ThreatQuotient

Group-IB Action

Version 1.0.0

November 18, 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

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.

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	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Group-IB action enriches ThreatQ indicators with information found in GroupIB Console. GroupIB is a provider of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection.

The integration provides the following action:

- **GroupIB Enrichment** - queries indicators contained in a threat-library against GroupIB collections and enriches them with the returned data.

The action is compatible with the following indicator object types:

- CVE
- Email Address
- File Path
- Filename
- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- Username

The action returns the following enriched system objects:

- Adversaries
- Asset
- Compromised Accounts
- Compromised Cards
- Identities
- IMEI
- Indicators
- Malware
- Money Mule
- Organizations
- Reports

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The following is required to install and use the integration:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A Group-IB username and API Key.
- The installation of the following custom objects:
  - Compromised Account
  - Compromised Card
  - IMEI
  - Money Mule
  - Organization
- A ThreatQ Data Collection containing at least one of the following indictor types:
  - CVE
  - Email Address
  - File Path
  - Filename
  - FQDN
  - IP Address
  - MD5
  - SHA-1
  - SHA-256
  - Username

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.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the following location:

```
cd /var/lib/threatq/misc/
```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
lib/threatq/misc/install.sh /var/lib/threatq/misc
```

   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.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

Use the following steps to install the custom objects in ThreatQ v5:

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
```

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

```
mkdir images
```

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

   The directory should resemble the following:

   - tmp
     - **groupib**
       - **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/imag
es/custom_objects/Account.svg'
'/tmp/group-ib/icons/CompromisedCard.svg' -> '/var/www/api/database/seeds/data/ic
ons/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/im]
ages/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
```

Installation

> The integration requires the installation of five custom objects before installing the actual action. 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 action gzip file.
3. Extract the files and install the required custom objects - see the Prerequisites chapter for more details.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

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

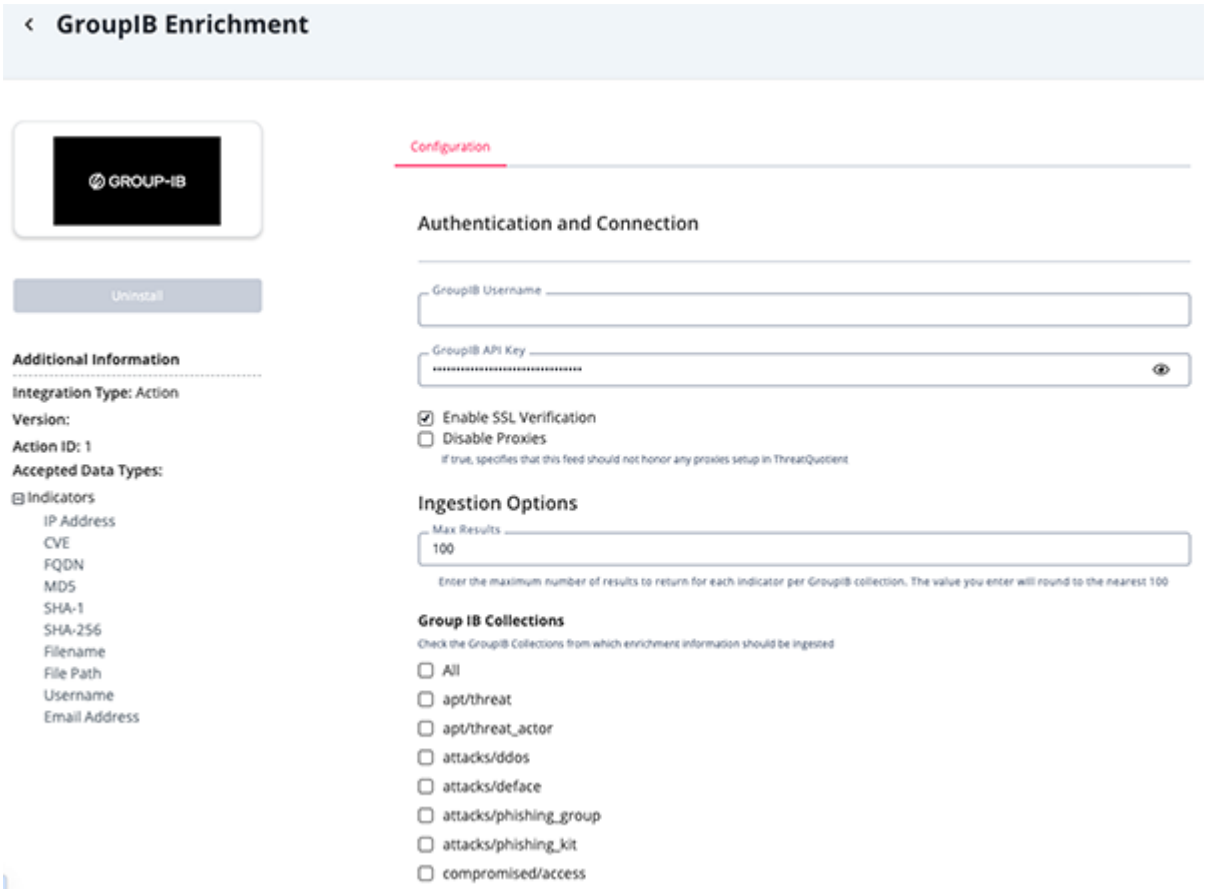
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
GroupIB Username	Enter the username used to connect to GroupIB Console.
GroupIB API Key	Enter the API Key to connect to GroupIB API.
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Max Results	Enter the maximum number of results to return for each indicator per GroupIB collection. The value you enter will round to the nearest 100.
Group IB Collections	Select the GroupIB Collections from which enrichment information should be ingested. Options include:

PARAMETER	DESCRIPTION
	◦ All ◦ apt/threat ◦ apt/threat_actor ◦ attacks/ddos ◦ attacks/deface ◦ attacks/phishing_group ◦ attacks/phishing_kit ◦ compromised/access ◦ compromised/account_group ◦ compromised/bank_card_group ◦ compromised/discord ◦ compromised/imei ◦ compromised/masked_card ◦ compromised/messenger ◦ compromised/mule ◦ hi/threat ◦ hi/threat_actor ◦ ioc/common ◦ malware/cnc ◦ malware/config ◦ malware/malware ◦ osi/public_leak ◦ osi/vulnerability ◦ suspicious_ip/open_proxy ◦ suspicious_ip/scanner ◦ suspicious_ip/socks_proxy ◦ suspicious_ip/tor_node ◦ suspicious_ip/vpn Selecting the **All** option may cause the GroupIB API to return a `500 Server Disconnected` error when running the action.
Save CVE Data as	Select the object type to ingest CVEs as into the ThreatQ platform. Options include **Indicators** and **Vulnerabilities**.
Objects Per Run	Enter the number of objects to process per run of the workflow.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
GroupIB Enrichment	Queries data regarding IoCs against GroupIB collections.	Indicator	IP Address, CVE, FQDN, MD5, SHA-1, SHA-256, Filename, File Path, Username, Email Address

GroupIB Enrichment

The GroupIB Enrichment action queries indicators against certain GroupIB collections and enriches them with the returned data. The GroupIB collections are selected using the user configuration `Group IB Collections`.

Some GroupIB collections might contain large number of results for one indicator. The maximum number of search results per GroupIB collection is controlled by the user configuration `Max Results`. If the value of `Max Results` is greater than 100, then the value is rounded to the nearest 100 (Example: if you enter 180, the integration will ingest 200).

ThreatQ Indicator Type to GroupIB Search Prefix Mapping

API Mapping is depends on the GroupIB collection that it is search. All the indicators from the input collection are related to the main objects returned by each mapping. Depending on the indicator type a prefix is added to the search query.

THREATQ INDICATOR TYPE	GROUPIB SEARCH PREFIX
IP Address	ip
FQDN	domain
CVE	N/A
MD5	hash
SHA-1	hash
SHA-256	hash
Filename	file
File Path	N/A
Username	username
Email Address	

GroupIB Collection attacks/phishing_group

`GET https://tap.group-ib.com/api/v2/attacks/phishing_group/updated?q=domain:traderspirits.io`

Sample Response:


```
{
  "count": 1,
  "items": [
    {
      "brand": "Meta",
      "countPhishing": 2,
      "date": {
        "added": "2024-09-01T00:02:32+04:00",
        "blocked": null,
        "detected": "2024-09-01T00:02:32+04:00",
        "updated": "2024-09-01T00:06:19+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": {},
      "seqUpdate": 1724632189898958,
      "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
    }
  ],
  "seqUpdate": 1724632189898958
}
```


ThreatQ provides the following default mapping for this GroupIB Collection:

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	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].date.detected	50	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].date.detected	50	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].date.detected	red	Updatable
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	.items[].date.detected	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (days)	.items[].date.detected	30	Updatable
.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
.items[].countPhishing	Indicator.Attribute	Count Phishing	.items[].date.detected	2	Updatable
.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 Collection attacks/ddos

`GET https://tap.group-ib.com/api/v2/attacks/ddos/updated?q=domain:peacecorps.gov`

Sample Response:


```
{
  "count": 1,
  "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": "https://peacecorps.gov"
      },
      "dateBegin": "2019-03-11T06:58:51+00:00",
      "dateEnd": "2019-03-11T06:58:51+00:00",
      "dateReg": "2019-03-11",
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 90,
        "reliability": 90,
        "severity": "red",
        "tlp": "green",
        "ttl": 30
      },
      "id": "3411bdc00c4f7ab43723f30205c31a20e183acf3",
      "isFavourite": false,
      "isHidden": false,
      "malware": {
        "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f69",
        "name": "Bootnet"
      },
      "messageLink": null,
      "oldId": "222",
      "portalLink": "https://bt-demo.group-ib.com/attacks/ddos?searchValue=id:3411bdc00c4f7ab43723f30205c31a20e183acf3",
      "protocol": "udp",
      "seqUpdate": 0,
```

```
      "target": {
        "ipv4": {
          "asn": "AS3223 Voxility S.R.L.",
          "city": "London",
          "countryCode": "GB",
          "countryName": "United Kingdom",
          "ip": "185.82.99.18",
          "provider": "Net 360 S.a.r.l",
          "region": "London, City of"
        },
        "url": "brot.net",
        "category": null,
        "domainsCount": 3,
        "port": 10913,
        "domain": null
      },
      "threatActor": null,
      "type": "DNS Reflection"
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cnc.url	Indicator.Value	URL	.items[].dateBegin	https://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.domain	Related Indicator.Value	FQDN	.items[].dateBegin	peacecorps.gov	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].dateBegin	A2	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateBegin	90	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateBegin	90	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateBegin	red	Updatable
.items[].evaluation.tlp	Indicator/Malware/ Adversary.TLP	Traffic Light Protocol	.items[].dateBegin	green	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (days)	.items[].dateBegin	30	Updatable
.items[].malware.name	Malware.Value	N/A	.items[].dateBegin	Bootnet	N/A
.items[].messageLink	Indicator.Attribute	Message Link	.items[].dateBegin	N/A	N/A
.items[].protocol	Indicator.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.Attribute	Category	.items[].dateBegin	N/A	N/A
.items[].target.port	Indicator.Attribute	Port	.items[].dateBegin	10913	N/A
.items[].target.domain	Indicator.Value	FQDN	.items[].dateBegin	N/A	N/A
.items[].threatActor.name	Adversary.Value	N/A	.items[].dateBegin	N/A	N/A
.items[].type	Indicator.Attribute	Type	.items[].dateBegin	DNS Reflection	N/A

GroupIB Collection attacks/deface

`GET https://tap.group-ib.com/api/v2/attacks/deface/updated?q=domain:med-supplies.de`

Sample Response:


```
{
  "count": 1,
  "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 GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].url	Indicator.Value	URL	.items[].date	http://httpswwwalibaba.com-spma2700homeloginngnsdc.steelcoat.co.in/FCH.php	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	.items[].date	B2	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].date	80	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].date	80	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].date	orange	Updatable
.items[].evaluation.tlp	Indicator/ Adversary.TLP	Traffic Light Protocol	.items[].date	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (days)	.items[].date	30	Updatable
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].date	https://tap.group-ib.com/attacks/deface\searchValue=id:645b7ff97400cb001883f9bf	N/A
.items[].source	Indicator.Attribute	Source	.items[].date	www.zone-h.org	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	httpswwwalibaba.com-spma2700homeloginngnsdc.steelcoat.co.in	N/A
.items[].threatActor.name	Adversary.Value	N/A	.items[].date	Mr.Pr4x0r	N/A

GroupIB Collection attacks/phishing_kit

`GET https://tap.group-ib.com/api/v2/attacks/phishing_kit/updated?q=email:jimjag@gmail.com`

Sample Response:


```
{
  "count": 1,
  "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": [
        {
          "date": "2018-02-17T20:55:08+03:00",
          "url": "hxxp://prvi8chemistrycal.com/scama-steam.zip",
          "phishingUrl": "hxxp://prvi8chemistrycal.com/scama-steam.zip",
          "domain": "prvi8chemistrycal.com",
          "fileName": ""
        }
      ],
      "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,
      "source": [
        "ci-PhishKit"
      ]
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

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[].downloadedFrom[].phishingUrl	Related Indicator.Value	URL	items[].dateDetected	hxxp://prvi8chemistrycal.com/scama-steam.zip	N/A
.items[].downloadedFrom[].domain	Related Indicator.Value	FQDN	items[].dateDetected	prvi8chemistrycal.com	N/A
.items[].evaluation.admiraltyCode	Indicator.Attribute	Admiralty Code	items[].dateDetected	A1	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	items[].dateDetected	90	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	items[].dateDetected	90	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	items[].dateDetected	red	Updatable
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	items[].dateDetected	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (days)	items[].dateDetected	30	Updatable
.items[].hash	Indicator.Value	MD5	items[].dateDetected	6b27ae3d9fee257551d4c480360fd762	N/A
.items[].targetBrand[]	Indicator.Attribute	Target Brand	items[].dateDetected	Bank of America	N/A
.items[].source	Indicator.Attribute	Source	items[].dateDetected	ci-PhishKit	N/A

GroupIB Collection apt/threat_actor, hi/threat_actor

`GET https://tap.group-ib.com/api/v2/apt/threat_actor/updated?q=hash:74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2`

Sample Response:


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

```
      "roles": [
        "agent"
      ],
      "seqUpdate": 16184067437615,
      "spokenOnLangs": [
        "en",
        "ru"
      ],
      "stat": {
        "countries": [
          "RU"
        ],
        "cve": [
          "CVE-2010-2883"
        ],
        "dateFirstSeen": "2021-10-24",
        "dateLastSeen": "2021-10-24",
        "malware": [
          "PhantomRAT"
        ],
        "regions": [
          "europe",
          "america:northern_america",
          "asia"
        ],
        "reports": [
          {
            "datePublished": "2021-01-05",
            "id": "9ffb44adf43abaaeea1f36c9d2a5adef38ba19e8",
            "name": {
              "en": "First mention on forums"
            }
          }
        ],
        "sectors": [
          "financial-services",
          "finance",
          "technology"
        ],
        "targetedCompany": [
          "Datagroup"
        ],
        "targetedPartnersAndClients": []
      },
      "techSeqUpdate": null,
      "updatedAt": "2021-04-14T16:25:43+03:00"
    }
  ]
}
```

ThreatQ provides the following default mapping for this GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].name	Adversary.Name	N/A	.items[].createdAt	'Amigos'	N/A
.items[].aliases[]	Adversary.Tag	N/A	.items[].createdAt	'a.m.i.g.o.s'	N/A
.items[].description	Adversary.Description	N/A	.items[].createdAt	'<figure class="image"> '	N/A
.items[].country	Adversary.Attribute	Country	.items[].createdAt	'RU'	N/A
.items[].goals[]	Adversary.Attribute	Goal	.items[].createdAt	'Goal'	N/A
.items[].labels[]	Adversary.Attribute	Label	.items[].createdAt	'hacker'	N/A
.items[].langs[]	Adversary.Attribute	Language	.items[].createdAt	'en'	N/A
.items[].roles[]	Adversary.Attribute	Role	.items[].createdAt	'agent'	N/A
.items[].spokenOnLangs[]	Adversary.Attribute	Language	.items[].createdAt	'ru'	N/A
.items[].stat.countries[]	Adversary.Attribute	Country	.items[].createdAt	'RU'	N/A
.items[].stat.dateFirstSeen	Adversary.Attribute	Date First Seen	.items[].createdAt	'2021-10-24'	N/A
.items[].stat.regions[]	Adversary.Attribute	Region	.items[].createdAt	'europe'	N/A
.items[].stat.sectors[]	Adversary.Attribute	Sector	.items[].createdAt	'financial-services'	N/A
.items[].stat.targetedCompany[]	Adversary.Attribute	Targeted Company	.items[].createdAt	'Datagroup'	N/A
.items[].files[].hash	Related Indicator.Value	SHA-256	.items[].createdAt	'74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2'	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	'74e83fabf0733838bc9398b793f5295057ccd75821b9f8be594f6851d1464dc2'	N/A
.items[].files[].size	Related Indicator.Attribute	File Size	.items[].createdAt	'216937'	N/A
.items[].stat.reports[].name.en	Related Intrusion Set	N/A	.items[].createdAt/ .items[].stat.reports[] .datePublished	'First mention on forums'	If `.items[].stat.reports[].datePublished` it's null we use the value of `.items[].createdAt`
.items[].stat.malware[]	Related Malware	N/A	.items[].createdAt	'PhantomRAT'	N/A
.items[].stat.cve[]	Related Vulnerability/ Indicator	N/A	.items[].createdAt	'CVE-2010-2883'	Ingested according to user configuration

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`Save CVE Data as`

GroupIB Collection apt/threat, hi/threat

`GET https://tap.group-ib.com/api/v2/apt/threat/updated?q=hash:ba835af7b8aa51797f95223676640be9c81dad9f`

Sample Response:


```
{
  "count": 1,
  "items": [
    {
      "contacts": [
        {
          "account": "alexjoe9983",
          "flag": "fake",
          "service": "twitter",
          "type": "social_network"
        }
      ],
      "countries": [
        "LB",
        "TR"
      ],
      "createdAt": "2021-04-13T16:49:27+03:00",
      "cveList": [
        {
          "name": "CVE-2021-27065"
        }
      ],
      "dateFirstSeen": "2019-05-01",
      "dateLastSeen": "2021-04-09",
      "datePublished": "2021-04-09",
      "description": "During the Operation",
      "displayOptions": {
        "isFavourite": false,
        "isHidden": false
      },
      "evaluation": {
        "admiraltyCode": "B2",
        "credibility": 80,
        "reliability": 80,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "expertise": [
        "0day",
        "CVE"
      ],
      "files": [
```

