ThreatQuotient

Group-IB CDF Guide

Version 2.1.0

August 23, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Versioning

- Current integration version: `2.0.0`
- Supported on ThreatQ versions >= `4.45.0`

Introduction

Group-IB is a provider of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection.

The Group-IB CDF for ThreatQ provides the following feeds:

- Group-IB Compromised Data Mules
- Group-IB Compromised Data IMEI
- Group-IB Human Intelligence Threat
- Group-IB Human Intelligence Threat Actor
- Group-IB APT Threat
- Group-IB APT Threat Actor
- Group-IB Malware C2
- Group-IB Suspicious IP Tor Node
- Group-IB Suspicious IP Open Proxy
- Group-IB Suspicious IP Socks Proxy
- Group-IB Compromised Account
- Group-IB Compromised Card
- Group-IB Attacks DDoS
- Group-IB Malware Targeted Malware
- Group-IB Attacks Phishing

Prerequisites

The Group-IB CDF requires the installation of the following custom objects:

- IMEI
- Money Mule
- Organization
- Compromised Account
- Compromised Card

The files associated with the custom objects must be downloaded separately from the ThreatQ Marketplace in a zipped file.

Custom Objects Installation

ThreatQuotient provides two methods to install the required custom objects: via script and manual installation.

> Before installing the custom objects, be sure that you unzipped the `GroupIB.zip` and copied all the files to your ThreatQ instance.
>
> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the custom object zip file from the ThreatQ Marketplace.
2. SSH into your ThreatQ instance.
3. Unzip and then copy the custom objects files to directory of your choice.

   > ThreatQuotient recommends uploading the files to the `/var/www/api/database/seeds/data/custom_objects/.`

4. Install the custom objects using one of the following methods:

   via Script

   a. Navigate to the directory with the custom objects files.
   b. Run the following command via the ThreatQ system's CLI:

   ```
   <> sudo ./installation.sh
   ```

   > You must be in the directory that houses the custom object files when running this command.

   Manually

   Run the following commands via the ThreatQ system's CLI:

   a. Navigate to the API directory:

   ```
   <> cd /var/www/api
   ```

   b. Put your ThreatQ instance into maintenance mode:

```
<> sudo php artisan down
```

c. Run the following command to install the Custom Object Definition:

```
<> sudo php artisan threatq:make-object-set --file=<Path To
   JSON File>

   sudo php artisan threatq:object-settings --code=money_mule
   --icon=<Path To Icon Folder>/MoneyMule.svg --background-
   color='#03ac14'

   sudo php artisan threatq:object-settings --code=imei --
   icon=<Path To Icon Folder>/IMEI.svg --background-
   color='#03ac14'

   sudo php artisan threatq:object-settings --
   code=organization --icon=<Path To Icon Folder>/
   Organization.svg --background-color='#03ac14'

   sudo php artisan threatq:object-settings --code=account --
   icon=<Path To Icon Folder>/Account.svg --background-
   color='#ED414D'

   sudo php artisan threatq:object-settings --code=card --
   icon=<Path To Icon Folder>/CompromisedCard.svg --
   background-color='#ED414D'
```

d. Clear the ThreatQ object cache and update permissions:

```
<> sudo php /var/www/api/artisan cache:clear

   sudo php /var/www/api/artisan threatq:update-permissions
```

e. Take your ThreatQ instance out of maintenance mode and restart Dynamo:

```
<> sudo php artisan up

   sudo systemctl restart threatq-dynamo
```

Installation

> The CDF requires the installation of three custom objects before installing the actual CDF. See the Prerequisites section for more details.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your Group-IB username.
API Key	Your Group-IB API Key.
Save CVE Data as	Select the object type(s) you would like CVEs to be ingested as.

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

Group-IB Compromised Data Mules

`GET https://bt.group-ib.com/api/v2/compromised/mule`

This feed ingests compromised Money Mule objects and any related Indicators, Malware, Organizations, Identities, and Adversaries.


```
{
  "resultId": "e6ab53a3a3e4a9265cb06f014a240bdab56ec206",
  "count": 33789,
  "items": [
    {
      "account": "9245316213",
      "cnc": {
        "cnc": "http://serv.sexura.ru",
        "domain": "serv.sexura.ru",
        "ipv4": {
          "asn": "AS16276 OVH SAS",
          "city": "Gravelines",
          "countryCode": "FR",
          "countryName": "France",
          "ip": "94.23.180.184",
          "provider": "OVH SAS",
          "region": "Hauts-de-France"
        },
        "ipv6": {
          "asn": "AS16276 OVH SAS",
          "city": "Gravelines",
          "countryCode": "FR",
          "countryName": "France",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "OVH SAS",
          "region": "Hauts-de-France"
        },
        "url": "http://serv.sexura.ru"
      },
      "dateAdd": "2020-10-16T01:06:09+00:00",
      "dateIncident": null,
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 80,
        "reliability": 100,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "id": "44bd99f372e2f78ec12513afcb7ee006d86392a2",
      "info": "Nothing",
      "isFavourite": false,
      "isHidden": false,
```

```
    "malware": {
      "id": "8790a290230b3b4c059c2516a6adace1eac16066",
      "name": "FlexNet"
    },
    "oldId": "352963098",
    "organization": {
      "bic": "SABRRUMMVH1",
      "bicRu": "SABRRUMMVH1",
      "bsb": "082489",
      "iban": "BIK044525225/30101810400000000225",
      "name": "SAVINGS BANK OF THE RUSSIAN FEDERATION (SBERBANK)",
      "swift": "SABRRUMMVH1"
    },
    "person": {
      "address": "224 Main St",
      "birthday": "01-01-1990",
      "city": "Wiggins",
      "countryCode": "US",
      "email": "jhon@fake.com",
      "name": "John",
      "passport": "123456789",
      "phone": "(555) 555-1234",
      "state": "Colorado",
      "taxNumber": "9999999999999",
      "zip": "80654"
    },
    "portalLink": "https://bt.group-ib.com/cd/mules?searchValue=id:44bd99f372e2f78ec12513afcb7ee006d86392a2",
    "seqUpdate": 1616672696468,
    "sourceType": "Botnet",
    "threatActor": {
      "id": "6c26d5dc4cc743535e7ab5bb205947540878dab9",
      "isAPT": false,
      "name": "CockSkunk"
    },
    "type": "Botnet"
  }
 ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].account	Money Mule.Value	N/A	.items[].dateAdd	'9245316213'	The object name is formed by adding Money Mule to this field, ex.: Money Mule 9245316213
.items[].evaluation.admiraltyCode	Money Mule.Attribute	Admiralty Code	.items[].dateAdd	'A2'	
.items[].evaluation.credibility	Money Mule.Attribute	Credibility	.items[].dateAdd	'80'	
.items[].evaluation.reliability	Money Mule.Attribute	Reliability	.items[].dateAdd	'100'	
.items[].evaluation.severity	Money Mule.Attribute	Severity	.items[].dateAdd	'red'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.tlp	Money Mule.TLP / Related Objects.TLP	N/A	N/A	'amber'	
.items[].evaluation.ttl	Money Mule.Attribute	Time To Live (seconds)	.items[].dateAdd	'30'	
.items[].info	Money Mule.Attribute	Info	.items[].dateAdd	'Nothing'	
.items[].portalLink	Money Mule.Attribute	Portal Link	.items[].dateAdd	'https://bt.group-ib.com/cd/mules?searchValue=id:44bd99f372e2f78ec12513afcb7ee006d86392a2'	
.items[].seqUpdate	Money Mule.Attribute	Sequence Update	.items[].dateAdd	'1616672696468'	
.items[].sourceType	Money Mule.Attribute	Source Type	.items[].dateAdd	'Botnet'	
.items[].type	Money Mule.Attribute	Type	.items[].dateAdd	'Botnet'	
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateAdd	'http://serv.sexura.ru'	
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateAdd	'serv.sexura.ru'	
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateAdd	'http://serv.sexura.ru'	If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateAdd	'94.23.180.184'	
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateAdd	'AS16276 OVH SAS'	
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateAdd	'Gravelines'	
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateAdd	'FR'	
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateAdd	'France'	
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateAdd	'OVH SAS'	
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateAdd	'Hauts-de-France'	
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateAdd	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateAdd	'AS16276 OVH SAS'	
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateAdd	'Gravelines'	
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateAdd	'FR'	
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateAdd	'France'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateAdd	'OVH SAS'	
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateAdd	'Hauts-de-France'	
.items[].malware.name	Related Malware.Value	N/A	.items[].dateAdd	'FlexNet'	
.items[].organization.name	Related Organization	N/A	.items[].dateAdd	'SAVINGS BANK OF THE RUSSIAN FEDERATION (SBERBANK)'	This is a custom object
.items[].organization.bic	Related Organization.Attribute	BIC	.items[].dateAdd	'SABRRUMMVH1'	
.items[].organization.bicRu	Related Organization.Attribute	RU BIC	.items[].dateAdd	'SABRRUMMVH1'	
.items[].organization.bsb	Related Organization.Attribute	BSB	.items[].dateAdd	'082489'	
.items[].organization.iban	Related Organization.Attribute	IBAN	.items[].dateAdd	'BIK044525225/30101810400000000225'	
.items[].organization.swift	Related Organization.Attribute	SWIFT	.items[].dateAdd	'SABRRUMMVH1'	
.items[].person.taxNumber	Related Identity	N/A	.items[].dateAdd	'9999999999999'	
.items[].person.address	Related Identity.Attribute	Address	.items[].dateAdd	'224 Main St'	
.items[].person.birthday	Related Identity.Attribute	Birthday	.items[].dateAdd	'01-01-1990'	
.items[].person.city	Related Identity.Attribute	City	.items[].dateAdd	'Wiggins'	
.items[].person.countryCode	Related Identity.Attribute	Country Code	.items[].dateAdd	'US'	
.items[].person.email	Related Identity.Attribute	Email Address	.items[].dateAdd	'jhon@fake.com'	
.items[].person.name	Related Identity.Attribute	Name	.items[].dateAdd	'Jhon'	
.items[].person.passport	Related Identity.Attribute	Passport Data	.items[].dateAdd	'123456789'	
.items[].person.phone	Related Identity.Attribute	Phone Number	.items[].dateAdd	'(555) 555-1234'	
.items[].person.state	Related Identity.Attribute	State	.items[].dateAdd	'Colorado'	
.items[].person.zip	Related Identity.Attribute	ZIP Code	.items[].dateAdd	'80654'	
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateAdd	'CockSkunk'	

Group-IB Compromised Data IMEI

`GET https://bt.group-ib.com/api/v2/compromised/imei`

This feed ingests IMEI objects and any related Indicators, Malware, and Adversaries.


