# ThreatQuotient

**A Securonix Company**



## Group-IB CDF

**Version 4.2.0**

October 26, 2026

**ThreatQuotient**
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

**ThreatQ Supported**

**Support**
Email: support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

# Contents

**Warning and Disclaimer** ..... **4**
**Support** ..... **5**
**Integration Details** ..... **6**
**Introduction** ..... **7**
**Prerequisites** ..... **9**
Custom Objects Installation ..... 9
ThreatQ V6 Steps ..... 9
ThreatQ v5 Steps ..... 10
**Installation** ..... **13**
**Configuration** ..... **14**
All Feeds ..... 14
Human Intelligence Threat, APT Threat, Malware Vulnerability - Additional Parameters ..... 14
Malware Signature and Malware Yara Rule - Additional Parameters ..... 15
OSI PublicLeak - Additional Parameters ..... 15
Compromised Account - Additional Parameters ..... 16
Suspicious Payment Details - Additional Parameters ..... 16
Open Threats - Additional Parameters ..... 17
**ThreatQ Mapping** ..... **18**
GroupIB Compromised Account ..... 18
GroupIB Compromised Bank Card ..... 25
GroupIB Compromised Data Mules ..... 32
GroupIB Compromised Data Git Leaks ..... 37
GroupIB Compromised Data IMEI ..... 41
GroupIB Compromised Data Shops ..... 46
GroupIB Compromised IM Discord ..... 50
GroupIB Compromised IM Telegram ..... 53
GroupIB Compromised Masked Bank Card ..... 56
GroupIB Human Intelligence Threat and GroupIB APT Threat ..... 62
GroupIB Human Intelligence Threat Actor and GroupIB APT Threat Actor ..... 74
GroupIB Malware C2 ..... 78
GroupIB Malware Configs ..... 82
GroupIB Suspicious IP Tor Node, GroupIB Suspicious IP Open Proxy and GroupIB Suspicious IP Socks Proxy ..... 84
GroupIB Suspicious IP Scanners ..... 86
GroupIB Suspicious IP VPN ..... 88
GroupIB Suspicious Payment Details ..... 90
GroupIB Attacks DDoS ..... 94
GroupIB Attacks Deface ..... 98
GroupIB Malware Report ..... 101
GroupIB Malware Signature, GroupIB Malware YARA Rule ..... 105
GroupIB Malware Vulnerability ..... 107
GroupIB Attacks Phishing ..... 114
GroupIB Attacks Phishing Group ..... 117
GroupIB Attack Phishing Kit ..... 122
GroupIB OSI PublicLeak ..... 124
GroupIB IOC Common ..... 128
GroupIB Open Threats ..... 130

**Average Feed Run** ..... **134**
GroupIB Compromised Account ..... 134
GroupIB Compromised Bank Card ..... 135
GroupIB Compromised Data Mules ..... 135
GroupIB Compromised Data GIT Leaks ..... 136
GroupIB Compromised Data IMEI ..... 136
GroupIB Compromised Data Shops ..... 137
GroupIB Compromised IM Discord ..... 137
GroupIB Compromised IM Telegram ..... 139
GroupIB Compromised Masked Bank Card ..... 139
GroupIB APT Threat ..... 140
GroupIB Human Malware C2 ..... 140
GroupIB Human Intelligence Threat Actor ..... 141
GroupIB Malware Configs ..... 141
GroupIB Suspicious IP Tor Node ..... 142
GroupIB Suspicious IP Scanners ..... 142
GroupIB Suspicious IP VPN ..... 143
GroupIB Suspicious Payment Details ..... 143
GroupIB Attacks DDoS ..... 143
GroupIB Attacks Deface ..... 144
GroupIB Malware Report ..... 144
GroupIB Malware Signature ..... 145
GroupIB Malware Yara Rule ..... 145
GroupIB Malware Vulnerability ..... 147
GroupIB Attacks Phishing ..... 147
GroupIB Attacks Phishing Group ..... 148
GroupIB Attacks Phishing Kit ..... 148
GroupIB OSI PublicLeak ..... 148
GroupIB IOC Common ..... 149
**Known Issues / Limitations** ..... **150**
**Change Log** ..... **151**

# Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email**: support@securonix.com
**Support Web**: https://ts.securonix.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** | 4.2.0 |
| **Compatible with ThreatQ Versions** | >= 5.20.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

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

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

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

Object types ingested from the feeds above include:

- Adversaries
- Asset
- Attack Patterns
- Malware
- Money Mule (custom object)
- Organizations (custom object)
- Reports

- Compromised Accounts (custom object)
- Compromised Cards (custom object)
- Discord Channel (custom object)
- Identities
- Indicators
- Intrusion Sets
- IMEIs (custom object)
- Signatures
- Telegram Channel (custom object)
- Tools
- Tags
- Vulnerabilities

# Prerequisites

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

- Compromised Account
- Compromised Card
- Discord Channel
- IMEI
- Money Mule
- Organization
- Telegram Channel

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

## Custom Objects Installation

Use the steps provided to install the custom objects.

⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

### 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. Set your install pathway environment variable. This command will retrieve the install pathway from your configuration file and set it as variable for use during this installation process.

```
INSTALL_CONF="/etc/threatq/platform/install.conf"

if [ -f "$INSTALL_CONF" ]; then source "$INSTALL_CONF"

fi

MISC_DIR="${INSTALL_BASE_PATH:-/var/lib/threatq}/misc"
```

5. Navigate to the tmp folder using the environment variable:

```
cd $MISC_DIR
```

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

   The directory structure should resemble the following:

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

7. 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.

8. Delete the install.sh, definition json file, and images directory from step 6 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_cdf
```

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

```
mkdir images
```

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

   The directory should resemble the following:

   - tmp
     - **groupib_cdf**
       - **groupib.json**
       - **install.sh**
       - **images**
         - **Account.svg**
         - **CompromisedCard.svg**
         - **IMEI.svg**
         - **MoneyMule.svg**
         - **Organization.svg**

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

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

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

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

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

Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)
[                                                                          ]
[Application is now in maintenance mode.                                   ]
Installing Custom Objects - Step 2 of 5 (Installing the GroupIB Custom Objects)

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

# Installation

The CDF requires the installation of five custom objects before installing the actual CDF. See the Prerequisites chapter for more details.

Perform the following steps to install the integration:

The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration zip file.
3. Extract the files and install the required custom objects.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine
7. Select the individual feeds to install, when prompted, and then click **Install**.

   ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
8. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

# Configuration

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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   If you are installing the integration for the first time, it will be located under the **Disabled** tab.
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

## All Feeds

The following parameters are included in all feeds provided by the integration.

| PARAMETER | DESCRIPTION |
|---|---|
| **Username** | Your Group-IB username. |
| **API Key** | Your Group-IB API Key. |
| **Enable SSL Certificate Verification** | Enable this parameter if the feed should validate the host-provided SSL certificate. |
| **Disable Proxies** | Enable this parameter if the feed should not honor proxies set in the ThreatQ UI. |

## Human Intelligence Threat, APT Threat, Malware Vulnerability - Additional Parameters

The following additional parameters are included for the Human Intelligence Threat, APT Threat, and Malware Vulnerability feeds.

| PARAMETER | DESCRIPTION |
|---|---|
| **Ingest Threat Feeds As** | Select whether to ingest the primary object as **Reports** *(default)* or **Intrusion Sets**. |
| **Save CVE Data as** | Select the object type you would like CVEs to be ingested as into the platform. |

## Malware Signature and Malware Yara Rule - Additional Parameters

The following additional parameters are included for the Malware Signatures and Malware Yara Rule feeds.

| PARAMETER | DESCRIPTION |
|---|---|
| **Parse Signatures for Context** | Enable this configuration parameter to parse ingested signatures for context. Metadata from YARA and Snort/ Suricata rules will be added as attribution, and hashes from the metadata and condition will be added as indicators. |
| **Default Signature Status** | Select the status to apply to all ingested signatures. Options include:<br>◦ Active (default)<br>◦ Review<br>◦ Inactive |

## OSI PublicLeak - Additional Parameters

The following additional parameter is included with the OSI PublicLeak feed.

| PARAMETER | DESCRIPTION |
|---|---|
| **Apply Hunting Rules** | Enable this parameter to include the `applyhunting_rules` parameter in the request. |

## Compromised Account - Additional Parameters

The following additional parameter is included with Compromised Account feed.

| PARAMETER | DESCRIPTION |
|---|---|
| **Prepend Account** | Enable this parameter to add the text string `Account` to the compromised account value.<br><br>`a.williams` would be ingested as `Account a.williams` in ThreatQ. |

## Suspicious Payment Details - Additional Parameters

The following additional parameter is included with the Suspicious Payment Details feed.

| PARAMETER | DESCRIPTION |
|---|---|
| **Payment Type Filtering** | Optional - filter records by payment identifier type. Options include:<br>◦ Bank Account Number<br>◦ Mobile Number<br>◦ Cryptocurrency Wallet<br>◦ IBAN<br>◦ Bank Card<br>◦ QR Payment String<br>◦ Unknown |

| PARAMETER | DESCRIPTION |
|---|---|
| **Search Query** *(Suspicious Payment Details feed only)* | Optional - enter a free-text search query or use `id:<record_id>` to retrieve a specific SPD record. |

## Open Threats - Additional Parameters

The following additional parameter is included with the Open Threats feed.

| PARAMETER | DESCRIPTION |
|---|---|
| **Save CVE Data as** | Select the object type you would like CVEs to be ingested as into the platform. |
| **Apply Hunting Rules** | Enable this parameter to send `apply_hunting_rules=1` with Open Threat `/updated` requests. |
| **Search Query** | Optional - filter Open Threat records with a query such as `id:<record-id>`, `ip:<ip>`, or `domain:<fqdn>`. |

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

# ThreatQ Mapping

## GroupIB Compromised Account

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

```
GET https://tap.group-ib.com/api/v2/compromised/account_group/updated
```

**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 these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].events[].client.ipv4.asn | Related Indicator.Attribute | ASN | .items[].dateFirstSeen | AS2854 | N/A |
| .items[].events[].client.ipv4.city | Related Indicator.Attribute | City | .items[].dateFirstSeen | Moscow | N/A |
| .items[].events[].client.ipv4.countryCode | Related Indicator.Attribute | Country Code | .items[].dateFirstSeen | RU | N/A |
| .items[].events[].client.ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateFirstSeen | Russian Federation | N/A |
| .items[].events[].client.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateFirstSeen | 192.168.0.1 | N/A |
| .items[].events[].client.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateFirstSeen | LLC Orange Business Services | N/A |
| .items[].events[].client.ipv4.region | Related Indicator.Attribute | Region | .items[].dateFirstSeen | Europe | N/A |
| .items[].events[].client.ipv6.asn | Related Indicator.Attribute | ASN | .items[].dateFirstSeen | AS13335 | N/A |
| .items[].events[].client.ipv6.city | Related Indicator.Attribute | City | .items[].dateFirstSeen | San Francisco | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].events[].client.ipv6.countryCode | Related Indicator.Attribute | Country Code | .items[].dateFirstSeen | US | N/A |
| .items[].events[].client.ipv6.countryName | Related Indicator.Attribute | Country Name | .items[].dateFirstSeen | United States | N/A |
| .items[].events[].client.ipv6.ip | Related Indicator.Value | IPv6 Address | .items[].dateFirstSeen | 2606:4700:4700::1000 | N/A |
| .items[].events[].client.ipv6.provider | Related Indicator.Attribute | Provider | .items[].dateFirstSeen | Cloudflare, Inc. | N/A |
| .items[].events[].client.ipv6.region | Related Indicator.Attribute | Region | .items[].dateFirstSeen | North America | N/A |
| .items[].events[].cnc.cnc | Related Indicator.Value | FQDN | .items[].dateFirstSeen | N/A | Emitted when non-empty. |
| .items[].events[].cnc.domain | Related Indicator.Value | FQDN | .items[].dateFirstSeen | stealer-control.test | N/A |
| .items[].events[].cnc.ipv4.asn | Related Indicator.Attribute | ASN | .items[].dateFirstSeen | AS64501 | N/A |
| .items[].events[].cnc.ipv4.city | Related Indicator.Attribute | City | .items[].dateFirstSeen | Ashburn | 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 | 203.0.113.17 | N/A |
| .items[].events[].cnc.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateFirstSeen | Example Hosting | N/A |
| .items[].events[].cnc.ipv4.region | Related Indicator.Attribute | Region | .items[].dateFirstSeen | North America | N/A |
| .items[].events[].cnc.ipv6.asn | Related Indicator.Attribute | ASN | .items[].dateFirstSeen | AS15169 | N/A |
| .items[].events[].cnc.ipv6.city | Related Indicator.Attribute | City | .items[].dateFirstSeen | Mountain View | N/A |
| .items[].events[].cnc.ipv6.countryCode | Related Indicator.Attribute | Country Code | .items[].dateFirstSeen | US | N/A |
| .items[].events[].cnc.ipv6.countryName | Related Indicator.Attribute | Country Name | .items[].dateFirstSeen | United States | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].events[].cnc.ipv6.ip | Related Indicator.Value | IPv6 Address | .items[].dateFirstSeen | 2001:4860:4860::8888 | N/A |
| .items[].events[].cnc.ipv6.provider | Related Indicator.Attribute | Provider | .items[].dateFirstSeen | Google LLC | N/A |
| .items[].events[].cnc.ipv6.region | Related Indicator.Attribute | Region | .items[].dateFirstSeen | North America | N/A |
| .items[].events[].cnc.url | Related Indicator.Value | URL | .items[].dateFirstSeen | https://panel.stealer-control.test/login | N/A |
| .items[].parsedLogin.domain | Related Indicator.Value | FQDN | .items[].dateFirstSeen | example.com | N/A |
| .items[].parsedLogin.ip | Related Indicator.Value | IP Address | .items[].dateFirstSeen | N/A | Emitted when present. |
| .items[].service.domain | Related Indicator.Value | FQDN | .items[].dateFirstSeen | example.example.com | N/A |
| .items[].service.ip | Related Indicator.Value | IP Address | .items[].dateFirstSeen | N/A | Emitted when present. |
| .items[].service.url | Related Indicator.Value | URL | .items[].dateFirstSeen | http://example.example.com/ | N/A |
| .items[].evaluation.admiraltyCode | Account.Attribute | Admiralty Code | .items[].dateFirstSeen | A2 | Updatable |
| .items[].evaluation.credibility | Account.Attribute | Credibility | .items[].dateFirstSeen | 80 | Updatable |
| .items[].evaluation.reliability | Account.Attribute | Reliability | .items[].dateFirstSeen | 100 | Updatable |
| .items[].evaluation.severity | Account.Attribute | Severity | .items[].dateFirstSeen | red | 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 | 30 | Updatable |
| .items[].malware[].name | Related Malware.Value | N/A | .items[].dateFirstSeen | Stealc | N/A |
| .items[].login | Account.Value | N/A | .items[].dateFirstSeen | Account examplelogin | Prepended with 'Account ' |
| .items[].password | Account.Attribute | Password | .items[].dateFirstSeen | 123456789 | N/A |
| .items[].sourceType | Account.Attribute | Source Type | .items[].dateFirstSeen | N/A | Emitted when present. |
| .items[].source[].id | Account.Attribute | Source Link | .items[].dateFirstSeen | N/A | Only HTTP(S) IDs are used. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `.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` | `LegendaryRescator` | `N/A` |

# GroupIB Compromised Bank Card

The GroupIB Compromised Bank Card feed ingests the custom object Compromised Card as well as any related Indicators and Malware.

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

**Sample Response:**