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

```
"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646e
fd0819dd8c088de1bd",
              "sha512":
"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e
0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b",
              "whirlpool": ""
            },
            "name":
"0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
            "size": null
          },
          "url": "http://strigigena.ru/cookie.php",
          "seqUpdate": 16183252904267,
          "techSeqUpdate": null,
          "title": null,
          "type": "file"
        }
      ],
      "indicatorsIds": [
        "3b67fc483bc2c22e0f21d68eabf6385f364a1eea"
      ],
      "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 this GroupIB collection:

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'	Updatable
.items[].evaluation.credibility	Intrusion Set.Attribute	Credibility	.items[].createdAt	'80'	Updatable
.items[].evaluation.reliability	Intrusion Set.Attribute	Reliability	.items[].createdAt	'80'	Updatable
.items[].evaluation.severity	Intrusion Set.Attribute	Severity	.items[].createdAt	'red'	Updatable
.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 (days)	.items[].createdAt	'30'	Updatable
.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
.items[].shortTitle	Intrusion Set.Attribute	Short Title	.items[].createdAt	'Attack'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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/Vulnerability.Value	CVE	.items[].createdAt	'CVE-2021-27065'	Depends on user configuration
.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'	N/A
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	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'	N/A
.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
.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	'0aef64991f9121a244c3f3bf75448bb8fb2c858bcf0ff26b3b663937af9ef40'	N/A
.items[].indicators[].params.hashes.sha384	Related Indicator.Value	SHA-384	.items[].createdAt	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	N/A
.items[].indicators[].params.hashes.sha512	Related Indicator.Value	SHA-512	.items[].createdAt	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f5167106461 5d645ae27acb15bfb1447f459b'	N/A
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].createdAt	'SysUpdate'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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 Collection compromised/access

`GET https://tap.group-ib.com/api/v2/compromised/access/updated?q=domain:russianmarket.to`

Sample Response:


```
{
  "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": "Racoon",
        "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 GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].target.domain	Indicator.Value	FQDN	.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[].target.provider	Indicator.Attribute	Provider	.items[].dateDetected	ZAIN	N/A
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	russianmarket.to	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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 Collection compromised/account_group

`GET https://tap.group-ib.com/api/v2/compromised/account_group/updated?q=ip:113.218.160.19`

Sample Response:


```
{
  "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": "4c48fd8197dba2eecc42d56bfbaba7483e497ea7",
  "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:4c48fd8197dba2eecc42d56bfbaba7483e497ea7",
      "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 this GroupIB collection:

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

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.credibility	Account.Attribute	Credibility	.items[].dateFirstSeen	50	Updatable
.items[].evaluation.reliability	Account.Attribute	Reliability	.items[].dateFirstSeen	80	Updatable
.items[].evaluation.severity	Account.Attribute	Severity	.items[].dateFirstSeen	orange	Updatable
.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	Updatable
.items[].malware[].name	Related Malware.Value	N/A	.items[].dateFirstSeen	QBot	N/A
.items[].login	Account.Value	N/A	.items[].dateFirstSeen	user511627	Prefended with 'Account '
.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
.items[].threatActor[].name	Related Adversary.Name	N/A	.items[].dateFirstSeen	Pontorez	N/A

GroupIB Collection compromised/bank_card_group

`GET https://tap.group-ib.com/api/v2/compromised/bank_card_group/updated?q=ip:56.151.217.119`

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"
        }
      ]
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

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

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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	Updatable
.items[].evaluation.credibility	Card.Attribute	Credibility	.items[].dateFirstSeen	50	Updatable
.items[].evaluation.reliability	Card.Attribute	Reliability	.items[].dateFirstSeen	80	Updatable
.items[].evaluation.severity	Card.Attribute	Severity	.items[].dateFirstSeen	orange	Updatable
.items[].evaluation.tlp	Card.TLP / Related Objects.TLP	N/A	.items[].dateFirstSeen	red	N/A
.items[].evaluation.ttl	Card.Attribute	Time to live (days)	.items[].dateFirstSeen	90	Updatable
.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 Collection compromised/discord

`GET https://tap.group-ib.com/api/v2/compromised/discord/updated?q=username:user1234`

Sample Response:


```
{
  "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"
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].author.name	Account.Value	N/A	.items[].ts	Discord Account user1234	Prepended with `Discord 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	Server	.items[].ts	server	N/A
.items[].channel.stat.firstMessageTs	Asset.Attribute	First Message Date	.items[].ts	2023-04-10T14:37:32+03:00	Updatable
.items[].channel.stat.lastMessageTs	Asset.Attribute	Last Message Date	.items[].ts	2023-04-10T14:37:32+03:00	Updatable
.items[].channel.stat.messageNum	Asset.Attribute	Message Count	.items[].ts	10	Updatable
.items[].channel.stat.userNum	Asset.Attribute	Users Count	.items[].ts	9	Updatable