```
{
  "resultId": "3aaee8a0e03f82ae38bfc96719b56d5ba95475d1",
  "count": 5408859,
  "items": [
    {
      "client": {
        "ipv4": {
          "asn": "AS15169 Google Inc.",
          "city": "Mountain View",
          "countryCode": "US",
          "countryName": "United States",
          "ip": "66.102.6.171",
          "provider": "Google Proxy",
          "region": "California"
        }
      },
      "cnc": {
        "cnc": "http://s1.paradu.ru",
        "domain": "s1.paradu.ru",
        "ipv4": {
          "asn": "AS48666 MAROSNET Telecommunication Company LLC",
          "city": "Moscow",
          "countryCode": "RU",
          "countryName": "Russian Federation",
          "ip": "31.148.99.117",
          "provider": "ALFA TELECOM s.r.o.",
          "region": "Central"
        },
        "ipv6": {
          "asn": "AS48666 MAROSNET Telecommunication Company LLC",
          "city": "Moscow",
          "countryCode": "RU",
          "countryName": "Russian Federation",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "ALFA TELECOM s.r.o.",
          "region": "Central"
        },
        "url": "http://s1.paradu.ru"
      },
      "dateCompromised": null,
      "dateDetected": "2021-04-10T01:37:36+00:00",
      "device": {
        "iccid": "891004234814455936F",
        "imei": "355266047901929",
        "imsi": "313460000000001",
        "model": "Nexus 5X/6.0.1 (Bot.v.5.0)",
        "os": "Android 6.0.1"
      },
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 80,
```

```
      "reliability": 100,
      "severity": "red",
      "tlp": "red",
      "ttl": 30
    },
    "id": "9bc865c330efb652cf876ae73e8b6ba7b047acf4",
    "isFavourite": false,
    "isHidden": false,
    "malware": {
      "id": "8790a290230b3b4c059c2516a6adace1eac16066",
      "name": "FlexNet"
    },
    "oldId": "441010555",
    "operator": {
      "countryCode": "RU",
      "name": "MegaFon",
      "number": "+358407192130"
    },
    "portalLink": "https://bt.group-ib.com/cd/imei?searchValue=id:9bc865c330efb652cf876ae73e8b6ba7b047acf4",
    "seqUpdate": 1621774969216,
    "sourceType": "Botnet",
    "threatActor": {
      "id": "6c26d5dc4cc743535e7ab5bb205947540878dab9",
      "isAPT": false,
      "name": "CockSkunk"
    }
  }
 ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].device.imei	IMEI.Value	N/A	.items[].dateDetected	'355266047901929'	
.items[].device.iccid	IMEI.Attribute	Device ICCID	.items[].dateDetected	'891004234814455936F'	
.items[].device.imsi	IMEI.Attribute	Device IMSI	.items[].dateDetected	'313460000000001'	
.items[].device.model	IMEI.Attribute	Device Model	.items[].dateDetected	'Nexus 5X/6.0.1 (Bot.v.5.0)'	
.items[].device.os	IMEI.Attribute	Device OS	.items[].dateDetected	'Android 6.0.1'	
.items[].evaluation.admiraltyCode	IMEI.Attribute	Admiralty Code	.items[].dateDetected	'A2'	
.items[].evaluation.credibility	IMEI.Attribute	Credibility	.items[].dateDetected	'80'	
.items[].evaluation.reliability	IMEI.Attribute	Reliability	.items[].dateDetected	'100'	
.items[].evaluation.severity	IMEI.Attribute	Severity	.items[].dateDetected	'red'	
.items[].evaluation.tlp	IMEI.TLP / Related Objects.TLP	N/A	N/A	'red'	
.items[].evaluation.ttl	IMEI.Attribute	Time To Live (seconds)	.items[].dateDetected	'30'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].operator.countryCode	IMEI.Attribute	Operator Country Code	.items[].dateDetected	'RU'	
.items[].operator.name	IMEI.Attribute	Operator Name	.items[].dateDetected	'MegaFon'	
.items[].operator.number	IMEI.Attribute	Operator Phone Number	.items[].dateDetected	'+3584071921 30'	
.items[].portalLink	IMEI.Attribute	Source Link	.items[].dateDetected	'https://bt.gro up-ib.com/cd/ imei?searchValue =id:9bc865c330ef b652cf876ae73e8 b6ba7b047acf4'	
.items[].sourceType	IMEI.Attribute	Source Type	.items[].dateDetected	'Botnet'	
.items[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	'66.102.6.171'	
.items[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	
.items[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	'Mountain View'	
.items[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'US'	
.items[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'United States'	
.items[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'Google Proxy'	
.items[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	'California'	
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateDetected	'http://s1.paradu.ru'	
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	's1.paradu.ru'	
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	'http://s1.paradu.ru'	If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	'31.148.99.117'	
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS48666 MAROSNET Telecommunication Company LLC'	
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	'Moscow'	
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'RU'	
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Russian Federation'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'ALFA TELECOM s.r.o.'	
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS48666 MAROSNET Telecommunication Company LLC'	
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateDetected	'Moscow'	
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'RU'	
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Russian Federation'	
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'ALFA TELECOM s.r.o.'	
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	
.items[].malware.name	Related Malware.Value	N/A	.items[].dateDetected	'FlexNet'	
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	'CockSkunk'	

