alerts[].instantMessage.links.authorActor.handle}}</code> |

## credential

### Sample Response:

```
{
  "credentials_total_count": 123,
  "credentials": [
    {
      "uid": "08c9a1e7e811617a79290108cdc23b36",
      "data": {
        "credential_login": "john.smith@test-domain.com",
        "credential_domain": "test-domain.com",
        "detection_domain": "test-domain.com",
        "affiliations": [
          "my_employees"
        ],
        "password": {
          "complexity": {
            "lowercase": 15,
            "uppercase": 0,
            "numbers": 17,
            "symbols": 0,
            "punctuation_marks": 0,
            "separators": 0,
            "other": 0,
            "length": 32,
            "score": 0.9525726035123216,
            "weakness": 0.09375,
            "entropy": 121.83535750584332
          },
          "strength": "excellent",
          "id": "81105f09",
          "password_plain": "bad_pswrd"
        },
        "credential_sets": [
          {
            "uid": "13951971fbce4bd11dc1eb13f04da669",
            "name": "Infostealer Collection"
          }
        ],
        "detected_malware": [
          {
            "family": "[Raccoon Stealer] - v1.0 Golden Master Release"
          },
          {
            "family": "Azorult V3+"
          },
          {
            "family": "KPOT"
          }
        ]
      }
    }
  ]
}
```

```

    ]
  },
  "statistics": {
    "accessed_urls_total_count": 1
  },
  "classification": {
    "intel_requirements": [
      "2.1.1.1",
      "2.2.1",
      "2.2.2"
    ]
  },
  "last_updated": 1583241868411,
  "activity": {
    "first": 1569271060000,
    "last": 1569271060000
  }
}
]
}

```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                                | THREATQ ENTITY     | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                  | EXAMPLES                         | NOTES |
|---------------------------------------------------------------|--------------------|--------------------------------------|---------------------------------|----------------------------------|-------|
| .alerts[].credential.data.credential_login                    | Identity.Value     | N/A                                  | .alerts[].credential.activeFrom | john.smith@test-domain.com       | N/A   |
| .alerts[].credential.uid                                      | Identity.Attribute | UID                                  | .alerts[].credential.activeFrom | 08c9a1e7e811617a79290108cdc23b36 | N/A   |
| .alerts[].credential.data.credential_domain                   | Identity.Attribute | Credential Domain                    | .alerts[].credential.activeFrom | test-domain.com                  | N/A   |
| .alerts[].credential.data.detection_domain                    | Identity.Attribute | Detection Domain                     | .alerts[].credential.activeFrom | test-domain.com                  | N/A   |
| .alerts[].credential.data.affiliations[]                      | Identity.Attribute | Affiliation                          | .alerts[].credential.activeFrom | my_employees                     | N/A   |
| .alerts[].credential.data.detected_malware[].family           | Related Malware    | N/A                                  | .alerts[].credential.activeFrom | Azorult V3+                      | N/A   |
| .alerts[].credential.statistics.accessed_urls_total_count     | Identity.Attribute | Accessed URLs Total Count            | .alerts[].credential.activeFrom | 12                               | N/A   |
| .alerts[].credential.data.classification.intel_requirements[] | Identity.Attribute | Intelligence Requirements            | .alerts[].credential.activeFrom | 1.1.2                            | N/A   |

## breachAlert

### Sample Response:

```
{
  "alertTotalCount": 112,
  "alerts": [
    {
      "uid": "ca4f7a860a14924b5cb74eeb",
      "status": "unread",
      "foundTime": 1649362530976,
      "watcherGroupUid": "a087c78d-8997-436a-9cb2-b7ccd3de7419",
      "breachAlert": {
        "activity": {
          "first": 1623248165000,
          "last": 1623314255000
        },
        "last_updated": 1623314255000,
        "uid": "6d4f1fafe5eadc654397e36b9001c9cb",
        "data": {
          "breach_alert": {
            "title": "BCN Telecom Inc. possibly compromised by actor/group
hakkr on Feb 22, 2021",
            "date_of_information": 1613952000000,
            "released_at": 1623248165000,
            "confidence": {
              "level": "low",
              "description": "The source credibility or accuracy of the
information cannot be judged."
            },
            "actor_or_group": "hakkr",
            "victim": {
              "name": "BCN Telecom Inc.",
              "urls": [
                "https://www.bcntele.com/"
              ],
              "industries": [
                {
                  "industry": "Telecommunications",
                  "sector": "Communications"
                }
              ],
              "revenue": "$19.9M",
              "region": "Northern America"
            },
            "sources": [
              {
                "type": "internal",
                "url": "https://titan.intel471.com/post_thread/
3e7e2a9a4efb78d9f6d1fc79035c1750?post_uid=a7906e947a62303d6afa026bbb90013d",
```

```

        "title": "Godzilla Loader",
        "date": 1534712400000,
        "source_type": "Post Thread"
    },
    {
        "type": "internal",
        "url": "https://titan.intel471.com/report/3bd7fde77e3818a12362efc5ac758395",
        "title": "Russian actor alfamale advertising a new cryptolocker dubbed TURBO.",
        "date": 1470258000000,
        "source_type": "Information Report"
    },
    {
        "type": "external",
        "url": "https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network",
        "title": "Citrix investigating unauthorized access to internal network",
        "date": 1552082400000,
        "source_type": "Citrix blog"
    }
],
"intel_requirements": [
    "1.1.3",
    "1.1.4",
    "1.1"
]
},
"entities": [
    {
        "type": "Handle",
        "value": "hakkr"
    },
    {
        "description": "One of the Google's IP",
        "geo_info": {
            "provider": "Google",
            "country": "US"
        },
        "type": "IPAddress",
        "value": "172.217.16.46"
    }
]
}
}
```

ThreatQ provides the following default mapping:

| FEED DATA PATH                                                                   | THREATQ ENTITY   | THREATQ OBJECT TYPE OR ATTRIBUTE KEY                                       | PUBLISHED DATE                                      | EXAMPLES                                                                                 | NOTES                                                                                |
|----------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| N/A                                                                              | Event. Attribute | Event Type                                                                 | .alerts[].breachAlert.data.breach_alert.released_at | Breach Alert                                                                             | Hardcoded attribute                                                                  |
| .alerts[].breachAlert.data.breach_alert.title                                    | Event. Attribute | BCN Telecom Inc. possibly compromised by actor/group hakkr on Feb 22, 2021 | .alerts[].breachAlert.data.breach_alert.released_at | Tokyo                                                                                    | N/A                                                                                  |
| .alerts[].breachAlert.uid                                                        | Event. Attribute | Intel 471 Breach Alert Link                                                | .alerts[].breachAlert.data.breach_alert.released_at | 014f7a860a14924b5cb74eeb                                                                 | Formatted as `https://titan.intel471.com/breachAlerts/{{.alerts[].breachAlert.uid}}` |
| .alerts[].breachAlert.data.breach_alert.confidence.description                   | Event. Attribute | Confidence                                                                 | .alerts[].breachAlert.data.breach_alert.released_at | low                                                                                      | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.confidence.level                         | Event. Attribute | Confidence Level                                                           | .alerts[].breachAlert.data.breach_alert.released_at | The source credibility or accuracy of the information cannot be judged.                  | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.sensitive_source                         | Event. Attribute | Sensitive Source                                                           | .alerts[].breachAlert.data.breach_alert.released_at | True                                                                                     | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.intel_requirements[]                     | Event. Attribute | Intelligence Requirements                                                  | .alerts[].breachAlert.data.breach_alert.released_at | 1.1.3                                                                                    | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.name                              | Event. Attribute | Victim                                                                     | .alerts[].breachAlert.data.breach_alert.released_at | BCN Telecom Inc.                                                                         | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.urls[]                            | Event. Attribute | Victim URL                                                                 | .alerts[].breachAlert.data.breach_alert.released_at | https://www.bcntele.com/                                                                 | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.industries[].industry             | Event. Attribute | Victim Industry                                                            | .alerts[].breachAlert.data.breach_alert.released_at | Telecommunications                                                                       | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.industries[].sector               | Event. Attribute | Victim Sector                                                              | .alerts[].breachAlert.data.breach_alert.released_at | Communications                                                                           | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.region                            | Event. Attribute | Victim Region                                                              | .alerts[].breachAlert.data.breach_alert.released_at | \$19.9M                                                                                  | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.victim.revenue                           | Event. Attribute | Victim Revenue                                                             | .alerts[].breachAlert.data.breach_alert.released_at | Northern America                                                                         | N/A                                                                                  |
| .alerts[].breachAlert.data.breach_alert.sources[].title - .alerts[].breachAlert. | Event. Attribute | Source                                                                     | .alerts[].breachAlert.data.breach_alert.released_at | Godzilla Loader - https://titan.intel471.com/post_thread/3e7e2a9a4efb78d9f6d1fc79035c175 | N/A                                                                                  |