GroupIB Collection compromised/imei

`GET https://tap.group-ib.com/api/v2/compromised/imei/updated?q=ip:66.102.6.171`

Sample Response:


```
{
  "count": 1,
  "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": "2021-04-10T01:37:36+00:00",
      "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 GroupIB collection:

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'	N/A
.items[].device.iccid	IMEI.Attribute	Device ICCID	.items[].dateDetected	'891004234814455936F'	N/A
.items[].device.imsi	IMEI.Attribute	Device IMSI	.items[].dateDetected	'313460000000001'	N/A
.items[].device.model	IMEI.Attribute	Device Model	.items[].dateDetected	'Nexus 5X/6.0.1 (Bot.v.5.0)'	N/A
.items[].device.os	IMEI.Attribute	Device OS	.items[].dateDetected	'Android 6.0.1'	N/A
.items[].evaluation.admiraltyCode	IMEI.Attribute	Admiralty Code	.items[].dateDetected	'A2'	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.credibility	IMEI.Attribute	Credibility	.items[].dateDetected	'80'	Updatable
.items[].evaluation.reliability	IMEI.Attribute	Reliability	.items[].dateDetected	'100'	Updatable
.items[].evaluation.severity	IMEI.Attribute	Severity	.items[].dateDetected	'red'	Updatable
.items[].evaluation.tlp	IMEI.TLP / Related Objects.TLP	N/A	N/A	'red'	N/A
.items[].evaluation.ttl	IMEI.Attribute	Time To Live (days)	.items[].dateDetected	'30'	Updatable
.items[].operator.countryCode	IMEI.Attribute	Operator Country Code	.items[].dateDetected	'RU'	N/A
.items[].operator.name	IMEI.Attribute	Operator Name	.items[].dateDetected	'MegaFon'	N/A
.items[].operator.number	IMEI.Attribute	Operator Phone Number	.items[].dateDetected	'+358407192130'	N/A
.items[].portalLink	IMEI.Attribute	Portal Link	.items[].dateDetected	'https://tap.group-ib.com/cd/imeisearchValue=id:9bc865c330efb652cf876ae73e8b6ba7b047acf4'	N/A
.items[].sourceType	IMEI.Attribute	Source Type	.items[].dateDetected	'Botnet'	N/A
.items[].dateCompromised	IMEI.Attribute	Compromised Date	.items[].dateDetected	'2020-05-19T12:39:15+00:00'	N/A
.items[].client.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	'66.102.6.171'	N/A
.items[].client.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	N/A
.items[].client.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	'Mountain View'	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.provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'Google Proxy'	N/A
.items[].client.ipv4.region	Related Indicator.Attribute	Region	.items[].dateDetected	'California'	N/A
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateDetected	's1.paradu.ru'	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateDetected	'http://s1.paradu.ru'	N/A
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateDetected	'31.148.99.117'	N/A
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS48666 MAROSNET Telecommunication Company LLC'	N/A
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateDetected	'Moscow'	N/A
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'RU'	N/A

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

GroupIB Collection compromised/masked_card

`GET https://tap.group-ib.com/api/v2/compromised/masked_card/updated?q=ip:56.151.217.119`

Sample Response:


```
{
  "count": 1,
  "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": []
    }
  ]
}
```

ThreatQ provides the following default mapping for this GroupIB collection:

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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
.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	Updatable
.items[].evaluation.credibility	Card.Attribute	Credibility	.items[].dateDetected	50	Updatable
.items[].evaluation.reliability	Card.Attribute	Reliability	.items[].dateDetected	80	Updatable
.items[].evaluation.severity	Card.Attribute	Severity	.items[].dateDetected	orange	Updatable
.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	Updatable
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].owner.email	Related Identity.Attribute	Email Address	.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 Collection compromised/messenger

`GET https://tap.group-ib.com/api/v2/compromised/messenger/updated?q=username:user1234`

Sample Response:


```
{
  "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"
    }
  ]
}
```

ThreatQ provides the following default mapping for this GroupIB collection:

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 .items[].chatStat.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	Updatable
.items[].chatStat.lastMessageDate	Asset.Attribute	Last Message Date	.items[].messageTs	2023-04-10T14:37:32+03:00	Updatable
.items[].chatStat.messageNum	Asset.Attribute	Message Count	.items[].messageTs	10	Updatable
.items[].chatStat.userNum	Asset.Attribute	Users Count	.items[].messageTs	9	Updatable
.items[].chatStat.type	Asset.Attribute	Type	.items[].messageTs	commercial	N/A

GroupIB Collection compromised/mule

`GET https://tap.group-ib.com/api/v2/compromised/mule/updated?q=ip:94.23.180.184`

Sample Response:


```
{
  "count": 33789,
  "items": [
    {
      "account": "9245316213",
      "cnc": {
        "cnc": "http://serv.sexura.ru",
        "domain": "serv.sexura.ru",
        "ipv4": {
          "asn": "AS16276 OVH SAS",
          "city": "Gravelines",
          "countryCode": "FR",
          "countryName": "France",
          "ip": "94.23.180.184",
          "provider": "OVH SAS",
          "region": "Hauts-de-France"
        },
        "ipv6": {
          "asn": "AS16276 OVH SAS",
          "city": "Gravelines",
          "countryCode": "FR",
          "countryName": "France",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "OVH SAS",
          "region": "Hauts-de-France"
        },
        "url": "http://serv.sexura.ru"
      },
      "dateAdd": "2020-10-16T01:06:09+00:00",
      "dateIncident": null,
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 80,
        "reliability": 100,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "id": "44bd99f372e2f78ec12513afcb7ee006d86392a2",
      "info": "Nothing",
      "isFavourite": false,
      "isHidden": false,
      "malware": {
        "id": "8790a290230b3b4c059c2516a6adace1eac16066",
```