Group-IB Human Intelligence Threat and GroupIB APT Threat

Group-IB Human Intelligence Threat

`GET https://bt.group-ib.com/api/v2/hi/threat`

Group-IB APT Threat

`GET https://bt.group-ib.com/api/v2/apt/threat`

This feed ingests Intrusion objects and any related Indicators, Malware, Adversaries, Attack Patterns, Identities, and Tools.


```
{
  "resultId": "194cf0b88b4244569e4d824b7607606b5abc0462",
  "count": 876,
  "items": [
    {
      "contacts": [
        {
          "account": "alexjoe9983",
          "flag": "fake",
          "service": "twitter",
          "type": "social_network"
        }
      ],
      "countries": [
        "LB",
        "TR"
      ],
      "createdAt": "2021-04-13T16:49:27+03:00",
      "cveList": [
        {
          "name": "CVE-2021-27065"
        }
      ],
      "dateFirstSeen": "2019-05-01",
      "dateLastSeen": "2021-04-09",
      "datePublished": "2021-04-09",
      "description": "During the Operation",
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "evaluation": {
        "admiraltyCode": "B2",
        "credibility": 80,
        "reliability": 80,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "expertise": [
```

```
      "0day",
      "CVE"
    ],
    "files": [
      {
        "hash": "f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0",
        "mime": "image/png",
        "name": "f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0",
        "size": 75438
      }
    ],
    "forumsAccounts": [
      {
        "messageCount": 1,
        "nickname": "nobody.gu3st",
        "registeredAt": "2012-07-13",
        "url": "http://www.iranhack.com/forum/member/186-nobody-gu3st"
      }
    ],
    "id": "3bcfabae7dc7a909ca692e702a9b6ca6627528b4",
    "indicatorMalwareRelationships": [
      {
        "indicatorId": "3c157cefdeae6a8403fbfe24790467215493b939",
        "malwareId": "132130dd0aa2f2ab8cb1e358974443276b28195d"
      }
    ],
    "indicatorRelationships": [
      {
        "sourceId": "a6c970a7f082513303a0466ca459329829e00143",
        "targetId": "2d6c6dbf99261a1c84eefec1bb395e4876346a4c"
      }
    ],
    "indicatorToolRelationships": [],
    "indicators": [
      {
        "description": null,
        "id": "3b67fc483bc2c22e0f21d68eabf6385f364a1eea",
        "langs": [
          "ru"
        ],
        "malwareList": [],
        "params": {
          "hashes": {
            "md4": "",
            "md5": "113044788a356aab6c693a3e80189141",
            "md6": "",
            "ripemd160": "",
            "sha1": "ba835af7b8aa51797f95223676640be9c81dad9f",
            "sha224": "2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b",
            "sha256": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
            "sha384":
"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd",
            "sha512":
"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb1
5bfb1447f459b",
            "whirlpool": ""
          },
          "name": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
          "size": null
        },
```

```
        "url": "http://strigigena.ru/cookie.php",
        "seqUpdate": 16183252904267,
        "techSeqUpdate": null,
        "title": null,
        "type": "file"
      },
      {
        "description": null,
        "id": "221f0e6b18af2cbf069131f2b7cf7e4552ae9d17",
        "langs": [
          "ru"
        ],
        "malwareList": [
          {
            "id": "13213Odd0aa2f2ab8cb1e358974443276b28195d",
            "name": "SysUpdate"
          }
        ],
        "params": {
          "domain": "ns162.nsakadns.com",
          "ipv4": [
            "85.204.74.143"
          ],
          "ipv6": [
            "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
          ],
          "ssl": [
            {
              "hashes": {
                "md5": "5765fafd258a5a1e87c0582a67862675",
                "sha1": "AB0B22AB421C001462AF4A9F382DC9284747B43D",
                "sha224": "2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b",
                "sha256": "ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb",
                "sha384":
"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd",
                "sha512":
"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb1
5bfb1447f459b"
              }
            }
          ],
          "url": ["http://strigigena.ru/cookie.php"],
          "address": "this2test.com",
          "message": {
            "body": "Body example",
            "subject": "Subject example"
          },
          "senderIp": "85.204.74.144",
          "serverIp": "85.204.74.145"
        },
        "seqUpdate": 16183273671915,
        "techSeqUpdate": null,
        "title": null,
        "type": "network"
      }
    ],
    "indicatorsIds": [
      "3b67fc483bc2c22e0f21d68eabf6385f364a1eea",
      "340ac49012b02435315f1dfca9628319b4c9dae9"
    ],
```

```
"isTailored": false,
"labels": [
  "campaign",
  "indicator"
],
"langs": [
  "ru",
  "en"
],
"malwareList": [
  {
    "id": "132130dd0aa2f2ab8cb1e358974443276b28195d",
    "name": "SysUpdate"
  }
],
"mitreMatrix": [
  {
    "attackPatternId": "attack-pattern--fddd81e9-dd3d-477e-9773-4fb8ae227234",
    "attackTactic": "build-capabilities",
    "attackType": "pre_attack_tactics",
    "id": "PRE-T1122",
    "params": {
      "data": "Just a string"
    }
  }
],
"oldId": "0c3429ce-c449-485d-aa02-effc62719818",
"regions": [
  "middle_east",
  "europe",
  "asia",
  "asia"
],
"relatedThreatActors": [
  {
    "id": "",
    "isAPT": "",
    "name": "actor",
    "type": "bad"
  }
],
"reportNumber": "CP-2504-1649",
"sectors": [
  "gambling",
  "government-national",
  "telecommunications",
  "energy",
  "finance"
],
"seqUpdate": 16184833571103,
"shortDescription": "This is an attack",
"shortTitle": "Attack",
"sources": [
  "https://www.trendmicro.com/en_us/research/21/d/iron.html"
],
"targetedCompany": [
  "TargetCompany"
],
"targetedPartnersAndClients": [
  "TargetPandC"
```

```
    ],
    "techSeqUpdate": null,
    "threatActor": {
      "country": "CN",
      "id": "55011fb96789bcb43c8e19e4e886924f803b6d30",
      "isAPT": true,
      "name": "IronTiger"
    },
    "title": "Discovered new toolkit",
    "toolList": [
      {
        "id": "123456789",
        "name": "Tools"
      }
    ],
    "type": "threat",
    "updatedAt": "2021-04-15T13:42:37+03:00"
  }
 ]
}
```


ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].title	Intrusion Set.Value	N/A	.items[].createdAt	'Discovered new toolkit'	
.items[].dateFirstSeen	Intrusion Set.Started_at	N/A	N/A	'2019-05-01'	
.items[].dateLastSeen	Intrusion Set.Ended_at	N/A	N/A	'2021-04-09'	
.items[].description	Intrusion Set.Description	N/A	N/A	'During the Operation'	
.items[].countries[]	Intrusion Set.Attribute	Country	.items[].createdAt	'LB'	
.items[].evaluation.admiraltyCode	Intrusion Set.Attribute	Admiralty Code	.items[].createdAt	'B2'	
.items[].evaluation.credibility	Intrusion Set.Attribute	Credibility	.items[].createdAt	'80'	
.items[].evaluation.reliability	Intrusion Set.Attribute	Reliability	.items[].createdAt	'80'	
.items[].evaluation.severity	Intrusion Set.Attribute	Severity	.items[].createdAt	'red'	
.items[].evaluation.tlp	Intrusion Set.TLP / Related Objects.TLP	N/A	N/A	'amber'	
.items[].evaluation.ttl	Intrusion Set.Attribute	Time To Live (seconds)	.items[].createdAt	'30'	
.items[].expertise[]	Intrusion Set.Attribute	Expertise	.items[].createdAt	'0day'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].labels[]	Intrusion Set.Attribute	STIX labels	.items[].createdAt	'campaign'	
.items[].langs[]	Intrusion Set.Attribute	Language	.items[].createdAt	'ru'	
.items[].regions[]	Intrusion Set.Attribute	Regions	.items[].createdAt	'middle_east'	
.items[].reportNumber	Intrusion Set.Attribute	Report Number	.items[].createdAt	'CP-2504-1649'	
.items[].sectors[]	Intrusion Set.Attribute	Sector	.items[].createdAt	'gambling'	
.items[].shortDescription	Intrusion Set.Attribute	Short Description	.items[].createdAt	'This is an attack'	
.items[].shortTitle	Intrusion Set.Attribute	Short Title	.items[].createdAt	'Attack'	
.items[].sources[]	Intrusion Set.Attribute	Source	.items[].createdAt	'https://www.trendmicro.com/en_us/research/21/d/iron.html'	
.items[].targetedCompany[]	Intrusion Set.Attribute	Target Company	.items[].createdAt	'TargetCompany'	
.items[].targetedPartnersAndClients[]	Intrusion Set.Attribute	Target Partner and Client	.items[].createdAt	'TargetPandC'	
.items[].type	Intrusion Set.Attribute	Type	.items[].createdAt	'threat'	
.items[].cveList[].name	Related Indicator.Value and/ or Related Vulnerability.Value	CVE	.items[].createdAt	'CVE-2021-27065'	
.items[].contacts[].account	Related Identity.Value	N/A	.items[].createdAt	'alexjoe9983'	
.items[].contacts[].flag	Related Identity.Attribute	Contact Flag	.items[].createdAt	'fake'	
.items[].contacts[].service	Related Identity.Attribute	Contact Service	.items[].createdAt	'twitter'	
.items[].contacts[].type	Related Identity.Attribute	Contact Type	.items[].createdAt	'social_network'	
.items[].files[].hash	Related Indicator.Value	SHA-256	.items[].createdAt	'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0'	
.items[].files[].mime	Related Indicator.Attribute	File Mime Type	.items[].createdAt	'image/png'	
.items[].files[].name	Related Indicator.Attribute	File Name	.items[].createdAt	'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0'	
.items[].files[].size	Related Indicator.Attribute	File Size	.items[].createdAt	'75438'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].forumsAccounts[].url	Related Indicator.Value	URL	.items[].createdAt	'http://www.iranhack.com/forum/member/186-nobody-gu3st'	If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator
.items[].forumsAccounts[].nickname	Related Indicator.Attribute	Forum Account Nickname	.items[].createdAt	'nobody.gu3st'	
.items[].indicators[].malwareList[].name	Related Malware.Value	N/A	.items[].createdAt	"SysUpdate"	
.items[].indicators[].params.domain	Related Indicator.Value	FQDN	.items[].createdAt	'ns162.nsakadns.com'	
.items[].indicators[].params.ipv4[]	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.143'	
.items[].indicators[].params.ipv6[]	Related Indicator.Value	IPv6 Address	.items[].createdAt	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	
.items[].indicators[].params.ssl[].hashes.md5	Related Indicator.Value	MD5	.items[].createdAt	'5765fafd258a5a1e87c0582a67862675'	
.items[].indicators[].params.ssl[].hashes.sha1	Related Indicator.Value	SHA-1	.items[].createdAt	'AB0B22AB421C001462AF4A9F382DC9284747B43D'	
.items[].indicators[].params.ssl[].hashes.sha256	Related Indicator.Value	SHA-256	.items[].createdAt	'ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb'	
.items[].indicators[].params.ssl[].hashes.sha384	Related Indicator.Value	SHA-384	.items[].createdAt	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	
.items[].indicators[].params.ssl[].hashes.sha512	Related Indicator.Value	SHA-512	.items[].createdAt	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	
.items[].indicators[].params.url	Related Indicator.Value	URL	.items[].createdAt	'http://strigigena.ru/cookie.php'	If a URL Indicator attempting to be consumed is a true FQDN, the API