```
{
  "count": 400,
  "items": [
    {
      "baseName": null,
      "cardInfo": {
        "bin": [
          "601129",
          "6011298",
          "60112988",
          "601129880",
          "6011298803"
        ],
        "issuer": {
          "countryCode": "IN",
          "countryName": "INDIA",
          "issuer": "STATE BANK OF INDIA"
        },
        "number": "4000174114732465",
        "system": "VISA",
        "type": "CLASSIC"
      },
      "eventCount": 1,
      "events": [
        {
          "cardInfo": {
            "cvv": "966",
            "dump": null,
            "pin": null,
            "validThru": "8/2016",
            "validThruDate": "2016-08-31"
          },
          "client": {
```

```
      "ipv4": {
        "asn": "AS497 754th Electronic Systems Group",
        "city": "Raleigh",
        "countryCode": "US",
        "countryName": "United States",
        "ip": "56.151.217.119",
        "provider": "United States Postal Service.",
        "region": "North Carolina"
      }
    },
    "cnc": {
      "cnc": "http://246.119.220.81/",
      "domain": "246.119.220.81",
      "ipv4": {
        "asn": "AS497 754th Electronic Systems Group",
        "city": "Raleigh",
        "countryCode": "US",
        "countryName": "United States",
        "ip": "246.119.220.81",
        "provider": "United States Postal Service",
        "region": "North Carolina"
      },
      "ipv6": null,
      "url": "http://246.119.220.81/"
    },
    "malware": {
      "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f60",
      "name": "Phishing"
    },
    "owner": {
      "address": null,
      "city": null,
      "countryCode": null,
      "email": null,
      "name": null,
      "passport": null,
      "phone": null,
      "state": null,
      "zip": null
    },
    "source": {
      "id": null,
```

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

```
      "serviceCode": null,
      "sourceType": [
        "Phishing"
      ],
      "threatActor": [
        {
          "country": null,
          "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
          "isAPT": false,
          "name": "MegaPony"
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

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

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

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `.items[].sourceType` | `Card.Attribute` | `Source Type` | `.items[].dateFirstSeen` | `Phishing` | `N/A` |
| `.items[].dateFirstCompromised` | `Card.Attribute` | `Compromised Date` | `.items[].dateFirstSeen` | `2020-05-19T12:39:15+00:00` | `N/A` |
| `.items[].threatActor[].name` | `Related Adversary.Name` | `N/A` | `.items[].dateFirstSeen` | `MegaPony` | `N/A` |

# GroupIB Compromised Data Mules

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

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

**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 feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].account | Money Mule.Value | N/A | .items[].dateAdd | '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 |
| .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[].seqUpdate | Money Mule.Attribute | Sequence Update | .items[].dateAdd | '1616672696468' | 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.cnc | Related Indicator.Value | FQDN | .items[].dateAdd | http://serv.sexura.ru | N/A |
| .items[].cnc.domain | Related Indicator.Value | FQDN | .items[].dateAdd | 'serv.sexura.ru' | 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[].dateAdd | http://serv.sexura.ru | If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator |
| .items[].cnc.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateAdd | '94.23.180.184' | 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 |
| .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 |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].organization.bic | Related Organization.Attribute | BIC | .items[].dateAdd | 'SABRRUMMVH1' | 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 Compromised Data Git Leaks

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

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

**Sample Response:**


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

```
          "ttl": 0
        },
        "id":
"391db5d5f17ab6cbbbf7c35d1f4d076cb4c830f097b2a9eddd2df7b0650709a7",
        "matchesType": [
          "commonKeywords",
          "keyword"
        ],
        "matchesTypeCount": {
          "commonKeywords": 1,
          "domain": 0,
          "dsn": 0
        },
        "name": "distress_aarch64-apple-darwin",
        "revisions": [
          {
            "bind": [
              {
                "bindBy": "cert",
                "companyId": 2692,
                "data": "cert",
                "ruleId": 0,
                "type": "keyword"
              }
            ],
            "data": {
              "commonKeywords": {
                "password": [
                  "password"
                ]
              }
            },
            "hash":
"391db5d5f17ab6cbbbf7c35d1f4d076cb4c830f097b2a9eddd2df7b0650709a7",
            "info": {
              "authorEmail": "yneth@gmail.ru",
              "authorName": "yneth",
              "timestamp": 1617794272
            }
          }
        ],
        "rules": {},
```

```
          "url": "https://github.com/Yneth/distress-releases/
releases/download/0.7.1/distress_aarch64-apple-darwin"
        }
      ],
      "id": "ead0d8ae9f2347789941ebacde88ad2e3b1ef691",
      "matchesTypes": [
        "commonKeywords",
        "keyword"
      ],
      "name": "vtdl",
      "numberOf": {
        "contributors": 1,
        "files": 1
      },
      "relations": {},
      "seqUpdate": 1591351984817,
      "source": "github"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

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

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

# GroupIB Compromised Data IMEI

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

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

**Sample Response:**


```
{
  "count": 5408859,
  "items": [
    {
      "client": {
        "ipv4": {
          "asn": "AS15169 Google Inc.",
          "city": "Mountain View",
          "countryCode": "US",
          "countryName": "United States",
          "ip": "66.102.6.171",
          "provider": "Google Proxy",
          "region": "California"
        }
      },
      "cnc": {
        "cnc": "http://s1.paradu.ru",
        "domain": "s1.paradu.ru",
        "ipv4": {
          "asn": "AS48666 MAROSNET Telecommunication Company LLC",
          "city": "Moscow",
          "countryCode": "RU",
          "countryName": "Russian Federation",
          "ip": "31.148.99.117",
          "provider": "ALFA TELECOM s.r.o.",
          "region": "Central"
        },
        "ipv6": {
          "asn": "AS48666 MAROSNET Telecommunication Company LLC",
          "city": "Moscow",
          "countryCode": "RU",
          "countryName": "Russian Federation",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "ALFA TELECOM s.r.o.",
```

```
          "region": "Central"
        },
        "url": "http://s1.paradu.ru"
      },
      "dateCompromised": null,
      "dateDetected": "2021-04-10T01:37:36+00:00",
      "device": {
        "iccid": "8910042348144559 36F",
        "imei": "355266047901929",
        "imsi": "313460000000001",
        "model": "Nexus 5X/6.0.1 (Bot.v.5.0)",
        "os": "Android 6.0.1"
      },
      "evaluation": {
        "admiraltyCode": "A2",
        "credibility": 80,
        "reliability": 100,
        "severity": "red",
        "tlp": "red",
        "ttl": 30
      },
      "id": "9bc865c330efb652cf876ae73e8b6ba7b047acf4",
      "isFavourite": false,
      "isHidden": false,
      "malware": {
        "id": "8790a290230b3b4c059c2516a6adace1eac16066",
        "name": "FlexNet"
      },
      "oldId": "441010555",
      "operator": {
        "countryCode": "RU",
        "name": "MegaFon",
        "number": "+358407192130"
      },
      "portalLink": "https://tap.group-ib.com/cd/imei?
searchValue=id:9bc865c330efb652cf876ae73e8b6ba7b047acf4",
      "seqUpdate": 1621774969216,
      "sourceType": "Botnet",
      "threatActor": {
        "id": "6c26d5dc4cc743535e7ab5bb205947540878dab9",
        "isAPT": false,
        "name": "CockSkunk"
```

```
        }
      }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].device.imei | IMEI.Value | N/A | .items[].dateDetected | '355266047901929' | N/A |
| .items[].device.iccid | IMEI.Attribute | Device ICCID | .items[].dateDetected | '8910042348144559 36F' | 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 |
| .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 | Source Link | .items[].dateDetected | https://tap.group-ib.com/cd/imei?searchValue=id:9bc865c330efb652cf876ae73e8b6ba7b047acf4 | N/A |
| .items[].sourceType | IMEI.Attribute | Source Type | .items[].dateDetected | 'Botnet' | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .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.cnc | Related Indicator.Value | FQDN | .items[].dateDetected | http://s1.paradu.ru | 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 | If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator |
| .items[].cnc.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateDetected | '31.148.99.117' | 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 |
| .items[].cnc.ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateDetected | 'Russian Federation' | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].cnc.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateDetected | 'ALFA TELECOM s.r.o.' | 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 Compromised Data Shops

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

`GET https://tap.group-ib.com/api/v2/compromised/access/updated`

**Truncated 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 feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].target.domain | Indicator.Value | N/A | .items[].dateDetected | helpcenter.threatq.com' | N/A |
| .items[].target.device.os | Indicator.Attribute | Operating System | .items[].dateDetected | Windows 10 Pro | N/A |
| .items[].target.geo.city | Indicator.Attribute | City | .items[].dateDetected | N/A | N/A |
| .items[].target.geo.country | Indicator.Attribute | Country | .items[].dateDetected | JO' | N/A |
| .items[].target.geo.state | Indicator.Attribute | State | .items[].dateDetected | Amman Governorate | N/A |
| .items[].cnc.cnc | Related Indicator.Value | FQDN | .items[].dateDetected | https://russianmarket.to/ | N/A |
| .items[].cnc.domain | Related Indicator.Value | FQDN | .items[].dateDetected | russianmarket.to | N/A |
| .items[].cnc.url | Related Indicator.Value | URL | .items[].dateDetected | https://russianmarket.to:443 | N/A |
| .items[].cnc.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateDetected | 172.67.168.114 | N/A |
| .items[].cnc.ipv4.asn | Related Indicator.Attribute | ASN | .items[].dateDetected | AS13335 | N/A |
| .items[].cnc.ipv4.city | Related Indicator.Attribute | City | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv4.countryCode | Related Indicator.Attribute | Country Code | .items[].dateDetected | US | N/A |
| .items[].cnc.ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateDetected | CLOUDFLARENET | N/A |
| .items[].cnc.ipv4.region | Related Indicator.Attribute | Region | .items[].dateDetected | North America | N/A |
| .items[].cnc.ipv6.ip | Related Indicator.Value | IP Address | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv6.asn | Related Indicator.Attribute | ASN | .items[].dateDetected | N/A | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].cnc.ipv6.city | Related Indicator.Attribute | City | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv6.countryCode | Related Indicator.Attribute | Country Code | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv6.countryName | Related Indicator.Attribute | Country Name | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv6.provider | Related Indicator.Attribute | Provider | .items[].dateDetected | N/A | N/A |
| .items[].cnc.ipv6.region | Related Indicator.Attribute | Region | .items[].dateDetected | N/A | N/A |
| .items[].evaluation.tlp | Related Indicators.TLP | N/A | N/A | red | N/A |
| .items[].malware.name | Related Malware.Value | N/A | .items[].dateDetected | Racoon | N/A |

# GroupIB Compromised IM Discord

The GroupIB Compromised IM Discord feed ingests information about Discord channels using the custom object `Discord Channel`. The authors of the messages are ingested as related Identities. The content of the messages are appended to the description of the object. This may result in messages that are not sorted chronologically. It was implemented a mechanism that prevents the ingestion of duplicate messages if the feed is run multiple times on the same time interval.