```
        "name": "FlexNet"
      },
      "oldId": "352963098",
      "organization": {
        "bic": "SABRRUMMVH1",
        "bicRu": "SABRRUMMVH1",
        "bsb": "082489",
        "iban": "BIK044525225/30101810400000000225",
        "name": "SAVINGS BANK OF THE RUSSIAN FEDERATION (SBERBANK)",
        "swift": "SABRRUMMVH1"
      },
      "person": {
        "address": "224 Main St",
        "birthday": "01-01-1990",
        "city": "Wiggins",
        "countryCode": "US",
        "email": "jhon@fake.com",
        "name": "John",
        "passport": "123456789",
        "phone": "(555) 555-1234",
        "state": "Colorado",
        "taxNumber": "9999999999999",
        "zip": "80654"
      },
      "portalLink": "https://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 GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].account	Money Mule.Value	N/A	.items[].dateAdd	'Money Mule 9245316213'	Prepended with `Money Mule`
.items[].evaluation.admiraltyCode	Money Mule.Attribute	Admiralty Code	.items[].dateAdd	'A2'	Updatable
.items[].evaluation.credibility	Money Mule.Attribute	Credibility	.items[].dateAdd	'80'	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.reliability	Money Mule.Attribute	Reliability	.items[].dateAdd	'100'	Updatable
.items[].evaluation.severity	Money Mule.Attribute	Severity	.items[].dateAdd	'red'	Updatable
.items[].evaluation.tlp	Money Mule.TLP / Related Objects.TLP	N/A	N/A	'amber'	N/A
.items[].evaluation.ttl	Money Mule.Attribute	Time To Live (days)	.items[].dateAdd	'30'	Updatable
.items[].info	Money Mule.Attribute	Info	.items[].dateAdd	'Nothing'	N/A
.items[].portalLink	Money Mule.Attribute	Portal Link	.items[].dateAdd	'https://tap.group-ib.com/cd/mules?searchValue=id:44bd99f372e2f78ec12513afcb7ee006d86392a2'	N/A
.items[].sourceType	Money Mule.Attribute	Source Type	.items[].dateAdd	'Botnet'	N/A
.items[].type	Money Mule.Attribute	Type	.items[].dateAdd	'Botnet'	N/A
.items[].cnc.domain	Related Indicator.Value	FQDN	.items[].dateAdd	'serv.sexura.ru'	N/A
.items[].cnc.url	Related Indicator.Value	URL	.items[].dateAdd	'http://serv.sexura.ru'	N/A
.items[].cnc.ipv4.ip	Related Indicator.Value	IP Address	.items[].dateAdd	'94.23.180.184'	N/A
.items[].cnc.ipv4.asn	Related Indicator.Attribute	ASN	.items[].dateAdd	'AS16276 OVH SAS'	N/A
.items[].cnc.ipv4.city	Related Indicator.Attribute	City	.items[].dateAdd	'Gravelines'	N/A
.items[].cnc.ipv4.countryCode	Related Indicator.Attribute	Country Code	.items[].dateAdd	'FR'	N/A
.items[].cnc.ipv4.countryName	Related Indicator.Attribute	Country Name	.items[].dateAdd	'France'	N/A
.items[].cnc.ipv4.provider	Related Indicator.Attribute	Provider	.items[].dateAdd	'OVH SAS'	N/A
.items[].cnc.ipv4.region	Related Indicator.Attribute	Region	.items[].dateAdd	'Hauts-de-France'	N/A
.items[].cnc.ipv6.ip	Related Indicator.Value	IPv6 Address	.items[].dateAdd	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	N/A
.items[].cnc.ipv6.asn	Related Indicator.Attribute	ASN	.items[].dateAdd	'AS16276 OVH SAS'	N/A
.items[].cnc.ipv6.city	Related Indicator.Attribute	City	.items[].dateAdd	'Gravelines'	N/A
.items[].cnc.ipv6.countryCode	Related Indicator.Attribute	Country Code	.items[].dateAdd	'FR'	N/A
.items[].cnc.ipv6.countryName	Related Indicator.Attribute	Country Name	.items[].dateAdd	'France'	N/A
.items[].cnc.ipv6.provider	Related Indicator.Attribute	Provider	.items[].dateAdd	'OVH SAS'	N/A
.items[].cnc.ipv6.region	Related Indicator.Attribute	Region	.items[].dateAdd	'Hauts-de-France'	N/A

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

GroupIB Collection ioc/common

```
GET https://tap.group-ib.com/api/v2/ioc/common/updated?
q=hash:1e37ae9a6d1ad9767b1510ceac2074764667d9bf
```

Sample Response:


```
{
  "count": 1,
  "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": [
        {
          "name": "Aggah",
          "title": "Aggah - New indicators have been found"
        }
      ]
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

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	'4adf0249073c4e0d 022823ee61ce002c'	The type of the indicator is determined by its length
.items[].ip[]	Indicator.Value	IP Address	.items[].dateFirstSeen	N/A	N/A
.items[].domain	Indicator.Value	FQDN	.items[].dateFirstSeen	N/A	N/A
.items[].type	Indicator.Attribute	Type	.items[].dateFirstSeen	'file'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].threatList[].name	Indicator.Attribute	Threat List	.items[].dateFirstSeen	'Aggah'	N/A
.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

GroupIB Collection malware/cnc

`GET https://tap.group-ib.com/api/v2/malware/cnc/updated?q=hash:ba835af7b8aa51797f95223676640be9c81dad9f`

Sample Response:


```
{
  "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":
"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646e
fd0819dd8c088de1bd",
            "sha512":
"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e
0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b"
          }
        }
      ],
      "id": "4fb5bbcaa61e77d5024b0f02256d3b78339606ef",
      "ipv4": [
        {
          "asn": "AS16276 OVH SAS",
          "city": "Singapore",
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "128.199.23.9",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "ipv6": [
        {
          "asn": "AS16276 OVH SAS",
```

```
          "city": "Singapore",
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "isFavourite": false,
      "isHidden": false,
      "malwareList": [
        {
          "id": "f9983dbd202159e87ca7ab517d1ca4b08aed542a",
          "name": "U-Admin"
        }
      ],
      "oldId": "448197320",
      "platform": null,
      "seqUpdate": 1622322902077,
      "ssl": [],
      "threatActor": {
        "country": "CN",
        "id": "55011fb96789bcb43c8e19e4e886924f803b6d30",
        "isAPT": true,
        "name": "IronTiger"
      },
      "url": "http://128.199.23.9/uadmin/gate.php"
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

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'	N/A
.items[].domain	Related Indicator.Value	FQDN	.items[].dateDetected	'www.0983212l.link'	N/A
.items[].url	Indicator.Value	URL	.items[].dateDetected	'http://128.199.23.9/uadmin/gate.php'	N/A
.items[].file[].hashes.md5	Related Indicator.Value	MD5	.items[].dateDetected	'5765fafd258a5a1e87c0582a67862675'	N/A
.items[].file[].hashes.sha1	Related Indicator.Value	SHA-1	.items[].dateDetected	'ba835af7b8aa51797f95223676640be9c81dad9f'	N/A
.items[].file[].hashes.sha256	Related Indicator.Value	SHA-256	.items[].dateDetected	'0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40'	N/A