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					normalize it to be an FQDN Indicator
.items[].indicators[].params.address	Related Indicator.Value	Email Address	.items[].createdAt	'this2test.com'	
.items[].indicators[].params.message.body	Related Indicator.Attribute	Email Body	.items[].createdAt	'Body example'	
.items[].indicators[].params.message.subject	Related Indicator.Attribute	Email Subject	.items[].createdAt	'Subject example'	
.items[].indicators[].params.senderIp	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.144'	
.items[].indicators[].params.serverIp	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.145'	
.items[].indicators[].params.hashes.md5	Related Indicator.Value	MD5	.items[].createdAt	'113044788a356aab6c693a3e80189141'	
.items[].indicators[].params.hashes.sha1	Related Indicator.Value	SHA-1	.items[].createdAt	'ba835af7b8aa51797f95223676640be9c81dad9f'	
.items[].indicators[].params.hashes.sha256	Related Indicator.Value	SHA-256	.items[].createdAt	'0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40'	
.items[].indicators[].params.hashes.sha384	Related Indicator.Value	SHA-384	.items[].createdAt	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	
.items[].indicators[].params.hashes.sha512	Related Indicator.Value	SHA-512	.items[].createdAt	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].createdAt	'SysUpdate'	
.items[].mitreMatrix[].id	Related Attack	Attack Pattern	.items[].createdAt	'attack-pattern--fddd81e9-dd3d-477e-9773-4fb8ae227234'	
.items[].mitreMatrix[].attackTactic	Related Attack.Attribute	Attack Tactic	.items[].createdAt	'build-capabilities'	
.items[].mitreMatrix[].attackType	Related Attack.Attribute	Attack Type	.items[].createdAt	'pre_attack_tactics'	
.items[].mitreMatrix[].params.data	Related Attack.Attribute	Attack Data	.items[].createdAt	'Just a string'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].relatedThreatActors[].name	Related Adversary.Name	N/A	.items[].createdAt	'actor'	
.items[].relatedThreatActors[].type	Related Adversary.Attribute	Type	.items[].createdAt	'bad'	
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].createdAt	'IronTiger'	
.items[].threatActor.country	Related Adversary.Attribute	Country	.items[].createdAt	'CN'	
.items[].toolList[].name	Related Tool	N/A	.items[].createdAt	'Tools'	

Group-IB Human Intelligence Threat Actor and Group-IB APT Threat Actor

Group-IB Human Intelligence Threat Actor

`GET https://bt.group-ib.com/api/v2/hi/threat_actor`

Group-IB APT Threat Actor

`GET https://bt.group-ib.com/api/v2/apt/threat_actor`

These feeds ingests Adversary objects and any related Indicators and Reports.


```
{
  "resultId": "06023dc62ccca179ee730b3ea57464c9249b5f9b",
  "count": 242,
  "items": [
    {
      "aliases": [
        "a.m.i.g.o.s",
        "AMIGOS0",
        "AMIGOS",
        "A.M.I.G.O.S",
        "Amigos",
        "amigos0"
      ],
      "country": "RU",
      "createdAt": "2019-02-20T17:44:21+00:00",
      "description": "<figure class=\"image\"><img src=\"/api/v2/hi/threat_actor/",
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "files": [
        {
          "hash": "74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2",
          "mime": "image/png",
          "name": "74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2",
          "size": 216937
        }
      ],
      "goals": [
        "Goal"
      ],
      "id": "bceee15371a475e59676d6cd1102048f139e50cb",
      "isAPT": false,
      "labels": [
        "hacker"
      ],
      "langs": [
        "en"
      ],
      "name": "Amigos",
      "oldId": null,
      "roles": [
```

```
        "agent"
    ],
    "seqUpdate": 16184067437615,
    "spokenOnLangs": [
      "en",
      "ru"
    ],
    "stat": {
      "countries": [
          "RU"
      ],
      "dateFirstSeen": "2021-10-24",
      "dateLastSeen": "2021-10-24",
      "regions": [
          "europe",
          "america:northern_america",
          "asia"
      ],
      "reports": [
        {
          "datePublished": "2021-01-05",
          "id": "9ffb44adf43abaaeea1f36c9d2a5adef38ba19e8",
          "name": {
            "en": "First mention on forums"
          }
        }
      ],
      "sectors": [
          "financial-services",
          "finance",
          "technology"
      ]
    },
    "techSeqUpdate": null,
    "updatedAt": "2021-04-14T16:25:43+03:00"
  }
 ]
}
```


ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].name	Adversary. Name	N/A	.items[].createdAt	'Amigos'	
.items[].aliases[]	Adversary. Tag	N/A	.items[].createdAt	'a.m.i.g.o.s'	
.items[].description	Adversary. Description	N/A	.items[].createdAt	'<figure class="image"><img src="/api/v2/hi/threat_actor/'	
.items[].country	Adversary. Attribute	Country	.items[].createdAt	'RU'	
.items[].goals[]	Adversary. Attribute	Goal	.items[].createdAt	'Goal'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].labels[]	Adversary. Attribute	Label	.items[].createdAt	'hacker'	
.items[].langs[]	Adversary. Attribute	Language	.items[].createdAt	'en'	
.items[].roles[]	Adversary. Attribute	Role	.items[].createdAt	'agent'	
.items[].spokenOnLangs[]	Adversary. Attribute	Language	.items[].createdAt	'ru'	
.items[].stat.countries[]	Adversary. Attribute	Country	.items[].createdAt	'RU'	
.items[].stat.dateFirstSeen	Adversary. Attribute	Date First Seen	.items[].createdAt	'2021-10-24'	
.items[].stat.regions[]	Adversary. Attribute	Region	.items[].createdAt	'europe'	
.items[].stat.sectors[]	Adversary. Attribute	Sector	.items[].createdAt	'financial-services'	
.items[].files[].hash	Related Indicator. Value	SHA-256	.items[].createdAt	'74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2'	
.items[].files[].mime	Related Indicator. Attribute	File Mime Type	.items[].createdAt	'image/png'	
.items[].files[].name	Related Indicator. Attribute	File Name	.items[].createdAt	'74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2'	
.items[].files[].size	Related Indicator. Attribute	File Size	.items[].createdAt	'216937'	
.items[].stat.reports[].name.en	Related Report	N/A	.items[].createdAt/ .items[].stat.reports[].datePublished	'First mention on forums'	If `.items[].stat.reports[].datePublished` it's null we use the value of `.items[].createdAt`