`GET https://tap.group-ib.com/api/v2/compromised/discord/updated`

**Sample Response (truncated):**


```
{
  "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": "message text",
      "translation": "string",
      "ts": "2023-04-10T14:37:32+03:00"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].author.name | Identity.Value | N/A | N/A | user1234 | N/A |
| .items[].author.discriminator | Identity.Attribute | Discriminator | N/A | 1234 | N/A |
| .items[].channel.name | Discord Channel.Value | N/A | .items[].ts | white_hackers | N/A |
| .items[].channel.server | Discord Channel.Attribute | Server | .items[].ts | server | N/A |
| .items[].channel.stat.firstMessageTs | Discord Channel.Attribute | First Message Date | .items[].ts | 2023-04-10T14:37:32+03:00 | Updatable |
| .items[].channel.stat.messageNum | Discord Channel.Attribute | Message Count | .items[].ts | 10 | Updatable |
| .items[].channel.stat.userNum | Discord Channel.Attribute | Users Count | .items[].ts | 9 | Updatable |
| .items[].text | Discord Channel.Description | N/A | N/A | 2023-04-10T14:37:32+03:00 user1234: message text | Appended to the existing description of the channel. |

# GroupIB Compromised IM Telegram

The GroupIB Compromised IM Telegram feed ingests information about Telegram channels, groups or supergroup using the custom object `Telegram Channel`. The authors of the messages are ingested as related Identities. The content of the messages are appended to the description of the object. This may result in messages that are not sorted chronologically. It was implemented a mechanism that prevents the ingestion of duplicate messages if the feed is run multiple times on the same time interval.

`GET https://tap.group-ib.com/api/v2/compromised/messenger/updated`

**Sample Response (truncated):**


```
{
  "count": 1,
  "items": [
     {
      "author": {
        "id": "string",
        "userName": "user1234",
        "firstName": "Denial",
        "lastName": "Service",
        "type": "user"
      },
      "chatStat": {
        "avatar": {
          "detected": "2023-04-10T14:37:32+03:00",
          "hash": "string",
          "id": "string"
        },
        "firstMessageDate": "2023-04-10T14:37:32+03:00",
        "id": 0,
        "lastMessageDate": "2023-04-10T14:37:32+03:00",
        "messageNum": 10,
        "name": "white_hackers",
        "title": "White Hackers",
        "type": "group",
        "userNum": 9
      },
      "edits": {},
      "highlight": [
        "string"
```

```
      ],
      "id": "string",
      "isReply": true,
      "message": "This message was compromised",
      "messageTs": "2023-04-10T14:37:32+03:00",
      "name": "white_hackers",
      "rules": [
        "183963"
      ],
      "seqUpdate": 0,
      "translatedMessage": "string"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].author.userName | Identity.Value | N/A | N/A | Account user1234 | N/A |
| .items[].author.firstName | Identity.Attribute | First Name | N/A | Denial | N/A |
| .items[].author.lastName | Identity.Attribute | Last Name | N/A | Service | N/A |
| .items[].author.type | Identity.Attribute | Type | N/A | user | N/A |
| .items[].name | Telegram Channel.Value | N/A | .items[].messageTs | Telegram group white_hackers | N/A |
| .items[].chatStat.title | Telegram Channel.Attribute | Title | .items[].messageTs | White Hackers | N/A |
| .items[].chatStat.firstMessageDate | Telegram Channel.Attribute | First Message Date | .items[].messageTs | 2023-04-10T14:37:32+03:00 | Updatable |
| .items[].chatStat.messageNum | Telegram Channel.Attribute | Message Count | .items[].messageTs | 10 | Updatable |
| .items[].chatStat.userNum | Telegram Channel.Attribute | Users Count | .items[].messageTs | 9 | Updatable |
| .items[].chatStat.type | Telegram Channel.Attribute | Type | .items[].messageTs | commercial | N/A |
| .items[].message | Telegram Channel.Description | N/A | N/A | 2023-04-10T14:37:32+03:00 user1234: message text | Appended to the existing description of the channel. |

# GroupIB Compromised Masked Bank Card

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

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

**Sample Response:**


```
{
  "count": 400,
  "items": [
    {
      "baseName": null,
      "cardInfo": {
        "cvv": 946,
        "dump": null,
        "issuer": {
          "countryCode": "IN",
          "countryName": "INDIA",
          "issuer": "STATE BANK OF INDIA"
        },
        "number": "4000174114732465",
        "system": "VISA",
        "type": "CLASSIC",
        "validThru": "8/2016"
      },
      "client": {
        "ipv4": {
          "asn": "AS497 754th Electronic Systems Group",
          "city": "Raleigh",
          "countryCode": "US",
          "countryName": "United States",
          "ip": "56.151.217.119",
          "provider": "United States Postal Service.",
          "region": "North Carolina"
        }
      },
      "cnc": {
        "cnc": "http://246.119.220.81/",
        "domain": "246.119.220.81",
        "ipv4": {
          "asn": "AS497 754th Electronic Systems Group",
```

```
        "city": "Raleigh",
        "countryCode": "US",
        "countryName": "United States",
        "ip": "246.119.220.81",
        "provider": "United States Postal Service",
        "region": "North Carolina"
      },
      "ipv6": null,
      "url": "http://246.119.220.81/"
    },
    "dateCompromised": "2020-06-05T10:07:26+00:00",
    "dateDetected": "2020-06-05T10:07:26+00:00",
    "evaluation": {
      "admiraltyCode": "B3",
      "credibility": 50,
      "reliability": 80,
      "severity": "orange",
      "tlp": "red",
      "ttl": 90
    },
    "externalId": "",
    "id": "b3d87b6af5532ee8d41baac000bba2d1c46662c8",
    "isFavourite": false,
    "isHidden": false,
    "isIgnore": false,
    "malware": {
      "id": "3e9e68a2f267f45f970ee84ff5dac37d05761f60",
      "name": "Phishing"
    },
    "oldId": "2308",
    "owner": {
      "address": null,
      "birthday": null,
      "city": null,
      "countryCode": null,
      "email": null,
      "name": null,
      "passport": null,
      "phone": null,
      "state": null,
      "taxNumber": null,
      "zip": null
```

```
      },
      "portalLink": "https://bt-demo.group-ib.com/cd/cards?
searchValue=id:b3d87b6af5532ee8d41baac000bba2d1c46662c8",
      "price": {
        "currency": null,
        "value": null
      },
      "seqUpdate": 1591351984817,
      "serviceCode": null,
      "sourceLink": "https://breached.to/Thread-Selling-CLOUT-WITH-
MORE-THAN-970-000-LOGS-JUNE-SEPT-2022",
      "sourceType": "Phishing",
      "threatActor": {
        "country": null,
        "id": "051cbdad0eb17cb52d7b635187a922f97850bfc3",
        "isAPT": false,
        "name": "MegaPony"
      },
      "track": []
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

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

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].cnc.ipv4.countryCode | Related Indicator.Attribute | Country Code | .items[].dateDetected | US | N/A |
| .items[].cnc.ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateDetected | United States | N/A |
| .items[].cnc.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateDetected | 246.119.220.81 | N/A |
| .items[].cnc.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateDetected | United States Postal Service | N/A |
| .items[].cnc.ipv4.region | Related Indicator.Attribute | Region | .items[].dateDetected | North Carolina | N/A |
| .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 |

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

# GroupIB Human Intelligence Threat and GroupIB APT Threat

By default, the **Group-IB Human Intelligence Threat** and **Group-IB APT Threat** feeds ingest intelligence as **Report** objects. If **Ingest Threat Feeds As** is set to **Intrusion Sets**, the feeds ingest **Intrusion Set** objects instead. In both cases, the feeds also ingest any related **Indicators**, **Malware**, **Adversaries**, **Attack Patterns**, **Identities**, and **Tools**.

**GroupIB Human Intelligence Threat**

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

**GroupIB APT Threat**

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

**Sample Response (truncated):**


```
{
  "count": 876,
  "items": [
    {
      "contacts": [
        {
          "account": "alexjoe9983",
          "flag": "fake",
          "service": "twitter",
          "type": "social_network"
        }
      ],
      "countries": [
        "LB",
        "TR"
      ],
      "createdAt": "2021-04-13T16:49:27+03:00",
      "cveList": [
        {
          "name": "CVE-2021-27065"
        }
      ],
      "dateFirstSeen": "2019-05-01",
      "dateLastSeen": "2021-04-09",
      "datePublished": "2021-04-09",
      "description": "During the Operation",
      "displayOptions": {
```

```
        "isFavourite": false,
        "isHidden": false
      },
      "evaluation": {
        "admiraltyCode": "B2",
        "credibility": 80,
        "reliability": 80,
        "severity": "red",
        "tlp": "amber",
        "ttl": 30
      },
      "expertise": [
        "0day",
        "CVE"
      ],
      "files": [
        {
          "hash":

"f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0",
          "mime": "image/png",
          "name":

"f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0",
          "size": 75438
        }
      ],
      "forumsAccounts": [
        {
          "messageCount": 1,
          "nickname": "nobody.gu3st",
          "registeredAt": "2012-07-13",
          "url":
            "http://www.iranhack.com/forum/member/186-nobody-gu3st"
        }
      ],
      "id": "3bcfabae7dc7a909ca692e702a9b6ca6627528b4",
      "indicatorMalwareRelationships": [
        {
          "indicatorId":
            "3c157cefdeae6a8403fbfe24790467215493b939",
          "malwareId":
```

```
            "132130dd0aa2f2ab8cb1e358974443276b28195d"
          }
        ],
        "indicatorRelationships": [
          {
            "sourceId":
              "a6c970a7f082513303a0466ca459329829e00143",
            "targetId":
              "2d6c6dbf99261a1c84eefec1bb395e4876346a4c"
          }
        ],
        "indicatorToolRelationships": [],
        "indicators": [
          {
            "description": null,
            "id": "3b67fc483bc2c22e0f21d68eabf6385f364a1eea",
            "langs": [
              "ru"
            ],
            "malwareList": [],
            "params": {
              "hashes": {
                "md4": "",
                "md5": "113044788a356aab6c693a3e80189141",
                "md6": "",
                "ripemd160": "",
                "sha1": "ba835af7b8aa51797f95223676640be9c81dad9f",
                "sha224":

"2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b",
                "sha256":

"0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
                "sha384":

"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3e"
                  "417cb71ce646efd0819dd8c088de1bd",
                "sha512":

"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27"

"e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b",
```

```
            "whirlpool": ""
          },
          "name":

"0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40",
          "size": null
        },
        "url": "http://strigigena.ru/cookie.php",
        "seqUpdate": 16183252904267,
        "techSeqUpdate": null,
        "title": null,
        "type": "file"
      },
      {
        "description": null,
        "id": "221f0e6b18af2cbf069131f2b7cf7e4552ae9d17",
        "langs": [
          "ru"
        ],
        "malwareList": [
          {
            "id": "132130dd0aa2f2ab8cb1e358974443276b28195d",
            "name": "SysUpdate"
          }
        ],
        "params": {
          "domain": "ns162.nsakadns.com",
          "ipv4": [
            "85.204.74.143"
          ],
          "ipv6": [
            "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
          ],
          "ssl": [
            {
              "hashes": {
                "md5": "5765fafd258a5a1e87c0582a67862675",
                "sha1": "AB0B22AB421C001462AF4A9F382DC9284747B43D",
                "sha224":

"2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b",
                "sha256":
```

```
"ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb",
                  "sha384":

"fdbd8e75a67f29f701a4e040385e2e23986303ea10239211af907fcbb83578b3"
                    "e417cb71ce646efd0819dd8c088de1bd",
                  "sha512":

"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f2"

"7e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b"
                }
              }
            ],
            "url": [
              "http://strigigena.ru/cookie.php"
            ],
            "address": "this2test.com",
            "message": {
              "body": "Body example",
              "subject": "Subject example"
            },
            "senderIp": "85.204.74.144",
            "serverIp": "85.204.74.145"
          },
          "seqUpdate": 16183273671915,
          "techSeqUpdate": null,
          "title": null,
          "type": "network"
        }
      ],
      "indicatorsIds": [
        "3b67fc483bc2c22e0f21d68eabf6385f364a1eea",
        "340ac49012b02435315f1dfca9628319b4c9dae9"
      ],
      "isTailored": false,
      "labels": [
        "campaign",
        "indicator"
      ],
      "langs": [
        "ru",
```

```
      "en"
    ],
    "malwareList": [
      {
        "id": "132130dd0aa2f2ab8cb1e358974443276b28195d",
        "name": "SysUpdate"
      }
    ],
    "mitreMatrix": [
      {
        "attackPatternId":
          "attack-pattern--fddd81e9-dd3d-477e-9773-4fb8ae227234",
        "attackTactic": "build-capabilities",
        "attackType": "pre_attack_tactics",
        "id": "PRE-T1122",
        "params": {
          "data": "Just a string"
        }
      }
    ],
    "oldId": "0c3429ce-c449-485d-aa02-effc62719818",
    "regions": [
      "middle_east",
      "europe",
      "asia",
      "asia"
    ],
    "relatedThreatActors": [
      {
        "id": "",
        "isAPT": "",
        "name": "actor",
        "type": "bad"
      }
    ],
    "reportNumber": "CP-2504-1649",
    "sectors": [
      "gambling",
      "government-national",
      "telecommunications",
      "energy",
      "finance"
```