| FEED DATA PATH                                                  | THREATQ ENTITY                       | THREATQ OBJECT TYPE OR ATTRIBUTE KEY           | PUBLISHED DATE                                          | EXAMPLES                                           | NOTES                                  |
|-----------------------------------------------------------------|--------------------------------------|------------------------------------------------|---------------------------------------------------------|----------------------------------------------------|----------------------------------------|
| data.breach<br>_alert.sources[].url                             |                                      |                                                |                                                         | 0post_uid=a7906e947a62<br>303d6afa<br>026bbb90013d |                                        |
| .alerts[].breachAlert.<br>data.entities<br>[].value             | Related<br>Adversary.<br>Value       | N/A                                            | .alerts[].breachAlert.data.<br>breach_alert.released_at | LAPSUS\$                                           | If `` is HandLe                        |
| .alerts[].breachAlert.<br>data.entities<br>[].value             | Related<br>Indicator.<br>Value       | .alerts[].breachAlert.<br>data.entities[].type | .alerts[].breachAlert.data.<br>breach_alert.released_at | 72.217.16.46                                       | View Indicator Type<br>Map table below |
| .alerts[].breachAlert.<br>data.entities<br>[].description       | Related<br>Indicator.<br>Description | N/A                                            | .alerts[].breachAlert.data.<br>breach_alert.released_at | One of the Google's IP                             | N/A                                    |
| .alerts[].breachAlert.<br>data.entities<br>[].geo_info.provider | Related<br>Indicator.<br>Attribute   | Provider                                       | .alerts[].breachAlert.data.<br>breach_alert.released_at | Google                                             | N/A                                    |
| .alerts[].breachAlert.<br>data.entities<br>[].geo_info.country  | Related<br>Indicator.<br>Attribute   | Country                                        | .alerts[].breachAlert.data.<br>breach_alert.released_at | US                                                 | N/A                                    |

## Get Report by ID (Supplemental)

The value of `.alerts[].report.id` from the Intel471 Alerts feed is used as the `reportId` parameter.

GET - <https://api.intel471.com/v1/reports/{reportId}>

### Sample Response:

```
{
  "uid": "4bb9dc1c4385259236a2104227eed0c739eb5fe6c8914a955d516982c60bf358",
  "documentFamily": "INFOREP",
  "documentType": "INFOREP",
  "admiraltyCode": "B2",
  "motivation": [
    "CC"
  ],
  "subject": "Russian actor, bulletproof hoster yalishanda (aka downlow, stas_vl) adds 33 front-end proxies to fast-flux offering; Current proxy-net size sits at 305 IP addresses",
  "created": 1636119112000,
  "dateOfInformation": 1636070400000,
  "sourceCharacterization": "Information was derived from a reliable source in direct contact with yalishanda and visibility into the actor's bulletproof hosting service.",
  "relatedReports": [
    {
      "uid": "d2e15d5df8fe208de17733c3ed9d95c46aa5e995dca1003d3731d5e4137d6551",
      "documentFamily": "INFOREP"
    },
    {
      "uid": "aa210760432ea8bf21ed3bf42068c365bf8fa34fd4c678d321ef066055625e45",
      "documentFamily": "INFOREP"
    },
    {
      "uid": "b15c66f6ac04d8ffdb9a7034d41bd83ae27e0cf67714ec789ac4de9dfd708677",
      "documentFamily": "INFOREP"
    },
    {
      "uid": "e8899fead398c0aea60922861289dfae9ed29b9e893319af92925221027e2bdb",
      "documentFamily": "INFOREP"
    },
    {
      "uid": "64fbf40197070ae0745a8e37d5e5b6a8ae39ba512017bd1fecb795b1f37b9aab",
      "documentFamily": "INFOREP"
    }
  ]
}
```

```

],
"locations":[
  {
    "region":"Asia",
    "country":"Vietnam",
    "link":"impacts"
  }
],
"entities":[
  {
    "type":"IPAddress",
    "value":"109.248.201.128"
  },
  {
    "type":"IPAddress",
    "value":"176.118.164.123"
  },
  {
    "type":"IPAddress",
    "value":"176.57.220.153"
  },
  {
    "type":"IPAddress",
    "value":"178.208.75.53"
  }
],
"tags":[
  "Banking & Finance",
  "Bulletproof Hosting",
  "Bulletproof Hosting Tracking",
  "Extortion",
  "Malware - Usage",
  "Phishing",
  "Ransomware"
],
"portalReportUrl":"https://titan.intel471.com/report/inforep/
119363037d964917a1a109897da0488f",
"lastUpdated":1636119114000,
"actorSubjectOfReport":[
  {
    "handle":"yalishanda"
  }
],
"classification":{
  "intelRequirements":[
    "3.1.1"
  ]
},
"reportAttachments":[
  {