GroupIB Malware C2

```
GET https://bt.group-ib.com/api/v2/malware/cnc
```

These feeds ingests Indicators, Malware, and Adversaries.


```
{
  "resultId": "a90504337510806e189d401bb0e3cf22f836d362",
  "count": 22000,
  "items": [
    {
      "cnc": "http://128.199.23.9/uadmin/gate.php",
      "dateDetected": "2021-04-16T07:15:50+00:00",
      "dateLastSeen": "2021-04-16T07:15:50+00:00",
      "domain": "www.09832121.link",
      "file": [
        {
          "hashes": {
            "md4": "",
            "md5": "5765fafd258a5a1e87c0582a67862675",
            "md6": "",
            "ripemd160": "",
            "sha1": "ba835af7b8aa51797f95223676640be9c81dad9f",
            "sha224": "",
            "sha256": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
            "sha384":
"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd",

"sha512":"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d64
5ae27acb15bfb1447f459b"
          }
        }
      ],
      "id": "4fb5bbcaa61e77d5024b0f02256d3b78339606ef",
      "ipv4": [
        {
          "asn": "AS16276 OVH SAS",
          "city": "Singapore",
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "128.199.23.9",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "ipv6": [
        {
          "asn": "AS16276 OVH SAS",
          "city": "Singapore",
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "isFavourite": false,
      "isHidden": false,
      "malwareList": [
        {
          "id": "f9983dbd202159e87ca7ab517d1ca4b08aed542a",
          "name": "U-Admin"
        }
      ],
```

```
      "oldId": "448197320",
      "platform": null,
      "seqUpdate": 1622322902077,
      "ssl": [],
      "threatActor": {
        "country": "CN",
        "id": "55011fb96789bcb43c8e19e4e886924f803b6d30",
        "isAPT": true,
        "name": "IronTiger"
      },
      "url": "http://128.199.23.9/uadmin/gate.php"
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc	Related Indicator.Value	FQDN	.items[].dateDetected	'http://128.199.23.9/uadmin/gate.php'	
.items[].domain	Related Indicator.Value	FQDN	.items[].dateDetected	'www.0983212l.link'	
.items[].file[].hashes.md5	Related Indicator.Value	MD5	.items[].dateDetected	'5765fafd258a5a1e87c0582a67862675'	
.items[].file[].hashes.sha1	Related Indicator.Value	SHA-1	.items[].dateDetected	'ba835af7b8aa51797f95223676640be9c81dad9f'	
.items[].file[].hashes.sha256	Related Indicator.Value	SHA-256	.items[].dateDetected	'0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40'	
.items[].file[].hashes.sha384	Related Indicator.Value	SHA-384	.items[].dateDetected	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	
.items[].file[].hashes.sha512	Related Indicator.Value	SHA-512	.items[].dateDetected	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	
.items[].ipv4[].ip	Related Indicator.Value	IP Address	.items[].dateDetected	'128.199.23.9'	
.items[].ipv4[].asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	
.items[].ipv4[].city	Related Indicator.Attribute	City	.items[].dateDetected	'Singapore'	
.items[].ipv4[].countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'SG'	
.items[].ipv4[].countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Singapore'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].ipv4[].provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'DigitalOcean'	
.items[].ipv4[].region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	
.items[].ipv6[].ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	
.items[].ipv6[].asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	
.items[].ipv6[].city	Related Indicator.Attribute	City	.items[].dateDetected	'Singapore'	
.items[].ipv6[].countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'SG'	
.items[].ipv6[].countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Singapore'	
.items[].ipv6[].provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'DigitalOcean'	
.items[].ipv6[].region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].dateDetected	'U-Admin'	
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	'IronTiger'	
.items[].threatActor.country	Related Adversary.Attribute	Country	.items[].dateDetected	'CN'	
.items[].url	Related Indicator.Value	URL	.items[].dateDetected	'http://128.199.23.9/uadmin/gate.php'	If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator

Group-IB Suspicious IP Tor Node, Group-IB Suspicious IP Open Proxy and Group-IB Suspicious IP Socks Proxy

Group-IB Suspicious IP Tor Node

```
GET https://bt.group-ib.com/api/v2/suspicious_ip/tor_node
```

Group-IB Suspicious IP Open Proxy

```
GET https://bt.group-ib.com/api/v2/suspicious_ip/tor_node
```

Group-IB Suspicious IP Socks Proxy

```
GET https://bt.group-ib.com/api/v2/suspicious_ip/tor_node
```

These feeds ingests Indicators objects.


```
{
  "resultId": "ce0d600cdffbcbf9671552e201a92e5e4df730a9",
  "count": 132912,
  "items": [
    {
      "dateFirstSeen": "2020-05-27T14:57:33+00:00",
      "dateLastSeen": "2021-04-15T15:31:43+00:00",
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 90,
        "reliability": 90,
        "severity": "green",
        "tlp": "green",
        "ttl": 30
      },
      "id": "199.249.230.184",
      "ipv4": {
        "asn": "AS16276 OVH SAS",
        "city": "Singapore",
        "countryCode": "SG",
        "countryName": "Singapore",
        "ip": "128.199.23.10",
        "provider": "DigitalOcean",
        "region": "Central"
      },
      "nodes": [],
      "portalLink": "https://bt.group-ib.com/suspicious/tor?searchValue=id:199.249.230.184",
      "seqUpdate": 16182431110000,
      "source": "check.torproject.org",
      "port": "80",
      "type": "http"
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].ipv4.ip	Indicator.Value	IP Address	.items[].dateFirstSeen	'128.199.23.10'
.items[].ipv4.asn	Indicator.Attribute	ASN	.items[].dateFirstSeen	'AS16276 OVH SAS'
.items[].ipv4.city	Indicator.Attribute	City	.items[].dateFirstSeen	'Singapore'
.items[].ipv4.countryCode	Indicator.Attribute	Country Code	.items[].dateFirstSeen	'SG'
.items[].ipv4.countryName	Indicator.Attribute	Country Name	.items[].dateFirstSeen	'Singapore'
.items[].ipv4.provider	Indicator.Attribute	Provider	.items[].dateFirstSeen	'DigitalOcean'
.items[].ipv4.region	Indicator.Attribute	Region	.items[].dateFirstSeen	'Central'
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].dateFirstSeen	'B2'
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (seconds)	.items[].dateFirstSeen	'30'
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].dateFirstSeen	'https://bt.group-ib.com/suspicious/tor?searchValue=id:199.249.230.184'
.items[].source	Indicator.Attribute	Source	.items[].dateFirstSeen	'check.torproject.org'
.items[].type	Indicator.Attribute	Proxy Type	.items[].dateFirstSeen	'http'
.items[].port	Indicator.Attribute	Port	.items[].dateFirstSeen	'80'

