

ThreatQuotient



Group-IB CDF User Guide

Version 3.4.6

February 26, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	4
Support	5
Integration Details.....	6
Introduction	7
Prerequisites	8
Custom Objects Installation	8
Installation.....	10
Configuration	11
ThreatQ Mapping.....	13
GroupIB Compromised Account.....	13
GroupIB Compromised Bank Card.....	19
GroupIB Compromised Data Mules	25
GroupIB Compromised Data Git Leaks.....	29
GroupIB Compromised Data IMEI	33
GroupIB Compromised Data Shops.....	37
GroupIB Compromised IM Discord	40
GroupIB Compromised IM Telegram	43
GroupIB Compromised Masked Bank Card.....	46
GroupIB Human Intelligence Threat and GroupIB APT Threat	52
GroupIB Human Intelligence Threat Actor and GroupIB APT Threat Actor	61
GroupIB Malware C2	69
GroupIB Malware Configs.....	73
GroupIB Suspicious IP Tor Node, GroupIB Suspicious IP Open Proxy and GroupIB Suspicious IP	75
Socks Proxy	75
GroupIB Suspicious IP Scanners	77
GroupIB Suspicious IP VPN.....	79
GroupIB Attacks DDoS	81
GroupIB Attacks Deface	85
GroupIB Malware Report.....	87
GroupIB Malware Signature, GroupIB Malware YARA Rule.....	91
GroupIB Malware Vulnerability.....	93
GroupIB Attacks Phishing	99
GroupIB Attacks Phishing Group	102
GroupIB Attack Phishing Kit	106
GroupIB OSI PublicLeak	108
GroupIB IOC Common	111
Average Feed Run.....	113
GroupIB Compromised Account.....	113
GroupIB Compromised Bank Card.....	114
GroupIB Compromised Data Mules	114
GroupIB Compromised Data IMEI	115
GroupIB Compromised Data Shops.....	116

GroupIB Compromised IM Discord	116
GroupIB Compromised IM Telegram	117
GroupIB Compromised Masked Bank Card	117
GroupIB APT Threat Actors.....	118
GroupIB Human Malware C2	118
GroupIB Human Intelligence Threat Actor.....	119
GroupIB Malware Configs.....	119
GroupIB Suspicious IP Tor Node.....	120
GroupIB Suspicious IP Scanners	120
GroupIB Suspicious IP VPN.....	120
GroupIB Attacks DDoS	121
GroupIB Attacks Deface	121
GroupIB Malware Report.....	121
GroupIB Malware Signature	122
GroupIB Malware Vulnerability.....	123
GroupIB Attacks Phishing	123
GroupIB Attacks Phishing Group	124
GroupIB OSI PublicLeak	124
GroupIB IOC Common	124
Known Issues / Limitations	125
Change Log	126

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 © 2024 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

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	3.4.6
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

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:

- GroupIB Compromised Account
- GroupIB Compromised Bank Card
- GroupIB Compromised Data Git Leaks
- GroupIB Compromised Data Mules
- GroupIB Compromised Data IMEI
- GroupIB Compromised IM Discord
- GroupIB Compromised IM Telegram
- GroupIB Compromised Masked Band Card
- GroupIB Compromised Shops
- GroupIB Human Intelligence Threat
- GroupIB Human Intelligence Threat Actor
- GroupIB APT Threat
- GroupIB APT Threat Actor
- GroupIB Malware C2
- GroupIB Suspicious IP Open Proxy
- GroupIB Suspicious IP Socks Proxy
- GroupIB Suspicious IP VPN
- GroupIB Malware Configs
- GroupIB Suspicious IP Tor Node
- GroupIB Suspicious IP Scanner
- GroupIB Malware Report
- GroupIB Malware Signature
- GroupIB Malware YARA Rule
- GroupIB Malware Vulnerability
- GroupIB Attacks DDoS
- GroupIB Attacks Deface
- GroupIB Attacks Phishing
- GroupIB Attacks Phishing Group
- GroupIB Attacks Abuse Phishing Kit
- GroupIB OSI PublicLeak
- GroupIB IOC Common

Object types ingested from the feeds above include:

- Adversaries
- Attack Patterns
- Compromised Accounts (custom object)
- Compromised Cards (custom object)
- Identities
- IMEIs (custom object)
- Indicators
- Intrusion Sets
- Malware
- Money Mule (custom object)
- Organizations (custom object)
- Tools

Prerequisites

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

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

 The custom objects listed above must be installed prior to installing the CDF. Attempting to install the integration without the required custom objects will cause the install process to fail.

Custom Objects Installation

Use the steps provided to install the custom objects.

 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 and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
<> cd /tmp/
```

4. Create a new directory:

```
<> mkdir groupib_cdf
```

5. Upload the **groupib.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the groupib_cdf directory.

```
<> mkdir images
```

7. Upload the svg files.
8. Navigate to **/tmp/groupib_cdf**.

The directory should resemble the following:

- tmp
 - groupib_cdf
 - groupib.json
 - install.sh
 - images
 - Account.svg

- CompromisedCard.svg
- IMEI.svg
- MoneyMule.svg
- Organization.svg

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
<> chmod +x install.sh
```

10. Run the following command:

```
<> sudo ./install.sh
```



You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

```
----- Installing GroupIB Custom Objects -----
```

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)
```

```
[
[Application is now in maintenance mode.
]
```

```
Installing Custom Objects - Step 2 of 5 (Installing the GroupIB Custom Objects)
```

```
'/tmp/group-ib/icons/Account.svg' -> '/var/www/api/database/seeds/data/icons/images/custom_objects/Account.svg'
```

```
'/tmp/group-ib/icons/CompromisedCard.svg' -> '/var/www/api/database/seeds/data/icons/images/custom_objects/CompromisedCard.svg'
```

```
'/tmp/group-ib/icons/IMEI.svg' -> '/var/www/api/database/seeds/data/icons/images/custom_objects/IMEI.svg'
```

```
['/tmp/group-ib/icons/MoneyMule.svg' -> '/var/www/api/database/seeds/data/icons/images/custom_objects/MoneyMule.svg'
```

```
'/tmp/group-ib/icons/Organization.svg' -> '/var/www/api/database/seeds/data/icons/images/custom_objects/Organization.svg'
```

```
'/tmp/group-ib/groupib.json' -> '/var/www/api/database/seeds/data/custom_objects/groupib.json'
```

```
Installing Custom Objects - Step 3 of 5 (Configuring icons for the GroupIB Custom Objects)
```

```
[
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
]
```

```
[
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode and Restarting Dynamo)
]
```

```
Application is now live. _
```

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf groupib_cdf
```

Installation



The CDF requires the installation of five custom objects before installing the actual CDF. See the [Prerequisites](#) chapter 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 zip file.
3. Extract the files and install the required custom objects.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml 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.

7. 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
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.  This parameter supports the following feeds: GroupIB Human Threat Intelligence, GroupIB APT Threat, and GroupIB Malware Vulnerability.

< GroupIB Compromised Account



Disabled ☒ Enabled
 Run Integration
 Uninstall

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration

Activity Log

Username

API Key 

Set indicator status to...
Active 

Run Frequency

Every 24 Hours 

Next scheduled run:
2023-09-19 04:44am (-04:00)

☒ 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

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

ThreatQ Mapping

GroupIB Compromised Account

The Group IB Compromised Account feed ingests custom object Compromised Account and any related Indicators, Malware, and Adversaries.

GET <https://tap.group-ib.com/api/v2/compromised/account>

Sample Response:

```
{
  "resultId": "52638d2b8ff60727c93e4476a32d66b09f12ed52",
  "count": 1,
  "items": [
    {
      "dateFirstCompromised": "2022-11-29T12:57:33+00:00",
      "dateFirstSeen": "2023-01-11T15:44:55+00:00",
      "dateLastCompromised": "2022-11-29T12:57:33+00:00",
      "dateLastSeen": "2023-01-11T15:44:55+00:00",
      "evaluation": {
        "admiraltyCode": "B3",
        "credibility": 50,
        "reliability": 80,
        "severity": "orange",
        "tlp": "red",
        "ttl": 90
      },
      "eventCount": 1,
      "events": [
        {
          "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": null,
"dateDetected": "2022-05-25T13:37:04+00:00",
"id": "3d633aba8b867ad7ffae42fa4ad01c123d54d989",
"malware": {
    "category": [],
    "class": null,
    "id": "487aa3cd765901009e9582c809d8737e4639863f",
    "name": "Ologin",
    "platform": [],
    "stixGuid": "e0dbd349-855c-9fc5-82d7-6ccd1d177977",
    "threatLevel": null
},
"oldId": "1135330344",
"person": null,
"source": {
    "id": "",
    "idType": "http_link",
    "type": "Phishing"
},
"stixGuid": "25570f61-cc8b-f3dc-a940-67d0ccd83523",
"threatActor": null
}
],
"id": "4c48fd8197dba2eccc42d56bfbaba7483e497ea7",
"displayOptions": {
    "favouriteForCompanies": [],
    "hideForCompanies": [],
    "isFavourite": false,
    "isHidden": false
},
"login": "user511627",
"malware": [
    {
        "id": "e323de16fc8162e02aad6683b0f48a0e4008cbae",
        "name": "QBot"
    }
],
"parsedLogin": {
    "domain": "test-company-1.com",
    "ip": null
},

```

```

"service": {
  "domain": "www.my.commbank.com.au",
  "ip": null,
  "url": "https://www.my.commbank.com.au/netbank/Logon/Logon.aspx",
  "host": "www.my.commbank.com.au"
},
"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:4c48fd8197dba2eccc42d56bfbaba7483e497ea7",
"seqUpdate": 1589893516084,
"source": [
  {
    "id": "https://breachforums.is/Thread-SELLING-Naz-API-Dataset",
    "type": "Stealer log's combolist",
    "idType": "naz.API"
  }
],
"sourceType": [
  "Stealer log's combolist"
],
"threatActor": {
  "country": null,
  "id": "4fde44244b3ed5f4ced23dc890efacf8aceb306a",
  "isAPT": false,
  "name": "Pontorez"
}
}
]
}

```

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[].events[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	AS9797 Nexon Asia Pacific P/L	N/A
.items[].events[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	Canberra	N/A
.items[].events[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	AU	N/A
.items[].events[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	Australia	N/A
.items[].events[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateFirstSeen	210.215.170.103	N/A
.items[].events[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	Nexon Asia Pacific P/L	N/A
.items[].events[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	Australian Capital Territory	N/A
.items[].events[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateFirstSeen	http://113.218.160.19/	N/A
.items[].events[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateFirstSeen	113.218.160.19	N/A
.items[].events[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	AS4134 No.31,Jin-rong Street	N/A
.items[].events[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	Changsha	N/A
.items[].events[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	CN	N/A
.items[].events[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	China	N/A
.items[].events[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateFirstSeen	113.218.160.19	N/A
.items[].events[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	China Telecom Hunan	N/A
.items[].events[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	Hunan	N/A
.items[].events[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].events[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.url	Related Indicator.Value	URL	.items[].dateFirstSeen	http://113.218.160.19/	N/A
.items[].parsedLogin.domain	Related Indicator.Value	FQDN	.items[].dateFirstSeen	test-company-1.com	N/A
.items[].service.domain	Related Indicator.Value	FQDN	.items[].dateFirstSeen	www.my.commbank.com.au	N/A
.items[].service.url	Related Indicator.Value	URL	.items[].dateFirstSeen	https://www.my.commbank.com.au/netbank/Logon/Logon.aspx	N/A
.items[].evaluation.admiraltyCode	Account.Attribute	Admiralty Code	.items[].dateFirstSeen	B3	If the attribute already exists, the value will be updated
.items[].evaluation.credibility	Account.Attribute	Credibility	.items[].dateFirstSeen	50	If the attribute already exists, the value will be updated
.items[].evaluation.reliability	Account.Attribute	Reliability	.items[].dateFirstSeen	80	If the attribute already exists, the value will be updated
.items[].evaluation.severity	Account.Attribute	Severity	.items[].dateFirstSeen	orange	If the attribute already exists, the value will be updated
.items[].evaluation.tlp	Account.TLP / Related Objects.TLP	N/A	.items[].dateFirstSeen	red	N/A
.items[].evaluation.ttl	Account.Attribute	Time to live (days)	.items[].dateFirstSeen	90	If the attribute already exists, the value will be updated
.items[].malware[].name	Related Malware.Value	N/A	.items[].dateFirstSeen	QBot	N/A
.items[].login	Account.Value	N/A	.items[].dateFirstSeen	user511627	The value is composed of 'Account' + .items[].login'
.items[].password	Account.Attribute	Password	.items[].dateFirstSeen	605f3ea202c9	N/A
.items[].sourceType	Account.Attribute	Source Type	.items[].dateFirstSeen	Stealer log's combolist	N/A
.items[].source[].id	Account.Attribute	Source Link	.items[].dateFirstSeen	https://breachforums.is/Thread-SELLING-Naz-API-Dataset	N/A
.items[].dateFirstCompromised	Account.Attribute	Compromised Date	.items[].dateFirstSeen	2022-11-29T12:57:33+00:00	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].threatActor[].name	Related Adversary.Name	N/A	.items[].dateFirstSeen	Pontorez	N/A

GroupIB Compromised Bank Card

The GroupIB Compromised Bank Card feed ingests custom object Compromised Card and any related Indicators, and Malware.