```

```

        "url": "https://api.intel471.com/v1/reports/download/
119363037d964917a1a109897da0488f/
6637dcf7c72836a7a9a0610b7f7c5d5fbe78846b71ad75fce5a2c836efe7e595",
        "fileName": "2021-11-05_yalishanda_report.csv",
        "malicious": false,
        "mimeType": "text/csv",
        "fileSize": 1669595
    }
],
    "researcherComments": "<p>Through the course of our research, we identified
the following new domain names and malware hashes associated with the hosts
featured in the latest snapshot of <strong>yalishanda's</strong> fast-flux
network. </p><p>Note that:</p><p>(1) If an IP address is not included in the
table below, this indicates no new domain names or malware hashes were
associated with that IP address.</p><p>(2) When attributing or classifying this
activity, it should be kept in mind these likely are the efforts of clients
using <strong>yalishanda's</strong> fast-flux service. The service rotates IP
addresses on an unknown schedule and pattern, so it's unclear whether proxies
are shared across clients, specific to subsets of clients, etc.</p><p>(3) All
hashes were classified as malware-related based on automated antivirus
detection and may not be accurate.</p><p>(4) The domain names listed below were
the result of passive domain name system (DNS) resolution only for the last few
days.</p><p>(5) A full list of all domain names and hashes previously and
recently observed at the actor's fast-flux infrastructure is provided (see:
Attachment). </p><figure class=\"table\"><table><thead><tr><th>IP address</
th><th>Entity type</th><th>Entity</th></tr></thead><tbody><tr><td>5.8.76.183</
td><td>MaliciousURL</td><td>nksa-abn.ru</td></tr><tr><td>5.8.76.183</
td><td>MaliciousURL</td><td>5qe71b9pqv.xixa-abn.ru</td></
tr><tr><td>5.8.76.183</td><td>MaliciousURL</td><td>adx-abn.ru</td></
tr><tr><td>5.8.76.183</td><td>MaliciousURL</td><td>uka-abn.ru</td></
tr><tr><td>5.8.76.183</td><td>MaliciousURL</td><td>ixax-abn.ru</td></
tr><tr><td>5.8.76.183</td><td>MaliciousURL</td><td>xixa-abn.ru</td></
tr><tr><td>5.8.76.203</td><td>MaliciousURL</td><td>mobi-credits.com</td></
tr><tr><td>5.8.76.203</td><td>MaliciousURL</td><td>nationaleqc-bnc.com</td></
tr><tr><td>5.8.76.203</td><td>MaliciousURL</td><td>login-bncapp.com</td></
tr><tr><td>8.209.67.54</td><td>MaliciousURL</td><td>parcel-support-
redelivery.com</td></tr><tr><td>8.209.67.54</td><td>MaliciousURL</
td><td>www.parcel-support-redelivery.com</td></tr><tr><td>8.209.73.107</
td><td>MaliciousURL</td><td>hsydv.wordmerry.link</td></
tr><tr><td>8.209.73.107</td><td>MaliciousURL</td><td>ca0r43.brightfair.link</
td></tr><tr><td>8.209.73.107</td><td>MaliciousURL</td><td>z4i6r.nur-fur-
sie.link</td></tr><tr><td>8.209.73.107</td><td>MaliciousURL</td><td>wso18.nur-
fur-sie.link</td></tr><tr><td>8.209.73.107</td><td>MaliciousURL</
td><td>g2aqf.shakyhot.link</td></tr><tr><td>8.209.73.107</td><td>MaliciousURL</
td><td>wjsb1.wordmerry.link</td></tr><tr><td>8.209.73.107</
td><td>MaliciousURL</td><td>8tm4o.wordmerry.link</td></
tr><tr><td>8.209.73.107</td><td>MaliciousURL</td><td>vvrd9.wordmerry.link</
td></tr><tr><td>8.209.73.107</td><td>MaliciousURL</
td><td>3gqpf.wordmerry.link</td></tr><tr><td>8.209.76.37</td><td>MaliciousURL</
td><td>www.wwrbcwrd.com</td></tr><tr><td>8.209.79.72</td><td>MaliciousURL</

```

```

td><td>www.nhs.gov-covid-applications.com</td></tr><tr><td>8.209.79.72</
td><td>MaliciousURL</td><td>nhs.gov-covid-form.com</td></
tr><tr><td>8.209.79.72</td><td>MaliciousURL</td><td>gov-covid-
applications.com</td></tr><tr><td>8.209.79.72</td><td>MaliciousURL</
td><td>nhs.gov-covid-apply.com</td></tr><tr><td>8.209.115.212</
td><td>MaliciousURL</td><td>vaccinepass-status-apply.com</td></
tr><tr><td>45.8.127.42</td><td>MaliciousURL</td><td>wfaccount.com</td></
tr><tr><td>45.8.127.42</td><td>MaliciousURL</
td><td>wellsfargosecurityaccount.com</td></tr><tr><td>45.8.127.174</
td><td>MaliciousURL</td><td>perc30.top</td></tr><tr><td>47.74.85.56</
td><td>MaliciousURL</td><td>omgevingskeuzelogin.info</td></
tr><tr><td>47.74.89.219</td><td>MaliciousURL</td><td>xas.mworx-sia.com</td></
tr><tr><td>47.74.91.80</td><td>MaliciousURL</td><td>online-
ups.ups.com.houseonlysaveor.com</td></tr><tr><td>47.88.0.94</
td><td>MaliciousURL</td><td>pancakeswoap.finance</td></tr><tr><td>47.88.0.94</
td><td>MaliciousURL</td><td>pancakeswoap.finance</td></tr><tr><td>47.88.0.94</
td><td>MaliciousURL</td><td>pakaceswoap.finance</td></tr><tr><td>47.88.0.94</
td><td>MaliciousURL</td><td>pancoclswaop.finance</td></tr><tr><td>47.88.0.94</
td><td>MaliciousURL</td><td>www.pancociswap-financial.com</td></
tr><tr><td>47.88.0.94</td><td>MaliciousURL</td><td>pankoceswaop.finance</td></
tr><tr><td>47.88.0.94</td><td>MaliciousURL</td><td>pankaceswwap-invest.com</
td></tr><tr><td>47.88.0.94</td><td>MaliciousURL</td><td>pancociswap-
market.com</td></tr><tr><td>47.88.0.94</td><td>MaliciousURL</
td><td>pancociswap.finance</td></tr><tr><td>47.88.0.94</td><td>MaliciousURL</
td><td>pankakiswaop.finance</td></tr><tr><td>47.88.0.94</td><td>MaliciousURL</
td><td>pancokiswaop-api.com</td></tr><tr><td>47.89.253.69</
td><td>MaliciousURL</td><td>nob4m.top</td></tr><tr><td>47.91.91.52</
td><td>MaliciousURL</td><td>www1.amigos.gs</td></tr><tr><td>47.91.91.52</
td><td>MaliciousURL</td><td>wap.amigos.gs</td></tr><tr><td>47.91.94.163</
td><td>MaliciousURL</td><td>www.airdrop-token8398.quest</td></
tr><tr><td>47.251.7.156</td><td>MaliciousURL</td><td>cpanel.unicshop.su</td></
tr><tr><td>47.251.7.156</td><td>MaliciousURL</td><td>mail.unicshop.su</td></
tr><tr><td>47.254.35.165</td><td>MaliciousURL</td><td>lbreal-coaching.com</
td></tr><tr><td>47.254.170.157</td><td>MaliciousURL</td><td>verwalten-
pushtan.com</td></tr><tr><td>47.254.177.70</td><td>MaliciousURL</td><td>nksa-
abn.ru</td></tr><tr><td>47.254.177.70</td><td>MaliciousURL</td><td>ixax-
abn.ru</td></tr><tr><td>47.254.177.70</td><td>MaliciousURL</td><td>xixa-
abn.ru</td></tr><tr><td>47.254.177.70</td><td>MaliciousURL</td><td>adx-abn.ru</
td></tr><tr><td>47.254.177.70</td><td>MaliciousURL</td><td>uka-abn.ru</td></
tr><tr><td>47.254.184.183</td><td>MaliciousURL</td><td>hh3valve.com</td></
tr><tr><td>77.87.212.198</td><td>MaliciousURL</td><td>bazfdr35.top</td></
tr><tr><td>77.220.213.77</td><td>MaliciousURL</td><td>fumueb14.top</td></
tr><tr><td>77.220.213.77</td><td>MaliciousURL</td><td>morimk03.top</td></
tr><tr><td>77.232.42.200</td><td>MaliciousURL</td><td>m.teledata.top</td></
tr><tr><td>79.141.171.22</td><td>MaliciousURL</td><td>80145.closeresult.link</
td></tr><tr><td>79.141.171.22</td><td>MaliciousURL</
td><td>9zyt.wordmerry.link</td></tr><tr><td>80.71.158.91</
td><td>MaliciousURL</td><td>8tm4o.wordmerry.link</td></
tr><tr><td>80.71.158.91</td><td>MaliciousURL</td><td>v7dv8.wordmerry.link</
td></tr><tr><td>80.71.158.91</td><td>MaliciousURL</
td><td>9pwm1.wordmerry.link</td></tr><tr><td>80.71.158.91</