```
      ],
      "seqUpdate": 16184833571103,
      "shortDescription": "This is an attack",
      "shortTitle": "Attack",
      "sources": [
        "https://www.trendmicro.com/en_us/research/21/d/iron.html"
      ],
      "targetedCompany": [
        "TargetCompany"
      ],
      "targetedPartnersAndClients": [
        "TargetPandC"
      ],
      "techSeqUpdate": null,
      "threatActor": {
        "country": "CN",
        "id": "55011fb96789bcb43c8e19e4e886924f803b6d30",
        "isAPT": true,
        "name": "IronTiger"
      },
      "title": "Discovered new toolkit",
      "toolList": [
        {
          "id": "123456789",
          "name": "Tools"
        }
      ],
      "type": "threat",
      "updatedAt": "2021-04-15T13:42:37+03:00"
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `.items[].title` | `Report.Value / Intrusion Set.Value` | `N/A` | `.items[].createdAt` | `'Discovered new toolkit'` | `Depends on Ingest Threat Feeds As` |
| `.items[].dateFirstSeen` | `Report.Started_at / Intrusion Set.Started_at` | `N/A` | `N/A` | `'2019-05-01'` | `Depends on Ingest Threat Feeds As` |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].dateLastSeen | Report.Ended_at / Intrusion Set.Ended_at | N/A | N/A | '2021-04-09' | Depends on Ingest Threat Feeds As |
| .items[].description | Report.Description / Intrusion Set.Description | N/A | N/A | 'During the Operation' | Depends on Ingest Threat Feeds As |
| .items[].countries[] | Report.Attribute / Intrusion Set.Attribute | Country | .items[].createdAt | 'LB' | Depends on Ingest Threat Feeds As |
| .items[].evaluation.admiraltyCode | Report.Attribute / Intrusion Set.Attribute | Admiralty Code | .items[].createdAt | 'B2' | Updatable; depends on Ingest Threat Feeds As |
| .items[].evaluation.credibility | Report.Attribute / Intrusion Set.Attribute | Credibility | .items[].createdAt | '80' | Updatable; depends on Ingest Threat Feeds As |
| .items[].evaluation.reliability | Report.Attribute / Intrusion Set.Attribute | Reliability | .items[].createdAt | '80' | Updatable; depends on Ingest Threat Feeds As |
| .items[].evaluation.severity | Report.Attribute / Intrusion Set.Attribute | Severity | .items[].createdAt | 'red' | Updatable; depends on Ingest Threat Feeds As |
| .items[].evaluation.tlp | Report.TLP / Intrusion Set.TLP / Related Objects.TLP | N/A | N/A | 'amber' | Depends on Ingest Threat Feeds As |
| .items[].evaluation.ttl | Report.Attribute / Intrusion Set.Attribute | Time To Live (days) | .items[].createdAt | '30' | Updatable; depends on Ingest Threat Feeds As |
| .items[].expertise[] | Report.Attribute / Intrusion Set.Attribute | Expertise | .items[].createdAt | '0day' | Depends on Ingest Threat Feeds As |
| .items[].labels[] | Report.Attribute / Intrusion Set.Attribute | STIX labels | .items[].createdAt | 'campaign' | Depends on Ingest Threat Feeds As |
| .items[].langs[] | Report.Attribute / Intrusion Set.Attribute | Language | .items[].createdAt | 'ru' | Depends on Ingest Threat Feeds As |
| .items[].regions[] | Report.Attribute / Intrusion Set.Attribute | Regions | .items[].createdAt | 'middle_east' | Depends on Ingest Threat Feeds As |
| .items[].reportNumber | Report.Attribute / Intrusion Set.Attribute | Report Number | .items[].createdAt | 'CP-2504-1649' | Depends on Ingest Threat Feeds As |
| .items[].sectors[] | Report.Attribute / Intrusion Set.Attribute | Sector | .items[].createdAt | 'gambling' | Depends on Ingest Threat Feeds As |
| .items[].shortDescription | Report.Attribute / Intrusion Set.Attribute | Short Description | .items[].createdAt | 'This is an attack' | Depends on Ingest Threat Feeds As |
| .items[].shortTitle | Report.Attribute / Intrusion Set.Attribute | Short Title | .items[].createdAt | 'Attack' | Depends on Ingest Threat Feeds As |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].sources[] | Report.Attribute / Intrusion Set.Attribute | Source | .items[].createdAt | https://www.trendmicro.com/en_us/research/21/d/iron.html | Depends on Ingest Threat Feeds As |
| .items[].targetedCompany[] | Report.Attribute / Intrusion Set.Attribute | Target Company | .items[].createdAt | 'TargetCompany' | Depends on Ingest Threat Feeds As |
| .items[].targetedPartnersAndClients[] | Report.Attribute / Intrusion Set.Attribute | Target Partner and Client | .items[].createdAt | 'TargetPandC' | Depends on Ingest Threat Feeds As |
| .items[].type | Report.Attribute / Intrusion Set.Attribute | Type | .items[].createdAt | 'threat' | Depends on Ingest Threat Feeds As |
| .items[].cveList[].name | Related Indicator.Value and/or Related Vulnerability.Value | CVE | .items[].createdAt | 'CVE-2021-27065' | N/A |
| .items[].contacts[].account | Related Identity.Value | N/A | .items[].createdAt | 'alexjoe9983' | N/A |
| .items[].contacts[].flag | Related Identity.Attribute | Contact Flag | .items[].createdAt | 'fake' | N/A |
| .items[].contacts[].service | Related Identity.Attribute | Contact Service | .items[].createdAt | 'twitter' | N/A |
| .items[].contacts[].type | Related Identity.Attribute | Contact Type | .items[].createdAt | 'social_network' | N/A |
| .items[].files[].hash | Related Indicator.Value | SHA-256 | .items[].createdAt | 'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0' | N/A |
| .items[].files[].mime | Related Indicator.Attribute | File Mime Type | .items[].createdAt | 'image/png' | N/A |
| .items[].files[].name | Related Indicator.Attribute | File Name | .items[].createdAt | 'f1724b95fdac1541bb416bff08b209b8750e23928b5868ec1ce34dad2a740dc0' | N/A |
| .items[].files[].size | Related Indicator.Attribute | File Size | .items[].createdAt | '75438' | N/A |
| .items[].forumsAccounts[].url | Related Indicator.Value | URL | .items[].createdAt | http://www.iranhack.com/forum/member/186-nobody-gu3st | If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator |
| .items[].forumsAccounts[].nickname | Related Indicator.Attribute | Forum Account Nickname | .items[].createdAt | 'nobody.gu3st' | N/A |
| .items[].indicators[].ma | 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 |
|---|---|---|---|---|---|
| lwareList[].name | | | | | |
| .items[].indicators[].params.domain | Related Indicator.Value | FQDN | .items[].createdAt | 'ns162.nsakadns.com' | N/A |
| .items[].indicators[].params.ipv4[] | Related Indicator.Value | IP Address | .items[].createdAt | '85.204.74.143' | N/A |
| .items[].indicators[].params.ipv6[] | Related Indicator.Value | IPv6 Address | .items[].createdAt | '2001:0db8:85a3:0000:0000:8a2e:0370:7334' | N/A |
| .items[].indicators[].params.ssl[].hashes.md5 | Related Indicator.Value | MD5 | .items[].createdAt | '5765fafd258a5a1e87c0582a67862675' | N/A |
| .items[].indicators[].params.ssl[].hashes.sha1 | Related Indicator.Value | SHA-1 | .items[].createdAt | 'AB0B22AB421C001462AF4A9F382DC9284747B43D' | N/A |
| .items[].indicators[].params.ssl[].hashes.sha256 | Related Indicator.Value | SHA-256 | .items[].createdAt | 'ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb' | N/A |
| .items[].indicators[].params.ssl[].hashes.sha384 | Related Indicator.Value | SHA-384 | .items[].createdAt | '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 | If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator |
| .items[].indicators[].params.address | Related Indicator.Value | Email Address | .items[].createdAt | 'this2test.com' | N/A |
| .items[].indicators[].params.message.body | Related Indicator.Attribute | Email Body | .items[].createdAt | 'Body example' | N/A |
| .items[].indicators[].params.message.subject | Related Indicator.Attribute | Email Subject | .items[].createdAt | 'Subject example' | N/A |
| .items[].indicators[].params.senderIp | Related Indicator.Value | IP Address | .items[].createdAt | '85.204.74.144' | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .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 | '0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40' | 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 | '2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b' | N/A |
| .items[].malwareList[].name | Related Malware.Value | N/A | .items[].createdAt | 'SysUpdate' | N/A |
| .items[].mitreMatrix[].id | Related Attack | Attack Pattern | .items[].createdAt | 'attack-pattern--fddd81e9-dd3d-477e-9773-4fb8ae227234' | N/A |
| .items[].mitreMatrix[].attackTactic | Related Attack.Attribute | Attack Tactic | .items[].createdAt | 'build-capabilities' | N/A |
| .items[].mitreMatrix[].attackType | Related Attack.Attribute | Attack Type | .items[].createdAt | 'pre_attack_tactics' | N/A |
| .items[].mitreMatrix[].params.data | Related Attack.Attribute | Attack Data | .items[].createdAt | 'Just a string' | N/A |
| .items[].relatedThreatActors[].name | Related Adversary.Name | N/A | .items[].createdAt | 'actor' | N/A |
| .items[].relatedThreatActors[].type | Related Adversary.Attribute | Type | .items[].createdAt | 'bad' | N/A |
| .items[].threatActor.name | Related Adversary.Name | N/A | .items[].createdAt | 'IronTiger' | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .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 Human Intelligence Threat Actor and GroupIB APT Threat Actor

The GroupIB Human Intelligence Threat Actor and APT Threat Actor feeds ingest Adversary objects and any related Indicators and Reports.

**GroupIB Human Intelligence Threat Actor**

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

**GroupIB APT Threat Actor**

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

**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"
    ],
    "dateFirstSeen": "2021-10-24",
    "dateLastSeen": "2021-10-24",
    "regions": [
        "europe",
        "america:northern_america",
        "asia"
    ],
    "reports": [
      {
        "datePublished": "2021-01-05",
        "id": "9ffb44adf43abaaeea1f36c9d2a5adef38ba19e8",
        "name": {
          "en": "First mention on forums"
        }
      }
    ],
```

```
        "sectors": [
            "financial-services",
            "finance",
            "technology"
        ],
        "targetedCompany": [
          "Datagroup"
        ],
        "targetedPartnersAndClients": []
      },
      "techSeqUpdate": null,
      "updatedAt": "2021-04-14T16:25:43+03:00"
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].name | Adversary.Name | N/A | .items[].createdAt | 'Amigos' | 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 |

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

# GroupIB Malware C2

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

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

**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":
"0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b
                      3b663937af9ef40",
            "sha384": "fdbd8e75a67f29f701a4e040385e2e23
                      986303ea10239211af907fcbb83578
                      b3e417cb71ce646efd0819dd8c088de1bd",

"sha512":"2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246f
b30382f27e853d8585719e0e67cbda0daa8f5167
1064615d645ae27acb15bfb1447f459b"
          }
        }
      ],
      "id": "4fb5bbcaa61e77d5024b0f02256d3b78339606ef",
      "ipv4": [
        {
          "asn": "AS16276 OVH SAS",
          "city": "Singapore",
```

```
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "128.199.23.9",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "ipv6": [
        {
          "asn": "AS16276 OVH SAS",
          "city": "Singapore",
          "countryCode": "SG",
          "countryName": "Singapore",
          "ip": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
          "provider": "DigitalOcean",
          "region": "Central"
        }
      ],
      "isFavourite": false,
      "isHidden": false,
      "malwareList": [
        {
          "id": "f9983dbd202159e87ca7ab517d1ca4b08aed542a",
          "name": "U-Admin"
        }
      ],
      "oldId": "448197320",
      "platform": null,
      "seqUpdate": 1622322902077,
      "ssl": [],
      "threatActor": {
        "country": "CN",
        "id": "55011fb96789bcb43c8e19e4e886924f803b6d30",
        "isAPT": true,
        "name": "IronTiger"
      },
      "url": "http://128.199.23.9/uadmin/gate.php"
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].cnc | Related Indicator.Value | FQDN | .items[].dateDetected | http://128.199.23.9/uadmin/gate.php | N/A |
| .items[].domain | Related Indicator.Value | FQDN | .items[].dateDetected | 'www.0983212l.link' | 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 |
| .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 |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .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 |
| .items[].url | Related Indicator.Value | URL | .items[].dateDetected | http://128.199.23.9/uadmin/gate.php | If a URL Indicator attempting to be consumed is a true FQDN, the API normalize it to be an FQDN Indicator |

# GroupIB Malware Configs

The GroupIB Malware Configs feed ingests Indicators and Malware.

```
GET https://tap.group-ib.com/api/v2/malware/config/updated
```

**Sample Response:**


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


ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].malware.name | Malware.Value | N/A | .items[].dateFirstSeen | 'Lockbit' | N/A |
| .items[].content | Malware.Description | N/A | .items[].dateFirstSeen | 'LockBit 2.0 Ransomware... ' | The content was truncated |
| .items[].hash | Related 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 |
| .items[].file.name | Related Indicator.Attribute | File name | .items[].dateFirstSeen | 'vtdl_85dg97ui' | N/A |

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

These feeds ingests Indicators objects.

**GroupIB Suspicious IP Tor Node**

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

**GroupIB Suspicious IP Open Proxy**

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

**GroupIB Suspicious IP Socks Proxy**

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

**Sample Response:**


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

```
      "seqUpdate": 16182431110000,
      "source": "check.torproject.org",
      "port": "80",
      "type": "http"
    }
  ]
}
```

ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].ipv4.ip | Indicator.Value | IP Address | .items[].dateFirstSeen | '128.199.23.10' | 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[].type | Indicator.Attribute | Proxy Type | .items[].dateFirstSeen | 'http' | N/A |
| .items[].port | Indicator.Attribute | Port | .items[].dateFirstSeen | '80' | N/A |

# GroupIB Suspicious IP Scanners

The GroupIB Suspicious IP Scanners feed ingests Indicators objects.