GET https://tap.group-ib.com/api/v2/compromised/bank_card_group

Sample Response:

```
{
  "resultId": "e1c62dc66e72e0fb9992183fbf82d5739d927d41",
  "count": 400,
  "items": [
    {
      "baseName": null,
      "cardInfo": {
        "bin": [
          "601129",
          "6011298",
          "60112988",
          "601129880",
          "6011298803"
        ],
        "issuer": {
          "countryCode": "IN",
          "countryName": "INDIA",
          "issuer": "STATE BANK OF INDIA"
        },
        "number": "4000174114732465",
        "system": "VISA",
        "type": "CLASSIC"
      },
      "eventCount": 1,
      "events": [
        {
          "cardInfo": {
            "cvv": "966",
            "dump": null,
            "pin": null,
            "validThru": "8/2016",
            "validThruDate": "2016-08-31"
          },
          "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/"
    },
    "malware": {
        "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f60",
        "name": "Phishing"
    },
    "owner": {
        "address": null,
        "city": null,
        "countryCode": null,
        "email": null,
        "name": null,
        "passport": null,
        "phone": null,
        "state": null,
        "zip": null
    },
    "source": {
        "id": null,
        "idType": null,
        "type": "Phishing"
    },
    "threatActor": {
        "country": null,
        "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
        "isAPT": false,
        "name": "MegaPony"
    },
    "track": []
},
"dateFirstCompromised": "2020-06-05T10:07:26+00:00",
"dateLastCompromised": "2020-06-05T10:07:26+00:00",
"dateFirstSeen": "2020-06-05T10:07:26+00:00",

```

```

    "dateLastSeen": "2020-06-05T10:07:26+00:00",
    "evaluation": {
      "admiraltyCode": "B3",
      "credibility": 50,
      "reliability": 80,
      "severity": "orange",
      "tlp": "red",
      "ttl": 90
    },
    "externalId": "",
    "id": "b3d87b6af5532ee8d41baac000bba2d1c46662c8",
    "displayOptions": {
      "favouriteForCompanies": [],
      "hideForCompanies": [],
      "isFavourite": false,
      "isHidden": false
    },
    "malware": [
      {
        "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f60",
        "name": "Phishing"
      }
    ],
    "oldId": "2308",
    "portalLink": "https://bt-demo.group-ib.com/cd/cards?searchValue=id:b3d87b6af5532ee8d41baac000bba2d1c46662c8",
    "seqUpdate": 1591351984817,
    "serviceCode": null,
    "sourceType": [
      "Phishing"
    ],
    "threatActor": [
      {
        "country": null,
        "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
        "isAPT": false,
        "name": "MegaPony"
      }
    ]
  }
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].events[].cardInfo.cvv	Card.Attribute	Card CVV	.items[].dateFirstSeen	966	N/A
.items[].cardInfo.issuer.countryCode	Card.Attribute	Card Issuer Country Code	.items[].dateFirstSeen	IN	N/A
.items[].cardInfo.issuer.countryName	Card.Attribute	Card Issuer Country	.items[].dateFirstSeen	INDIA	N/A
.items[].cardInfo.issuer.issuer	Card.Attribute	Card Issuer	.items[].dateFirstSeen	STATE BANK OF INDIA	N/A
.items[].cardInfo.number	Card.Value	Card Number	.items[].dateFirstSeen	4000174114732465	N/A
.items[].cardInfo.system	Card.Attribute	Card System	.items[].dateFirstSeen	VISA	N/A
.items[].cardInfo.type	Card.Attribute	Card Type	.items[].dateFirstSeen	CLASSIC	N/A
.items[].cardInfo.bin	Card.Attribute	Bank Identification Number	.items[].dateFirstSeen	601129	N/A
.items[].events[].cardInfo.validThru	Card.Attribute	Card Expiration	.items[].dateFirstSeen	8/2016	N/A
.items[].events[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	AS497 754th Electronic Systems Group	N/A
.items[].events[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	Raleigh	N/A
.items[].events[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	US	N/A
.items[].events[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	United States	N/A
.items[].events[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateFirstSeen	56.151.217.119	N/A
.items[].events[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	United States Postal Service	N/A
.items[].events[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	North Carolina	N/A
.items[].events[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateFirstSeen	http://246.119.220.81/	N/A
.items[].events[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateFirstSeen	246.119.220.81	N/A
.items[].events[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	AS497 754th Electronic Systems Group	N/A
.items[].events[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	Raleigh	N/A
.items[].events[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	US	N/A
.items[].events[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	United States	N/A
.items[].events[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateFirstSeen	246.119.220.81	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].events[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	United States Postal Service	N/A
.items[].events[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	North Carolina	N/A
.items[].events[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateFirstSeen	N/A	N/A
.items[].events[].cnc.url	Related Indicator.Value	URL	.items[].dateFirstSeen	http://246.119.220.81/	N/A
.items[].evaluation.admiraltyCode	Card.Attribute	Admiralty Code	.items[].dateFirstSeen	B3	If the attribute already exists, the value will be updated
.items[].evaluation.credibility	Card.Attribute	Credibility	.items[].dateFirstSeen	50	If the attribute already exists, the value will be updated
.items[].evaluation.reliability	Card.Attribute	Reliability	.items[].dateFirstSeen	80	If the attribute already exists, the value will be updated
.items[].evaluation.severity	Card.Attribute	Severity	.items[].dateFirstSeen	orange	If the attribute already exists, the value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					will be updated
.items[].evaluation.tlp	Card.TLP / Related Objects.TLP	N/A	.items[].dateFirstSeen	red	N/A
.items[].evaluation.ttl	Card.Attribute	Time to live (seconds)	.items[].dateFirstSeen	90	If the attribute already exists, the value will be updated
.items[].malware[].name	Related Malware.Value	N/A	.items[].dateFirstSeen	Trochilus	N/A
.items[].sourceType	Card.Attribute	Source Type	.items[].dateFirstSeen	Phishing	N/A
.items[].dateFirstCompromised	Card.Attribute	Compromised Date	.items[].dateFirstSeen	2020-05-19T12:39:15+00:00	N/A
.items[].threatActor[].name	Related Adversary.Name	N/A	.items[].dateFirstSeen	MegaPony	N/A

GroupIB Compromised Data Mules

The GroupIB Compromised Data Mules feed ingests compromised Money Mule objects and any related Indicators, Malware, Organizations, Identities, and Adversaries.

GET <https://tap.group-ib.com/api/v2/compromised/mule>

Sample Response:

```
{
  "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": "SABRRUMMH1"
  },
  "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": "999999999999",
    "zip": "80654"
  },
  "portalLink": "https://tap.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'	
.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://tap.group-ib.com/cd/mules?searchValue=id:44bd99f372e2f78ec12513afcb7ee006d86392a2'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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'	
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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	'BIK044525225/3010 1810400000000225'	
.items[].organization.swift	Related Organization.Attribute	SWIFT	.items[].dateAdd	'SABRRUMMVH1'	
.items[].person.taxNumber	Related Identity	N/A	.items[].dateAdd	'999999999999'	
.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'	

GroupIB Compromised Data Git Leaks

The GroupIB Compromised Data Git Leaks feed ingests Indicator objects and any related Identities.

GET https://tap.group-ib.com/api/v2/osi/git_repository

Sample Response:

```
{
  "resultId": "2ce743885dde121bb04986fef4bd56a82357afcd",
  "count": 1,
  "items": [
    {
      "contributors": [
        {
          "authorEmail": "yneth@gmail.ru",
          "authorName": "yneth"
        }
      ],
      "dataFound": {},
      "dateCreated": "2020-03-12T01:12:00+00:00",
      "dateDetected": "2020-03-12T01:12:00+00:00",
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 100,
        "reliability": 100,
        "severity": "red",
        "tlp": "red",
        "ttl": 0
      },
      "files": [
        {
          "dataFound": [
            "password"
          ],
          "dateCreated": "2020-03-12T01:12:00+00:00",
          "dateDetected": "2020-03-12T01:12:00+00:00",
          "evaluation": {
            "admiraltyCode": "A1",
            "credibility": 100,
            "reliability": 100,
            "severity": "red",
            "tlp": "red",
            "ttl": 0
          },
          "id":
"391db5d5f17ab6cbbbf7c35d1f4d076cb4c830f097b2a9eddd2df7b0650709a7",
          "matchesType": [
            "commonKeywords",
            "keyword"
          ]
        }
      ]
    }
  ]
}
```

```

    ],
    "matchesTypeCount": {
      "commonKeywords": 1,
      "domain": 0,
      "dsn": 0
    },
    "name": "distress_aarch64-apple-darwin",
    "revisions": [
      {
        "bind": [
          {
            "bindBy": "cert",
            "companyId": 2692,
            "data": "cert",
            "ruleId": 0,
            "type": "keyword"
          }
        ],
        "data": {
          "commonKeywords": {
            "password": [
              "password"
            ]
          }
        },
        "hash":
"391db5d5f17ab6cbbbf7c35d1f4d076cb4c830f097b2a9eddd2df7b0650709a7",
        "info": {
          "authorEmail": "yneth@gmail.ru",
          "authorName": "yneth",
          "timestamp": 1617794272
        }
      }
    ],
    "rules": {},
    "url": "https://github.com/Yneth/distress-releases/releases/download/
0.7.1/distress_aarch64-apple-darwin"
  }
],
  "id": "ead0d8ae9f2347789941ebacde88ad2e3b1ef691",
  "matchesTypes": [
    "commonKeywords",
    "keyword"
  ],
  "name": "vtddl",
  "numberOf": {
    "contributors": 1,
    "files": 1
  },
  "relations": {},

```

```

    "seqUpdate": 1591351984817,
    "source": "github"
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].files[].name	Indicator.Value	Filename	.items[].files[].dateDetected	distress_aarch64-apple-darwin	N/A
.items[].files[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].files[].dateDetected	A1	If the attribute already exists, the value will be updated
.items[].files[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].files[].dateDetected	100	If the attribute already exists, the value will be updated
.items[].files[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].files[].dateDetected	100	If the attribute already exists, the value will be updated
.items[].files[].evaluation.severity	Indicator.Attribute	Severity	.items[].files[].dateDetected	red	If the attribute already exists, the value will be updated
.items[].files[].evaluation.tlp	Indicator.tlp / Related Objects.tlp	N/A	.items[].files[].dateDetected	red	N/A
.items[].files[].evaluation.ttl	Indicator.Attribute	Time to live (days)	.items[].files[].dateDetected	0	If the attribute already exists, the value will be updated
.items[].files[].matchesTypeCount	Indicator.Attribute	{Type} match count	.items[].files[].dateDetected	1	{Type} is replaced with all the keys
.items[].files[].dataFound	Indicator.Attribute	Data Found	.items[].files[].dateDetected	password	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].files[].url	Related Indicator.Value	URL	.items[].files[].dateDetected	https://github.com/Yneth/distress-releases/releases/download/0.7.1/distress_aarch64-apple-darwin	N/A
.items[].files[].revisions[].info.authorName	Related Identity.Value	N/A	.items[].files[].dateDetected	yneth	N/A
.items[].files[].revisions[].info.authorEmail	Related Identity.Attribute	Email Address	.items[].files[].dateDetected	yneth@gmail.ru	N/A

GroupIB Compromised Data IMEI

The GroupIB Compromised Data IMEI feed ingests IMEI objects and any related Indicators, Malware, and Adversaries.

GET <https://tap.group-ib.com/api/v2/compromised/imei>

Sample Response:

```
{
  "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://tap.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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'	
.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	'+358407192130'	
.items[].portalLink	IMEI.Attribute	Source Link	.items[].dateDetected	'https://tap.group-ib.com/cd/imei?searchValue=id:9bc865c330efb652cf876ae73e8b6ba7b047acf4'	
.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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'	
.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'	

GroupIB Compromised Data Shops

The GroupIB Compromised Data Shops feed ingests Indicators and related Malware.