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	'fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e417cb71ce646efd0819dd8c088de1bd'	N/A
.items[].file[].hashes.sha512	Related Indicator.Value	SHA-512	.items[].dateDetected	'2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b'	N/A
.items[].ipv4[].ip	Related Indicator.Value	IP Address	.items[].dateDetected	'128.199.23.9'	N/A
.items[].ipv4[].asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	N/A
.items[].ipv4[].city	Related Indicator.Attribute	City	.items[].dateDetected	'Singapore'	N/A
.items[].ipv4[].countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'SG'	N/A
.items[].ipv4[].countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Singapore'	N/A
.items[].ipv4[].provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'DigitalOcean'	N/A
.items[].ipv4[].region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	N/A
.items[].ipv6[].ip	Related Indicator.Value	IPv6 Address	.items[].dateDetected	'2001:0db8:85a3:0000:0000:8a2e:0370:7334'	N/A
.items[].ipv6[].asn	Related Indicator.Attribute	ASN	.items[].dateDetected	'AS16276 OVH SAS'	N/A
.items[].ipv6[].city	Related Indicator.Attribute	City	.items[].dateDetected	'Singapore'	N/A
.items[].ipv6[].countryCode	Related Indicator.Attribute	Country Code	.items[].dateDetected	'SG'	N/A
.items[].ipv6[].countryName	Related Indicator.Attribute	Country Name	.items[].dateDetected	'Singapore'	N/A
.items[].ipv6[].provider	Related Indicator.Attribute	Provider	.items[].dateDetected	'DigitalOcean'	N/A
.items[].ipv6[].region	Related Indicator.Attribute	Region	.items[].dateDetected	'Central'	N/A
.items[].malwareList[].name	Related Malware.Value	N/A	.items[].dateDetected	'U-Admin'	N/A
.items[].threatActor.name	Related Adversary.Name	N/A	.items[].dateDetected	'IronTiger'	N/A
.items[].threatActor.country	Related Adversary.Attribute	Country	.items[].dateDetected	'CN'	N/A

GroupIB Collection malware/config

`GET https://tap.group-ib.com/api/v2/malware/config/updated?q=hash:0ddf7e2c44fc7b9df73b56c0c081e082d7249f33`

Sample Response:


```
{
  "count": 1,
  "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 GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].malware.name	Related Malware.Value	N/A	.items[].dateFirstSeen	'Lockbit'	N/A
.items[].content	Related Malware.Description	N/A	.items[].dateFirstSeen	'LockBit 2.0 Ransomware... '	The content

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					was truncated
.items[].hash	Indicator.Value	SHA-1	.items[].dateFirstSeen	'433d976b1a7fbd76193c583d150d75ed74dbe04c'	N/A
.items[].file.md5	Related Indicator.Value	MD5	.items[].dateFirstSeen	'9bfcf1adb9cbcefe33d6077f02fc4a91'	N/A
.items[].file.sha1	Related Indicator.Value	SHA-1	.items[].dateFirstSeen	'0ddf7e2c44fc7b9df73b56c0c081e082d7249f33'	N/A
.items[].file.sha256	Related Indicator.Value	SHA-256	.items[].dateFirstSeen	'5df9c5633ff349ce87964b23ca33cd7548e57adcdb585a4234dc789e658f9d2f'	N/A

GroupIB Collection malware/malware

`GET https://tap.group-ib.com/api/v2/malware/malware/updated?q=hash:c116cc30b2bff85a6f21bb8013b35eeef4c7e75851ba42c9405c4f44624b972e`

Sample Response:


```
{
  "count": 1,
  "items": [
    {
      "aliases": [
        "BRATARAT"
      ],
      "attachedFile": [
        {
          "hash":
"dd28c28bcbafa605febc2b3b9a8ccd23ebfedf126aa66a72e598d305bd55bdd4",
          "mime": "image/png",
          "name":
"dd28c28bcbafa605febc2b3b9a8ccd23ebfedf126aa66a72e598d305bd55bdd4",
          "size": 173847
        },
        {
          "hash":
"c116cc30b2bff85a6f21bb8013b35eeef4c7e75851ba42c9405c4f44624b972e",
          "mime": "image/png",
          "name":
"c116cc30b2bff85a6f21bb8013b35eeef4c7e75851ba42c9405c4f44624b972e",
          "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": [
      {
        "id": "8f8b2e715cf5990f3e0eb5f6485c0d3fe67b2611",
        "name": "Jcookie"
      }
    ],
    "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 GroupIB collection:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].name	Malware.Value	N/A	N/A	BRATA	N/A
.items[].aliases	Malware.Tags	N/A	N/A	BRATARAT, Banking Trojan	N/A
.items[].category	Malware.Tags	N/A	N/A	BRATARAT, Banking Trojan	N/A
.items[].shortDescription	Malware.Description	N/A	N/A	BRATA (Brazilian Android Rat) is an Android Rat discovered in 2019.	N/A
.items[].geoRegion	Malware.Attribute	Region	N/A	america:south_america	N/A
.items[].langs	Malware.Attribute	Language	N/A	en	N/A
.items[].platform	Malware.Attribute	Operating System	N/A	Android	N/A
.items[].sourceCountry	Malware.Attribute	Source Country	N/A	BR	N/A
.items[].threatLevel	Malware.Attribute	Threat Level	N/A	Medium	Updatable
.items[].attachedFile[].hash	Related Indicator.Value	SHA-256	N/A	dd28c28bcbafa605febc2b3b9a8ccd23ebfedf126aa66a72e598d305bd55bdd4	N/A
.items[].attachedFile[].size	Related Indicator.Attribute	File Size	N/A	173847	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].threatActorList[].name	Related Adversary.Value	N/A	N/A	Donot Team	N/A
.items[].linkedMalware[].name	Related Malware.Value	N/A	N/A	Jcookie	N/A

GroupIB Collection osi/public_leak

`GET https://tap.group-ib.com/api/v2/osi/public_leak/updated?q=hash:60df36b3bf7abcb5e540e68fc3193cecb724814e`