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

**Sample Response:**


```
{
  "count": 132912,
  "items": [
    {
      "categories": [
        "Hacking",
        "FTP Brute-Force"
      ],
      "dateFirstSeen": "2020-05-27T14:57:33+00:00",
      "dateLastSeen": "2021-04-15T15:31:43+00:00",
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 90,
        "reliability": 90,
        "severity": "green",
        "tlp": "green",
        "ttl": 30
      },
      "id": "134.209.127.189",
      "ipv4": {
        "asn": "AS16276 OVH SAS",
        "city": "Singapore",
        "countryCode": "SG",
        "countryName": "Singapore",
        "ip": "134.209.127.189",
        "provider": "DigitalOcean",
        "region": "Central"
      },
      "portalLink": null,
      "seqUpdate": 16182431110000,
      "sources": [
        "AbuseIPDB",
        "GIB-HoneyPot"
      ]
    }
```

```
  ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].ipv4.ip | Indicator.Value | IP Address | .items[].dateFirstSeen | '134.209.127.189' | N/A |
| .items[].categories | Indicator.Tags | N/A | .items[].dateFirstSeen | 'Hacking, FTP Brute-Force' | N/A |
| .items[].ipv4.asn | Indicator.Attribute | ASN | .items[].dateFirstSeen | 'AS16276 OVH SAS' | N/A |
| .items[].ipv4.city | Indicator.Attribute | City | .items[].dateFirstSeen | 'Singapore' | N/A |
| .items[].ipv4.countryCode | Indicator.Attribute | Country Code | .items[].dateFirstSeen | 'SG' | N/A |
| .items[].ipv4.countryName | Indicator.Attribute | Country Name | .items[].dateFirstSeen | 'Singapore' | N/A |
| .items[].ipv4.provider | Indicator.Attribute | Provider | .items[].dateFirstSeen | 'DigitalOcean' | N/A |
| .items[].ipv4.region | Indicator.Attribute | Region | .items[].dateFirstSeen | 'Central' | N/A |
| .items[].evaluation.admiraltyCode | Indicator.Attribute | Admiralty Code | .items[].dateFirstSeen | 'B2' | 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 Suspicious IP VPN

The GroupIB Suspicious IP VPN feed ingests Indicators objects.

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

**Sample Response:**


```
{
  "count": 132912,
  "items": [
    {
      "dateFirstSeen": "2020-05-27T14:57:33+00:00",
      "dateLastSeen": "2021-04-15T15:31:43+00:00",
      "evaluation": {
        "admiraltyCode": "A1",
        "credibility": 90,
        "reliability": 90,
        "severity": "green",
        "tlp": "green",
        "ttl": 30
      },
      "id": "66.235.168.192",
      "ipv4": {
        "asn": "AS16276 OVH SAS",
        "city": "Singapore",
        "countryCode": "SG",
        "countryName": "Singapore",
        "ip": "66.235.168.192",
        "provider": "DigitalOcean",
        "region": "Central"
      },
      "names": [
        "Pulse Connect Secure"
      ],
      "portalLink": null,
      "rules": [
        "Pulse Connect Secure VPN"
      ],
      "seqUpdate": 16182431110000,
      "sources": [
        "playbook"
      ],
```

```
      "types": [
        "public"
      ]
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].ipv4.ip | Indicator.Value | IP Address | .items[].dateFirstSeen | '66.235.168.192' | N/A |
| .items[].types | Indicator.Tags | N/A | .items[].dateFirstSeen | 'public' | N/A |
| .items[].ipv4.asn | Indicator.Attribute | ASN | .items[].dateFirstSeen | 'AS16276 OVH SAS' | N/A |
| .items[].ipv4.city | Indicator.Attribute | City | .items[].dateFirstSeen | 'Singapore' | N/A |
| .items[].ipv4.countryCode | Indicator.Attribute | Country Code | .items[].dateFirstSeen | 'SG' | N/A |
| .items[].ipv4.countryName | Indicator.Attribute | Country Name | .items[].dateFirstSeen | 'Singapore' | N/A |
| .items[].ipv4.provider | Indicator.Attribute | Provider | .items[].dateFirstSeen | 'DigitalOcean' | N/A |
| .items[].ipv4.region | Indicator.Attribute | Region | .items[].dateFirstSeen | 'Central' | N/A |
| .items[].evaluation.admiraltyCode | Indicator.Attribute | Admiralty Code | .items[].dateFirstSeen | 'B2' | 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 |

# GroupIB Suspicious Payment Details

The GroupIB Suspicious Payment Details feed ingests custom object Compromised Account and any related Indicators, Cards, Malware, and Adversaries.

```
GET https://tap.group-ib.com/api/v2/compromised/spd/updated
```

**Sample Response:**


```
{
  "count": 1,
  "seqUpdate": 1751526185843,
  "items": [
    {
      "id": "example_id_hash",
      "type": "Cryptocurrency Wallet",
      "serviceType": "BTCLike",
      "ownerName": "Example Owner",
      "illegalScore": 100,
      "displayOptions": {
        "isFavourite": false
      },
      "value": {
        "value": "bc1qexampleexampleexampleexampleexamplexxxxx",
        "email": "payments@example.com",
        "bankCard": "4000174114732465",
        "iban": "DE893704004405320130000"
      },
      "events": [
        {
          "compromisedAt": "2025-04-29T00:00:00Z",
          "detectedAt": "2025-04-29T00:00:00Z",
          "source": {
            "name": "Example Leak",
            "type": "Example Leak"
          },
          "malware": [
            {
              "id": "b92907366a537a0f0315e32b0342f9c55f29b9a5",
              "name": "Stealc"
            }
          ],
          "threatActor": [
```

```
        {
          "country": "RU",
          "id": "8ff8a368c2266216cf5763b8e9eff144abd6fe26",
          "isAPT": false,
          "name": "LegendaryRescator",
          "stixGuid": null
        }
      ],
      "tags": [
        "crypto",
        "leak"
      ],
      "illegalScore": 100
    }
  ],
  "seqUpdate": 1751526184752,
  "createdAt": "2025-07-03T07:03:04.752Z",
  "firstSeenAt": "2025-04-29T00:00:00Z",
  "lastSeenAt": "2025-04-29T00:00:00Z",
  "evaluation": {
    "admiraltyCode": "A2",
    "credibility": 80,
    "reliability": 100,
    "severity": "red",
    "tlp": "amber",
    "ttl": 30
  },
  "malware": [
    {
      "id": "b92907366a537a0f0315e32b0342f9c55f29b9a5",
      "name": "Stealc"
    }
  ],
  "threatActor": [
    {
      "country": "RU",
      "id": "8ff8a368c2266216cf5763b8e9eff144abd6fe26",
      "isAPT": false,
      "name": "LegendaryRescator",
      "stixGuid": null
    }
  ],
```

```
      "tags": [
        "laundering",
        "ransomware"
      ],
      "sources": [],
      "country": [
        "DE",
        "RU"
      ]
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].value.value | Account.Value | N/A | .items[].firstSeenAt | bc1qexampleexampleexampleexampleexamplexxxxx | N/A |
| .items[].type | Account.Attribute | Type | .items[].firstSeenAt | Cryptocurrency Wallet | N/A |
| .items[].serviceType | Account.Attribute | Service | .items[].firstSeenAt | BTCLike | N/A |
| .items[].firstSeenAt | Account.Attribute | First Seen | .items[].firstSeenAt | 2025-04-29T00:00:00Z | N/A |
| .items[].lastSeenAt | Account.Attribute | Last Seen | .items[].firstSeenAt | 2025-04-29T00:00:00Z | N/A |
| .items[].ownerName | Account.Attribute | Owner Name | .items[].firstSeenAt | Example Owner | N/A |
| .items[].illegalScore | Account.Attribute | Illegal Score | .items[].firstSeenAt | 100 | Updatable |
| .items[].createdAt | Account.Attribute | Created At | .items[].firstSeenAt | 2025-07-03T07:03:04.752Z | N/A |
| .items[].seqUpdate | Account.Attribute | Sequence Update | .items[].firstSeenAt | 1751526184752 | N/A |
| .items[].country[] | Account.Attribute | Country | .items[].firstSeenAt | DE | N/A |
| .items[].evaluation.admiraltyCode | Account.Attribute | Admiralty Code | .items[].firstSeenAt | A2 | Updatable |
| .items[].evaluation.credibility | Account.Attribute | Credibility | .items[].firstSeenAt | 80 | Updatable |
| .items[].evaluation.reliability | Account.Attribute | Reliability | .items[].firstSeenAt | 100 | Updatable |
| .items[].evaluation.severity | Account.Attribute | Severity | .items[].firstSeenAt | red | Updatable |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].evaluation.tlp | Account.TLP / Related Objects.TLP | N/A | .items[].firstSeenAt | amber | N/A |
| .items[].evaluation.ttl | Account.Attribute | Time to live (days) | .items[].firstSeenAt | 30 | Updatable |
| .items[].tags[] | Account.Tag | N/A | .items[].firstSeenAt | ransomware | N/A |
| .items[].events[].source.name | Account.Attribute | Source | .items[].firstSeenAt | Example Leak | N/A |
| .items[].events[].source.type | Account.Attribute | Source Type | .items[].firstSeenAt | Example Leak | N/A |
| .items[].value.email | Related Indicator.Value | Email Address | .items[].firstSeenAt | payments@example.com | N/A |
| .items[].value.bankCard | Related Card.Value | Card Number | .items[].firstSeenAt | 4000174114732465 | N/A |
| .items[].value.iban | Account.Attribute | IBAN | .items[].firstSeenAt | DE893704004405320130000 | N/A |
| .items[].malware[].name | Related Malware.Value | N/A | .items[].firstSeenAt | Stealc | N/A |
| .items[].threatActor[].name | Related Adversary.Name | N/A | .items[].firstSeenAt | LegendaryRescator | N/A |
| .items[].events[].compromisedAt | Account.Attribute | Compromised Date | .items[].firstSeenAt | 2025-04-29T00:00:00Z | N/A |
| .items[].events[].detectedAt | Account.Attribute | Detected Date | .items[].firstSeenAt | 2025-04-29T00:00:00Z | N/A |
| .items[].events[].illegalScore | Account.Attribute | Event Illegal Score | .items[].firstSeenAt | 100 | N/A |

# GroupIB Attacks DDoS

The GroupIB Attacks DDoS feed ingests Indicators objects.

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

**Sample Response:**


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

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


ThreatQ provides the following default mapping for these feeds:

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

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | |
|---|---|---|---|---|---|
| .items[].cnc.ipv6.countryName | Indicator.Attribute | Country Name | .items[].dateBegin | N/A | N/A |
| .items[].cnc.ipv6.ip | Indicator.Value | IPv6 Address | .items[].dateBegin | N/A | N/A |
| .items[].cnc.ipv6.provider | Indicator.Attribute | Provider | .items[].dateBegin | N/A | N/A |
| .items[].cnc.ipv6.region | Indicator.Attribute | Region | .items[].dateBegin | N/A | N/A |
| .items[].cnc.url | Related Indicator.Value | URL | .items[].dateBegin | N/A | N/A |
| .items[].evaluation.admiraltyCode | Indicator/Malware/Adversary.Attribute | Admiralty Code | .items[].dateBegin | A2 | Updatable |
| .items[].evaluation.credibility | Indicator/Malware/Adversary.Attribute | Credibility | .items[].dateBegin | 90 | Updatable |
| .items[].evaluation.reliability | Indicator/Malware/Adversary.Attribute | Reliability | .items[].dateBegin | 90 | Updatable |
| .items[].evaluation.severity | Indicator/Malware/Adversary.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/Malware/Adversary.Attribute | Time to live (days) | .items[].dateBegin | 30 | Updatable |
| .items[].malware.name | Malware.Value | N/A | .items[].dateBegin | Bootnet | N/A |
| .items[].messageLink | Indicator/Malware/Adversary.Attribute | Message Link | .items[].dateBegin | N/A | N/A |
| .items[].portalLink | Indicator/Malware/Adversary.Attribute | Source Link | .items[].dateBegin | https://tap.group-ib.com/attacks/ddos?searchValue=id:053e63f81d0e1ebef83b0d3a5cbfebbe1a2b28a7 | N/A |
| .items[].protocol | Indicator/Malware/Adversary.Attribute | Protocol | .items[].dateBegin | udp | N/A |
| .items[].target.ipv4.asn | Related Indicator.Attribute | ASN | .items[].dateBegin | AS3223 Voxility S.R.L. | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | |
|---|---|---|---|---|---|
| .items[].target.ipv4.city | Related Indicator.Attribute | City | .items[].dateBegin | London | N/A |
| .items[].target.ipv4.countryCode | Related Indicator.Attribute | Country Code | .items[].dateBegin | GB | N/A |
| .items[].target.ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateBegin | United Kingdom | N/A |
| .items[].target.ipv4.ip | Related Indicator.Value | IP Address | .items[].dateBegin | 185.82.99.18 | N/A |
| .items[].target.ipv4.provider | Related Indicator.Attribute | Provider | .items[].dateBegin | Net 360 S.a.r.l | N/A |
| .items[].target.ipv4.region | Related Indicator.Attribute | Region | .items[].dateBegin | London, City of | N/A |
| .items[].target.url | Indicator.Value | URL | .items[].dateBegin | brot.net | N/A |
| .items[].target.category | Indicator/Malware/Adversary.Attribute | Category | .items[].dateBegin | N/A | N/A |
| .items[].target.port | Indicator/Malware/Adversary.Attribute | Port | .items[].dateBegin | 10913 | N/A |
| .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/Malware/Adversary.Attribute | Type | .items[].dateBegin | DNS Reflection | N/A |

# GroupIB Attacks Deface

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

```
GET https://tap.group-ib.com/api/v2/attacks/deface/updated
```

**Sample Response:**


```
{
    "count": 100,
    "items": [
        {
            "contacts": [],
            "date": "2023-05-10T11:17:43+00:00",
            "evaluation": {
                "admiraltyCode": "B2",
                "credibility": 80,
                "reliability": 80,
                "severity": "orange",
                "tlp": "amber",
                "ttl": 30
            },
            "id": "645b7fe87400cb001883f9b2",
            "portalLink": "https://tap.group-ib.com/attacks/deface?
searchValue=id:645b7fe87400cb001883f9b2",
            "seqUpdate": 1683718118053866,
            "source": "www.zone-h.org",
            "targetDomain": "mandrill.steelcoat.co.in",
            "targetDomainProvider": null,
            "targetIp": {
                "asn": null,
                "city": "Scottsdale",
                "countryCode": null,
                "countryName": "United States",
                "ip": "184.168.108.77",
                "provider": null,
                "region": null
            },
            "threatActor": {
                "country": null,
                "id": "be2da8bce084d842dedb59b2ecf079cbba091cdf",
                "isAPT": false,
                "name": "Mr.Pr4x0r"
```

```
            },
            "url": "http://mandrill.steelcoat.co.in/FCH.php"
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].url | Indicator.Value | URL | .items[].date | http://httpswwwalibaba.com-spma2700homeloginngnsdc.steelcoat.co.in/FCH.php | N/A |
| .items[].evaluation.admiraltyCode | Indicator/Adversary.Attribute | Admiralty Code | .items[].date | B2 | Updatable |
| .items[].evaluation.credibility | Indicator/Adversary.Attribute | Credibility | .items[].date | 80 | Updatable |
| .items[].evaluation.reliability | Indicator/Adversary.Attribute | Reliability | .items[].date | 80 | Updatable |
| .items[].evaluation.severity | Indicator/Adversary.Attribute | Severity | .items[].date | orange | Updatable |
| .items[].evaluation.tlp | Indicator/Adversary.TLP | Traffic Light Protocol | .items[].date | amber | N/A |
| .items[].evaluation.ttl | Indicator/Adversary.Attribute | Time to live (days) | .items[].date | 30 | Updatable |
| .items[].portalLink | Indicator/Adversary.Attribute | Source Link | .items[].dateBegin | https://tap.group-ib.com/attacks/deface?searchValue=id:645b7ff97400cb001883f9bf | N/A |
| .items[].targetIp.ip | Related Indicator.Value | IP Address | .items[].date | 184.168.108.77 | N/A |
| .items[].targetIp.asn | Related Indicator.Attribute | ASN | .items[].date | N/A | N/A |
| .items[].targetIp.city | Related Indicator.Attribute | City | .items[].date | Scottsdale | N/A |
| .items[].targetIp.countryCode | Related Indicator.Attribute | Country Code | .items[].date | N/A | N/A |
| .items[].targetIp.countryName | Related Indicator.Attribute | Country Name | .items[].date | United States | N/A |
| .items[].targetIp.provider | Related Indicator.Attribute | Provider | .items[].date | N/A | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .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 Malware Report