```

```

td><td>MaliciousURL</td><td>10zjo.wordmerry.link</td></
tr><tr><td>80.71.158.91</td><td>MaliciousURL</td><td>xnena.wordmerry.link</
td></tr><tr><td>85.143.175.87</td><td>MaliciousURL</
td><td>269377.simplecloud.ru</td></tr><tr><td>85.143.175.133</
td><td>MaliciousURL</td><td>fedalgaberezvomendes.net</td></
tr><tr><td>85.143.175.133</td><td>MaliciousURL</
td><td>yolemezgayredohlazgabrides.net</td></tr><tr><td>85.143.175.133</
td><td>MaliciousURL</td><td>olivezfaredenfoydereseq.net</td></
tr><tr><td>85.143.175.201</td><td>MaliciousURL</td><td>fumueb14.top</td></
tr><tr><td>85.143.175.201</td><td>MaliciousURL</td><td>fumnar04.top</td></
tr><tr><td>85.143.175.201</td><td>MaliciousURL</td><td>fumhac05.top</td></
tr><tr><td>85.143.175.201</td><td>MaliciousURL</td><td>nkb-mod.top</td></
tr><tr><td>85.143.175.201</td><td>MaliciousURL</td><td>nkb-mod.xyz</td></
tr><tr><td>91.240.242.17</td><td>MaliciousURL</td><td>morimk03.top</td></
tr><tr><td>91.240.242.17</td><td>MaliciousURL</td><td>fumueb14.top</td></
tr><tr><td>91.240.242.108</td><td>MaliciousURL</
td><td>static.108.242.240.91.ip.webhost1.net</td></tr><tr><td>93.189.41.99</
td><td>MaliciousURL</td><td>ch-blockchain.com</td></tr><tr><td>93.189.42.100</
td><td>MaliciousURL</td><td>fumnar04.top</td></tr><tr><td>94.142.143.206</
td><td>MaliciousURL</td><td>adx-abn.ru</td></tr><tr><td>94.142.143.206</
td><td>MaliciousURL</td><td>uka-abn.ru</td></tr><tr><td>94.142.143.206</
td><td>MaliciousURL</td><td>nksa-abn.ru</td></tr><tr><td>94.142.143.206</
td><td>MaliciousURL</td><td>ixax-abn.ru</td></tr><tr><td>94.142.143.206</
td><td>MaliciousURL</td><td>pushtan-verwalten.info</td></
tr><tr><td>94.142.143.206</td><td>MaliciousURL</td><td>xixa-abn.ru</td></
tr><tr><td>109.248.201.128</td><td>MaliciousURL</td><td>knp-mod.xyz</td></
tr><tr><td>109.248.201.128</td><td>MaliciousURL</td><td>oneographmh.site</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>bazmoz34.top</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>baznsu31.top</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>bazfdr35.top</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>bazwio38.top</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>bazzko33.top</td></
tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>vds2144387.my-ihor.ru</
td></tr><tr><td>185.87.48.171</td><td>MaliciousURL</td><td>bazwuk32.top</td></
tr><tr><td>185.104.114.127</td><td>MaliciousURL</td><td>ch-blockchain.com</
td></tr><tr><td>185.186.142.46</td><td>MaliciousURL</td><td>national-bnc-
qc.com</td></tr><tr><td>185.186.142.46</td><td>MaliciousURL</td><td>amaz-
team.com</td></tr><tr><td>185.186.142.56</td><td>MaliciousURL</
td><td>spookyswab.com</td></tr><tr><td>185.186.142.56</td><td>MaliciousURL</
td><td>www.kyberswab.com</td></tr><tr><td>185.186.142.56</td><td>MaliciousURL</
td><td>swibe.org</td></tr><tr><td>185.186.142.56</td><td>MaliciousURL</
td><td>mooniswab.exchange</td></tr><tr><td>185.186.142.206</
td><td>MaliciousURL</td><td>pancakeswaps.name</td></tr><tr><td>185.224.212.78</
td><td>MaliciousURL</td><td>www.eguntong.com</td></tr><tr><td>185.237.206.157</
td><td>MaliciousURL</td><td>fumueb14.top</td></tr><tr><td>185.237.206.157</
td><td>MaliciousURL</td><td>fumnar04.top</td></tr><tr><td>185.246.154.135</
td><td>MaliciousURL</td><td>dev.realpem.com</td></tr><tr><td>185.246.154.140</
td><td>MaliciousURL</td><td>0ql9a.wordmerry.link</td></
tr><tr><td>188.225.33.123</td><td>MaliciousURL</td><td>686973-
cu96401.tmweb.ru</td></tr><tr><td>193.42.113.55</td><td>MaliciousURL</
td><td>auth-certify2a.online</td></tr><tr><td>193.106.175.27</

