GROUP-IB

Threat intelligence

# Web portal manual

# Sequence List

**Summary**

Disclaimer: This is an endpoint-specific documentation. For common information including Authentication, Response Status Codes, Rate Limits, Additional Notes, and Troubleshooting, please refer to related articles in Integrations.

This endpoint retrieves a list of sequence update numbers for all available collections based on a specified date. This is useful for determining the starting seqUpdate value when you want to begin iterating through feeds from a specific date, rather than starting from the beginning (seqUpdate=0).

**Collection-Specific Information**

| Property | Value |
|---|---|
| Method | GET |
| Path | /api/v2/sequence_list |
| Collection Name | Sequence List |
| Type | Utility |
| Rate Limit | 1 request per second per company per feed (see API Limitations) |
| Short Description | Utility endpoint to retrieve sequence update numbers for all collections based on a specific date. |

**Request**

**Request URL**
GET /api/v2/sequence_list
**Query Parameters**

| Parameter | Type | Required | Default | Description | Example |
|---|---|---|---|---|---|
| date | string | Yes | - | Date for which the sequence list is requested. Format: YYYY-MM-DD | 2024-10-14 |

| Parameter | Type | Required | Default | Description | Example |
|---|---|---|---|---|---|
| collection | string | No | - | Optional collection name to filter results for a specific collection. If provided, returns only the sequence update number for that collection. | apt/threat |

Query Parameter Details:

- date:
  - Required parameter
  - Format: YYYY-MM-DD (e.g., 2024-10-14)
  - Returns sequence update numbers for all collections as of this date
- collection:
  - Optional parameter
  - If specified, returns only the sequence update number for the specified collection
  - Collection name format: module/submodule (e.g., apt/threat, malware/malware)

**Request Headers**

| Header | Type | Required | Description | Example |
|---|---|---|---|---|
| Accept | string | No | Content type accepted by the client | application/json |
| Authorization | string | Yes | Basic authentication credentials (see Initial Steps) | Basic base64(LOGIN:API_KEY) |
| User-Agent | string | No | User-Agent string with product metadata (optional but recommended - especially useful in troubleshooting on our end). Format: ////_ | SIEM/QRadar_2020.10.6/GroupIB_TI_1.0.0/gibuser@group-ib.com/cyberintegrations_0.13.1 |

**Response**

Note: For response status codes and error handling, see Troubleshooting and Error Codes.

**Response Headers**

| Header | Description | Example |
|---|---|---|
| Content-Type | Response content type | application/json |
| Content-Encoding | Content encoding | gzip |
| Cache-Control | Cache control directives | no-cache, private |
| Allow | Allowed HTTP methods | GET |

**Response Body Schema**

**Root Object**
{ "list": { "collection_name": integer, ... } }

| Field | Type | Required | Description |
|---|---|---|---|
| list | object | Yes | Object containing collection names as keys and their corresponding sequence update numbers as values |

**List Object**

The list object contains key-value pairs where: - Key: Collection name (e.g., "apt/threat", "malware/malware", "suspicious_ip/vpn") - Value: Sequence update number (integer) for that collection as of the specified date

Example structure:
{ "list": { "apt/threat": 17287776262152, "apt/threat_actor": 17286912357507, "attacks/ddos": 1728853572756170, "malware/malware": 17287232595059, "suspicious_ip/vpn": 1728863618842723 } }
**Example Request**

**Basic Request (All Collections)**
curl -X GET 'https://tap.group-ib.com/api/v2/sequence_list?date=2024-10-14' \ -u 'LOGIN:API_KEY' \ -H 'Accept: application/json'
**Request for Specific Collection**
curl -X GET 'https://tap.group-ib.com/api/v2/sequence_list?date=2024-10-14&collection=apt/threat' \ -u 'LOGIN:API_KEY' \ -H 'Accept: application/json'
**Example Response**

**Success Response (200 OK) - All Collections**
{ "list": { "apt/threat": 17287776262152, "apt/threat_actor": 17286912357507, "attacks/ddos": 1728853572756170, "attacks/deface": 1728159944011312, "attacks/phishing_group": 1728863999999999, "attacks/phishing_kit": 1728861626744927, "compromised/account_group": 1720706185734061, "compromised/bank_card_group": 1719857916092329, "compromised/masked_card": 1728845300540036, "compromised/messenger": 1728853200000000, "compromised/discord": 1727905789379160, "hi/threat": 17288283676769, "hi/threat_actor": 17288283685184, "hi/open_threats": 1728834812506702, "ioc/common": 17288526154476, "malware/cnc": 1728777672644977, "malware/config": 17288510093459, "malware/malware": 17287232595059, "malware/signature": 17288479212942, "malware/yara": 17219413666444, "osi/git_repository": 1728734319944338, "osi/public_leak": 1728863904288975, "osi/vulnerability": 17288546508036, "suspicious_ip/open_proxy": 1728863532650054, "suspicious_ip/scanner": 1728863423033642,

"suspicious_ip/socks_proxy": 1728863966244699, "suspicious_ip/tor_node": 1728846278012000, "suspicious_ip/vpn": 1728863618842723 } }

**Success Response (200 OK) - Specific Collection**

If the collection parameter is provided, the response will contain only that collection:

{ "list": { "apt/threat": 17287776262152 } }

**Usage Patterns**

**Getting Sequence Update for a Specific Date**

To start iterating through feeds from a specific date:

- Get sequence update for the desired date:
  curl 'https://tap.group-ib.com/api/v2/sequence_list?date=2024-10-14&collection=apt/threat' \ -u 'LOGIN:API_KEY'
- Extract the sequence update number from the response:
  { "list": { "apt/threat": 17287776262152 } }
- Use this sequence update number in your first request to the collection endpoint:
  curl 'https://tap.group-ib.com/api/v2/apt/threat/updated?seqUpdate=17287776262152&limit=10' \ -u 'LOGIN:API_KEY'
- Continue iterating using the top-level seqUpdate from subsequent responses

**Getting All Collections' Sequence Updates**

To get sequence updates for all collections at once:

curl 'https://tap.group-ib.com/api/v2/sequence_list?date=2024-10-14' \ -u 'LOGIN:API_KEY'

This is useful for: - Monitoring multiple collections - Determining which collections have updates on a specific date - Bulk synchronization across collections

**Related Endpoints**

- Get active collections: GET /api/v2/user/granted_collections

GROUP-IB

Threat intelligence

# Preventing and investigating cybercrime since 2003

intelligence@group-ib.com
+65 3159-3798
www.group-ib.com
blog.group-ib.com