Sample Response:


```
{
  "count": 1,
  "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! */\nÂ \nimport java.util.*;\nimport java.lang.*;\nimport
java.io.*;\nÂ \n/* Name of the class has to be \"Main\" only if the class is
public. */\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": "ideone",
          "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": "Highlights"
        }
      ],
      "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 this GroupIB collection:

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].created	orange	Updatable
.items[].evaluation.tlp	Indicator.TLP / Related Objects.TLP	N/A	.items[].created	amber	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time to live (days)	.items[].created	30	Updatable
.items[].hash	Indicator.Value	SHA-1	.items[].created	9ea9e8f70f76b774ebbffa58869275a78d1031e4	N/A
.items[].language	Indicator.Attribute	Language	.items[].created	json	N/A
.items[].linkList[].hash	Related Indicator.Value	SHA-1	.items[].created	68664b9e631ff8d35247645fad364775f0ce4073	N/A
.items[].linkList[].itemSource	Related Indicator.Attribute	Source	.items[].created	api	N/A
.items[].linkList[].link	Related Indicator.Value	URL	.items[].created	https://pastebin.com/FCuAjGC5	N/A
.items[].linkList[].size	Related Indicator.Attribute	Size	.items[].created	1316	N/A
.items[].linkList[].author	Related Indicator.Attribute	Author	.items[].created	ideone	N/A
.items[].linkList[].title	Related Indicator.Attribute	Title	.items[].created	Highlights	N/A
.items[].linkList[].source	Related Indicator.Value	FQDN	.items[].created	pastebin.com	N/A
.items[].matches.email.email[]	Related Indicator.Value	Email Address	.items[].created	somesampleemail@mail.ru	N/A

GroupIB Collection osi/vulnerability

`GET https://tap.group-ib.com/api/v2/osi/vulnerability/updated?q=CVE-2019-11068`

Sample Response:


```
{
  "count": 1,
  "items": [
    {
      "affectedSoftware": [
        {
          "name": "shrimptest",
          "operator": "lt",
          "version": "1.0b3"
        }
      ],
      "bulletinFamily": "NVD",
      "cpeTable": [],
      "cveList": [
        "CVE-2019-11068"
      ],
      "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 GroupIB collection:

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	Updatable
.items[].evaluation.credibility	Indicator/ Vulnerability.Attribute	Credibility	.items[].datePublished	100	Updatable
.items[].evaluation.reliability	Indicator/ Vulnerability.Attribute	Reliability	.items[].datePublished	100	Updatable
.items[].evaluation.severity	Indicator/ Vulnerability.Attribute	Severity	.items[].datePublished	red	Updatable
.items[].evaluation.tlp	Indicator/ Vulnerability.TLP	N/A	.items[].datePublished	green	N/A
.items[].evaluation.ttl	Indicator/Vulnerability	Time to live (days)	.items[].datePublished	30	Updatable
.items[].title	Indicator/ Vulnerability.Value	N/A	.items[].datePublished	CVE-2017-11197	Ingested according to user configuration
.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
.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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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
.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 `softwareName` and `softwareVersion`
.items[].affectedSoftware	Indicator/ Vulnerability.Attribute	Software	.items[].datePublished	shrimptest version: 1.0b3	Concatenate `name` and `version`
.items[].reporter	Related Identity.Value	N/A	.items[].datePublished	cve@mitre.org	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cveList	Related Indicator/ Vulnerability.Value	CVE	.items[].datePublished	CVE-2019-11068	Ingested according to user configuration

GroupIB Collection suspicious_ip/open_proxy, suspicious_ip/socks_proxy, suspicious_ip/tor_node

`GET https://tap.group-ib.com/api/v2/suspicious_ip/open_proxy/updated?q=ip:128.199.23.10`

Sample Response:


```
{
  "count": 1,
  "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",
      "sources": [
        "check.torproject.org"
      ],
      "port": "80",
      "type": "http"
    }
  ]
}
```


ThreatQ provides the following default mapping for this GroupIB collection:

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'	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'	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'	Updatable
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (days)	.items[].dateFirstSeen	'30'	Updatable
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].dateFirstSeen	'https://tap.group-ib.com/suspicious/tor?searchValue=id:199.249.230.184'	N/A
.items[].source	Indicator.Attribute	Source	.items[].dateFirstSeen	'check.torproject.org'	N/A
.items[].sources	Indicator.Attribute	Source	.items[].dateFirstSeen	'check.torproject.org'	N/A
.items[].type	Indicator.Attribute	Proxy Type	.items[].dateFirstSeen	'http'	N/A
.items[].port	Indicator.Attribute	Port	.items[].dateFirstSeen	'80'	N/A

GroupIB Collection suspicious_ip/scanner

`GET https://tap.group-ib.com/api/v2/suspicious_ip/scanner/updated?q=ip:134.209.127.189`

Sample Response:


```
{
  "count": 1,
  "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 GroupIB collection:

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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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'	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'	Updatable
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (days)	.items[].dateFirstSeen	'30'	Updatable
.items[].portalLink	Indicator.Attribute	Portal Link	.items[].dateFirstSeen	N/A	N/A
.items[].sources	Indicator.Attribute	Source	.items[].dateFirstSeen	'AbuseIPDB'	N/A

GroupIB Collection suspicious_ip/vpn

`GET https://tap.group-ib.com/api/v2/suspicious_ip/vpn/updated?q=ip:66.235.168.192`

Sample Response:


```
{
  "count": 1,
  "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 GroupIB collection:

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'	Updatable
.items[].evaluation.credibility	Indicator.Attribute	Credibility	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.reliability	Indicator.Attribute	Reliability	.items[].dateFirstSeen	'80'	Updatable
.items[].evaluation.severity	Indicator.Attribute	Severity	.items[].dateFirstSeen	'red'	Updatable
.items[].evaluation.tlp	Indicator.TLP	N/A	.items[].dateFirstSeen	'amber'	N/A
.items[].evaluation.ttl	Indicator.Attribute	Time To Live (days)	.items[].dateFirstSeen	'30'	Updatable
.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

Enriched Data

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

METRIC	RESULT
Run Time	5 minutes
Indicators	600
Indicator Attributes	4,800
Adversaries	20
Adversary Attributes	20
Malware	120
Malware Attributes	0

Use Case Example

1. A Threat Analyst identifies a collection of indicators they would like to enrich with GroupIB data.
2. The Threat Analyst adds the GroupIB Enrichment Action to a Workflow.
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
4. The Workflow executes all Actions in the graph, including GroupIB Enrichment.
5. The action ingests all the attributes and related objects found for the input values.

Known Issues / Limitations

- Selecting the `All` option for the **Group IB Collections** parameter may cause the GroupIB API to return a `500 Server Disconnected` error.
- GroupIB returns results matching exactly the input value for the following indicators types:
  - IP Address
  - CVE
  - FQDN
  - MD5
  - SHA-1
  - SHA-256
  - Username
  - Email Address
- For the following indicator types GroupIB might return unrelated results:
  - Filename
  - File Path

Change Log

- **Version 1.0.0**
  - Initial release