GET <https://tap.group-ib.com/api/v2/compromised/access>

Truncated Sample Response:

```
{
  "resultId": "3aaee8a0e03f82ae38bfc96719b56d5ba95475d1",
  "count": 1,
  "items": [
    {
      "accessType": null,
      "cnc": {
        "cnc": "https://russianmarket.to/",
        "domain": "russianmarket.to",
        "ipv4": {
          "asn": "AS13335",
          "city": null,
          "countryCode": "US",
          "countryName": null,
          "ip": "172.67.168.114",
          "provider": "CLOUDFLARENET",
          "region": "North America"
        },
        "ipv6": null,
        "url": "https://russianmarket.to:443"
      },
      "dateCompromised": "2023-04-30T04:50:47+00:00",
      "dateDetected": "2023-04-30T04:50:47+00:00",
      "description": null,
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 80,
        "reliability": 100,
        "severity": "red",
        "tlp": "red",
        "ttl": 30
      },
      "id": "2aa8ed4aeb201eb61a6462471e884adc07e3907a",
      "malware": {
        "category": [],
        "class": null,
        "id": "2086397a5d1d08446656429fec5906de3bc5ebc8",
        "name": "Raccoon",

```

```

        "platform": [],
        "threatLevel": null
    },
    "price": {
        "currency": "USD",
        "value": "10"
    },
    "rawData": "",
    "rawDataHighlighted": "",
    "seqUpdate": 1682964164818724749,
    "sourceInfo": {
        "externalId": "10604145(7)",
        "name": "russianmarket",
        "seller": "Mo####yf"
    },
    "target": {
        "device": {
            "os": "Windows 10 Pro"
        },
        "domain": "helpcenter.threatq.com",
        "geo": {
            "city": null,
            "country": "JO",
            "state": "Amman Governorate",
            "zip": null
        },
        "ipv4": null,
        "ipv6": null,
        "provider": "ZAIN",
        "url": null
    },
    "techSeqUpdate": null,
    "type": "Logs"
}
]
}

```

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[].target.domain	Indicator.Value	N/A	.items[].dateDetected	helpcenter.threatq.com'	N/A
.items[].target.device.os	Indicator.Attribute	Operating System	.items[].dateDetected	Windows 10 Pro	N/A
.items[].target.geo.city	Indicator.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].target.geo.country	Indicator.Attribute	Country	.items[].dateDetected	JO'	N/A
.items[].target.geo.state	Indicator.Attribute	State	.items[].dateDetected	Amman Governorate	N/A
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateDetected	https://russianmarket.to/	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	russianmarket.to	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	https://russianmarket.to:443	N/A
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	172.67.168.114	N/A
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS13335	N/A
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	US	N/A
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	CLOUDFLARENET	N/A
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	North America	N/A
.items[].cnc.ipv6.ip	Related Indicator.Value	IP Address	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateDetected	N/A	N/A
.items[].evaluation.tlp	Related Indicators.TLP	N/A	N/A	red	N/A
.items[].malware.name	Related Malware.Value	N/A	.items[].dateDetected	Racoon	N/A

GroupIB Compromised IM Discord

The GroupIB Compromised IM Discord feed ingests custom object Compromised Account and saves Discord channels as Assets.

GET <https://tap.group-ib.com/api/v2/compromised/discord>

Sample Response (truncated):

```
{
  "resultId": "2ce743885dde121bb04986fef4bd56a82357afcd",
  "count": 1,
  "items": [
    {
      "author": {
        "avatar": "string",
        "discriminator": "1234",
        "id": "string",
        "name": "user1234"
      },
      "channel": {
        "avatar": "string",
        "description": {},
        "id": "string",
        "name": "white_hackers",
        "parsedCounters": {
          "channels": 0,
          "domain": 0,
          "files": 0,
          "ip": 0,
          "links": 0,
          "media": 0
        },
        "server": "server",
        "serverId": "string",
        "stat": {
          "firstMessageDate": "2023-04-10T14:37:32+03:00",
          "id": "string",
          "lastMessageDate": "2023-04-10T14:37:32+03:00",
          "messageNum": 8,
          "name": "string",
          "userNum": 5
        }
      },
      "deleted": "string",
      "edits": {},
      "highlight": [
        "string"
      ],
      "id": "string",
```

```

    "media": {
      "name": "string",
      "size": 0,
      "type": "string"
    },
    "repliedMessage": {
      "author": {
        "avatar": "string",
        "discriminator": "string",
        "id": "string",
        "name": "string"
      },
      "id": "string",
      "text": "string",
      "translation": "string"
    },
    "rules": [
      183963
    ],
    "seqUpdate": 0,
    "text": "chanel text",
    "translation": "string",
    "ts": "2023-04-10T14:37:32+03:00"
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].author.name	Account.Value	N/A	.items[].ts	Account user1234	Prepended with Account
.items[].author.discriminator	Account.Attribute	Discriminator	.items[].ts	1234	N/A
.items[].rules	Account.Attribute	Rule	.items[].ts	183963	N/A
.items[].channel.name	Asset.Value	N/A	.items[].ts	Discord Channel white_hackers	Prepended with Discord Channel
.items[].channel.server	Asset.Attribute	Channel Server	.items[].ts	server	N/A
.items[].channel.stat.firstMessageTs	Asset.Attribute	First Message Date	.items[].ts	2023-04-10T14:37:32+03:00	If the attribute already exists, the value will be updated
.items[].channel.stat.lastMessageTs	Asset.Attribute	Last Message Date	.items[].ts	2023-04-10T14:37:32+03:00	If the attribute already exists, the value will be updated
.items[].channel.stat.messageNum	Asset.Attribute	Message Count	.items[].ts	10	If the attribute already exists, the value will be updated
.items[].channel.stat.userNum	Asset.Attribute	Users Count	.items[].ts	9	If the attribute already exists, the value will be updated

GroupIB Compromised IM Telegram

The GroupIB Compromised IM Telegram feed ingests custom object Compromised Account and saves Telegram channels/groups as Assets.

GET <https://tap.group-ib.com/api/v2/compromised/messenger>

Sample Response (truncated):

```
{
  "resultId": "2ce743885dde121bb04986fef4bd56a82357afcd",
  "count": 1,
  "items": [
    {
      "author": {
        "id": "string",
        "userName": "user1234",
        "firstName": "Denial",
        "lastName": "Service",
        "type": "user"
      },
      "chatStat": {
        "avatar": {
          "detected": "2023-04-10T14:37:32+03:00",
          "hash": "string",
          "id": "string"
        },
        "firstMessageDate": "2023-04-10T14:37:32+03:00",
        "id": 0,
        "lastMessageDate": "2023-04-10T14:37:32+03:00",
        "messageNum": 10,
        "name": "white_hackers",
        "title": "White Hackers",
        "type": "group",
        "userNum": 9
      },
      "edits": {},
      "highlight": [
        "string"
      ],
      "id": "string",
      "isReply": true,
      "message": "This message was compromised",
      "messageTs": "2023-04-10T14:37:32+03:00",
      "name": "white_hackers",
      "rules": [
        "183963"
      ],
      "seqUpdate": 0,
      "translatedMessage": "string"
    }
  ]
}
```

```
}  
  ]  
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].author.userName	Account.Value	N/A	.items[].messageTs	user1234	N/A
.items[].author.firstName	Account.Attribute	First Name	.items[].messageTs	Denial	N/A
.items[].author.lastName	Account.Attribute	Last Name	.items[].messageTs	Service	N/A
.items[].author.type	Account.Attribute	Type	.items[].messageTs	user	N/A
.items[].rules	Account.Attribute	Rule	.items[].messageTs	183963	N/A
.items[].chatStat.name	Asset.Value	N/A	.items[].messageTs	Telegram group white_hackers	Prepended with Telegram .it ems[] .chatSt at.type
.items[].chatStat.title	Asset.Attribute	Title	.items[].messageTs	White Hackers	N/A
.items[].chatStat.firstMessageDate	Asset.Attribute	First Message Date	.items[].messageTs	2023-04-10T14:37:32+03:00	If the attribute already exists, the value will be updated
.items[].chatStat.lastMessageDate	Asset.Attribute	Last Message Date	.items[].messageTs	2023-04-10T14:37:32+03:00	If the attribute already exists, the value will be updated
.items[].chatStat.messageNum	Asset.Attribute	Message Count	.items[].messageTs	10	If the attribute already exists, the value will be updated
.items[].chatStat.userNum	Asset.Attribute	Users Count	.items[].messageTs	9	If the attribute already exists, the value will be updated
.items[].chatStat.type	Asset.Attribute	Type	.items[].messageTs	commercial	N/A

GroupIB Compromised Masked Bank Card

The GroupIB Compromised Masked Bank Card feed ingests custom object Compromised Card and any related Indicators, Malware, Adversary and Identity.

GET https://tap.group-ib.com/api/v2/compromised/masked_card

Sample Response:

```
{
  "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": "https://breached.to/Thread-Selling-CLOUT-WITH-MORE-THAN-970-000-LOGS-JUNE-SEPT-2022",
  "sourceType": "Phishing",
  "threatActor": {
    "country": null,

```

```
    "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
    "isAPT": false,
    "name": "MegaPony"
  },
  "track": []
]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cardInfo.cvv	Card.Attribute	Card CVV	.items[].dateDetected	966	N/A
.items[].cardInfo.issuer.countryCode	Card.Attribute	Card Issuer Country Code	.items[].dateDetected	IN	N/A
.items[].cardInfo.issuer.countryName	Card.Attribute	Card Issuer Country	.items[].dateDetected	INDIA	N/A
.items[].cardInfo.issuer.issuer	Card.Attribute	Card Issuer	.items[].dateDetected	STATE BANK OF INDIA	N/A
.items[].cardInfo.number	Card.Value	Card Number	.items[].dateDetected	4000174114732465	N/A
.items[].cardInfo.system	Card.Attribute	Card System	.items[].dateDetected	VISA	N/A
.items[].cardInfo.type	Card.Attribute	Card Type	.items[].dateDetected	CLASSIC	N/A
.items[].cardInfo.validThru	Card.Attribute	Card Expiration	.items[].dateDetected	8/2016	N/A
.items[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS497 754th Electronic Systems Group	N/A
.items[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Raleigh	N/A
.items[].client.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	US	N/A
.items[].client.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	United States	N/A
.items[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	56.151.217.119	N/A
.items[].client.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	United States Postal Service	N/A
.items[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	North Carolina	N/A
.items[].cnc.cnc	Related Indicator.Value	FQDN	.items[].dateDetected	http://246.119.220.81/	N/A
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	246.119.220.81	N/A
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS497 754th Electronic Systems Group	N/A
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	Raleigh	N/A
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	US	N/A
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	United States	N/A
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	246.119.220.81	N/A
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	United States Postal Service	N/A
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	North Carolina	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A	N/A
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateDetected	N/A	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	http://246.119.220.81/	N/A
.items[].evaluation.admiraltyCode	Card.Attribute	Admiralty Code	.items[].dateDetected	B3	If the attribute already exists, the value will be updated
.items[].evaluation.credibility	Card.Attribute	Credibility	.items[].dateDetected	50	If the attribute already exists, the value will be updated
.items[].evaluation.reliability	Card.Attribute	Reliability	.items[].dateDetected	80	If the attribute already exists, the value will be updated
.items[].evaluation.severity	Card.Attribute	Severity	.items[].dateDetected	orange	If the attribute already exists, the value will be updated
.items[].evaluation.tlp	Card.TLP / Related Objects.TLP	N/A	.items[].dateDetected	red	N/A
.items[].evaluation.ttl	Card.Attribute	Time to live (days)	.items[].dateDetected	90	If the attribute already exists, the value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					will be updated
.items[].malware.name	Related Malware.Value	N/A	.items[].dateDetected	Trochilus	N/A
.items[].owner.address	Related Identity.Attribute	Address	.items[].dateDetected	N/A	N/A
.items[].owner.birthday	Related Identity.Attribute	Birthday	.items[].dateDetected	N/A	N/A
.items[].owner.city	Related Identity.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].owner.countryCode	Related Identity.Attribute	Country Code	.items[].dateDetected	N/A	N/A
.items[].owner.email	Related Identity.Attribute	Email	.items[].dateDetected	N/A	N/A
.items[].owner.name	Related Identity.Attribute	Name	.items[].dateDetected	N/A	N/A
.items[].owner.passport	Related Identity.Attribute	Passport data	.items[].dateDetected	N/A	N/A
.items[].owner.phone	Related Identity.Attribute	Phone Number	.items[].dateDetected	N/A	N/A
.items[].owner.state	Related Identity.Attribute	State	.items[].dateDetected	N/A	N/A
.items[].owner.taxNumber	Related Identity.Value	N/A	.items[].dateDetected	N/A	N/A
.items[].owner.zip	Related Identity.Attribute	ZIP Code	.items[].dateDetected	N/A	N/A
.items[].sourceType	Card.Attribute	Source Type	.items[].dateDetected	Phishing	N/A
.items[].dateCompromised	Card.Attribute	Compromised Date	.items[].dateDetected	2020-05-19T12:39:15+00:00	N/A
.items[].sourceLink	Card.Attribute	Source Link	.items[].dateDetected	https://breached.to/Thread-Selling	N/A
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	MegaPony	N/A

GroupIB Human Intelligence Threat and GroupIB APT Threat

These feeds ingests Intrusion objects and any related Indicators, Malware, Adversaries, Attack Patterns, Identities, and Tools.

GroupIB Human Intelligence Threat

GET <https://tap.group-ib.com/api/v2/hi/threat>

GroupIB APT Threat

GET <https://tap.group-ib.com/api/v2/apt/threat>

Sample Response:

```
{
  "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": "f1724b95fdac1541bb416bff08b209b8750e23928b58
68ec1ce34dad2a740dc0",
      "mime": "image/png",
      "name": "f1724b95fdac1541bb416bff08b209b8750e23928b58
68ec1ce34dad2a740dc0",
      "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": "2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522
a563582b",
        "sha256": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26
b3b663937af9ef40",
        "sha384": "fdbd8e75a67f29f701a4e040385e2e239863
03ea10239211af907fcbb83578b3e41
7cb71ce646efd0819dd8c088de1bd",
        "sha512": "2c74fd17edafd80e8447b0d46741ee243b7eb
74dd2149a0ab1b9246fb30382f27e853d858571
9e0e67cbda0daa8f51671064615d645ae27acb1
5bfb1447f459b",
        "whirlpool": ""
    },
    "name": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0f
f26b3b663937af9ef40",
    "size": null
},
"url": "http://strigigena.ru/cookie.php",
"seqUpdate": 16183252904267,
"techSeqUpdate": null,
"title": null,
"type": "file"
},
{
    "description": null,
    "id": "221f0e6b18af2cbf069131f2b7cf7e4552ae9d17",
    "langs": [
        "ru"
    ],
    "malwareList": [
        {
            "id": "132130dd0aa2f2ab8cb1e358974443276b28195d",
            "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":
"ca978112ca1bbdcfac231b39a23dc4da786eff8147c4e72b9807785afee48bb",
            "sha384": "fdbd8e75a67f29f701a4e040385e2e23986303ea1023
9211af907fcbb83578b3e417cb71ce646efd
0819dd8c088de1bd",
            "sha512": "2c74fd17edafd80e8447b0d46741ee243b7eb
74dd2149a0ab1b9246fb30382f27e8
53d8585719e0e67cbda0daa8f51671064615d64
5ae27acb15bfb1447f459b"
        }
    },
    "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'	
.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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	'f1724b95fdac1541bb416bffb08b209b8750e23928b5868ec1ce34dad2a740dc0'	
.items[].files[].mime	Related Indicator.Attribute	File Mime Type	.items[].createdAt	'image/png'	
.items[].files[].name	Related Indicator.Attribute	File Name	.items[].createdAt	'f1724b95fdac1541bb416bffb08b209b8750e23928b5868ec1ce34dad2a740dc0'	
.items[].files[].size	Related Indicator.Attribute	File Size	.items[].createdAt	'75438'	
.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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	'ca978112ca1bbdcafca231b39a23dc4da786eff8147c4e72b9807785afee48bb'	
.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	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbd a0daa8f51671064615d645ae27acb15bfb1447f459b'	
.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 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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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'	
.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'	

GroupIB Human Intelligence Threat Actor and GroupIB APT Threat Actor

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

GroupIB Human Intelligence Threat Actor

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

GroupIB APT Threat Actor

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

Sample Response:

```
{
  "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": "f1724b95fdac1541bb416bfff08b209b8750e23928b5868ec1ce34dad2a740dc0",

```

```

    "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": "3c157cefdae6a8403fbfe24790467215493b939",
    "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": "fdbd8e75a67f29f701a4e040385e2e23986303ea10239
          211af907fcbb83578b3e417cb71ce646ef0819dd
          8c088de1bd",
        "sha512": "2c74fd17edafd80e8447b0d46741ee243b7eb74dd214
          9a0ab1b9246fb30382f27e853d8585719e0e67
          cbda0daa8f51671064615d645ae27acb15bfb1447f459b",
        "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": "132130dd0aa2f2ab8cb1e358974443276b28195d",
    "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": "fdbd8e75a67f29f701a4e040385e2e23986303e
          a10239211af907fcbb83578b3e417cb71ce646efd081
          9dd8c088de1bd",
        "sha512": "2c74fd17edafd80e8447b0d46741ee243b7eb74dd
          2149a0ab1b9246fb30382f27e853d8585719e0e67cb
          da0daa8f51671064615d645ae27acb15bfb1447f459b"
      }
    }
  ],
  "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-efc62719818",
"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'	N/A
.items[].dateFirstSeen	Intrusion Set.Started_at	N/A	N/A	'2019-05-01'	N/A
.items[].dateLastSeen	Intrusion Set.Ended_at	N/A	N/A	'2021-04-09'	N/A
.items[].description	Intrusion Set.Description	N/A	N/A	'During the Operation'	N/A
.items[].countries[]	Intrusion Set.Attribute	Country	.items[].createdAt	'LB'	N/A
.items[].evaluation.admiraltyCode	Intrusion Set.Attribute	Admiralty Code	.items[].createdAt	'B2'	N/A
.items[].evaluation.credibility	Intrusion Set.Attribute	Credibility	.items[].createdAt	'80'	N/A
.items[].evaluation.reliability	Intrusion Set.Attribute	Reliability	.items[].createdAt	'80'	N/A
.items[].evaluation.severity	Intrusion Set.Attribute	Severity	.items[].createdAt	'red'	N/A
.items[].evaluation.tlp	Intrusion Set.TLP / Related Objects.TLP	N/A	N/A	'amber'	N/A
.items[].evaluation.ttl	Intrusion Set.Attribute	Time To Live (seconds)	.items[].createdAt	'30'	N/A
.items[].expertise[]	Intrusion Set.Attribute	Expertise	.items[].createdAt	'0day'	N/A
.items[].labels[]	Intrusion Set.Attribute	STIX labels	.items[].createdAt	'campaign'	N/A
.items[].langs[]	Intrusion Set.Attribute	Language	.items[].createdAt	'ru'	N/A
.items[].regions[]	Intrusion Set.Attribute	Regions	.items[].createdAt	'middle_east'	N/A
.items[].reportNumber	Intrusion Set.Attribute	Report Number	.items[].createdAt	'CP-2504-1649'	N/A
.items[].sectors[]	Intrusion Set.Attribute	Sector	.items[].createdAt	'gambling'	N/A
.items[].shortDescription	Intrusion Set.Attribute	Short Description	.items[].createdAt	'This is an attack'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].shortTitle	Intrusion Set.Attribute	Short Title	.items[].createdAt	'Attack'	N/A
.items[].sources[]	Intrusion Set.Attribute	Source	.items[].createdAt	'https://www.trendmicro.com/en_us/research/21/d/iron.html'	N/A
.items[].targetedCompany[]	Intrusion Set.Attribute	Target Company	.items[].createdAt	'TargetCompany'	N/A
.items[].targetedPartnersAndClients[]	Intrusion Set.Attribute	Target Partner and Client	.items[].createdAt	'TargetPandC'	N/A
.items[].type	Intrusion Set.Attribute	Type	.items[].createdAt	'threat'	N/A
.items[].cveList[].name	Related Indicator.Value and/or Related Vulnerability.Value	CVE	.items[].createdAt	'CVE-2021-27065'	N/A
.items[].contacts[].account	Related Identity.Value	N/A	.items[].createdAt	'alexjoe9983'	N/A
.items[].contacts[].flag	Related Identity.Attribute	Contact Flag	.items[].createdAt	'fake'	N/A
.items[].contacts[].service	Related Identity.Attribute	Contact Service	.items[].createdAt	'twitter'	N/A
.items[].contacts[].type	Related Identity.Attribute	Contact Type	.items[].createdAt	'social_network'	N/A
.items[].files[].hash	Related Indicator.Value	SHA-256	.items[].createdAt	'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0'	N/A
.items[].files[].mime	Related Indicator.Attribute	File Mime Type	.items[].createdAt	'image/png'	N/A
.items[].files[].name	Related Indicator.Attribute	File Name	.items[].createdAt	'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0'	N/A
.items[].files[].size	Related Indicator.Attribute	File Size	.items[].createdAt	'75438'	N/A
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].forumsAccounts[].nickname	Related Indicator.Attribute	Forum Account Nickname	.items[].createdAt	'nobody.gu3st'	N/A
.items[].indicators[].malwareList[].name	Related Malware.Value	N/A	.items[].createdAt	"SysUpdate"	N/A
.items[].indicators[].params.domain	Related Indicator.Value	FQDN	.items[].createdAt	'ns162.nsakadns.com'	N/A
.items[].indicators[].params.ipv4[]	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.143'	N/A
.items[].indicators[].params.ipv6[]	Related Indicator.Value	IPv6 Address	.items[].createdAt	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	N/A
.items[].indicators[].params.ssl[].hashes.md5	Related Indicator.Value	MD5	.items[].createdAt	'5765fafd258a5a1e87c0582a67862675'	N/A
.items[].indicators[].params.ssl[].hashes.sha1	Related Indicator.Value	SHA-1	.items[].createdAt	'AB0B22AB421C001462AF4A9F382DC9284747B43D'	N/A
.items[].indicators[].params.ssl[].hashes.sha256	Related Indicator.Value	SHA-256	.items[].createdAt	'ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb'	N/A
.items[].indicators[].params.ssl[].hashes.sha384	Related Indicator.Value	SHA-384	.items[].createdAt	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcb83578b3e417cb71ce646efd0819dd8c088de1bd'	N/A
.items[].indicators[].params.ssl[].hashes.sha512	Related Indicator.Value	SHA-512	.items[].createdAt	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	N/A
.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 normalize it to be an FQDN Indicator
.items[].indicators[].params.address	Related Indicator.Value	Email Address	.items[].createdAt	'this2test.com'	N/A
.items[].indicators[].params.message.body	Related Indicator.Attribute	Email Body	.items[].createdAt	'Body example'	N/A
.items[].indicators[].params.message.subject	Related Indicator.Attribute	Email Subject	.items[].createdAt	'Subject example'	N/A
.items[].indicators[].params.senderIp	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.144'	N/A
.items[].indicators[].params.serverIp	Related Indicator.Value	IP Address	.items[].createdAt	'85.204.74.145'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].indicators[].params.hashes.md5	Related Indicator.Value	MD5	.items[].createdAt	'113044788a356aab6c693a3e80189141'	N/A
.items[].indicators[].params.hashes.sha1	Related Indicator.Value	SHA-1	.items[].createdAt	'ba835af7b8aa51797f95223676640be9c81dad9f'	N/A
.items[].indicators[].params.hashes.sha256	Related Indicator.Value	SHA-256	.items[].createdAt	'0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40'	N/A
.items[].indicators[].params.hashes.sha384	Related Indicator.Value	SHA-384	.items[].createdAt	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcb83578b3e417cb71ce646efd0819dd8c088de1bd'	N/A
.items[].indicators[].params.hashes.sha512	Related Indicator.Value	SHA-512	.items[].createdAt	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	N/A
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].createdAt	'SysUpdate'	N/A
.items[].mitreMatrix[].id	Related Attack	Attack Pattern	.items[].createdAt	'attack-pattern--fddd81e9-dd3d-477e-9773-4fb8ae227234'	N/A
.items[].mitreMatrix[].attackTactic	Related Attack.Attribute	Attack Tactic	.items[].createdAt	'build-capabilities'	N/A
.items[].mitreMatrix[].attackType	Related Attack.Attribute	Attack Type	.items[].createdAt	'pre_attack_tactics'	N/A
.items[].mitreMatrix[].params.data	Related Attack.Attribute	Attack Data	.items[].createdAt	'Just a string'	N/A
.items[].relatedThreatActors[].name	Related Adversary.Name	N/A	.items[].createdAt	'actor'	N/A
.items[].relatedThreatActors[].type	Related Adversary.Attribute	Type	.items[].createdAt	'bad'	N/A
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].createdAt	'IronTiger'	N/A
.items[].threatActor.country	Related Adversary.Attribute	Country	.items[].createdAt	'CN'	N/A
.items[].toolList[].name	Related Tool	N/A	.items[].createdAt	'Tools'	N/A

GroupIB Malware C2

The GroupIB Malware C2 feed ingests Indicators, Malware, and Adversaries.

GET <https://tap.group-ib.com/api/v2/malware/cnc>

Sample Response:

```
{
  "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.0983212l.link",
      "file": [
        {
          "hashes": {
            "md4": "",
            "md5": "5765fafd258a5a1e87c0582a67862675",
            "md6": "",
            "ripemd160": "",
            "sha1": "ba835af7b8aa51797f95223676640be9c81dad9f",
            "sha224": "",
            "sha256": "0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
            "sha384": "fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd",
            "sha512": "2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b"
          },
          "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 these feeds:

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.09832121.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].file[].hashes.sha384	Related Indicator.Value	SHA-384	.items[].dateDetected	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcb83578b3e417cb71ce646efd0819dd8c088de1bd'	
.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'	
.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'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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

GroupIB Malware Configs

The GroupIB Malware Configs feed ingests Indicators and Malware.

GET <https://tap.group-ib.com/api/v2/malware/config>

Sample Response:

```
{
  "resultId": "a90504337510806e189d401bb0e3cf22f836d362",
  "count": 2000,
  "items": [
    {
      "configSummary": null,
      "content": "LockBit 2.0 Ransomware...",
      "contentLen": 512,
      "dateFirstSeen": "2023-04-27",
      "dateLastSeen": "2023-04-27",
      "domainList": [],
      "file": [
        {
          "md5": "9bfcf1adb9cbcefe33d6077f02fc4a91",
          "name": "vtdl_85dg97ui",
          "sha1": "0ddf7e2c44fc7b9df73b56c0c081e082d7249f33",
          "sha256": "5df9c5633ff349ce87964b23ca33cd7548e57adcdb585a4234dc789e658f9d2f",
          "timestamp": "2023-04-27T03:21:09+00:00"
        }
      ],
      "hash": "433d976b1a7fbd76193c583d150d75ed74dbe04c",
      "id": "433d976b1a7fbd76193c583d150d75ed74dbe04c",
      "ipList": [],
      "malware": {
        "id": "01b0e643235e668704b92833a23224e4c64434e4",
        "name": "Lockbit"
      },
      "malwareId": "01b0e643235e668704b92833a23224e4c64434e4",
      "seqUpdate": 16825684080671
    }
  ]
}
```

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[].malware.name	Malware.Value	N/A	.items[].dateFirstSeen	'Lockbit'	N/A
.items[].content	Malware.Description	N/A	.items[].dateFirstSeen	'LockBit 2.0 Ransomware...'	The content was truncated

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].hash	Related Indicator.Value	SHA-1	.items[].dateFirstSeen	'433d976b1a7fbd76193c583 d150d75ed74dbe04c'	N/A
.items[].file.md5	Related Indicator.Value	MD5	.items[].dateFirstSeen	'9bfcf1adb9cbcefe33d6077f0 2fc4a91'	N/A
.items[].file.sha1	Related Indicator.Value	SHA-1	.items[].dateFirstSeen	'0ddf7e2c44fc7b9df73b56c0c 081e082d7249f33'	N/A
.items[].file.sha256	Related Indicator.Value	SHA-256	.items[].dateFirstSeen	'5df9c5633ff349ce87964b23ca 33cd7548e57adcbd585a4234d c789e658f9d2f'	N/A
.items[].file.name	Related Indicator.Attribute	File name	.items[].dateFirstSeen	'vtdl_85dg97ui'	N/A

GroupIB Suspicious IP Tor Node, GroupIB Suspicious IP Open Proxy and GroupIB Suspicious IP Socks Proxy

These feeds ingests Indicators objects.