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

```
GET https://tap.group-ib.com/api/v2/malware/malware/updated
```

**Truncated 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": [],
        "malwareAliasList": [
            "BRATARAT"
        ],
        "mitreCount": 0,
        "name": "BRATA",
        "networkCount": 0,
        "networkIocList": [],
        "partCount": 0,
        "platform": [
            "Android"
        ],
        "platformOptions": [
```

```
                {
                    "label": "Android",
                    "value": "android"
                }
            ],
            "portalLink": null,
            "reportRating": null,
            "reportSeen": [
                "9498"
            ],
            "seenCount": 1,
            "seqUpdate": 16563360102488,
            "shortDescription": "BRATA (Brazilian Android Rat) is an
Android Rat",
            "signatureCount": 0,
            "signatureList": [],
            "sourceCountry": [
                "BR",
                "IT"
            ],
            "stixGuid": null,
            "threatActorList": [
                {
                    "id": "19a0a76e206404e203b2e3f5cbebcd56d20ea473",
                    "isApt": false,
                    "name": "Donot Team",
                    "url": ""
                }
            ],
            "threatLevel": "Medium",
            "threatLevelOptions": {
                "label": "Medium",
                "value": "Medium"
            },
            "updatedAt": "2023-04-23T20:04:17+03:00",
            "yaraCount": 0,
            "yaraRuleList": []
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].name | Malware.Value | N/A | .items[].history[0].date | BRATA | N/A |
| .items[].aliases | Malware.Tags | N/A | .items[].history[0].date | BRATARAT, Banking Trojan | Concatenated with .items[].category |
| .items[].category | Malware.Tags | N/A | .items[].history[0].date | BRATARAT, Banking Trojan | Concatenated with .items[].aliases |
| .items[].shortDescription | Malware.Description | N/A | .items[].history[0].date | BRATA (Brazilian Android Rat) is an Android Rat discovered in 2019. | N/A |
| .items[].geoRegion | Malware.Attribute | Region | .items[].history[0].date | america:south_america | N/A |
| .items[].langs | Malware.Attribute | Language | .items[].history[0].date | en | N/A |
| .items[].platform | Malware.Attribute | Operating System | .items[].history[0].date | Android | N/A |
| .items[].sourceCountry | Malware.Attribute | Source Country | .items[].history[0].date | BR | N/A |
| .items[].threatLevel | Malware.Attribute | Threat Level | .items[].history[0].date | Medium | N/A |
| .items[].attachedFile[].hash | Related Indicator.Value | SHA-256 | .items[].history[0].date | dd28c28bcbafa605febc2b3b9a8<br>ccd23ebfedf126aa66a72e598d3<br>05bd55bdd4 | N/A |
| .items[].attachedFile[].size | Related Indicator.Attribute | File Size | .items[].history[0].date | 173847 | N/A |
| .items[].threatActorList[].name | Related Adversary.Value | N/A | .items[].history[0].date | Donot Team | N/A |

# GroupIB Malware Signature, GroupIB Malware YARA Rule

The Group IB Malware Signature and Malware YARA Rule feeds ingest Events and any related Malware.

**GroupIB Malware Signature** - `GET https://tap.group-ib.com/api/v2/malware/signature/updated`

**GroupIB Malware Yara Rule** - `GET https://tap.group-ib.com/api/v2/malware/yara/updated`

**(Truncated) Sample Response:**


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


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].name | Signature.Name | Incident | .items[].createdAt | CURRENT_EVENTS Driveby bredolab hidden div served by nginx | N/A |
| .items[].class | Signature.Tags | N/A | .items[].createdAt | backdoor | N/A |
| .items[].content | Signature.Value | N/A | .items[].createdAt | alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:\"CURRENT_EVENTS Driveby bredolab hidden div served by nginx\"; | N/A |
| .items[].severity | Signature.Attribute | Severity | .items[].createdAt | 5 | Updatable |
| .items[].sourceName | Signature.Attribute | Source | .items[].createdAt | N/A | N/A |
| .items[].malware[].name | Related Malware.Value | N/A | .items[].createdAt | Bredolab | N/A |
| .items[].content | Signature.Attribute, Signature.Indicator, Signature.Tag | N/A | N/A | N/A | Context is parsed from the signature content (when enabled) |

# GroupIB Malware Vulnerability

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

```
GET https://tap.group-ib.com/api/v2/osi/vulnerability/updated
```

**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 feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].evaluation.admiraltyCode | Indicator/Vulnerability.Attribute | Admiralty Code | .items[].datePublished | A1 | 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.Attribute | Time to live (days) | .items[].datePublished | 30 | Updatable |
| .items[].title | Indicator/Vulnerability.Value | N/A | .items[].datePublished | CVE-2017-11197 | N/A |
| .items[].description | Indicator/Vulnerability.Description | N/A | .items[].datePublished | In CyberArk Viewfinity 5.5.10.95 and 6.x before 6.1.1.220, a low privilege user can escalate to an administrative | N/A |
| .items[].bulletinFamily | Indicator/Vulnerability.Attribute | Bulletin Family | .items[].datePublished | NVD | N/A |
| .items[].cvss.score | Indicator/Vulnerability.Attribute | CVSS Score | .items[].datePublished | 3.3 | Updatable |
| .items[].cvss.vector | Indicator/Vulnerability.Attribute | CVSS Vector | .items[].datePublished | II:P/RC:UR/AC:L/AU:M/AV:N/E:ND/CI:N/AI:N/RL:ND | N/A |
| .items[].extCvss.base | Indicator/Vulnerability.Attribute | CVSS Base Score | .items[].datePublished | 2.4 | Updatable |
| .items[].extCvss. | Indicator/Vulnerability.Attribute | CVSS Environmental Score | .items[].datePublished | 0 | Updatable |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| environmental | | | | | |
| .items[].extCvss.exploitability | Indicator/Vulnerability.Attribute | CVSS Exploitability Subscore | .items[].datePublished | 1.0 | Updatable |
| .items[].extCvss.impact | Indicator/Vulnerability.Attribute | CVSS Impact Subscore | .items[].datePublished | 1.5 | Updatable |
| .items[].extCvss.mImpact | Indicator/Vulnerability.Attribute | CVSS Modified Impact Subscore | .items[].datePublished | 0.0 | Updatable |
| .items[].extCvss.overall | Indicator/Vulnerability.Attribute | CVSS Overall Score | .items[].datePublished | 2.4 | Updatable |
| .items[].extCvss.temporal | Indicator/Vulnerability.Attribute | CVSS Temporal Score | .items[].datePublished | 2.4 | Updatable |
| .items[].exploitCount | Indicator/Vulnerability.Attribute | Exploit count | .items[].datePublished | 1 | Updatable |
| .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 softwareType, |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| | | | | | software Name and software Version |
| .items[].affected Software | Indicator/ Vulnerability.Attribute | Software | .items[].date Published | shrimptest version: 1.0b3 | Concatenate software Type, software Name and software Version |
| .items[].reporter | Related Identity.Value | N/A | .items[].date Published | cve@mitre.org | N/A |
| .items[].cveList | Related Indicator/ Vulnerability.Value | N/A | .items[].date Published | CVE-2019-11068 | N/A |

# GroupIB Attacks Phishing

The GroupIB Attacks Phishing feed ingests Indicator objects.

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

**Sample Response:**


```
{
  "count": 12,
  "items": [
    {
        "dateBlocked": "2019-03-21T05:53:05+00:00",
        "dateDetected": "2019-03-20T08:46:36+00:00",
        "evaluation": {
            "admiraltyCode": "A2",
            "credibility": 80,
            "reliability": 90,
            "severity": "red",
            "tlp": "amber",
            "ttl": 30
        },
        "history": [
            {
                "date": "2019-03-20T08:47:54+00:00",
                "field": "Detected",
                "reason": null,
                "reporter": "Group-IB Intelligence",
                "value": "In response"
            },
            {
                "date": "2019-03-21T07:46:51+00:00",
                "field": "Status has been changed",
                "reason": null,
                "reporter": "Group-IB Intelligence",
                "value": "In response"
            }
        ],
        "id": "fb2c54adc40a6cc1dbe5ad9771c9787db4fabb64",
        "ipv4": {
            "asn": "AS43260",
            "city": null,
            "countryCode": "CY",
            "countryName": "Cyprus",
            "ip": "185.71.216.171",
            "provider": null,
            "region": "AS"
        },
        "isFavourite": false,
        "isHidden": false,
        "objective": "Card harvest",
```

```
        "oldId": "1331",
        "phishingDomain": {
            "domain": "kdrbilisim.com",
            "local": "kdrbilisim.com",
            "dateRegistered": "2012-09-09 13:03:26",
            "title": "ANKARA BİLGİSAYAR TEKNİK SERVİS 0312 226 50 40 | 0312 226 50
40",
            "registrar": "PDR Ltd. d/b/a PublicDomainRegistry.com"
        },
        "portalLink": "https://tap-demo.group-ib.com/attacks/phishing?
searchValue=id:fb2c54adc40a6cc1dbe5ad9771c9787db4fabb64",
        "seqUpdate": 1553180722582,
        "status": "In response",
        "targetBrand": "Bank of America",
        "targetCategory": "Finance & Investment",
        "targetCountryName": null,
        "targetDomain": "bankofamerica.com",
        "type": "Phishing",
        "url": "https://www.kdrbilisim.com/Boa"
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].evaluation.admiraltyCode | Indicator.Attribute | Admiralty Code | .items[].dateDetected | A2 | Updatable |
| .items[].evaluation.credibility | Indicator.Attribute | Credibility | .items[].dateDetected | 80 | 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 Object.TLP | Traffic Light Protocol | .items[].dateDetected | amber | N/A |
| .items[].evaluation.ttl | Indicator.Attribute | Time to live (days) | .items[].dateDetected | 30 | Updatable |
| .items[].ipv4.asn | Related Indicator.Attribute | ASN | .items[].dateDetected | AS43260 | N/A |
| .items[].ipv4.city | Related Indicator.Attribute | City | .items[].dateDetected | N/A | N/A |
| .items[].ipv4.countryCode | Related Indicator.Attribute | Country Code | .items[].dateDetected | CY | N/A |
| .items[].ipv4.countryName | Related Indicator.Attribute | Country Name | .items[].dateDetected | Cyprus | N/A |

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

# GroupIB Attacks Phishing Group

The GroupIB Attacks Phishing Group feed ingests Indicators and Adversaries related to Phishing Attacks. The feed ingests all the attacks updated during the feed run time interval.

> The seqUpdate parameter is obtained by making a a call to: `https://tap.group-ib.com/api/v2/sequence_list?collection=attacks/phishing_groupANDdate=2024-09-01`.

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

**Request Parameters:**

```
{
  "seqUpdate": 1724632189898957,
  "limit": 100
}
```

**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": "11 Internet AG",
          "region": null
        }
      ],
      "objective": [
        "Login harvest"
      ],
      "phishingKitArray": [],
      "screenshot": {
        "pageHtml": {
          "fileHashMd5": "a28d22149f080eb037b2b3eb66631358",
          "filename": "phishing_screen/
c9975a1cd65becbfb3b10c9d05e39ee9970a32b13d8d88f72fed4b3122b82dfa",
          "filetype": "pageHtml",
          "hashSha256":
"c9975a1cd65becbfb3b10c9d05e39ee9970a32b13d8d88f72fed4b3122b82dfa",
          "mime": "text/html"
        },
```

```
        "pageScreen": {
          "fileHashMd5": "ce04341e8047b76f0479027a18d84891",
          "filename": "phishing_screen/
7e15cd3290770ad218b8256b5875f14563c48feee8ccd3c8dd6d3645831e3042",
          "filetype": "pageScreen",
          "hashSha256":
"7e15cd3290770ad218b8256b5875f14563c48feee8ccd3c8dd6d3645831e3042",
          "mime": "image/jpeg"
        }
      },
      "seqUpdate": 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 feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].evaluation.admiraltyCode | Indicator.Attribute | Admiralty Code | .items[].date.detected | C3 | 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 | N/A |
| .items[].domainInfo.registered | Indicator.Attribute | Register Date | .items[].date.detected | 2022-07-04 14:58:08+00:00 | N/A |
| .items[].domainInfo.expirationDate | Indicator.Attribute | Expiration Date | .items[].date.detected | 2023-07-04 14:58:08+00:00 | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].domainInfo.registrar | Indicator.Attribute | Registrar | .items[].date.detected | GoDaddy.com, LLC | N/A |
| .items[].domainInfo.tld | Indicator.Attribute | Top-level domain | .items[].date.detected | io | N/A |
| .items[].source | Indicator.Attribute | Source | .items[].date.detected | urlscan | N/A |
| .items[].domain | Indicator.Value | FQDN | .items[].date.detected | traderspirits.io | N/A |
| .items[].threatActor.name | Related Adversary.Name | N/A | .items[].date.detected | N/A | N/A |
| .items[].threatActor.country | Related Adversary.Attribute | Country | .items[].date.detected | N/A | N/A |

# GroupIB Attack Phishing Kit

The GroupIP Attack Phishing Phishing Kit feed ingests Indicator objects.

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

**Sample Response:**


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

```
      "seqUpdate": 1553191374631,
      "targetBrand": [
        "Bank of America"
      ],
      "tsFirstSeen": null,
      "tsLastSeen": null,
      "variables": null
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].emails[] | Related Indicator.Value | Email Address | items[].dateDetected | jimjag@gmail.com | N/A |
| .items[].downloadedFrom[].phishingUrl | Related Indicator.Value | URL | items[].dateDetected | N/A | N/A |
| .items[].downloadedFrom[].url | Related Indicator.Value | URL | items[].dateDetected | hxxps://gt-mywyty186338.codeanyapp.com/cb.zip | N/A |
| .items[].downloadedFrom[].domain | Related Indicator.Value | FQDN | items[].dateDetected | gt-mywyty186338.codeanyapp.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/SHA-1/SHA-256/SHA-384/SHA-512 | items[].dateDetected | 6b27ae3d9fee257551d4c480360fd762 | N/A |
| .items[].targetBrand[] | Indicator.Attribute | Target Brand | items[].dateDetected | Bank of America | N/A |

# GroupIB OSI PublicLeak

The GroupIB OSI PublicLeak feed ingests Indicator objects.