```

```
td><td>MaliciousURL</td><td>www.gov.uk-tax-refund896.com</td></tr><tr><td>193.106.175.59</td><td>MaliciousURL</td><td>ch-blockchain.com</td></tr><tr><td>193.106.175.59</td><td>MaliciousURL</td><td>www.tesla-santander.com</td></tr></tbody></table></figure><p>A full list of domain names that resolved to the 305 IP addresses above during the period is provided (see: Attachment).</p>",
```

```
"rawText": "<p>On Nov. 5, 2021, a reliable source who has direct visibility of the actor <strong>yalishanda's</strong> fast-flux infrastructure provided the following information:</p><p>---<br>As of 10 a.m. GMT, Nov. 5, 2021, the actor <strong>yalishanda's</strong> fast-flux infrastructure comprised the following hosts:</p><figure class=\"table\"><table><thead><tr><th>IP address</th><th>Country</th><th>Hosting Company</th></tr></thead><tbody><tr><td>2.57.184.90</td><td>RUS</td><td>CloudLite LLC</td></tr><tr><td>2.57.184.107</td><td>RUS</td><td>CloudLite LLC</td></tr><tr><td>2.59.36.16</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.20</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.42</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.43</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.73</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.82</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>5.8.76.183</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.185</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.203</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.205</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.207</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.208</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.8.76.216</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.53.125.140</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.101.51.33</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.101.51.39</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>5.101.51.48</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.101.51.195</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.188.3.56</td><td>RUS</td><td>G-Core Labs S.A.</td></tr><tr><td>5.188.88.14</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>5.188.88.20</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>5.188.88.118</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>5.188.88.120</td><td>USA</td><td>PINVDS</td></tr><tr><td>5.188.88.133</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>5.188.88.187</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>5.188.89.11</td><td>RUS</td><td>PINVDS OU</td></tr><tr><td>8.209.64.21</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.64.34</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.64.110</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.65.190</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.65.206</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.66.156</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.67.54</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.67.97</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.68.244</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.69.172</td><td>DEU</td><td>Alibaba</td></tr></tbody></table></figure>
```

```
tr><tr><td>8.209.69.173</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.70.250</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.73.107</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.76.37</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.77.15</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.78.144</td><td>USA</td><td>Alibaba.com LLC</td></tr><tr><td>8.209.78.156</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.79.72</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.112.76</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.115.212</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.210.134.143</td><td>HKG</td><td>Alibaba</td></tr><tr><td>31.41.44.221</td><td>RUS</td><td>Relink LTD</td></tr><tr><td>31.184.253.64</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>31.184.254.110</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>37.72.131.27</td><td>RUS</td><td>Fop Iliushenko Volodymyr Olexandrovuch</td></tr><tr><td>37.72.131.116</td><td>RUS</td><td>Fop Iliushenko Volodymyr Olexandrovuch</td></tr><tr><td>37.228.117.150</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>45.8.124.7</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.124.70</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.124.204</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.124.234</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.127.42</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.127.94</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.8.127.174</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.10.110.236</td><td>RUS</td><td>GlavTel ltd</td></tr><tr><td>45.12.5.127</td><td>RUS</td><td>MnogoByte LLC</td></tr><tr><td>45.137.152.30</td><td>RUS</td><td>RETN Limited</td></tr><tr><td>46.173.215.218</td><td>RUS</td><td>Garant-Park-Internet LLC</td></tr><tr><td>47.74.84.188</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.85.32</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.85.54</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.85.56</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.85.140</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.87.19</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.87.177</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.87.193</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.87.214</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.88.232</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.89.144</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.89.149</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.89.219</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.89.251</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.91.80</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.74.91.126</td><td>AUS</td><td>Alibaba</td></tr><tr><td>47.88.0.94</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.88.23.43</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.88.29.110</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.89.251.202</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.89.253.69</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.89.254.220</td><td>USA</td><td>Alibaba</td></tr>
```

```
tr><tr><td>47.91.74.155</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.91.88.236</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.91.91.52</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.91.93.218</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.91.94.163</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.251.7.113</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.7.156</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.34.7</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.38.254</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.40.77</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.43.180</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.251.44.14</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.254.32.57</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.254.35.165</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.254.41.110</td><td>USA</td><td>Alibaba</td></tr><tr><td>47.254.128.79</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.128.193</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.144.211</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.169.225</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.170.99</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.170.157</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.173.79</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.173.187</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.174.244</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.175.52</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.177.70</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.177.93</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.179.42</td><td>DEU</td><td>Alibaba</td></tr><tr><td>47.254.184.25</td><td>DEU</td><td>Alibaba.com LLC</td></tr><tr><td>47.254.184.183</td><td>DEU</td><td>Alibaba</td></tr><tr><td>77.87.212.182</td><td>RUS</td><td>Filanco LLC</td></tr><tr><td>77.87.212.198</td><td>RUS</td><td>Filanco LLC</td></tr><tr><td>77.220.213.77</td><td>NLD</td><td>Zomro B.V.</td></tr><tr><td>77.223.96.189</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.96.215</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.98.3</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.98.12</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.99.3</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>77.223.99.91</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>77.223.99.108</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.99.121</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>77.223.99.148</td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>77.223.99.185</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.223.99.210</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>77.232.42.200</td><td>RUS</td><td>Cloud assets LLC</td></tr><tr><td>78.155.222.151</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>79.141.171.22</td><td>GBR</td><td>HZ Hosting Ltd</td></tr><tr><td>79.141.175.228</td><td>SWE</td><td>GleSYS Internet Services AB</td></tr><tr><td>79.143.29.96</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>79.143.31.206</td><td>RUS</td><td>Selectel Ltd.</td></tr>
```

```

td></tr><tr><td>80.71.158.86</td><td>UKR</td><td>Rices Privately owned
enterprise</td></tr><tr><td>80.71.158.89</td><td>UKR</td><td>Rices Privately
owned enterprise</td></tr><tr><td>80.71.158.91</td><td>UKR</td><td>Rices
Privately owned enterprise</td></tr><tr><td>80.71.158.94</td><td>UKR</
td><td>Rices Privately owned enterprise</td></tr><tr><td>80.71.158.106</
td><td>UKR</td><td>Rices Privately owned enterprise</td></
tr><tr><td>80.71.158.121</td><td>UKR</td><td>Rices Privately owned enterprise</
td></tr><tr><td>80.249.144.83</td><td>RUS</td><td>000 Network of data-centers
Selectel</td></tr><tr><td>80.249.145.91</td><td>RUS</td><td>000 Network of
data-centers Selectel</td></tr><tr><td>80.249.149.87</td><td>RUS</td><td>000
Network of data-centers Selectel</td></tr><tr><td>80.249.149.129</td><td>RUS</
td><td>Selectel Ltd.</td></tr><tr><td>80.249.150.55</td><td>RUS</
td><td>Selectel Ltd.</td></tr><tr><td>80.249.150.124</td><td>RUS</
td><td>Selectel Ltd.</td></tr><tr><td>80.249.150.215</td><td>RUS</
td><td>Selectel Ltd.</td></tr><tr><td>81.163.28.116</td><td>RUS</td><td>000
Network of data-centers Selectel</td></tr><tr><td>81.163.30.42</td><td>RUS</
td><td>000 Network of data-centers Selectel</td></tr><tr><td>82.148.16.142</
td><td>RUS</td><td>Selectel Ltd.</td></tr><tr><td>82.148.17.175</td><td>RUS</
td><td>Selectel Ltd.</td></tr><tr><td>82.148.18.41</td><td>RUS</td><td>Selectel
Ltd.</td></tr><tr><td>82.148.18.132</td><td>RUS</td><td>000 Network of data-
centers Selectel</td></tr><tr><td>82.148.28.91</td><td>RUS</td><td>Selectel
Ltd.</td></tr><tr><td>84.38.181.213</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.182.88</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.182.191</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.182.236</td><td>RUS</td><td>000 Network of data-centers
Selectel</td></tr><tr><td>84.38.183.36</td><td>RUS</td><td>000 Network of data-
centers Selectel</td></tr><tr><td>84.38.183.45</td><td>RUS</td><td>Selectel
Ltd.</td></tr><tr><td>84.38.183.78</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.183.79</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.183.198</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.183.214</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.183.215</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>84.38.183.222</td><td>RUS</td><td>Selectel Ltd.</td></
tr><tr><td>85.117.235.228</td><td>RUS</td><td>LLC Baxet</td></
tr><tr><td>85.143.174.172</td><td>RUS</td><td>Federal State Institution Federal
Scientific Resea</td></tr><tr><td>85.143.174.227</td><td>RUS</td><td>Federal
State Institution Federal Scientific Resea</td></tr><tr><td>85.143.175.87</
td><td>RUS</td><td>Federal State Institution Federal Scientific Resea</td></
tr><tr><td>85.143.175.133</td><td>RUS</td><td>Federal State Institution Federal
Scientific Resea</td></tr><tr><td>85.143.175.148</td><td>RUS</td><td>Federal
State Institution Federal Scientific Resea</td></tr><tr><td>85.143.175.201</
td><td>RUS</td><td>Federal State Institution Federal Scientific Resea</td></
tr><tr><td>87.249.53.12</td><td>RUS</td><td>TimeWeb Ltd.</td></
tr><tr><td>87.249.54.139</td><td>RUS</td><td>TimeWeb Ltd.</td></
tr><tr><td>89.223.65.105</td><td>RUS</td><td>TimeWeb Ltd.</td></
tr><tr><td>89.223.100.211</td><td>RUS</td><td>GlavTel ltd</td></
tr><tr><td>91.132.102.82</td><td>RUS</td><td>Ihor Hosting LLC</td></
tr><tr><td>91.132.102.118</td><td>RUS</td><td>Ihor Hosting LLC</td></
tr><tr><td>91.132.102.198</td><td>RUS</td><td>Ihor Hosting LLC</td></
tr><tr><td>91.142.78.54</td><td>RUS</td><td>Cloud assets LLC</td></
tr><tr><td>91.193.17.105</td><td>GBR</td><td>HZ Hosting Ltd</td></