Group-IB Compromised Account

`GET https://bt.group-ib.com/api/v2/compromised/account`

This feed ingests custom object Compromised Account and any related Indicators, Malware, and Adversaries.


```
{
  "resultId": "52638d2b8ff60727c93e4476a32d66b09f12ed52",
  "count": 300,
  "items": [
      {
          "botId": null,
          "client": {
              "ipv4": {
                  "asn": "AS9797 Nexon Asia Pacific P/L",
                  "city": "Canberra",
                  "countryCode": "AU",
                  "countryName": "Australia",
                  "ip": "210.215.170.103",
                  "provider": "Nexon Asia Pacific P/L",
                  "region": "Australian Capital Territory"
              }
          },
          "cnc": {
              "cnc": "http://113.218.160.19/",
              "domain": "113.218.160.19",
              "ipv4": {
                  "asn": "AS4134 No.31,Jin-rong Street",
                  "city": "Changsha",
                  "countryCode": "CN",
                  "countryName": "China",
                  "ip": "113.218.160.19",
                  "provider": "China Telecom Hunan",
                  "region": "Hunan"
              },
              "ipv6": null,
              "url": "http://113.218.160.19/"
          },
          "dateCompromised": "2020-05-19T12:39:15+00:00",
          "dateDetected": "2020-05-19T12:39:15+00:00",
          "device": null,
          "domain": "test-company-1.com",
          "evaluation": {
              "admiraltyCode": "B3",
              "credibility": 50,
              "reliability": 80,
              "severity": "orange",
              "tlp": "red",
              "ttl": 90
          },
          "id": "4c48fd8197dba2eecc42d56bfbaba7483e497ea7",
          "isFavourite": false,
          "isHidden": false,
          "login": "user511627",
```

```
            "malware": {
                "id": "e323de16fc8162e02aad6683b0f48a0e4008cbae",
                "name": "QBot"
            },
            "oldId": "1590",
            "password": "605f3ea202c9",
            "person": {
                "address": null,
                "birthday": null,
                "city": null,
                "countryCode": null,
                "email": null,
                "name": null,
                "passport": null,
                "phone": null,
                "state": null,
                "taxNumber": null,
                "zip": null
            },
            "port": null,
            "portalLink": "https://bt-demo.group-ib.com/cd/accounts?searchValue=id:
4c48fd8197dba2eecc42d56bfbaba7483e497ea7",
            "seqUpdate": 1589893516084,
            "sourceLink": "",
            "sourceType": "Phishing",
            "threatActor": {
                "country": null,
                "id": "4fde44244b3ed5f4ced23dc890efacf8aceb306a",
                "isAPT": false,
                "name": "Pontorez"
            }
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS9797 Nexon Asia Pacific P/L	
.items[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Canberra	
.items[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	AU	
.items[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	Australia	
.items[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	210.215.170.103	
.items[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	Nexon Asia Pacific P/L	
.items[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	Australian Capital Territory	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateDetected	http://113.218.160.19/	
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	113.218.160.19	
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS4134 No.31,Jin-rong Street	
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Changsha	
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	CN	
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	China	
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	113.218.160.19	
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	China Telecom Hunan	
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	Hunan	
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	N/A	
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	N/A	
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	N/A	
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	N/A	
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A	
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateDetected	N/A	
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	http://113.218.160.19/	
.items[].domain	Related Indicator.Value	FQDN	.items[].dateDetected	test-company-1.com	
.items[].evaluation.admiraltyCode	Account.Attribute	Admiralty Code	.items[].dateDetected	B3	
.items[].evaluation.credibility	Account.Attribute	Credibility	.items[].dateDetected	50	
.items[].evaluation.reliability	Account.Attribute	Reliability	.items[].dateDetected	80	
.items[].evaluation.severity	Account.Attribute	Severity	.items[].dateDetected	orange	
.items[].evaluation.tlp	Account.TLP / Related Objects.TLP	N/A	.items[].dateDetected	red	
.items[].evaluation.ttl	Account.Attribute	Time to live (seconds)	.items[].dateDetected	90	
.items[].malware.name	Related Malware.Value	N/A	.items[].dateDetected	QBot	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].login	Account.Value	N/A	.items[].dateDetected	user511627	The value is composed of 'Account + .items[].login'
.items[].password	Account.Attribute	Password	.items[].dateDetected	605f3ea202c9	
.items[].sourceType	Account.Attribute	Source Type	.items[].dateDetected	Phishing	
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	Pontorez	

Group-IB Compromised Card

`GET https://bt.group-ib.com/api/v2/compromised/card`

This feed ingests custom object Compromised Card and any related Indicators, and Malware.


```
{
  "resultId": "e1c62dc66e72e0fb9992183fbf82d5739d927d41",
    "count": 400,
    "items": [
        {
            "baseName": null,
            "cardInfo": {
                "cvv": 946,
                "dump": null,
                "issuer": {
                    "countryCode": "IN",
                    "countryName": "INDIA",
                    "issuer": "STATE BANK OF INDIA"
                },
                "number": "4000174114732465",
                "system": "VISA",
                "type": "CLASSIC",
                "validThru": "8/2016"
            },
            "client": {
                "ipv4": {
                    "asn": "AS497 754th Electronic Systems Group",
                    "city": "Raleigh",
                    "countryCode": "US",
                    "countryName": "United States",
                    "ip": "56.151.217.119",
                    "provider": "United States Postal Service.",
                    "region": "North Carolina"
                }
            },
            "cnc": {
                "cnc": "http://246.119.220.81/",
                "domain": "246.119.220.81",
                "ipv4": {
                    "asn": "AS497 754th Electronic Systems Group",
                    "city": "Raleigh",
                    "countryCode": "US",
                    "countryName": "United States",
                    "ip": "246.119.220.81",
                    "provider": "United States Postal Service",
                    "region": "North Carolina"
                },
                "ipv6": null,
                "url": "http://246.119.220.81/"
            },
            "dateCompromised": "2020-06-05T10:07:26+00:00",
            "dateDetected": "2020-06-05T10:07:26+00:00",
            "evaluation": {
                "admiraltyCode": "B3",
                "credibility": 50,
```

```
                "reliability": 80,
                "severity": "orange",
                "tlp": "red",
                "ttl": 90
            },
            "externalId": "",
            "id": "b3d87b6af5532ee8d41baac000bba2d1c46662c8",
            "isFavourite": false,
            "isHidden": false,
            "isIgnore": false,
            "malware": {
                "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f60",
                "name": "Phishing"
            },
            "oldId": "2308",
            "owner": {
                "address": null,
                "birthday": null,
                "city": null,
                "countryCode": null,
                "email": null,
                "name": null,
                "passport": null,
                "phone": null,
                "state": null,
                "taxNumber": null,
                "zip": null
            },
            "portalLink": "https://bt-demo.group-ib.com/cd/cards?
searchValue=id:b3d87b6af5532ee8d41baac000bba2d1c46662c8",
            "price": {
                "currency": null,
                "value": null
            },
            "seqUpdate": 1591351984817,
            "serviceCode": null,
            "sourceLink": "",
            "sourceType": "Phishing",
            "threatActor": {
                "country": null,
                "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
                "isAPT": false,
                "name": "MegaPony"
            },
            "track": []
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].cardInfo.cvv	Card.Attribute	Card CVV	.items[].dateDetected	966
.items[].cardInfo.issuer.countryCode	Card.Attribute	Card Issuer Country Code	.items[].dateDetected	IN
.items[].cardInfo.issuer.countryName	Card.Attribute	Card Issuer Country	.items[].dateDetected	INDIA

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].cardInfo.issuer.issuer	Card.Attribute	Card Issuer	.items[].dateDetected	STATE BANK OF INDIA
.items[].cardInfo.number	Card.Value	Card Number	.items[].dateDetected	4000174114732465
.items[].cardInfo.system	Card.Attribute	Card System	.items[].dateDetected	VISA
.items[].cardInfo.type	Card.Attribute	Card Type	.items[].dateDetected	CLASSIC
.items[].cardInfo.validThru	Card.Attribute	Card Expiration	.items[].dateDetected	8/2016
.items[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS497 754th Electronic Systems Group
.items[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Raleigh
.items[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	US
.items[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	United States
.items[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	56.151.217.119
.items[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	United States Postal Service
.items[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	North Carolina
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateDetected	http://246.119.220.81/
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	246.119.220.81
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS497 754th Electronic Systems Group
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Raleigh
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	US
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	United States
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	246.119.220.81
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	United States Postal Service
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	North Carolina
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	N/A
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	N/A
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	N/A
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	N/A
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateDetected	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	http://246.119.220.81/
.items[].evaluation.admiraltyCode	Card.Attribute	Admiralty Code	.items[].dateDetected	B3
.items[].evaluation.credibility	Card.Attribute	Credibility	.items[].dateDetected	50
.items[].evaluation.reliability	Card.Attribute	Reliability	.items[].dateDetected	80
.items[].evaluation.severity	Card.Attribute	Severity	.items[].dateDetected	orange
.items[].evaluation.tlp	Card.TLP / Related Objects.TLP	N/A	.items[].dateDetected	red
.items[].evaluation.ttl	Card.Attribute	Time to live (seconds)	.items[].dateDetected	90
.items[].malware.name	Related Malware.Value	N/A	.items[].dateDetected	Trochilus
.items[].owner.address	Related Identity.Attribute	Address	.items[].dateDetected	N/A
.items[].owner.birthday	Related Identity.Attribute	Birthday	.items[].dateDetected	N/A
.items[].owner.city	Related Identity.Attribute	City	.items[].dateDetected	N/A
.items[].owner.countryCode	Related Identity.Attribute	Country Code	.items[].dateDetected	N/A
.items[].owner.email	Related Identity.Attribute	Email	.items[].dateDetected	N/A
.items[].owner.name	Related Identity.Attribute	Name	.items[].dateDetected	N/A
.items[].owner.passport	Related Identity.Attribute	Passport data	.items[].dateDetected	N/A
.items[].owner.phone	Related Identity.Attribute	Phone Number	.items[].dateDetected	N/A
.items[].owner.state	Related Identity.Attribute	State	.items[].dateDetected	N/A
.items[].owner.taxNumber	Related Identity.Value	N/A	.items[].dateDetected	N/A
.items[].owner.zip	Related Identity.Attribute	ZIP Code	.items[].dateDetected	N/A
.items[].sourceType	Card.Attribute	Source Type	.items[].dateDetected	Phishing
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	MegaPony