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

**Request Parameters**

```
{
  "seqUpdate": "1632736036790688",
  "limit": "100",
  "applyhunting_rules": "1"
}
```

**Sample Response:**

```
{
  "count": 18138702,
  "items": [
    {
      "bind": [],
      "created": "2021-09-27T12:47:16+03:00",
      "data": "<!--/**\n * GeSHi (C) 2004 - 2007 Nigel McNie, 2007 -
2008 Benny Baumann\n * (http://qbnz.com/highlighter/ and http://
geshi.org/)\n */\n.java  {font-family:monospace;color:
#000066;}\n.java a:link {color: #000060;}\n.java a:hover {background-
color: #f0f000;}\n.java .head {font-family: Verdana, Arial, sans-
serif; color: #808080; font-size: 70%; font-weight: bold;  padding:
2px;}\n.java .imp {font-weight: bold; color: red;}\n.java .kw1
{color: #000000; font-weight: bold;}\n.java .kw2 {color: #000066;
font-weight: bold;}\n.java .kw3 {color: #003399;}\n.java .kw4 {color:
#000066; font-weight: bold;}\n.java .co1 {color: #666666; font-style:
italic;}\n.java .co2 {color: #006699;}\n.java .co3 {color: #008000;
font-style: italic; font-weight: bold;}\n.java .coMULTI {color:
#666666; font-style: italic;}\n.java .es0 {color: #000099; font-
weight: bold;}\n.java .br0 {color: #009900;}\n.java .sy0 {color:
#339933;}\n.java .st0 {color: #0000ff;}\n.java .nu0 {color: #cc66cc;}
\n.java .me1 {color: #006633;}\n.java .me2 {color: #006633;}\n.java
span.xtra { display:block; }\n.ln, .ln{ vertical-align: top; }
\n.coMULTI, .java span{ line-height:13px !important;}\n-->/* package
whatever; // don't place package name! */\n \nimport java.util.*;
\nimport java.lang.*;\nimport java.io.*;\n \n/* Name of the class has
to be \"Main\" only if the class is public. */\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\">Except
ion</a>\n\t{\n\t\t<a href=\"http://www.google.com/search?
hl=en&q=allinurl%3Adocs.oracle.com+javase+docs+api+system\">System</
a>.out.println(\"A13V1IB3VIYZZH\".length());\n\t}\n}",
      "displayOptions": null,
      "evaluation": {
        "admiraltyCode": "C3",
        "credibility": 50,
        "reliability": 50,
        "severity": "green",
        "tlp": "amber",
        "ttl": 30
      },
      "hash": "db0cd0519335470b6ae614ccbe65ef358b93b349",
      "id": "db0cd0519335470b6ae614ccbe65ef358b93b349",
      "language": "",
      "linkList": [
        {
          "author": "",
          "dateDetected": "2021-09-27T12:47:16+03:00",
          "datePublished": "2021-09-27T11:46:51+03:00",
          "hash": "60df36b3bf7abcb5e540e68fc3193cecb724814e",
          "itemSource": "link",
          "link": "http://ideone.com/4XU0fh",
          "sequenceUpdate": null,
          "size": 1767,
          "source": "ideone.com",
          "status": 1,
          "title": ""
        }
      ],
      "matches": {
                "email": {
                    "email": [
                        "somesampleemail@mail.ru"
                    ]
                }
            },
      "oldId": null,
```

```
      "portalLink": "https://tap.group-ib.com/osi/public_leak?
searchValue=id:db0cd0519335470b6ae614ccbe65ef358b93b349",
      "seqUpdate": 1632736036790689,
      "size": "1,73 KB",
      "updated": "2021-09-27T12:47:16+03:00",
      "useful": 1
    }
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | |
|---|---|---|---|---|---|
| .items[].bind[].key | Related Indicator.Value | FQDN | .items[].created | mail.ru | 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 |
| .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 |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | |
|---|---|---|---|---|---|
| .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[].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 |
| .items[].size | Indicator.Attribute | Size | .items[].created | 1,29 KB | N/A |

# GroupIB IOC Common

The GroupIB IOC Common feed ingests Indicators and Malware.

```
GET https://tap.group-ib.com/api/v2/ioc/common/updated
```

**Sample Response:**


```
{
  "count": 46781,
  "items": [
    {
      "id": "9518c854e6c1f59fd12089cfe9ed078a22977dc0",
      "type": "file",
      "dateFirstSeen": "2023-04-02T00:00:00+03:00",
      "dateLastSeen": "2023-04-02T00:00:00+03:00",
      "seqUpdate": 16803953345526,
      "hash": [
        "4adf0249073c4e0d022823ee61ce002c",
        "1e37ae9a6d1ad9767b1510ceac2074764667d9bf",

"cc6cefaacbdce7b595169106f2109afeabf6b24c7325663526162O2f2010d689"
      ],
      "malwareList": [
        {
          "name": "DCRat",
          "aliases": [
            "DarkCrystal"
          ]
        }
      ],
      "threatList": null
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].hash[] | Indicator.Value | MD5/SHA-1/SHA-256 | .items[].dateFirstSeen | '4adf0249073c4e0d022823ee61ce002c' | The type of the indicator is determined by its length |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].ip[] | Indicator.Value | IP Address | .items[]/dateFirstSeen | N/A | N/A |
| .items[].domains[] | Indicator.Value | FQDN | .items[]/dateFirstSeen | N/A | N/A |
| .items[].type | Indicator.Attribute | Type | .items[].dateFirstSeen | 'file' | N/A |
| .items[].dateFirstSeen | Indicator.Attribute | Date First Seen | .items[].dateFirstSeen | '2023-04-02 00:00:00+03:00' | N/A |
| .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 Open Threats

The GroupIB Open Threats feed ingests Open Threat records as Report objects and adds related Indicators, Malware, Adversaries, Tags, and CVEs. CVEs are ingested as Indicators and/or Vulnerabilities according to the Save CVE Data as selection. Open Threat Indicators default to the Review status because the collection contains public-source data.

```
GET https://tap.group-ib.com/api/v2/hi/open_threats/updated
```