```

```
tr><tr><td>91.215.153.105</td><td>BGR</td><td>Friendhosting LTD</td></tr><tr><td>91.224.22.75</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.224.22.88</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.224.22.231</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.224.22.232</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.224.22.236</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.224.22.239</td><td>RUS</td><td>Domain names registrar REG.RU, Ltd</td></tr><tr><td>91.240.242.17</td><td>MDA</td><td>PQ HOSTING S.R.L</td></tr><tr><td>91.240.242.26</td><td>MDA</td><td>PQ HOSTING S.R.L</td></tr><tr><td>91.240.242.39</td><td>MDA</td><td>PQ HOSTING S.R.L</td></tr><tr><td>91.240.242.108</td><td>MDA</td><td>PQ HOSTING S.R.L</td></tr><tr><td>92.38.130.247</td><td>RUS</td><td>G-Core Labs S.A.</td></tr><tr><td>92.53.97.75</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>92.53.105.229</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>92.255.76.36</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>92.255.76.49</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>92.255.78.114</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>93.189.40.77</td><td>RUS</td><td>Limited Liability Company NTCOM</td></tr><tr><td>93.189.41.99</td><td>RUS</td><td>Limited Liability Company NTCOM</td></tr><tr><td>93.189.42.100</td><td>RUS</td><td>Limited Liability Company NTCOM</td></tr><tr><td>93.189.42.167</td><td>RUS</td><td>Limited Liability Company NTCOM</td></tr><tr><td>93.189.47.205</td><td>RUS</td><td>Limited Liability Company NTCOM</td></tr><tr><td>94.142.140.81</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>94.142.140.182</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>94.142.140.218</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>94.142.140.223</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>94.142.143.206</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>95.142.35.241</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>95.213.165.6</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.165.7</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.165.20</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.165.21</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.165.238</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.216.148</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>95.213.216.204</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>109.248.201.128</td><td>RUS</td><td>Kontel LLC</td></tr><tr><td>176.57.220.153</td><td>RUS</td><td>TimeWeb Ltd.</td></tr><tr><td>176.118.164.123</td><td>RUS</td><td>Digital Energy LLC</td></tr><tr><td>178.208.75.53</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>178.208.75.56</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>178.208.77.95</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>185.45.192.86</td><td>NLD</td><td>Host Sailor Ltd</td></tr><tr><td>185.45.192.252</td><td>NLD</td><td>Host Sailor Ltd</td></tr><tr><td>185.82.202.202</td><td>NLD</td><td>Host Sailor Ltd.</td></tr><tr><td>185.87.48.171</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>185.87.51.78</td><td>RUS</td><td>Ihor Hosting LLC</td></tr><tr><td>185.98.87.197</td><td>RUS</td><td>CloudLite LLC</td></tr><tr><td>185.104.114.127</td><td>RUS</td><td>TimeWeb Ltd.</td></tr>
```

```

tr><tr><td>185.123.53.164</td><td>EST</td><td>HZ Hosting Ltd</td></tr>
tr><tr><td>185.125.217.21</td><td>RUS</td><td>Ihor Hosting LLC</td></tr>
tr><tr><td>185.125.217.155</td><td>RUS</td><td>Ihor Hosting LLC</td></tr>
tr><tr><td>185.162.11.18</td><td>NLD</td><td>EUROHOSTER Ltd.</td></tr>
tr><tr><td>185.183.96.36</td><td>NLD</td><td>Host Sailor Ltd</td></tr>
tr><tr><td>185.183.96.206</td><td>NLD</td><td>Host Sailor Ltd</td></tr>
tr><tr><td>185.183.98.30</td><td>NLD</td><td>Host Sailor Ltd</td></tr>
tr><tr><td>185.186.142.46</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.56</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.69</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.79</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.206</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.217</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.186.142.237</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>185.188.182.72</td><td>RUS</td><td>Network Management Ltd</td></tr>
tr><tr><td>185.189.69.11</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr>
tr><tr><td>185.189.69.17</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr>
tr><tr><td>185.189.69.33</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr>
tr><tr><td>185.189.69.82</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr>
tr><tr><td>185.189.69.129</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr>
tr><tr><td>185.203.118.165</td><td>BGR</td><td>Belcloud LTD</td></tr>
tr><tr><td>185.207.137.113</td><td>UKR</td><td>Tehnologii Budushego LLC</td></tr>
tr><tr><td>185.217.198.251</td><td>RUS</td><td>Network Management Ltd</td></tr>
tr><tr><td>185.217.199.119</td><td>RUS</td><td>Network Management Ltd</td></tr>
tr><tr><td>185.217.199.126</td><td>RUS</td><td>Network Management Ltd</td></tr>
tr><tr><td>185.224.212.70</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.71</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.78</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.79</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.81</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.82</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.93</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.224.212.94</td><td>RUS</td><td>2Day Telecom LLP</td></tr>
tr><tr><td>185.233.80.54</td><td>DEU</td><td>Network Management Ltd</td></tr>
tr><tr><td>185.237.206.156</td><td>UKR</td><td>ITL LLC</td></tr>
tr><tr><td>185.237.206.157</td><td>UKR</td><td>ITL LLC</td></tr>
tr><tr><td>185.237.206.159</td><td>UKR</td><td>ITL LLC</td></tr>
tr><tr><td>185.237.206.160</td><td>UKR</td><td>ITL LLC</td></tr>
tr><tr><td>185.237.206.166</td><td>UKR</td><td>ITL LLC</td></tr>
tr><tr><td>185.246.152.88</td><td>NLD</td><td>Melbikomas UAB</td></tr>
tr><tr><td>185.246.154.135</td><td>RUS</td><td>Melbikomas UAB</td></tr>
tr><tr><td>185.246.154.140</td><td>RUS</td><td>Melbikomas UAB</td></tr>
tr><tr><td>185.255.132.174</td><td>RUS</td><td>Network Management Ltd</td></tr>
tr><tr><td>188.68.220.41</td><td>RUS</td><td>000 Network of data-centers
Selectel</td></tr>
tr><tr><td>188.119.120.28</td><td>RUS</td><td>Perviy TSOD LLC</td></tr>
tr><tr><td>188.130.139.233</td><td>RUS</td><td>Kontel LLC</td></tr>
tr><tr><td>188.225.18.251</td><td>RUS</td><td>TimeWeb Ltd.</td></tr>
tr><tr><td>188.225.33.123</td><td>RUS</td><td>TimeWeb Ltd.</td></tr>
tr><tr><td>193.38.55.67</td><td>NLD</td><td>Intersect LTD</td></tr>
tr><tr><td>193.38.55.157</td><td>NLD</td><td>Intersect LTD</td></tr>
tr><tr><td>193.42.113.29</td><td>RUS</td><td>RETN Limited</td></tr>