GroupIB Suspicious IP Tor Node

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

GroupIB Suspicious IP Open Proxy

GET https://tap.group-ib.com/api/v2/suspicious_ip/open_proxy

GroupIB Suspicious IP Socks Proxy

GET https://tap.group-ib.com/api/v2/suspicious_ip/socks_proxy

Sample Response:

```
{
  "resultId": "ce0d600cdfbcbf9671552e201a92e5e4df730a9",
  "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://tap.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	NOTES
.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://tap.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'	

GroupIB Suspicious IP Scanners

The GroupIB Suspicious IP Scanners feed ingests Indicators objects.

GET https://tap.group-ib.com/api/v2/suspicious_ip/scanner

Sample Response:

```
{
  "resultId": "ce0d600cdfbcbf9671552e201a92e5e4df730a9",
  "count": 132912,
  "items": [
    {
      "categories": [
        "Hacking",
        "FTP Brute-Force"
      ],
      "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": "134.209.127.189",
      "ipv4": {
        "asn": "AS16276 OVH SAS",
        "city": "Singapore",
        "countryCode": "SG",
        "countryName": "Singapore",
        "ip": "134.209.127.189",
        "provider": "DigitalOcean",
        "region": "Central"
      },
      "portalLink": null,
      "seqUpdate": 16182431110000,
      "sources": [
        "AbuseIPDB",
        "GIB-HoneyPot"
      ]
    }
  ]
}
```

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[].ipv4.ip	Indicator.Value	IP Address	.items[].dateFirstSeen	'134.209.127.189'	N/A
.items[].categories	Indicator.Tags	N/A	.items[].dateFirstSeen	'Hacking, FTP Brute-Force'	N/A
.items[].ipv4.asn	Indicator.Attribute	ASN	.items[].dateFirstSeen	'AS16276 OVH SAS'	N/A
.items[].ipv4.city	Indicator.Attribute	City	.items[].dateFirstSeen	'Singapore'	N/A
.items[].ipv4.countryCode	Indicator.Attribute	Country Code	.items[].dateFirstSeen	'SG'	N/A
.items[].ipv4.countryName	Indicator.Attribute	Country Name	.items[].dateFirstSeen	'Singapore'	N/A
.items[].ipv4.provider	Indicator.Attribute	Provider	.items[].dateFirstSeen	'DigitalOcean'	N/A
.items[].ipv4.region	Indicator.Attribute	Region	.items[].dateFirstSeen	'Central'	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].dateFirstSeen	'B2'	N/A
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'	N/A
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'	N/A
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'	N/A
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (seconds)	.items[].dateFirstSeen	'30'	N/A
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].dateFirstSeen	N/A	N/A
.items[].sources	Indicator.Attribute	Source	.items[].dateFirstSeen	'AbuseIPDB'	N/A

GroupIB Suspicious IP VPN

The GroupIB Suspicious IP VPN feed ingests Indicators objects.

GET https://tap.group-ib.com/api/v2/suspicious_ip/vpn

Sample Response:

```
{
  "resultId": "ce0d600cdfbcbf9671552e201a92e5e4df730a9",
  "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": "66.235.168.192",
      "ipv4": {
        "asn": "AS16276 OVH SAS",
        "city": "Singapore",
        "countryCode": "SG",
        "countryName": "Singapore",
        "ip": "66.235.168.192",
        "provider": "DigitalOcean",
        "region": "Central"
      },
      "names": [
        "Pulse Connect Secure"
      ],
      "portalLink": null,
      "rules": [
        "Pulse Connect Secure VPN"
      ],
      "seqUpdate": 16182431110000,
      "sources": [
        "playbook"
      ],
      "types": [
        "public"
      ]
    }
  ]
}
```

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[].ipv4.ip	Indicator.Value	IP Address	.items[].dateFirstSeen	'66.235.168.192'	N/A
.items[].types	Indicator.Tags	N/A	.items[].dateFirstSeen	'public'	N/A
.items[].ipv4.asn	Indicator.Attribute	ASN	.items[].dateFirstSeen	'AS16276 OVH SAS'	N/A
.items[].ipv4.city	Indicator.Attribute	City	.items[].dateFirstSeen	'Singapore'	N/A
.items[].ipv4.countryCode	Indicator.Attribute	Country Code	.items[].dateFirstSeen	'SG'	N/A
.items[].ipv4.countryName	Indicator.Attribute	Country Name	.items[].dateFirstSeen	'Singapore'	N/A
.items[].ipv4.provider	Indicator.Attribute	Provider	.items[].dateFirstSeen	'DigitalOcean'	N/A
.items[].ipv4.region	Indicator.Attribute	Region	.items[].dateFirstSeen	'Central'	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].dateFirstSeen	'B2'	N/A
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'	N/A
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'	N/A
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'	N/A
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (seconds)	.items[].dateFirstSeen	'30'	N/A
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].dateFirstSeen	N/A	N/A
.items[].sources	Indicator.Attribute	Source	.items[].dateFirstSeen	'AbuseIPDB'	N/A
.items[].names	Indicator.Attribute	Name	.items[].dateFirstSeen	'Pulse Connect Secure'	N/A
.items[].rules	Indicator.Attribute	Rule	.items[].dateFirstSeen	'Pulse Connect Secure VPN'	N/A

GroupIB Attacks DDoS

The GroupIB Attacks DDoS feed ingests Indicators objects.

GET <https://tap.group-ib.com/api/v2/attacks/ddos>

Sample Response:

```
{
  "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://tap-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 these feeds:

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].evaluation.admiraltyCode	Indicator/Malware/Adversary.Attribute	Admiralty Code	.items[].dateBegin	A2 N/A
.items[].evaluation.credibility	Indicator/Malware/Adversary.Attribute	Credibility	.items[].dateBegin	90 N/A
.items[].evaluation.reliability	Indicator/Malware/Adversary.Attribute	Reliability	.items[].dateBegin	90 N/A
.items[].evaluation.severity	Indicator/Malware/Adversary.Attribute	Severity	.items[].dateBegin	red N/A
.items[].evaluation.tlp	Indicator/Malware/Adversary.TLP	Traffic Light Protocol	.items[].dateBegin	green N/A
.items[].evaluation.ttl	Indicator/Malware/Adversary.Attribute	Time to live (seconds)	.items[].dateBegin	30 N/A
.items[].malware.name	Malware.Value	N/A	.items[].dateBegin	Botnet N/A
.items[].messageLink	Indicator/Malware/Adversary.Attribute	Message Link	.items[].dateBegin	N/A N/A
.items[].portalLink	Indicator/Malware/Adversary.Attribute	Source Link	.items[].dateBegin	https://tap.group-ib.com/attacks/ddos?searchValue=id:053e63f81d0e1ebef83b0d3a5cbfebb e1a2b28a7 N/A
.items[].protocol	Indicator/Malware/Adversary.Attribute	Protocol	.items[].dateBegin	udp N/A
.items[].target.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateBegin	AS3223 Voxility S.R.L. N/A
.items[].target.ipv4.city	Related Indicator.Attribute	City	.items[].dateBegin	London N/A
.items[].target.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateBegin	GB N/A
.items[].target.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateBegin	United Kingdom N/A
.items[].target.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateBegin	185.82.99.18 N/A
.items[].target.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateBegin	Net 360 S.a.r.l N/A
.items[].target.ipv4.region	Related Indicator.Attribute	Region	.items[].dateBegin	London, City of N/A
.items[].target.url	Indicator.Value	URL	.items[].dateBegin	brot.net N/A
.items[].target.category	Indicator/Malware/Adversary.Attribute	Category	.items[].dateBegin	N/A N/A
.items[].target.port	Indicator/Malware/Adversary.Attribute	Port	.items[].dateBegin	10913 N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.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

GroupIB Attacks Deface

The GroupIB Attacks Deface feed ingests Indicators objects and related Adversaries.

GET <https://tap.group-ib.com/api/v2/attacks/deface>

Sample Response:

```
{
  "resultId": "7545813d204a0ab3cb233da144bc06a4ef6223b6",
  "count": 100,
  "items": [
    {
      "contacts": [],
      "date": "2023-05-10T11:17:43+00:00",
      "evaluation": {
        "admiraltyCode": "B2",
        "credibility": 80,
        "reliability": 80,
        "severity": "orange",
        "tlp": "amber",
        "ttl": 30
      },
      "id": "645b7fe87400cb001883f9b2",
      "portalLink": "https://tap.group-ib.com/attacks/deface?searchValue=id:645b7fe87400cb001883f9b2",
      "seqUpdate": 1683718118053866,
      "source": "www.zone-h.org",
      "targetDomain": "mandrill.steelcoat.co.in",
      "targetDomainProvider": null,
      "targetIp": {
        "asn": null,
        "city": "Scottsdale",
        "countryCode": null,
        "countryName": "United States",
        "ip": "184.168.108.77",
        "provider": null,
        "region": null
      },
      "threatActor": {
        "country": null,
        "id": "be2da8bce084d842dedb59b2ecf079cbba091cdf",
        "isAPT": false,
        "name": "Mr.Pr4x0r"
      },
      "url": "http://mandrill.steelcoat.co.in/FCH.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[].url	Indicator.Value	URL	.items[].date	http://httpswwwwalibaba.com-spma2700homeloginnngnsdc.steelcoat.co.in/FCH.php	N/A
.items[].evaluation.admiraltyCode	Indicator/Adversary.Attribute	Admiralty Code	.items[].date	B2	N/A
.items[].evaluation.credibility	Indicator/Adversary.Attribute	Credibility	.items[].date	80	N/A
.items[].evaluation.reliability	Indicator/Adversary.Attribute	Reliability	.items[].date	80	N/A
.items[].evaluation.severity	Indicator/Adversary.Attribute	Severity	.items[].date	orange	N/A
.items[].evaluation.tlp	Indicator/Adversary.TLP	Traffic Light Protocol	.items[].date	amber	N/A
.items[].evaluation.ttl	Indicator/Adversary.Attribute	Time to live (seconds)	.items[].date	30	N/A
.items[].portalLink	Indicator/Adversary.Attribute	Source Link	.items[].dateBegin	https://tap.group-ib.com/attacks/deface?searchValue=id:645b7ff97400cb001883f9bf	N/A
.items[].targetIp.ip	Related Indicator.Value	IP Address	.items[].date	184.168.108.77	N/A
.items[].targetIp.asn	Related Indicator.Attribute	ASN	.items[].date	N/A	N/A
.items[].targetIp.city	Related Indicator.Attribute	City	.items[].date	Scottsdale	N/A
.items[].targetIp.countryCode	Related Indicator.Attribute	Country Code	.items[].date	N/A	N/A
.items[].targetIp.countryName	Related Indicator.Attribute	Country Name	.items[].date	United States	N/A
.items[].targetIp.provider	Related Indicator.Attribute	Provider	.items[].date	N/A	N/A
.items[].targetIp.region	Related Indicator.Attribute	Region	.items[].date	N/A	N/A
.items[].targetDomain	Related Indicator.Value	FQDN	.items[].date	httpswwwwalibaba.com-spma2700homeloginnngnsdc.steelcoat.co.in	N/A
.items[].threatActor.name	Adversary.Value	N/A	.items[].date	Mr.Pr4x0r	N/A

GroupIB Malware Report

The GroupIB Malware Report feed ingests Malware objects and any related Indicators, and Adversary.

GET <https://tap.group-ib.com/api/v2/malware/malware>

Truncated Sample Response:

```
{
  "resultId": "6c78425a2879a39b4ef0d12b09a7e6ae53f0b0de",
  "count": 1,
  "items": [
    {
      "aliases": [
        "BRATARAT"
      ],
      "attachedFile": [
        {
          "hash":
"dd28c28bcbaafa605febcb2b3b9a8ccd23ebfedf126aa66a72e598d305bd55bdd4",
          "mime": "image/png",
          "name":
"dd28c28bcbaafa605febcb2b3b9a8ccd23ebfedf126aa66a72e598d305bd55bdd4",
          "size": 173847
        },
        {
          "hash":
"c116cc30b2bfff85a6f21bb8013b35eeef4c7e75851ba42c9405c4f44624b972e",
          "mime": "image/png",
          "name":
"c116cc30b2bfff85a6f21bb8013b35eeef4c7e75851ba42c9405c4f44624b972e",
          "size": 399114
        }
      ],
      "author": null,
      "category": [
        "Banking Trojan"
      ],
      "categoryOptions": [
        {
          "label": "banking trojan",
          "value": "banking trojan"
        }
      ],
      "class": null,
      "configCount": 0,
      "configList": [],
      "deleted": false,
      "dislikeCount": 0,
      "fileCount": 0,

```