Group-IB Attacks DDoS

`GET https://bt.group-ib.com/api/v2/attacks/ddos`

This feed ingests Indicators objects.


```
{
  "resultId": "7545813d204a0ab3cb233da144bc06a4ef6223b6",
    "count": 100,
    "items": [
        {
            "cnc": {
                "cnc": "peacecorps.gov",
                "domain": "peacecorps.gov",
                "ipv4": {
                    "asn": "AS14618 Amazon.com, Inc.",
                    "city": "Ashburn",
                    "countryCode": "US",
                    "countryName": "United States",
                    "ip": "52.202.206.232",
                    "provider": "Amazon.com",
                    "region": "Virginia"
                },
                "ipv6": null,
                "url": null
            },
            "dateBegin": "2019-03-11T06:58:51+00:00",
            "dateEnd": "2019-03-11T06:58:51+00:00",
            "dateReg": "2019-03-11",
            "evaluation": {
                "admiraltyCode": "A2",
                "credibility": 90,
                "reliability": 90,
                "severity": "red",
                "tlp": "green",
                "ttl": 30
            },
            "id": "3411bdc00c4f7ab43723f30205c31a20e183acf3",
            "isFavourite": false,
            "isHidden": false,
            "malware": {
                "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f69",
                "name": "Bootnet"
            },
            "messageLink": null,
            "oldId": "222",
            "portalLink": "https://bt-demo.group-ib.com/attacks/ddos?searchValue=id:
3411bdc00c4f7ab43723f30205c31a20e183acf3",
            "protocol": "udp",
            "seqUpdate": 0,
            "target": {
                "ipv4": {
                    "asn": "AS3223 Voxility S.R.L.",
                    "city": "London",
                    "countryCode": "GB",
                    "countryName": "United Kingdom",
```

```
                    "ip": "185.82.99.18",
                    "provider": "Net 360 S.a.r.l",
                    "region": "London, City of"
                },
                "url": "brot.net",
                "category": null,
                "domainsCount": 3,
                "port": 10913,
                "domain": null
            },
            "threatActor": null,
            "type": "DNS Reflection"
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].cnc.cnc	Indicator.Value	FQDN	.items[].dateBegin	peacecorps.gov
.items[].cnc.domain	Indicator.Value	FQDN	.items[].dateBegin	peacecorps.gov
.items[].cnc.ipv4.asn	Indicator.Attribute	ASN	.items[].dateBegin	AS14618 Amazon.com, Inc.
.items[].cnc.ipv4.city	Indicator.Attribute	City	.items[].dateBegin	Ashburn
.items[].cnc.ipv4.countryCode	Indicator.Attribute	Country Code	.items[].dateBegin	US
.items[].cnc.ipv4.countryName	Indicator.Attribute	Country Name	.items[].dateBegin	United States
.items[].cnc.ipv4.ip	Indicator.Value	IP Address	.items[].dateBegin	52.202.206.232
.items[].cnc.ipv4.provider	Indicator.Attribute	Provider	.items[].dateBegin	Amazon.com
.items[].cnc.ipv4.region	Indicator.Attribute	Region	.items[].dateBegin	Virginia
.items[].cnc.ipv6.asn	Indicator.Attribute	ASN	.items[].dateBegin	N/A
.items[].cnc.ipv6.city	Indicator.Attribute	City	.items[].dateBegin	N/A
.items[].cnc.ipv6.countryCode	Indicator.Attribute	Country Code	.items[].dateBegin	N/A
.items[].cnc.ipv6.countryName	Indicator.Attribute	Country Name	.items[].dateBegin	N/A
.items[].cnc.ipv6.ip	Indicator.Value	IPv6 Address	.items[].dateBegin	N/A
.items[].cnc.ipv6.provider	Indicator.Attribute	Provider	.items[].dateBegin	N/A
.items[].cnc.ipv6.region	Indicator.Attribute	Region	.items[].dateBegin	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateBegin	N/A
.items[].evaluation.admiraltyCode	Indicator/Malware/ Adversary.Attribute	Admiralty Code	.items[].dateBegin	A2
.items[].evaluation.credibility	Indicator/Malware/ Adversary.Attribute	Credibility	.items[].dateBegin	90
.items[].evaluation.reliability	Indicator/Malware/ Adversary.Attribute	Reliability	.items[].dateBegin	90
.items[].evaluation.severity	Indicator/Malware/ Adversary.Attribute	Severity	.items[].dateBegin	red

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].evaluation.tlp	Indicator/Malware/ Adversary.TLP	Traffic Light Protocol	.items[].dateBegin	green
.items[].evaluation.ttl	Indicator/Malware/ Adversary.Attribute	Time to live (seconds)	.items[].dateBegin	30
.items[].malware.name	Malware.Value	N/A	.items[].dateBegin	Bootnet
.items[].messageLink	Indicator/Malware/ Adversary.Attribute	Message Link	.items[].dateBegin	N/A
.items[].portalLink	Indicator/Malware/ Adversary.Attribute	Source Link	.items[].dateBegin	https://bt.group-ib.com/attacks/ddos?searchValue=id:053e63f81d0e1ebef83b0d3a5cbfebbe1a2b28a7
.items[].protocol	Indicator/Malware/ Adversary.Attribute	Protocol	.items[].dateBegin	udp
.items[].target.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateBegin	AS3223 Voxility S.R.L.
.items[].target.ipv4.city	Related Indicator.Attribute	City	.items[].dateBegin	London
.items[].target.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateBegin	GB
.items[].target.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateBegin	United Kingdom
.items[].target.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateBegin	185.82.99.18
.items[].target.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateBegin	Net 360 S.a.r.l
.items[].target.ipv4.region	Related Indicator.Attribute	Region	.items[].dateBegin	London, City of
.items[].target.url	Indicator.Value	URL	.items[].dateBegin	brot.net
.items[].target.category	Indicator/Malware/ Adversary.Attribute	Category	.items[].dateBegin	N/A
.items[].target.port	Indicator/Malware/ Adversary.Attribute	Port	.items[].dateBegin	10913
.items[].target.domain	Indicator.Value	FQDN	.items[].dateBegin	N/A
.items[].threatActor.name	Adversary.Value	N/A	.items[].dateBegin	N/A
.items[].type	Indicator/Malware/ Adversary.Attribute	Type	.items[].dateBegin	DNS Reflection

Group-IB Malware Targeted Malware

`GET https://bt.group-ib.com/api/v2/malware/targeted_malware`

This feed ingests Malware objects and any related Indicators, and Adversary.


```
{
    "resultId": "6c78425a2879a39b4ef0d12b09a7e6ae53f0b0de",
    "count": 1,
    "items": [
        {
            "date": "2019-03-14T01:01:21+00:00",
            "dateAnalyzeEnded": null,
            "dateAnalyzeStarted": null,
            "evaluation": {
                "admiraltyCode": "A1",
                "credibility": 100,
                "reliability": 100,
                "severity": "red",
                "tlp": "red",
                "ttl": null
            },
            "fileName": null,
            "fileType": "PE32 executable (GUI) Intel 80386, for MS Windows",
            "fileVersion": null,
            "hasReport": false,
            "id": "c3685e16913400be5745e16f895cf13c431275b4",
            "injectDump": "{\n\"integers\": [\n\"10\",\n\"12\",\n\"60\",\n\"600\",\n\"1000\",\n\"300\",\n\"1000\",
\n\"300\",\n\"10\",\n\"3231\",\n\"200\"\n],\n\"family\": \"gozi\",\n\"key\": [\n\"10291029JSJUYNHG\"\n],\n\"urls\":
[\n\"xoblaiseoj.email\"\n],\n\"domains\": [\n\"com ru org\", \"test-company-1.com\"\n],\n\"hex\": []\n}",
            "injectMd5": "067e7db771471182ecab5d7a14ec4c1e",
            "isFavourite": false,
            "isHidden": false,
            "malware": {
                "id": "71362b4e63a086af61ac1fde632be254c761d8f0",
                "name": "GoziLoader"
            },
            "md5": "c9d002ba70208570bfc624309b9413ed",
            "oldId": "1296",
            "portalLink": "https://bt-demo.group-ib.com/targeted_malware/GoziLoader/sample/
c3685e16913400be5745e16f895cf13c431275b4/show",
            "seqUpdate": 1553104463529,
            "sha1": null,
            "sha256": null,
            "size": 229376,
            "source": "Sandbox service",
            "threatActor": null
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.admiraltyCode	Malware.Attribute	Admiralty Code	.items[].date	A1	
.items[].evaluation.credibility	Malware.Attribute	Credibility	.items[].date	100	
.items[].evaluation.reliability	Malware.Attribute	Reliability	.items[].date	100	
.items[].evaluation.severity	Malware.Attribute	Severity	.items[].date	red	
.items[].evaluation.tlp	Malware.TLP / Related Objects.TLP	N/A	.items[].date	red	
.items[].evaluation.ttl	Malware.Attribute	Time to live (seconds)	.items[].date	N/A	
.items[].fileName	Malware.Attribute	File Name	.items[].date	N/A	
.items[].fileType	Malware.Attribute	File Type	.items[].date	PE32 executable (GUI) Intel 80386, for MS Windows	
.items[].fileVersion	Malware.Attribute	File Version	.items[].date	N/A	
.items[].injectMd5	Related Indicator.Value	MD5	.items[].date	067e7db771471182ecab5d7a14ec4c1e	
.items[].malware.name	Malware.Value	N/A	.items[].date	GoziLoader	
.items[].md5	Related Indicator.Value	MD5	.items[].date	c9d002ba70208570bfc624309b9413ed	
.items[].sha1	Related Indicator.Value	SHA-1	.items[].date	N/A	
.items[].sha256	Related Indicator.Value	SHA-256	.items[].date	N/A	
.items[].size	Malware.Attribute	File Size	.items[].date	229376	
.items[].source	Malware.Attribute	Source	.items[].date	Sandbox service	
.items[].threatActor.name	Related Adversary.Value	N/A	.items[].date	N/A	