```

```
tr><tr><td>193.42.113.55</td><td>RUS</td><td>RETN Limited</td></tr><tr><td>193.106.175.27</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.106.175.54</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.106.175.59</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.106.175.99</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.106.175.102</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.106.175.105</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.232.179.69</td><td>RUS</td><td>Chernyshov Aleksandr Aleksandrovich</td></tr><tr><td>194.38.20.181</td><td>UKR</td><td>Rices Privately owned enterprise</td></tr><tr><td>194.87.185.127</td><td>CZE</td><td>000 Network of data-centers Selectel</td></tr><tr><td>194.87.239.115</td><td>RUS</td><td>JSC Mediasoft ekspert</td></tr><tr><td>194.190.152.223</td><td>RUS</td><td>Baykov Ilya Sergeevich</td></tr><tr><td>195.123.219.214</td><td>NLD</td><td>ITL LLC</td></tr><tr><td>195.123.219.227</td><td>NLD</td><td>ITL LLC</td></tr><tr><td>195.133.10.184</td><td>CZE</td><td>LLC Baxet</td></tr><tr><td>195.161.68.120</td><td>RUS</td><td>Rostelecom</td></tr><tr><td>213.183.53.75</td><td>RUS</td><td>Melbikomas UAB</td></tr><tr><td>213.183.53.234</td><td>RUS</td><td>Melbikomas UAB</td></tr><tr><td>213.183.59.54</td><td>NLD</td><td>Melbikomas UAB</td></tr><tr><td>213.183.59.219</td><td>NLD</td><td>Melbikomas UAB</td></tr></tbody></table></figure><p>In the last 24 hours, the following hosts were added to the actor's fast-flux infrastructure:</p><figure class=\"table\"><table><thead><tr><th>IP address</th><th>Country</th><th>Hosting Company</th></tr></thead><tbody><tr><td>2.59.36.16</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>2.59.36.82</td><td>JPN</td><td>DataWeb Global Group B.V.</td></tr><tr><td>5.8.76.216</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>5.188.3.56</td><td>RUS</td><td>G-Core Labs S.A.</td></tr><tr><td>8.209.64.34</td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.67.97</td><td>DEU</td><td>Alibaba</td></tr><tr><td>45.8.124.204</td><td>RUS</td><td>000 Network of data-centers Selectel</td></tr><tr><td>45.10.110.236</td><td>RUS</td><td>GlavTel ltd</td></tr><tr><td>80.71.158.121</td><td>UKR</td><td>Rices Privately owned enterprise</td></tr><tr><td>85.143.174.227</td><td>RUS</td><td>Federal State Institution Federal Scientific Resea</td></tr><tr><td>89.223.100.211</td><td>RUS</td><td>GlavTel ltd</td></tr><tr><td>91.215.153.105</td><td>BGR</td><td>Friendhosting LTD</td></tr><tr><td>92.38.130.247</td><td>RUS</td><td>G-Core Labs S.A.</td></tr><tr><td>178.208.75.53</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>178.208.75.56</td><td>RUS</td><td>EuroByte LLC</td></tr><tr><td>185.162.11.18</td><td>NLD</td><td>EUROHOSTER Ltd.</td></tr><tr><td>185.186.142.237</td><td>RUS</td><td>Kontel LLC</td></tr><tr><td>185.189.69.82</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr><tr><td>185.189.69.129</td><td>USA</td><td>DataWeb Global Group B.V.</td></tr><tr><td>185.203.118.165</td><td>BGR</td><td>Belcloud LTD</td></tr><tr><td>185.224.212.93</td><td>RUS</td><td>2Day Telecom LLP</td></tr><tr><td>185.224.212.94</td><td>RUS</td><td>2Day Telecom LLP</td></tr><tr><td>185.237.206.166</td><td>UKR</td><td>ITL LLC</td></tr><tr><td>188.119.120.28</td><td>RUS</td><td>Perviy TSOD LLC</td></tr><tr><td>193.38.55.67</td><td>NLD</td><td>Intersect LTD</td></tr><tr><td>193.38.55.157</td><td>NLD</td><td>Intersect LTD</td></tr><tr><td>193.106.175.105</td><td>RUS</td><td>IQHost Ltd</td></tr><tr><td>193.232.179.69</td><td>RUS</td><td>Chernyshov Aleksandr
```

```

Aleksandrovich</td></tr><tr><td>194.190.152.223</td><td>RUS</td><td>Baykov Ilya
Sergeevich</td></tr><tr><td>195.123.219.214</td><td>NLD</td><td>ITL LLC</td></
tr><tr><td>195.123.219.227</td><td>NLD</td><td>ITL LLC</td></
tr><tr><td>213.183.53.75</td><td>RUS</td><td>Melbikomas UAB</td></
tr><tr><td>213.183.53.234</td><td>RUS</td><td>Melbikomas UAB</td></tr></
tbody></table></figure><p>The following hosts were removed from the fast-flux
infrastructure in the last 24 hours:</p><figure
class=\"table\"><table><thead><tr><th>IP address</th><th>Country</
th><th>Hosting Company</th></tr></thead><tbody><tr><td>8.209.69.185</
td><td>DEU</td><td>Alibaba</td></tr><tr><td>8.209.72.110</td><td>DEU</
td><td>Alibaba</td></tr><tr><td>45.142.36.161</td><td>RUS</td><td>JSC Mediasoft
ekspert</td></tr><tr><td>46.17.43.223</td><td>RUS</td><td>LLC Baxet</td></
tr><tr><td>46.17.104.58</td><td>RUS</td><td>Network Management Ltd</td></
tr><tr><td>47.88.7.92</td><td>USA</td><td>Alibaba</td></
tr><tr><td>47.251.4.88</td><td>USA</td><td>Alibaba</td></
tr><tr><td>79.141.170.17</td><td>GBR</td><td>HZ Hosting Ltd</td></
tr><tr><td>82.202.194.9</td><td>RUS</td><td>000 Network of data-centers
Selectel</td></tr><tr><td>91.240.242.16</td><td>MDA</td><td>PQ HOSTING S.R.L</
td></tr><tr><td>91.240.242.107</td><td>MDA</td><td>PQ HOSTING S.R.L</td></
tr><tr><td>95.142.35.150</td><td>RUS</td><td>EuroByte LLC</td></
tr><tr><td>95.142.35.171</td><td>RUS</td><td>EuroByte LLC</td></
tr><tr><td>95.142.38.6</td><td>RUS</td><td>EuroByte LLC</td></
tr><tr><td>178.208.92.39</td><td>RUS</td><td>EuroByte LLC</td></
tr><tr><td>185.246.152.49</td><td>NLD</td><td>Melbikomas UAB</td></
tr><tr><td>194.40.243.133</td><td>UKR</td><td>Rices Privately owned
enterprise</td></tr><tr><td>194.87.215.89</td><td>CZE</td><td>LLC Baxet</td></
tr><tr><td>195.69.187.21</td><td>UKR</td><td>Scientific Production Enterprise
Technaukservice L</td></tr><tr><td>195.69.187.114</td><td>UKR</
td><td>Scientific Production Enterprise Technaukservice L</td></
tr><tr><td>195.69.187.141</td><td>UKR</td><td>Scientific Production Enterprise
Technaukservice L</td></tr><tr><td>195.69.187.219</td><td>UKR</
td><td>Scientific Production Enterprise Technaukservice L</td></
tr><tr><td>213.183.53.159</td><td>RUS</td><td>Melbikomas UAB</td></
tr><tr><td>213.183.59.161</td><td>NLD</td><td>Melbikomas UAB</td></tr></
tbody></table></figure><p>---</p>\",
  "executiveSummary": "<p>As of 10 a.m. GMT, Nov. 5, 2021, the actor
<strong>yalishanda's </strong>fast-flux network stands at 305 total hosts.
There were 33 hosts added to the network in the last 24 hours, while 24 hosts
were dropped during this period. </p><p>The actor hosted phishing campaigns
targeting ABN AMRO, Amazon, Blockchain, Santander, UPS and Wells Fargo
customers.</p>\"
}