**Sample Response:**


```
{
  "count": 1,
  "seqUpdate": 1664217109400513,
  "items": [
    {
      "id": "4b5f9b40d0207d32412338000bbb24b4a7eb4397",
      "title": "Example Open Threat Report",
      "text": "Example Open Threat report text containing contextual
information about the reported threat.",
      "createdAt": "2026-09-30T08:00:00+00:00",
      "dateDetected": "2026-09-30T08:15:00+00:00",
      "updatedAt": "2026-09-30T08:30:00+00:00",
      "author": {
        "name": "Example Author",
        "profileUrl": "https://example.com/profile",
        "screenName": "example_author",
        "userId": "123456789"
      },
      "evaluation": {
        "admiraltyCode": "B3",
        "credibility": 50,
        "reliability": 50,
        "severity": "green",
        "tlp": "white",
        "ttl": 0
      },
      "data": {
        "countries": [{"country": "United States", "countryCode":
"US"}],
        "companyTags": ["onlinesbi"],
        "cryptoWallets":
```

```
["bc1qexampleexampleexampleexampleexamplexxxxx"],
        "cve": ["CVE-2019-11068"],
        "domains": ["sturtevantinc.xyz"],
        "emails": ["test@threatq.com"],
        "files": [{"name": "index.php", "md5":
"ae23f779e9c36219f83bf8ea2e74f662"}],
        "hashes":
["5cf5afc22dfa08252e990c9e3fc51e287ff54dc53742767a7428dc31b25dd606"],
        "ip": ["146.19.191.138"],
        "malware": [{"id":
"10ba3e1b85d8e2f72560f6917b5d428cd740af40", "name": "bashlite",
"threatLevel": "None"}],
        "pdbPaths": ["C:\\build\\example\\client.pdb"],
        "rules": ["onlinesbi"],
        "tags": ["laundering", "ransomware"],
        "telegramApiKeys": null
      },
      "threatActors": [{"id":
"8c2a033b17f3a44d95c46e82bbadb90ee1752932", "name": "DarkStormTeam"}]
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].title | Report.Value | N/A | .items[].createdAt | Example Open Threat Report | Primary Report value. |
| .items[].text | Report.Description | N/A | .items[].createdAt | Example Open Threat report text... | Ingested when present. |
| .items[].id | Report.Attribute | Open Threat ID | .items[].createdAt | 4b5f9b40... | Provider record identifier. |
| .items[].createdAt | Report.Attribute | Created At | .items[].createdAt | 2026-09-30T08:00:00+00:00 | Also used as the Report published date. |
| .items[].updatedAt | Report.Attribute | Last Updated | .items[].createdAt | 2026-09-30T08:30:00+00:00 | Ingested when present. |
| .items[].dateDetected | Report.Attribute | Date Detected | .items[].createdAt | 2026-09-30T08:15:00+00:00 | The source has no equivalent end timestamp. |
| .items[].link | Report.Attribute | Source Link | .items[].createdAt | https://example.com/research/example-open-threat | Ingested when present. |
| .items[].original | Report.Attribute | Original Source URL | .items[].createdAt | https://example.com/research/example-open-threat | Ingested when present. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].source | Report.Attribute | Source | .items[].createdAt | example.com | Ingested when present. |
| .items[].sourceType | Report.Attribute | Source Type | .items[].createdAt | Blog | Ingested when present. |
| .items[].author.name | Report.Attribute | Author Name | .items[].createdAt | Example Author | Ingested when non-empty. |
| .items[].author.profileUrl | Report.Attribute | Author Profile URL | .items[].createdAt | https://example.com/profile | Ingested when non-empty. |
| .items[].author.screenName | Report.Attribute | Author Screen Name | .items[].createdAt | example_author | Ingested when non-empty. |
| .items[].author.userId | Report.Attribute | Author User ID | .items[].createdAt | 123456789 | Ingested when non-empty. |
| .items[].evaluation.tlp | Report | TLP | .items[].createdAt | white | Sets the Report TLP. |
| .items[].evaluation.admiraltyCode | Report.Attribute | Admiralty Code | .items[].createdAt | B3 | Updatable. |
| .items[].evaluation.credibility | Report.Attribute | Credibility | .items[].createdAt | 50 | Numeric zero is retained when present. |
| .items[].evaluation.reliability | Report.Attribute | Reliability | .items[].createdAt | 50 | Numeric zero is retained when present. |
| .items[].evaluation.severity | Report.Attribute | Severity | .items[].createdAt | green | Updatable. |
| .items[].evaluation.ttl | Report.Attribute | Time to live (days) | .items[].createdAt | 0 | Numeric zero is retained when present. |
| .items[].data.countries[].country | Report.Attribute | Country | .items[].createdAt | United States | The Open Threat field contains country objects. |
| .items[].data.countries[].countryCode | Report.Attribute | Country Code | .items[].createdAt | US | ISO 3166-1 alpha-2 code. |
| .items[].data.companyTags[] | Report.Attribute | Company Tag | .items[].createdAt | onlinesbi | Preserved separately from Report Tags. |
| .items[].data.cryptoWallets[] | Report.Attribute | Cryptocurrency Wallet | .items[].createdAt | bc1qexample... | Context only; not a direct Indicator. |
| .items[].data.pdbPaths[] | Report.Attribute | PDB Path | .items[].createdAt | C:\\build\\example\\client.pdb | Context only; not a direct Indicator. |
| .items[].data.rules[] | Report.Attribute | Security Rule | .items[].createdAt | onlinesbi | Context only; no Signature is created. |
| .items[].data.tags[] | Tag.Name | N/A | .items[].createdAt | ransomware | Related to the Report. |
| .items[].threatActors[].name | Related Adversary.Name | N/A | .items[].createdAt | DarkStormTeam | Ingested when present. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .items[].threatActors[].id | Related Adversary.Attribute | Threat Actor ID | .items[].createdAt | 8c2a033b... | Applied to the related Adversary. |
| .items[].data.malware[].name | Related Malware.Value | N/A | .items[].createdAt | bashlite | Ingested when present. |
| .items[].data.malware[].id | Related Malware.Attribute | Malware ID | .items[].createdAt | 10ba3e1b... | Applied to the related Malware. |
| .items[].data.malware[].threatLevel | Related Malware.Attribute | Threat Level | .items[].createdAt | high | Applied when present. |
| .items[].data.malware[].platform | Related Malware.Attribute | Platform | .items[].createdAt | Windows | Applied when present. |
| .items[].data.malware[].category | Related Malware.Attribute | Category | .items[].createdAt | Trojan | Applied when present. |
| .items[].data.malware[].class | Related Malware.Attribute | Class | .items[].createdAt | Example | Applied when present. |
| .items[].data.cve[] | Related Indicator.Value and/or Related Vulnerability.Value | CVE | .items[].createdAt | CVE-2019-11068 | Controlled by Save CVE Data as. |
| .items[].data.domains[] | Related Indicator.Value | FQDN | .items[].createdAt | sturtevantinc.xyz | Ingested when present. |
| .items[].data.ip[] | Related Indicator.Value | IP Address | .items[].createdAt | 146.19.191.138 | The provider documents these as IPv4 values. |
| .items[].data.files[].md5 | Related Indicator.Value | MD5 | .items[].createdAt | ae23f779e9c36219f83bf8ea2e74f662 | Applied to the related file Indicator. |
| .items[].data.files[].sha1 | Related Indicator.Value | SHA-1 | .items[].createdAt | b74cf5c4b66e0de94875a6182fa40cdfa89096b9 | Applied to the related file Indicator. |
| .items[].data.files[].sha256 | Related Indicator.Value | SHA-256 | .items[].createdAt | 9c6a6d73ea89f2891cf33fe47cdef721e9688c8154f967dad741794be085e48b | Applied to the related file Indicator. |
| .items[].data.files[].name | Related Indicator.Attribute | File Name | .items[].createdAt | index.php | Applied to each related file-hash Indicator from the same file object. |
| .items[].data.hashes[] | Related Indicator.Value | Derived from hash length | .items[].createdAt | 5cf5afc2... | Recognized lengths map to MD5, SHA-1, SHA-256, SHA-384, or SHA-512. |

# Average Feed Run

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

## GroupIB Compromised Account

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

## GroupIB Compromised Bank Card

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

## GroupIB Compromised Data Mules

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

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

## GroupIB Compromised Data GIT Leaks

| METRIC | RESULT |
|---|---|
| **Run Time** | 2 minutes |
| **Indicators** | 3,720 |
| **Indicator Attributes** | 13,132 |
| **Identity** | 153 |
| **Identity Attributes** | 165 |

## GroupIB Compromised Data IMEI

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Adversaries** | 1 |
| **Adversary Attributes** | 1 |

| METRIC | RESULT |
|---|---|
| **IMEI** | 397 |
| **IMEI Attributes** | 4,006 |
| **Indicators** | 63 |
| **Indicator Attributes** | 286 |
| **Malware** | 3 |
| **Malware Attributes** | 3 |

## GroupIB Compromised Data Shops

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

## GroupIB Compromised IM Discord

| METRIC | RESULT |
|---|---|
| **Run Time** | 4 minutes |
| **Discord Channel** | 91 |

| METRIC | RESULT |
| --- | --- |
| **Discord Channel Attributes** | 91 |
| **Identities** | 72 |
| **Identity Attributes** | 333 |

## GroupIB Compromised IM Telegram

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Identities** | 17 |
| **Identity Attributes** | 34 |
| **Telegram Channel** | 55 |
| **Telegram Channel Attributes** | 342 |

## GroupIB Compromised Masked Bank Card

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

## GroupIB APT Threat

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

## GroupIB Human Malware C2

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Adversaries** | 19 |

| METRIC | RESULT |
|---|---|
| **Indicators** | 439 |
| **Indicator Attributes** | 152 |
| **Malware** | 18 |

## GroupIB Human Intelligence Threat Actor

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

## GroupIB Malware Configs

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Indicators** | 860 |
| **Indicator Attributes** | 767 |

| METRIC | RESULT |
| --- | --- |
| **Malware** | 21 |

## GroupIB Suspicious IP Tor Node

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

## GroupIB Suspicious IP Scanners

| METRIC | RESULT |
| --- | --- |
| **Run Time** | 37 minutes |
| **Indicators** | 29,571 |
| **Indicator Attributes** | 182,708 |

## GroupIB Suspicious IP VPN

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

## GroupIB Suspicious Payment Details

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Accounts** | 50 |
| **Account Attributes** | 200 |
| **Adversaries** | 50 |
| **Indicators** | 30 |
| **Cards** | 50 |
| **Malware** | 50 |

## GroupIB Attacks DDoS

| METRIC | RESULT |
|---|---|
| **Run Time** | 20 minutes |

| METRIC | RESULT |
|---|---|
| **Indicators** | 7,053 |
| **Indicator Attributes** | 73,807 |
| **Adversaries** | 2 |
| **Adversary Attributes** | 7 |
| **Malware** | 6 |
| **Malware Attributes** | 120 |

## GroupIB Attacks Deface

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Indicators** | 743 |
| **Indicator Attributes** | 3,852 |
| **Adversaries** | 36 |
| **Adversary Attributes** | 519 |

## GroupIB Malware Report

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |

| METRIC | RESULT |
|---|---|
| **Indicators** | 213 |
| **Indicator Attributes** | 213 |
| **Malware** | 38 |
| **Malware Attributes** | 309 |
| **Adversaries** | 16 |

## GroupIB Malware Signature

| METRIC | RESULT |
|---|---|
| **Run Time** | 13 hours 12 minutes |
| **Events** | 977,748 |
| **Event Attributes** | 977,801 |
| **Malware** | 725 |

## GroupIB Malware Yara Rule

| METRIC | RESULT |
|---|---|
| **Run Time** | 21 minutes |
| **Events** | 27,609 |
| **Event Attributes** | 27,820 |

| METRIC | RESULT |
| --- | --- |
| **Malware** | 237 |

## GroupIB Malware Vulnerability

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

## GroupIB Attacks Phishing

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 hour 34 minutes |
| **Indicators** | 61,898 |
| **Indicator Attributes** | 412,185 |

## GroupIB Attacks Phishing Group

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Indicators** | 516 |
| **Indicator Attributes** | 4,301 |

## GroupIB Attacks Phishing Kit

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Indicators** | 51 |
| **Indicator Attributes** | 72 |

## GroupIB OSI PublicLeak

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

# GroupIB IOC Common

| METRIC | RESULT |
|---|---|
| **Run Time** | 2 minutes |
| **Indicators** | 2,667 |
| **Indicator Attributes** | 5,334 |
| **Malware** | 55 |

# Known Issues / Limitations

- The maximum allowable range is 30 consecutive days. If a larger date range is selected, the feed will change the end date to start date plus 30 days.
- There is a known known issue with the GroupIB API that can cause a feed to ignore set date parameters.  This can cause more data to be returned, resulting in longer run times.
- **GroupIB Compromised IM Discord** and **GroupIB Compromised IM Telegram** feeds:
    - These feeds may ingest data that contains characters not supported by the database which results in the feed run finishing with a `500 Internal Error` error message.  This issue will be addressed in a future ThreatQ platform release.
    - These feeds may not append all messages to the description in the event that messages for one channel are split across multiple pages. This is because the messages from the previous page did not have enough time to be ingested into the platform.

# Change Log

- **Version 4.2.0**
  - Improved data retrieval for the **APT Threat Actor** and **Malware Signature** feeds by using the requested run date to identify and retrieve subsequent updates.
- **Version 4.1.0**
  - Added the **Group-IB Open Threats** feed that ingests Open Threat records as Reports, along with related Indicators, Malware, Adversaries, Tags, and CVEs.
  - The **Group-IB Compromised Data IMEI** feed now initializes through `sequence_list` and paginates the `/updated` endpoint using the top-level `seqUpdate` field instead of the `df` and `dt` parameters.
- **Version 4.0.0**
  - Updated the **GroupIB Human Intelligence Threat**, **GroupIB APT Threat**, **GroupIB Attacks DDoS**, **GroupIB Compromised Account**, and **GroupIB Suspicious Payment Details** feeds to improve incremental data retrieval and pagination.
  - Updated the **GroupIB Compromised Account** feed to use supported pagination parameters and retrieve up to 500 records per request.
  - Added indicator mappings for related client IPv6 addresses, IP addresses parsed from login data, and service IP addresses in the **GroupIB Compromised Account** feed.
- **Version 3.6.0**
  - Added a feed, **GroupIB Suspicious Payment Details,** that ingests suspicious payment records and their related context.
- **Version 3.5.6**
  - Added an **Ingest Threat Feeds As** configuration option to the **Group-IB Human Intelligence Threat** and **Group-IB APT Threat** feeds. By default, threat feeds are ingested as **Report** objects, with the option to ingest them as **Intrusion Set** objects instead.
- **Version 3.5.5**
  - Fixed date parameter formatting for the **GroupIB Attacks DDoS** feed by sending `df` and `dt` values in `YYYY-MM-DD` format, preventing HTTP 400 errors returned by the Group-IB API.

- Added support for report ingestion for **GroupIB Compromised Account** records.

- **Version 3.5.4 rev-a**
  - Guide Update - updated custom object installation steps for ThreatQ v6 instances.
- **Version 3.5.4**
  - Added a new configuration parameter for the **Group IB - Compromised Accounts** feed:
    - **Prepend Account** - enable this parameter to add the text string `Account` to the beginning of a compromised account value.
- **Version 3.5.3**
  - Added a new configuration parameter, **Apply Hunting Rules**, to the **GroupIB OSI Public Leak** feed. This enables you to include the `applyhunting_rules` parameter to the feed's request.
  - Added the following new configuration parameters to all feeds:
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determine if the feed should honor proxy settings set in the ThreatQ UI.
- **Version 3.5.2**
  - GroupIB Malware C2 feed - resolved a `Filter-Mapping` issue that could occur when certain keys were not present in the API response.
- **Version 3.5.1**
  - Added two new required custom objects utilized by the **Group IB Compromised IM Discord** and **Group IB Compromised IM Telegrams** feeds:
    - Telegram Channel
    - Discord Channel
  - The **Group IB Compromised IM Discord** and **Group IB Compromised IM Telegrams** feeds now add the content of the messages to the description of ThreatQ objects.
- **Version 3.5.0**
  - Made the following updates to the **Group IB Malware Signature** and **Group IB Malware Yara Rule** feeds:
    - intelligence from these feeds will now be ingested as Signature objects.  Prior to version 3.5.0, the intelligence was ingested as ThreatQ Events.

        - users can now parse the Signatures from these feeds for further context such as attributes and relationships.
    - The **Group IB Attacks Phishing Kit** feed can now ingest multiple hash types and phishing URLs.
    - The **Group IB Malware Vulnerability** feed now ingests related CVEs.
- **Version 3.4.9**
    - GroupIB OSI PublicLeak feed - long descriptions are now truncated.
    - GroupIB IOC Common feed - additional indicators subtypes have been added: `.items[].ip[]` (IP Address) and `.items[]domain` (FQDN).
- **Version 3.4.8**
    - Resolved an issue regarding the parsing of `First Message Date` and `Last Message Date` for the **GroupIB Compromised IM Telegram** feed.
    - The **GroupIB Attacks Phishing Group** feed has been updated to ingest all updated entries.
- **Version 3.4.7**
    - Resolved a Filter-Mapping error that would occur with the GroupIB Human Intelligence Threat feed when the `evaluation` field is not present in API response.
- **Version 3.4.6**
    - Optimized the date format used by **GroupIB Compromised IM Telegram feed** to prevent `ServerDisconnected` errors.
- **Version 3.4.5**
    - Updated the **GroupIB Compromised Account** feed to reflect updates to the GroupIB API schema.
- **Version 3.4.4**
    - GroupIB Compromised Account feed - resolved a filter mapping issue when the ipv4 is not present in the API response.
- **Version 3.4.3**
    - Updated the authentication method from headers to basic authentication.
    - Unicode special characters  not supported by the ThreatQ database engine are no longer ingested.
- **Version 3.4.2**
    - Resolved a Filter Mapping issue with the Group-IB Malware Vulnerability feed.
- **Version 3.4.1**

- Existing attributes regarding data confidence levels will now be updated.
- Resolved an issue regarding the measurement unit for the Time to Live attribute.
- Re-enabled the GroupIB Compromised Account feed.
- Added the following feeds:
  - GroupIB Compromised Bank Card
  - GroupIB Compromised IM Discord
  - GroupIB Compromised IM Telegram
  - GroupIB Compromised Masked Bank Card
- Removed the GroupIB Malware Targeted Malware feed as it has been deprecated by the provider.
- Updated the Known Issues / Limitations chapter regarding an issue with the Compromised IM Discord and Compromised IM Telegram feeds.
- Updated minimum ThreatQ version to 5.20.0.

- **Version 3.4.0**
  - Added a delay for requests and extra retries (with delay) when encountering 429 errors.
  - Updated the minimum ThreatQ version to 5.19.0.
- **Version 3.3.0**
  - Added the following feeds:
    - GroupIB Compromised Data Shops
    - GroupIB Malware Configs
    - GroupIB Suspicious IP VPN
    - GroupIB Suspicious IP Scanners
    - GroupIB Attacks Deface
    - GroupIB Malware Report
    - GroupIB Malware Signature
    - GroupIB Malware YARA Rule
    - GroupIB Vulnerability
    - GroupIB Attacks Phishing Group
    - GroupIB Attacks Abuse Phishing Kit
    - GroupIB IOC Common

    - Removed the following feeds:
        - GroupIB Brand Abuse Phishing
        - GroupIB Brand Abuse Phishing Kit
        - GroupIB Compromised Data Darkweb
        - GroupIB Compromised Account
        - GroupIB Compromised Card
    - Added pagination.
    - Added support for Start and End date parameters. See the Known Issues / Limitations chapter for more details.
- **Version 3.2.0**
    - Updated the integration to use the new Group-IB endpoints, `tap.group.ib.com`. The previous endpoints, `bt.group-ib.com`, have been deprecated.
    - Removed deprecated endpoint: GroupIB Compromised Data Files.
- **Version 3.1.0**
    - GroupIB APT Threat Actor and Human Intelligence Threat Actors will now ingest data from the feed as Intrusion Sets opposed to Reports.
    - New attributes, Compromised Data and Source Link, have been added to the following feeds: GroupIBCompromised Account, Compromised Card, Compromised Data Files.
- **Version 3.0.0 rev-b**
    - Guide Update - Updated the custom object installation instructions in the Prerequisites chapter.
- **Version 3.0.0**
    - Added new endpoints to the CDF:
        - GroupIB Compromised Data Darkweb
        - GroupIB OSI PublicLeak
        - GroupIB Compromised Data Files
        - GroupIB Brand Abuse Phishing
        - GroupIB Brand Abuse Phishing Kit
- **Version 2.1.0**
    - Added new endpoints to the CDF. These new endpoints require the installation of additional custom objects: Compromised Account and Compromised Card. See the Prerequisites section for more details.

- **Version 2.0.0**
  - Initial release