Group-IB Attacks Phishing

`GET https://bt.group-ib.com/api/v2/attacks/phishing`

This feed ingests Indicator objects.


```
{
"resultId": "6138aa5622203a71b8c8fa07d9d3e79aef7ccde4",
"count": 12,
"items": [
    {
        "dateBlocked": "2019-03-21T05:53:05+00:00",
        "dateDetected": "2019-03-20T08:46:36+00:00",
        "evaluation": {
            "admiraltyCode": "A2",
            "credibility": 80,
            "reliability": 90,
            "severity": "red",
            "tlp": "amber",
            "ttl": 30
        },
        "history": [
            {
                "date": "2019-03-20T08:47:54+00:00",
                "field": "Detected",
                "reason": null,
                "reporter": "Group-IB Intelligence",
                "value": "In response"
            },
            {
                "date": "2019-03-21T07:46:51+00:00",
                "field": "Status has been changed",
                "reason": null,
                "reporter": "Group-IB Intelligence",
                "value": "In response"
            }
        ],
        "id": "fb2c54adc40a6cc1dbe5ad9771c9787db4fabb64",
        "ipv4": {
            "asn": "AS43260",
            "city": null,
            "countryCode": "CY",
            "countryName": "Cyprus",
            "ip": "185.71.216.171",
            "provider": null,
            "region": "AS"
        },
        "isFavourite": false,
        "isHidden": false,
        "objective": "Card harvest",
        "oldId": "1331",
        "phishingDomain": {
            "domain": "kdrbilisim.com",
            "local": "kdrbilisim.com",
            "dateRegistered": "2012-09-09 13:03:26",
            "title": "ANKARA BİLGİSAYAR TEKNİK SERVİS 0312 226 50 40 | 0312 226 50 40",
```

```
            "registrar": "PDR Ltd. d/b/a PublicDomainRegistry.com"
        },
        "portalLink": "https://bt-demo.group-ib.com/attacks/phishing?
searchValue=id:fb2c54adc40a6cc1dbe5ad9771c9787db4fabb64",
        "seqUpdate": 1553180722582,
        "status": "In response",
        "targetBrand": "Bank of America",
        "targetCategory": "Finance & Investment",
        "targetCountryName": null,
        "targetDomain": "bankofamerica.com",
        "type": "Phishing",
        "url": "https://www.kdrbilisim.com/Boa"
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].dateDetected	A2	
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateDetected	80	
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateDetected	90	
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateDetected	red	
.items[].evaluation.tlp	Indicator.TLP / Related Object.TLP	Traffic Light Protocol	.items[].dateDetected	amber	
.items[].evaluation.ttl	Indicator.Attribute	Time to live (seconds)	.items[].dateDetected	30	
.items[].ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS43260	
.items[].ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	
.items[].ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	CY	
.items[].ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	Cyprus	
.items[].ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	185.71.216.171	
.items[].ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A	
.items[].ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	AS	
.items[].objective	Indicator.Attribute	Objective	.items[].dateDetected	Card harvest	
.items[].phishingDomain.domain	Indicator.Value	FQDN	.items[].phishingDomain.dateRegistered	kdrbilisim.com	
.items[].phishingDomain.local	Indicator.Attribute	Local	.items[].phishingDomain.dateRegistered	kdrbilisim.com	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].phishingDomain.title	Indicator.Attribute	Title	.items[].phishingDomain.dateRegistered	ANKARA BİLGİSAYAR TEKNİK SERVİS 0312 226 50 40 0312 226 50 40	
.items[].phishingDomain.registrar	Indicator.Attribute	Registrar	.items[].phishingDomain.dateRegistered	PDR Ltd. d/b/a PublicDomainRegistry.com	
.items[].status	Indicator.Attribute	Status	.items[].dateDetected	In response	
.items[].targetBrand	Indicator.Attribute	Target Brand	.items[].dateDetected	Bank of America	
.items[].targetCategory	Indicator.Attribute	Target Category	.items[].dateDetected	Finance & Investment	
.items[].targetCountryName	Indicator.Attribute	Target Country	.items[].dateDetected	N/A	
.items[].targetDomain	Indicator.Attribute	Target Domain	.items[].dateDetected	bankofamerica.com	
.items[].type	Indicator.Attribute	Type	.items[].dateDetected	Phishing	
.items[].url	Related Indicator.Value	URL	.items[].dateDetected	https://www.kdrbilisim.com/Boa	

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.

Group-IB Compromised Data Mules

METRIC	RESULT
Run Time	3 minutes
Adversaries	3
Adversary Attributes	3
Indicators	7
Indicator Attributes	12
Malware	2
Malware Attributes	2
Money Mule	500
Money Mule Attributes	5,504
Organization	9

Group-IB Compromised Data IMEI

METRIC	RESULT
Run Time	1 minute
Adversaries	1
Adversary Attributes	1
IMEI	397
IMEI Attributes	4,006
Indicators	63
Indicator Attributes	286
Malware	3
Malware Attributes	3

Group-IB APT Threat

METRIC	RESULT
Run Time	25 minutes
Attack Pattern	350
Attack Pattern Attributes	795
Identity	210
Identity Attributes	444
Indicators	23,942
Indicator Attributes	3,160
Intrusion Set	483
Intrusion Set Attributes	9,358
Malware	255
Tool	37

Group-IB Human Intelligence Threat Actor

METRIC	RESULT
Run Time	3 minutes
Adversaries	241
Adversary Attributes	1,929
Indicators	114
Indicator Attributes	342
Report	392
Report Attributes	428

Group-IB Human Malware C2

METRIC	RESULT
Run Time	1 minute
Adversaries	19
Indicators	439
Indicator Attributes	152
Malware	18

Group-IB Human Intelligence Threat Actor

METRIC	RESULT
Run Time	5 minutes
Indicators	500
Indicator Attributes	7,884

GroupIB Compromised Account

METRIC	RESULT
Run Time	2 minutes
Accounts	300
Account Attributes	2,100
Adversaries	7
Indicators	584
Indicator Attributes	2,919
Malware	10

GroupIB Compromised Card

METRIC	RESULT
Run Time	2 minutes
Cards	400
Card Attributes	3,751
Indicators	761
Indicator Attributes	3,787
Malware	10

GroupIB Attacks DDoS

METRIC	RESULT
Run Time	1 minute
Indicators	84
Indicator Attributes	1,158

GroupIB Malware Targeted Malware

METRIC	RESULT
Run Time	1 minute
Indicators	1
Malware	1
Malware Attributes	7

GroupIB Attacks Phishing

METRIC	RESULT
Run Time	1 minute
Indicators	17
Indicator Attributes	87

Change Log

- **Version 2.1.0**
  - Added new endpoints to the CDF. These new endpoints require the installation of additional custom objects: Compromised Account and Compromised Card. See the Prerequisites section for more details.
- **Version 2.0.0**
  - Initial release