```

"fileIocList": [],
"geoRegion": [
  "america:south_america",
  "europe:european_union",
  "europe"
],
"history": [
  {
    "date": "2023-04-23T20:04:17+03:00",
    "editor": {
      "id": "shirshova@group-ib.com"
    }
  }
],
"id": "a36a740ab0dc910eea2c3760ec93d3b44d9a9a27",
"isDisliked": false,
"isLiked": false,
"isSeen": false,
"langs": [
  "en"
],
"likeCount": 0,
"linkedMalware": [],
"malwareAliasList": [
  "BRATARAT"
],
"mitreCount": 0,
"name": "BRATA",
"networkCount": 0,
"networkIocList": [],
"partCount": 0,
"platform": [
  "Android"
],
"platformOptions": [
  {
    "label": "Android",
    "value": "android"
  }
],
"portalLink": null,
"reportRating": null,
"reportSeen": [
  "9498"
],
"seenCount": 1,
"seqUpdate": 16563360102488,
"shortDescription": "BRATA (Brazilian Android Rat) is an Android
Rat",
"signatureCount": 0,

```

```

    "signatureList": [],
    "sourceCountry": [
      "BR",
      "IT"
    ],
    "stixGuid": null,
    "threatActorList": [
      {
        "id": "19a0a76e206404e203b2e3f5cbebcd56d20ea473",
        "isApt": false,
        "name": "Donot Team",
        "url": ""
      }
    ],
    "threatLevel": "Medium",
    "threatLevelOptions": {
      "label": "Medium",
      "value": "Medium"
    },
    "updatedAt": "2023-04-23T20:04:17+03:00",
    "yaraCount": 0,
    "yaraRuleList": []
  }
]
}

```

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[].name	Malware.Value	N/A	.items[].history[0].date	BRATA	N/A
.items[].aliases	Malware.Tags	N/A	.items[].history[0].date	BRATARAT, Banking Trojan	Concatenated with .items[].category
.items[].category	Malware.Tags	N/A	.items[].history[0].date	BRATARAT, Banking Trojan	Concatenated with .items[].aliases
.items[].shortDescription	Malware.Description	N/A	.items[].history[0].date	BRATA (Brazilian Android Rat) is an Android Rat discovered in 2019.	N/A
.items[].geoRegion	Malware.Attribute	Region	.items[].history[0].date	america:south_america	N/A
.items[].langs	Malware.Attribute	Language	.items[].history[0].date	en	N/A
.items[].platform	Malware.Attribute	Operating System	.items[].history[0].date	Android	N/A
.items[].sourceCountry	Malware.Attribute	Source Country	.items[].history[0].date	BR	N/A
.items[].threatLevel	Malware.Attribute	Threat Level	.items[].history[0].date	Medium	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].attachedFile[].hash	Related Indicator.Value	SHA-256	.items[].history[0].date	dd28c28cbafa605febc2b3b9a8 ccd23ebfedf126aa66a72e598d3 05bd55bdd4	N/A
.items[].attachedFile[].size	Related Indicator.Attribute	File Size	.items[].history[0].date	173847	N/A
.items[].threatActorList[].name	Related Adversary.Value	N/A	.items[].history[0].date	Donot Team	N/A

GroupIB Malware Signature, GroupIB Malware YARA Rule

This feed ingests Events and any related Malware.

GroupIB Malware Signature - GET <https://tap.group-ib.com/api/v2/malware/signature>

GroupIB Malware Yara Rule - GET <https://tap.group-ib.com/api/v2/malware/yara>

(Truncated) Sample Response:

```
{
  "resultId": "6c78425a2879a39b4ef0d12b09a7e6ae53f0b0de",
  "count": 1,
  "items": [
    {
      "alertHistory": [],
      "alertNum": 0,
      "class": "backdoor",
      "content": "alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg: \"CURRENT_EVENTS Driveby bredolab hidden div served by nginx\");",
      "createdAt": "2015-12-03T14:53:26+03:00",
      "id": 107709,
      "malware": [
        {
          "id": "490fcdb4491edc1ef30687eb2700fbd65727aca3",
          "name": "Bredolab"
        }
      ],
      "name": "CURRENT_EVENTS Driveby bredolab hidden div served by
nginx",
      "seqUpdate": 16752632631373,
      "severity": 5,
      "sid": 2011355,
      "sourceName": null
    }
  ]
}
```

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	Event.Title	Incident	.items[].createdAt	CURRENT_EVENTS Driveby bredolab hidden div served by nginx	N/A
.items[].class	Event.Tags	N/A	.items[].createdAt	backdoor	N/A
.items[].content	Event.Description	N/A	.items[].createdAt	alert http \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg: "CURRENT_EVENTS Driveby bredolab hidden div served by nginx";	N/A
.items[].severity	Event.Attribute	Severity	.items[].createdAt	5	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].sourceName	Event.Attribute	Source	.items[].createdAt	N/A	N/A
.items[].malware[].name	Related Malware.Value	N/A	.items[].createdAt	Bredolab	N/A

GroupIB Malware Vulnerability

If the type of the ingested object is CVE then it may be ingested as an Indicator, a Vulnerability or both, depending on the user field `Save CVE Data` as. If the type is not CVE, then this feed ingests the objects as Vulnerabilities.

GET <https://tap.group-ib.com/api/v2/osi/vulnerability>

Sample Response:

```
{
  "resultId": "6c78425a2879a39b4ef0d12b09a7e6ae53f0b0de",
  "count": 1,
  "items": [
    {
      "bulletinFamily": "NVD",
      "cpeTable": [],
      "cveList": [],
      "cvss": {
        "score": 0.0,
        "vector": "NONE"
      },
      "darkweb": [],
      "dateLastSeen": "2023-05-03T22:11:28+03:00",
      "dateModified": "2023-05-03T20:15:00+03:00",
      "datePublished": "2023-05-03T20:15:00+03:00",
      "description": "In CyberArk Viewfinity 5.5.10.95 and 6.x before 6.1.1.220, a low privilege user can escalate to an administrative",
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 100,
        "reliability": 100,
        "severity": "red",
        "tlp": "green",
        "ttl": 30
      },
      "exploitCount": 1,
      "exploitList": [
        {
          "aix": null,
          "aixFileset": [],
          "appercut": null,
          "assessment": null,
          "bounty": null,
          "bountyState": null,
          "bulletinFamily": "exploit",

```

```

    "bulletinSequenceId": null,
    "cpe": [],
    "cpe23": [],
    "cvelist": [
        "CVE-2017-11197"
    ],
    "cvss": {
        "score": 3.2999999999999998,
        "vector": "II:P/RC:UR/AC:L/AU:M/AV:N/E:ND/CI:N/AI:N/RL:ND"
    },
    "cvss3": [],
    "description": "",
    "edition": null,
    "h1reporter": null,
    "h1team": null,
    "hackapp": null,
    "href": "https://www.exploit-db.com/exploits/42319",
    "id": "EDB-ID:42319",
    "ioc": null,
    "isBulletin": "",
    "lastseen": "2018-11-30T12:32:43+03:00",
    "metasploitHistory": null,
    "metasploitReliability": null,
    "modified": "2017-07-13T00:00:00+03:00",
    "naslFamily": null,
    "nmap": null,
    "objectType": null,
    "objectTypes": [],
    "openbugbounty": null,
    "osvdbidlist": null,
    "pluginID": null,
    "provider": "vulners.com",
    "ptsecurityAffected": [],
    "published": "2017-07-13T00:00:00+03:00",
    "references": [],
    "reporter": "Exploit-DB",
    "scanner": [],
    "sequenceId": 16124324829172,
    "sourceData": "# Exploit Title: Privilege Escalation via CyberArk
Viewfinity <= 5.5 (5.5.10.95)",
    "sourceHref": "https://www.exploit-db.com/download/42319",
    "status": null,
    "taskMd5": "d22f61c5eb10abc520aaa7b0de636dff",
    "threatPostCategory": null,
    "title": "CyberArk Viewfinity 5.5.10.95 - Local Privilege
Escalation",
    "type": "exploitdb",
    "vuldb": [],
    "vulnerabilityCvedetails": null,
    "w3af": null

```

```

    }
  ],
  "exploitation": [],
  "extCvss": {
    "base": 2.3999999999999999,
    "environmental": 0.0,
    "exploitability": 1.0,
    "impact": 1.5,
    "mImpact": 0.0,
    "overall": 2.3999999999999999,
    "temporal": 2.3999999999999999,
    "vector": "A:N/AC:L/PR:H/C:N/E:X/I:L/RC:R/S:U/UI:R/AV:N/RL:X"
  },
  "extDescription": "",
  "githubLinkList": [],
  "href": "https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2017-11197",
  "id": "CVE-2017-11197",
  "lastseen": "2023-05-03T22:11:28+03:00",
  "portalLink": "https://tap.group-ib.com/osi/vulnerabilities?
searchValue=id:CVE-2017-11197",
  "provider": "vulners.com",
  "references": [
    "https://www.exploit-db.com/exploits/42319",
    "http://lp.cyberark.com/rs/316-CZP-275/images/ds-Viewfinity-102315-
web.pdf",
    "https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11197"
  ],
  "reporter": "cve@mitre.org",
  "seqUpdate": 16831814361349,
  "softwareMixed": [
    {
      "arch": [],
      "hardware": "",
      "hardwareVendor": "",
      "hardwareVersion": "",
      "os": "",
      "osVendor": "",
      "osVersion": "",
      "rel": [],
      "softwareFileName": "",
      "softwareName": [
        "cisco small business ip phones"
      ],
      "softwareType": [
        "software"
      ],
      "softwareVersion": [
        "any"
      ]
    }
  ],

```

```

        "softwareVersionString": "",
        "vendor": "Cisco",
        "versionOperator": ""
    }
],
"threats": [],
"threatsList": [],
"timeLineData": [],
"title": "CVE-2017-11197",
"twitter": [],
"type": "cve"
}
]
}

```

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/ Vulnerability.Attribute	Admiralty Code	.items[].datePublished	A1	If the attribute already exists, the value will be updated
.items[].evaluation.credibility	Indicator/ Vulnerability.Attribute	Credibility	.items[].datePublished	100	If the attribute already exists, the value will be updated
.items[].evaluation.reliability	Indicator/ Vulnerability.Attribute	Reliability	.items[].datePublished	100	If the attribute already exists, the value will be updated
.items[].evaluation.severity	Indicator/ Vulnerability.Attribute	Severity	.items[].datePublished	red	If the attribute already exists, the value will be updated
.items[].evaluation.tlp	Indicator/ Vulnerability.TLP	N/A	.items[].datePublished	green	N/A
.items[].evaluation.ttl	Indicator/Vulnerability	Time to live (seconds)	.items[].datePublished	30	If the attribute already exists, the value will be updated
.items[].title	Indicator/ Vulnerability.Value	N/A	.items[].datePublished	CVE-2017-11197	N/A
.items[].description	Indicator/ Vulnerability.Description	N/A	.items[].datePublished	In CyberArk Viewfinity 5.5.10.95 and 6.x before 6.1.1.220, a low privilege user can escalate to an administrative	N/A
.items[].bulletinFamily	Indicator/ Vulnerability.Attribute	Bulletin Family	.items[].datePublished	NVD	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cvss.score	Indicator/ Vulnerability.Attribute	CVSS Score	.items[].datePublished	3.3	N/A
.items[].cvss.vector	Indicator/ Vulnerability.Attribute	CVSS Vector	.items[].datePublished	II:P/RC:UR/AC:L/AU:M/AV:N/E:ND/CI:N/AI:N/RL:ND	N/A
.items[].extCvss.base	Indicator/ Vulnerability.Attribute	CVSS Base Score	.items[].datePublished	2.4	N/A
.items[].extCvss.environmental	Indicator/ Vulnerability.Attribute	CVSS Environmental Score	.items[].datePublished	0	N/A
.items[].extCvss.exploitability	Indicator/ Vulnerability.Attribute	CVSS Exploitability Subscore	.items[].datePublished	1.0	N/A
.items[].extCvss.impact	Indicator/ Vulnerability.Attribute	CVSS Impact Subscore	.items[].datePublished	1.5	N/A
.items[].extCvss.mImpact	Indicator/ Vulnerability.Attribute	CVSS Modified Impact Subscore	.items[].datePublished	0.0	N/A
.items[].extCvss.overall	Indicator/ Vulnerability.Attribute	CVSS Overall Score	.items[].datePublished	2.4	N/A
.items[].extCvss.temporal	Indicator/ Vulnerability.Attribute	CVSS Temporal Score	.items[].datePublished	2.4	N/A
.items[].exploitCount	Indicator/ Vulnerability.Attribute	Exploit count	.items[].datePublished	1	N/A
.items[].exploitList[].href	Indicator/ Vulnerability.Attribute	Exploit URL	.items[].datePublished	https://www.exploit-db.com/exploits/42319	N/A
.items[].exploitList[].provider	Indicator/ Vulnerability.Attribute	Exploit Provider	.items[].datePublished	vulners.com	N/A
.items[].exploitList[].reporter	Indicator/ Vulnerability.Attribute	Exploit Reporter	.items[].datePublished	Exploit-DB	N/A
.items[].exploitList[].title	Indicator/ Vulnerability.Attribute	Exploit Title	.items[].datePublished	CyberArk Viewfinity 5.5.10.95 - Local Privilege Escalation	N/A
.items[].exploitList[].type	Indicator/ Vulnerability.Attribute	Exploit Type	.items[].datePublished	exploitdb	N/A
.items[].href	Indicator/ Vulnerability.Attribute	Vulnerability Details URL	.items[].datePublished	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11197	N/A
.items[].portalLink	Indicator/ Vulnerability.Attribute	Portal Link	.items[].datePublished	https://tap.group-ib.com/osi/vulnerabilities?searchValue=id:CVE-2017-11197	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].provider	Indicator/ Vulnerability.Attribute	Provider	.items[].datePublished	vulners.com	N/A
.items[].softwareMixed	Indicator/ Vulnerability.Attribute	Software	.items[].datePublished	software cisco small business ip phones version: any	Concatenate softwareType, softwareName and softwareVersion
.items[].reporter	Related Identity.Value	N/A	.items[].datePublished	cve@mitre.org	N/A

GroupIB Attacks Phishing

The GroupIB Attacks Phishing feed ingests Indicator objects.

GET <https://tap.group-ib.com/api/v2/attacks/phishing>

Sample Response:

```
{
  "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://tap-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 these feeds:

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	If the attribute already exists, the value will be updated
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateDetected	80	If the attribute already exists, the value will be updated
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateDetected	90	If the attribute already exists, the value will be updated
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateDetected	red	If the attribute already exists, the value will be updated
.items[].evaluation.tlp	Indicator.TLP / Related Object.TLP	Traffic Light Protocol	.items[].dateDetected	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (seconds)	.items[].dateDetected	30	If the attribute already exists, the value will be updated
.items[].ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	AS43260	N/A
.items[].ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	N/A	N/A
.items[].ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	CY	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	Cyprus	N/A
.items[].ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	185.71.216.171	N/A
.items[].ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	N/A	N/A
.items[].ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	AS	N/A
.items[].objective	Indicator.Attribute	Objective	.items[].dateDetected	Card harvest	N/A
.items[].phishingDomain.domain	Indicator.Value	FQDN	.items[].phishingDomain. dateRegistered	kdrbilisim.com	N/A
.items[].phishingDomain.local	Indicator.Attribute	Local	.items[].phishingDomain. dateRegistered	kdrbilisim.com	N/A
.items[].phishingDomain.title	Indicator.Attribute	Title	.items[].phishingDomain. dateRegistered	ANKARA BİLGİSAYAR TEKNİK SERVİS 0312 226 50 40 0312 226 50 40	N/A
.items[].phishingDomain.registrar	Indicator.Attribute	Registrar	.items[].phishingDomain. dateRegistered	PDR Ltd. d/b/a PublicDomainRegistry.com	N/A
.items[].status	Indicator.Attribute	Status	.items[].dateDetected	In response	N/A
.items[].targetBrand	Indicator.Attribute	Target Brand	.items[].dateDetected	Bank of America	N/A
.items[].targetCategory	Indicator.Attribute	Target Category	.items[].dateDetected	Finance & Investment	N/A
.items[].targetCountryName	Indicator.Attribute	Target Country	.items[].dateDetected	N/A	N/A
.items[].targetDomain	Indicator.Attribute	Target Domain	.items[].dateDetected	bankofamerica.com	N/A
.items[].type	Indicator.Attribute	Type	.items[].dateDetected	Phishing	N/A
.items[].url	Related Indicator.Value	URL	.items[].dateDetected	https:// www.kdrbilisim.com/Boa	N/A

GroupIB Attacks Phishing Group

The GroupIB Attacks Phishing Group feed ingests Indicator objects and related Adversary.

GET https://tap.group-ib.com/api/v2/attacks/phishing_group

Sample Response:

```
{
  "resultId": "73565d8649a6cd5e57555695347cc94075ada805",
  "count": 5,
  "items": [
    {
      "brand": "Meta",
      "countPhishing": 2,
      "date": {
        "added": "2023-03-28T00:02:32+04:00",
        "blocked": null,
        "detected": "2023-03-28T00:02:32+04:00",
        "updated": "2023-03-28T00:06:19+04:00"
      },
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "domain": "traderspirits.io",
      "domainInfo": {
        "domain": "traderspirits.io",
        "domainPuny": "traderspirits.io",
        "expirationDate": "2023-07-04T14:58:08+00:00",
        "registered": "2022-07-04T14:58:08+00:00",
        "registrar": "GoDaddy.com, LLC",
        "tld": "io"
      },
      "domainTitle": "Utility & Community based NFT collection. Buy & Sell on  
Eth Blockchain",
      "evaluation": {
        "admiraltyCode": "C3",
        "credibility": 50,
        "reliability": 50,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "falsePositive": false,
      "groupLifetime": 44204,
      "id": "a80456e50a43c17391cee4328da63908628ac6a7d82348717da379069f0d88c1",
      "ip": [
        {
          "asn": "AS43260",
```

```

        "city": "Miami",
        "countryCode": "US",
        "countryName": "United States",
        "ip": "74.208.34.89",
        "provider": "1&1 Internet AG",
        "region": null
    }
],
"objective": [
    "Login harvest"
],
"phishingKitArray": [],
"screenshot": {
    "pageHtml": {
        "fileHashMd5": "a28d22149f080eb037b2b3eb66631358",
        "filename": "phishing_screen/
c9975a1cd65becbfb3b10c9d05e39ee9970a32b13d8d88f72fed4b3122b82dfa",
        "filetype": "pageHtml",
        "hashSha256":
"c9975a1cd65becbfb3b10c9d05e39ee9970a32b13d8d88f72fed4b3122b82dfa",
        "mime": "text/html"
    },
    "pageScreen": {
        "fileHashMd5": "ce04341e8047b76f0479027a18d84891",
        "filename": "phishing_screen/
7e15cd3290770ad218b8256b5875f14563c48feee8ccd3c8dd6d3645831e3042",
        "filetype": "pageScreen",
        "hashSha256":
"7e15cd3290770ad218b8256b5875f14563c48feee8ccd3c8dd6d3645831e3042",
        "mime": "image/jpeg"
    }
},
"seqUpdate": 1679947579307293,
"signature": {
    "manual": [],
    "resource": [
        "b0cc6de8186b85f20db454ee0f01bf528009269c060d890857a5bd96c20af15d"
    ],
    "screen": []
},
"source": [
    "urlscan"
],
"status": 7,
"threatActor": {
    "country": null,
    "id": null,
    "isAPT": false,
    "name": ""
},
},

```

```

    "uniqueTitles": [
      {
        "faviconHashes": {
          "md5": null,
          "sha1": null,
          "sha256": null
        },
        "title": "Utility & Community based NFT collection."
      }
    ],
    "urlListLink": "https://tap.group-ib.com/api/v2/attacks/phishing_group/a80456e50a43c17391cee4328da63908628ac6a7d82348717da379069f0d88c1/action/url_list",
    "whitelist": false
  }
]
}

```

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[].date.detected	C3	N/A
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].date.detected	50	N/A
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].date.detected	50	N/A
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].date.detected	red	N/A
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	.items[].date.detected	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (seconds)	.items[].date.detected	30	N/A
.items[].ip.asn	Related Indicator.Attribute	ASN	.items[].date.detected	AS43260	N/A
.items[].ip.city	Related Indicator.Attribute	City	.items[].date.detected	Miami	N/A
.items[].ip.countryCode	Related Indicator.Attribute	Country Code	.items[].date.detected	US	N/A
.items[].ip.countryName	Related Indicator.Attribute	Country Name	.items[].date.detected	United States	N/A
.items[].ip.ip	Related Indicator.Value	IP Address	.items[].date.detected	74.208.34.89	N/A
.items[].ip.provider	Related Indicator.Attribute	Provider	.items[].date.detected	1&1 Internet AG	N/A
.items[].ip.region	Related Indicator.Attribute	Region	.items[].date.detected	N/A	N/A
.items[].objective	Indicator.Attribute	Objective	.items[].date.detected	Login harvest	N/A
.items[].domainTitle	Indicator.Attribute	Domain Title	.items[].date.detected	Utility & Community based NFT collection.	N/A
.items[].brand	Indicator.Attribute	Brand	.items[].date.detected	Meta	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].countPhishing	Indicator.Attribute	Count Phishing	.items[].date.detected	2	N/A
.items[].domainInfo.registered	Indicator.Attribute	Register Date	.items[].date.detected	2022-07-04 14:58:08+00:00	N/A
.items[].domainInfo.expirationDate	Indicator.Attribute	Expiration Date	.items[].date.detected	2023-07-04 14:58:08+00:00	N/A
.items[].domainInfo.registrar	Indicator.Attribute	Registrar	.items[].date.detected	GoDaddy.com, LLC	N/A
.items[].domainInfo.tld	Indicator.Attribute	Top-level domain	.items[].date.detected	io	N/A
.items[].source	Indicator.Attribute	Source	.items[].date.detected	urlscan	N/A
.items[].domain	Indicator.Value	FQDN	.items[].date.detected	traderspirits.io	N/A
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].date.detected	N/A	N/A
.items[].threatActor.country	Related Adversary.Attribute	Country	.items[].date.detected	N/A	N/A

GroupIB Attack Phishing Kit

The GroupIP Attack Phishing Phishing Kit feed ingests Indicator objects.

GET https://tap.group-ib.com/api/v2/attacks/phishing_kit

Sample Response:

```
{
  "resultId": "b9a3b9dcea35e844cf57dc1b2c0972ba888452eb",
  "count": 12,
  "items": [
    {
      "dateDetected": "2019-03-21T18:00:40+00:00",
      "dateFirstSeen": "2019-03-21T18:00:40+00:00",
      "dateLastSeen": "2019-03-21T18:02:53+00:00",
      "downloadedFrom": [],
      "emails": [
        "jimjag@gmail.com",
        "codeworxtech@users.source",
        "coolbru@users.source",
        "mail@info.com",
        "mr.nix008@gmail.com",
        "wezza.marley@gmail.com",
        "mr.nix008@yandex.com"
      ],
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 90,
        "reliability": 90,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "hash": "6b27ae3d9fee257551d4c480360fd762",
      "id": "4ce31920791df53309a168117825452bc58b9264",
      "isFavourite": false,
      "isHidden": false,
      "oldId": "1359",
      "path": "https://tap.group-ib.com/api/api/v2/web/attacks/phishing_kit/4ce31920791df53309a168117825452bc58b9264/file/331af2756ec4b1297aa14ff38bf40c7a18f4fcb8899b1804b4dee6bb8d1c91f2",
      "portalLink": "https://bt-demo.group-ib.com/brand/phishing_kit?searchValue=id:4ce31920791df53309a168117825452bc58b9264",
      "seqUpdate": 1553191374631,
      "targetBrand": [
        "Bank of America"
      ],
      "tsFirstSeen": null,
      "tsLastSeen": null,
    }
  ]
}
```

```

    "variables": 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[].emails[]	Related Indicator.Value	Email Address	items[].dateDetected	jimjag@gmail.com	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	items[].dateDetected	A1	N/A
.items[].evaluation.credibility	Indicator.Attribute	Credibility	items[].dateDetected	90	N/A
.items[].evaluation.reliability	Indicator.Attribute	Reliability	items[].dateDetected	90	N/A
.items[].evaluation.severity	Indicator.Attribute	Severity	items[].dateDetected	red	N/A
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	items[].dateDetected	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (seconds)	items[].dateDetected	30	N/A
.items[].hash	Indicator.Value	MD5	items[].dateDetected	6b27ae3d9fee257551d4c480360fd762	N/A
.items[].targetBrand[]	Indicator.Attribute	Target Brand	items[].dateDetected	Bank of America	N/A

GroupIB OSI PublicLeak

The GroupIB OSI PublicLeak feed ingests Indicator objects.

GET https://tap.group-ib.com/api/v2/osi/public_leak

Sample Response:

```
{
  "resultId": "f727facffbe82e3946384cbaf71332a092161a73",
  "count": 18138702,
  "items": [
    {
      "bind": [],
      "created": "2021-09-27T12:47:16+03:00",
      "data": "<!--/**\n * GeSHi (C) 2004 - 2007 Nigel McNie, 2007 - 2008 Benny
Baumann\n * (http://qbnz.com/highlighter/ and http://geshi.org/)\n */\n.java
{font-family:monospace;color: #000066;}\n.java a:link {color: #000060;}\n.java
a:hover {background-color: #f0f000;}\n.java .head {font-family: Verdana, Arial,
sans-serif; color: #808080; font-size: 70%; font-weight: bold; padding: 2px;}\n.java .imp {font-weight: bold; color: red;}\n.java .kw1 {color: #000000;
font-weight: bold;}\n.java .kw2 {color: #000066; font-weight: bold;}\n.java .kw3 {color: #003399;}\n.java .kw4 {color: #000066; font-weight: bold;}\n.java .co1 {color: #666666; font-style: italic;}\n.java .co2 {color:
#006699;}\n.java .co3 {color: #008000; font-style: italic; font-weight: bold;}\n.java .coMULTI {color: #666666; font-style: italic;}\n.java .es0 {color:
#000099; font-weight: bold;}\n.java .br0 {color: #009900;}\n.java .sy0 {color:
#339933;}\n.java .st0 {color: #0000ff;}\n.java .nu0 {color: #cc66cc;}\n.java .me1 {color: #006633;}\n.java .me2 {color: #006633;}\n.java span.xtra
{ display:block; }\n.ln, .ln{ vertical-align: top; }\n.coMULTI, .java
span{ line-height:13px !important;}\n-->/* package whatever; // don't place
package name! */\n\nimport java.util.*;\nimport java.lang.*;\nimport
java.io.*;\n\n/* Name of the class has to be \"Main\" only if the class is
public. */\n\nclass Ideone\n{\n\tpublic static void main (<a href=\"http://
www.google.com/search?
hl=en&q=allinurl%3Adocs.oracle.com+javase+docs+api+string\">String</a>[] args)
throws java.lang.<a href=\"http://www.google.com/search?
hl=en&q=allinurl%3Adocs.oracle.com+javase+docs+api+exception\">Exception</
a>\n\t{\n\t\t<a href=\"http://www.google.com/search?
hl=en&q=allinurl%3Adocs.oracle.com+javase+docs+api+system\">System</
a>.out.println(\"A13V1IB3VIYZZH\".length());\n\t}\n}\",
      "displayOptions": null,
      "evaluation": {
        "admiraltyCode": "C3",
        "credibility": 50,
        "reliability": 50,
        "severity": "green",
        "tlp": "amber",
        "ttl": 30
      },
    },
  ],
}
```

```

"hash": "db0cd0519335470b6ae614ccbe65ef358b93b349",
"id": "db0cd0519335470b6ae614ccbe65ef358b93b349",
"language": "",
"linkList": [
  {
    "author": "",
    "dateDetected": "2021-09-27T12:47:16+03:00",
    "datePublished": "2021-09-27T11:46:51+03:00",
    "hash": "60df36b3bf7abcb5e540e68fc3193cecb724814e",
    "itemSource": "link",
    "link": "http://ideone.com/4XU0fh",
    "sequenceUpdate": null,
    "size": 1767,
    "source": "ideone.com",
    "status": 1,
    "title": ""
  }
],
"matches": {
  "email": {
    "email": [
      "somesampleemail@mail.ru"
    ]
  }
},
"oldId": null,
"portalLink": "https://tap.group-ib.com/osi/public_leak?searchValue=id:db0cd0519335470b6ae614ccbe65ef358b93b349",
"seqUpdate": 1632736036790689,
"size": "1,73 KB",
"updated": "2021-09-27T12:47:16+03:00",
"useful": 1
}
]
}

```

ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].bind[].key	Related Indicator.Value	FQDN	.items[].created	mail.ru
.items[].bind[].ruleValue	Related Indicator.Value	FQDN	.items[].created	mail.ru
.items[].bind[].type	Related Indicator.Attribute	Type	.items[].created	domains
.items[].data	Indicator.Description	N/A	.items[].created	["VehicleUsagePeriods": [{"endDa
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].created	C3
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].created	50
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].created	50

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].created	orange
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	.items[].created	amber
.items[].evaluation.ttl	Indicator.Attribute	Time to live (seconds)	.items[].created	30
.items[].hash	Indicator.Value	SHA-1	.items[].created	9ea9e8f70f76b774ebbf a58869275a78d1031e4
.items[].language	Indicator.Attribute	Language	.items[].created	json
.items[].linkList[].hash	Related Indicator.Value	SHA-1	.items[].created	68664b9e631ff8d352476 45fad364775f0ce4073
.items[].linkList[].itemSource	Related Indicator.Attribute	Source	.items[].created	api
.items[].linkList[].link	Related Indicator.Value	URL	.items[].created	https://pastebin.com/ FCuAjGC5
.items[].linkList[].size	Related Indicator.Attribute	Size	.items[].created	1316
.items[].linkList[].source	Related Indicator.Value	FQDN	.items[].created	pastebin.com
.items[].matches.email.email[]	Related Indicator.Value	Email Address	.items[].created	somesampleemail@mail.ru
.items[].size	Indicator.Attribute	Size	.items[].created	1,29 KB

GroupIB IOC Common

The GroupIB IOC Common feed ingests Indicators and Malware.

GET <https://tap.group-ib.com/api/v2/ioc/common>

Sample Response:

```
{
  "resultId": "fcfc8d0768745fbadc5e51087f46e1cc36d504ff",
  "count": 46781,
  "items": [
    {
      "id": "9518c854e6c1f59fd12089cfe9ed078a22977dc0",
      "type": "file",
      "dateFirstSeen": "2023-04-02T00:00:00+03:00",
      "dateLastSeen": "2023-04-02T00:00:00+03:00",
      "seqUpdate": 16803953345526,
      "hash": [
        "4adf0249073c4e0d022823ee61ce002c",
        "1e37ae9a6d1ad9767b1510ceac2074764667d9bf",
        "cc6cefaacbdce7b595169106f2109afeabf6b24c732566352616202f2010d689"
      ],
      "malwareList": [
        {
          "name": "DCRat",
          "aliases": [
            "DarkCrystal"
          ]
        }
      ],
      "threatList": 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[].hash[]	Indicator.Value	MD5/ SHA-1/ SHA-256	.items[].dateFirstSeen	'4adf0249073c4e0d022823ee61ce002c'	The type of the indicator is determined by its length
.items[].type	Indicator.Attribute	Type	.items[].dateFirstSeen	'file'	N/A
.items[].dateFirstSeen	Indicator.Attribute	Date First Seen	.items[].dateFirstSeen	'2023-04-02 00:00:00+03:00'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].dateFirstSeen	'DCRat'	N/A
.items[].malwareList.aliases[]	Related Malware.Tags	N/A	.items[].dateFirstSeen	'DarkCrystal'	N/A

Average Feed Run



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

GroupIB Compromised Account

METRIC	RESULT
Run Time	1 minute
Accounts	73
Account Attributes	584
Adversaries	1
Indicators	60
Indicator Attributes	136
Malware	4

GroupIB Compromised Bank Card

METRIC	RESULT
Run Time	1 minute
Cards	100
Card Attributes	1,861
Indicators	71
Indicator Attributes	205
Malware	16
Adversaries	6

GroupIB Compromised Data Mules

METRIC	RESULT
Run Time	3 minutes
Adversaries	3
Adversary Attributes	3
Indicators	7
Indicator Attributes	12
Malware	2

METRIC	RESULT
Malware Attributes	2
Money Mule	500
Money Mule Attributes	5,504
Organization	9

GroupIB 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

GroupIB Compromised Data Shops

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	10
Malware	1

GroupIB Compromised IM Discord

METRIC	RESULT
Run Time	1 minute
Accounts	33
Account Attributes	33
Asset	15
Asset Attributes	85

GroupIB Compromised IM Telegram

METRIC	RESULT
Run Time	1 minute
Accounts	17
Account Attributes	34
Assets	55
Asset Attributes	342

GroupIB Compromised Masked Bank Card

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

GroupIB APT Threat Actors

METRIC	RESULT
Run Time	1 minute
Adversaries	52
Adversary Attributes	2,978
Indicators	86
Indicator Attributes	258
Intrusion Set	112

GroupIB Human Malware C2

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

GroupIB Human Intelligence Threat Actor

METRIC	RESULT
Run Time	1 minute
Adversaries	52
Adversary Attributes	2978
Indicators	86
Indicator Attributes	258
Intrusion Set	112

GroupIB Malware Configs

METRIC	RESULT
Run Time	1 minute
Indicators	860
Indicator Attributes	767
Malware	21

GroupIB Suspicious IP Tor Node

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

GroupIB Suspicious IP Scanners

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	1,092

GroupIB Suspicious IP VPN

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	700

GroupIB Attacks DDoS

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

GroupIB Attacks Deface

METRIC	RESULT
Run Time	1 minute
Indicators	232
Indicator Attributes	1075
Adversaries	11
Adversary Attributes	155

GroupIB Malware Report

METRIC	RESULT
Run Time	1 minute
Indicators	213
Indicator Attributes	213

METRIC	RESULT
Malware	38
Malware Attributes	309
Adversaries	16

GroupIB Malware Signature

METRIC	RESULT
Run Time	1 minute
Events	100
Event Attributes	100
Malware	2

GroupIB Malware Vulnerability

METRIC	RESULT
Run Time	2 minutes
Indicators	97
Indicator Attributes	1,264
Vulnerabilities	3
Vulnerability Attributes	31
Identities	13
Identity Attributes	7

GroupIB Attacks Phishing

METRIC	RESULT
Run Time	1 minute
Indicators	17
Indicator Attributes	87

GroupIB Attacks Phishing Group

METRIC	RESULT
Run Time	1 minute
Indicators	51
Indicator Attributes	72

GroupIB OSI PublicLeak

METRIC	RESULT
Run Time	1 minute
Indicators	285
Indicator Attributes	1,063

GroupIB IOC Common

METRIC	RESULT
Run Time	1 minute
Indicators	300
Indicator Attributes	600
Malware	10

Known Issues / Limitations

- The maximum allowable range is 30 consecutive days. If a larger date range is selected, the feed will change the end date to start date plus 30 days.
- There is a known issue with the GroupIB API that can cause a feed to ignore set date parameters. This can cause more data to be returned, resulting in longer run times.
- The GroupIB Compromised IM Discord and GroupIB Compromised IM Telegram feeds may ingest data that contains characters not supported by the database which results in the feed run finishing with a 500 Internal Error error message. To avoid this error, special characters have been removed. This issue will be addressed in a future ThreatQ platform release.

Change Log

- **Version 3.4.6**
 - Optimized the date format used by **GroupIB Compromised IM Telegram feed** to prevent `ServerDisconnected` errors.
- **Version 3.4.5**
 - Updated the **GroupIB Compromised Account** feed to reflect updates to the GroupIB API schema.
- **Version 3.4.4**
 - GroupIB Compromised Account feed - resolved a filter mapping issue when the ipv4 is not present in the API response.
- **Version 3.4.3**
 - Updated the authentication method from headers to basic authentication.
 - Unicode special characters not supported by the ThreatQ database engine are no longer ingested.
- **Version 3.4.2**
 - Resolved a Filter Mapping issue with the Group-IB Malware Vulnerability feed.
- **Version 3.4.1**
 - Existing attributes regarding data confidence levels will now be updated.
 - Resolved an issue regarding the measurement unit for the Time to Live attribute.
 - Re-enabled the GroupIB Compromised Account feed.
 - Added the following feeds:
 - GroupIB Compromised Bank Card
 - GroupIB Compromised IM Discord
 - GroupIB Compromised IM Telegram
 - GroupIB Compromised Masked Bank Card
 - Removed the GroupIB Malware Targeted Malware feed as it has been deprecated by the provider.
 - Updated the [Known Issues / Limitations](#) chapter regarding an issue with the Compromised IM Discord and Compromised IM Telegram feeds.
 - Updated minimum ThreatQ version to 5.20.0.
- **Version 3.4.0**
 - Added a delay for requests and extra retries (with delay) when encountering 429 errors.
 - Updated the minimum ThreatQ version to 5.19.0.
- **Version 3.3.0**
 - Added the following feeds:
 - GroupIB Compromised Data Shops
 - GroupIB Malware Configs
 - GroupIB Suspicious IP VPN
 - GroupIB Suspicious IP Scanners
 - GroupIB Attacks Deface
 - GroupIB Malware Report
 - GroupIB Malware Signature
 - GroupIB Malware YARA Rule

- GroupIB Vulnerability
 - GroupIB Attacks Phishing Group
 - GroupIB Attacks Abuse Phishing Kit
 - GroupIB IOC Common
- Removed the following feeds:
 - GroupIB Brand Abuse Phishing
 - GroupIB Brand Abuse Phishing Kit
 - GroupIB Compromised Data Darkweb
 - GroupIB Compromised Account
 - GroupIB Compromised Card
- Added pagination.
- Added support for Start and End date parameters. See the [Known Issues / Limitations](#) chapter for more details.
- **Version 3.2.0**
 - Updated the integration to use the new Group-IB endpoints, `tap.group.ib.com`. The previous endpoints, `bt.group-ib.com`, have been deprecated.
 - Removed deprecated endpoint: GroupIB Compromised Data Files.
- **Version 3.1.0**
 - GroupIB APT Threat Actor and Human Intelligence Threat Actors will now ingest data from the feed as Intrusion Sets opposed to Reports.
 - New attributes, Compromised Data and Source Link, have been added to the following feeds: GroupIBCompromised Account, Compromised Card, Compromised Data Files.
- **Version 3.0.0 rev-b**
 - Guide Update - Updated the custom object installation instructions in the [Prerequisites](#) chapter.
- **Version 3.0.0**
 - Added new endpoints to the CDF:
 - GroupIB Compromised Data Darkweb
 - GroupIB OSI PublicLeak
 - GroupIB Compromised Data Files
 - GroupIB Brand Abuse Phishing
 - GroupIB Brand Abuse Phishing Kit
- **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