```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH               | THREATQ ENTITY     | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                                                              | NOTES                        |
|------------------------------|--------------------|--------------------------------------|----------------|-----------------------------------------------------------------------|------------------------------|
| .subject                     | report.value       | N/A                                  | .created       | Russian actor, bulletproof hoster yalishanda...                       | N/A                          |
| .executiveSummary + .rawText | report.description | N/A                                  | N/A            | Throughout the course of our research, we identified the following... | Retrieve .researcherComments |

| FEED DATA PATH                                   | THREATQ ENTITY                | THREATQ OBJECT TYPE OR ATTRIBUTE KEY                                                            | PUBLISHED DATE        | EXAMPLES                                                                                                                                            | NOTES                                                                                                                                           |
|--------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  |                               |                                                                                                 |                       |                                                                                                                                                     | and <code>.rawText</code> fields. Formatted as HTML markup.                                                                                     |
| <code>.documentFamily</code>                     | <code>report.attribute</code> | Document Family                                                                                 | <code>.created</code> | INFOREP                                                                                                                                             | N/A                                                                                                                                             |
| <code>.documentType</code>                       | <code>report.attribute</code> | Document Type                                                                                   | <code>.created</code> | INFOREP                                                                                                                                             | N/A                                                                                                                                             |
| <code>.admiraltyCode</code>                      | <code>report.attribute</code> | Admiralty Code                                                                                  | <code>.created</code> | B2                                                                                                                                                  | N/A                                                                                                                                             |
| <code>.motivation</code>                         | <code>report.attribute</code> | Motivation                                                                                      | <code>.created</code> | cc                                                                                                                                                  | N/A                                                                                                                                             |
| <code>.sourceCharacterization</code>             | <code>report.attribute</code> | Source Characterization                                                                         | <code>.created</code> | Information was derived from a reliable source...                                                                                                   | N/A                                                                                                                                             |
| <code>.portalReportUrl</code>                    | <code>report.attribute</code> | Intel471 Link                                                                                   | <code>.created</code> | <a href="https://titan.intel471.com/report/inforep/119363037d964917a1a10989">https://titan.intel471.com/report/inforep/119363037d964917a1a10989</a> | N/A                                                                                                                                             |
| <code>.classification.intelRequirements[]</code> | <code>report.attribute</code> | Intelligence Requirements                                                                       | <code>.created</code> | 3.1.1                                                                                                                                               | N/A                                                                                                                                             |
| <code>.actorSubjectOfReport[].handle</code>      | <code>Adversary.name</code>   | N/A                                                                                             | N/A                   | yalishanda                                                                                                                                          | N/A                                                                                                                                             |
| <code>.locations[].country</code>                | <code>report.attribute</code> | Country/Origin<br>Country/Impacted Country                                                      | <code>.created</code> | Vietnam                                                                                                                                             | Attribute name mapped based on the <code>.locations[].link</code> value based on the <code>country_link_map</code> table, defaulting to Country |
| <code>.entities[].value</code>                   | <code>indicator.value</code>  | Mapped based on the <code>indicator_type_map</code> table by using the <code>.type</code> value | <code>.created</code> | 109.248.201.128                                                                                                                                     | N/A                                                                                                                                             |
| <code>.tags[]</code>                             | <code>report.tag</code>       | N/A                                                                                             | N/A                   | Banking & Finance                                                                                                                                   | Each tag is trimmed to 50 chars                                                                                                                 |

## Get Watcher Group Name (Supplemental)

The value of `.alerts[].watcherGroupUid` from the Intel471 Alerts feed is used as the `groupId` parameter.

GET - <https://api.intel471.com/v1/watcherGroups/{groupId}>

### Sample Response:

```
{
  "name": "Apache Log4j Vulnerability (by Intel 471)",
  "description": "This Intel 471 Incident Watcher Group consists ...",
  "muted": false,
  "uid": "8d4a92f9-9946-4aa9-8a9f-58e8ae20f6b2",
  "owner": "Intel 471"
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES                                                                                                                           |
|----------------|-----------------|--------------------------------------|----------------|----------|---------------------------------------------------------------------------------------------------------------------------------|
| .name          | tag.name        | N/A                                  | N/A            | testG    | UIDs are mapped after using the data fetched from the Get Watcher Group Name supplemental feed. Each tag is trimmed to 50 chars |
| .name          | event.attribute | Watcher Group Name                   | N/A            | testG    | UIDs are mapped after using the data fetched from the Get Watcher Group Name supplemental feed.                                 |

## Indicator Type Mapping

The following a mapping table for indicators.

| INTEL471 VALUE | THREATQ VALUE |
|----------------|---------------|
| MD5            | MD5           |
| IPAddress      | IP Address    |
| ActorDomain    | FQDN          |
| ActorWebsite   | URL           |
| EmailAddress   | Email Address |
| MaliciousURL   | URL           |
| SHA256         | SHA-256       |
| SHA1           | SHA-1         |
| URL            | URL           |
| CVE            | CVE           |

# 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.

## Intel 471 Alerts

| METRIC               | RESULT    |
|----------------------|-----------|
| Run Time             | 2 minutes |
| Adversaries          | 20        |
| Adversary Attributes | 120       |
| Events               | 12        |
| Event Attributes     | 45        |
| Indicators           | 15        |
| Indicator Attributes | 6         |
| Vulnerabilities      | 7         |
| Report               | 7         |
| Report Attributes    | 190       |

---

# Change Log

- **Version 1.2.3**
  - Resolved an filtering issue where users would encounter an `Error applying filter` message.
  - The Ingest CVEs As is now set to Vulnerabilities by default.
  - Resolved an issue where certain event attributes were not mapped correctly.
- **Version 1.2.2**
  - Resolved a parsing attribute issue for events.
- **Version 1.2.1**
  - Fixed a `Get Report by ID` supplemental feed indicator ingestion bug.
  - Added the ability to parse CVEs from CVE Report Alerts description.
- **Version 1.2.0**
  - Fixed an issue with Spot Reports Events when the event did not have relationships.
  - Fixed an indicator bug where the relationship between the report and indicator was not created if the indicator was ingested into the ThreatQ platform by another feed.
- **Version 1.1.0**
  - Updated the integration to ingest more data about events and related items.
  - Added new configuration option: `Ingest CVEs As` . See the [Configuration](#) chapter for more information.
- **Version 1.0.0**
  - Initial Release