Campaign API

The information and data accessible via this API contain Proofpoint proprietary, confidential, and/or trade secret information. Sharing or providing the information to another party without Proofpoint's express written consent is prohibited. Please review the updated Terms of Use for Proofpoint APIs. The TAP API Terms of Use can be found online at API Terms of Use | Proofpoint US.

Overview

The Campaign API allows administrators to pull campaign IDs in a timeframe and specific details about campaigns, including:

- their description;
- the actor, malware family, and techniques associated with the campaign; and
- the threat variants which have been associated with the campaign

API Features

General Service Notes

1. All timestamps are in the returned events are in UTC.
2. Results are returned in JSON format.

Security

Each request:

- MUST use SSL.
- MUST use service credentials to authenticate to the API.
- MUST use the HTTP Basic Authorization method.
- MUST use the HTTP GET method

Standard responses

Requests to the endpoints can produce a response with a variety of HTTP status codes. The following table describes the scenarios in which these codes can be produced.

Code	Message	Scenarios
200	Success	At least one record matching the specified criteria was found and returned in the response body. In the case of JSON format, the structure is always returned, even if empty.
400	Bad Request	The request is missing a mandatory request parameter, a parameter contains data which is incorrectly formatted, or the API doesn't have enough information to determine the identity of the customer.
401	Unauthorized	There is no authorization information included in the request, the authorization information is incorrect, or the user is not authorized
404	Not Found	The campaign ID or threat ID does not exist.
500	Internal Server Error	The service has encountered an unexpected situation and is unable to give a better response to the request

Throttle Limits

The number of queries to this endpoint are limited by a simple, rolling 24-hour throttle. Once exceeded, the API will start returning *429 HTTP* status codes until 24 hours past the oldest request has elapsed.

Endpoint	Max Number of Requests
/v2/campaign/ids	50 per 24 hours
/v2/campaign/<campaignId>	no throttle limits and does not count toward the request quota of the above endpoint.

Available Endpoints

All endpoints are available on the *tap-api-v2.proofpoint.com* host. For example, *https://tap-api-v2.proofpoint.com/v2/campaign*.

/v2/campaign/ids

Fetch a list of IDs of campaigns active in a time window sorted by the last updated timestamp.

Parameters

Required Parameters

interval

A string containing an ISO8601-formatted interval. The minimum interval is 30 seconds. The maximum interval is 1 day.

Examples:

- **2020-05-01T12:00:00Z/2020-05-01T13:00:00Z -** an hour interval, beginning at noon UTC on 05-01-2020
- **PT30M/2020-05-01T12:30:00Z** - the thirty minutes beginning at noon UTC on 05-01-2020 and ending at 12:30pm UTC
- **2020-05-01T05:00:00-0700/PT30M -** the same interval as above, but using -0700 as the time zone

Optional Parameters

size

The maximum number of campaign IDs to produce in the response. Defaults to 100 and the max supported value is 200.

page

The page of results to return, in multiples of the specified size (or 100, if no size is explicitly chosen). Defaults to 1.

Example Command in Curl

The following command assumes that PRINCIPAL and SECRET are defined environment variables. They correspond to the service principal and secret that was created on the Settings page.

```
curl "https://tap-api-v2.proofpoint.com/v2/campaign/ids?interval=2020-08-28T00:00:00Z/2020-08-29T00:00:00Z&
page=1&size=100" --user "$PRINCIPAL:$SECRET" -s
```

Results Format

The campaign results object format is a JSON structure.

```
{
  "campaigns": [
    {
        "id":"e144426d-7bcd-4695-98a7-c9f6551f3d48", // campaign ID
        "lastUpdatedAt":"2020-05-13T16:35:30Z", // last updated timestamp of the campaign
        "notable": false,
        "verticallyTargeted": false
    },
    {
        "id": "4946e0af-c818-4c4e-818d-676e0d01a8c0",
        "lastUpdatedAt": "2024-12-22T22:05:05.000Z",
        "notable": true,
        "verticallyTargeted": false
    },
    {
       "id": "2c11d38e-2bb5-4398-994a-537ac7d1ceda",
       "lastUpdatedAt": "2024-12-22T18:18:49.000Z",
       "notable": true,
       "verticallyTargeted": false
    },
    {
       "id": "153f97ac-9539-4b81-aea6-22cb32e6f426",
       "lastUpdatedAt": "2024-12-20T03:42:57.000Z",
       "notable": false,
       "verticallyTargeted": true
    }
    ]
}
```

/v2/campaign/<campaignId>

Fetch detailed information for a given campaign.

Parameters

None.

Example Command in Curl

The following command assumes that PRINCIPAL and SECRET are defined environment variables. They correspond to the service principal and secret that was created on the Settings page. The campaignId is the identifier for the campaign. This is usually found in the events produced by the SIEM API.

```
curl "https://tap-api-v2.proofpoint.com/v2/campaign/<campaignId>" --user "$PRINCIPAL:$SECRET" -s
```

Results Format

The campaign results object format is a JSON structure that contains nested objects. The results provided by this API may not be in any sorted order.

Top-level Structure

The top-level structure contains the attributes of the campaign and its membership.

```
{
    "id": "string", // the campaign id
    "name" : "string", // the name of the campaign
    "description" : "string", // a description of the campaign written by one of Proofpoint's threat analysts
    "startDate" : "string", // an  ISO8601-formatted datetime corresponding to the time the campaign's first threat variants were first observed
    "campaignMembers" : [ list<CampaignMember> ] // an array of CampaignMember objects
    "actors" : [ list<Actor> ], // optional, an array of Actor objects
    "malware" : [ list<Malware> ], // optional, an array of Malware objects
    "techniques" : [ list<Technique> ], // optional, an array of Technique objects
}
```

Actor Objects

An *Actor* is an individual or a group of individuals who are coordinating one or more attacks against organizations on the Internet. The actor can be associated with a given campaign by correlating common infrastructure across campaigns, identifying authors within their payload, or other threat intelligence.

```
{
    "name" : "string", // the name of the actor
    "id" : "string" // the actor identifier
}
```

Malware Objects

The *Malware* object shows the specific family of crimeware used by malicious actors.

```
{
    "name" : "string", // the name of the malware family
    "id" : "string" // the malware family identifier
}
```

Technique Objects

The *Technique* object corresponds to the specific technique used to exploit users. Some examples of techniques include exploit-laden documents, drive-by downloads, and credential phishing.

```
{
    "name" : "string", // the name of the technique
    "id" : "string" // the technique identifier
}
```

CampaignMember Objects

The *CampaignMember* objects give details about each threat variant which have been correlated to this campaign.

```
{
    "id" : "string", // the threat identifier
    "threat" : "string", // the attachment hash or URL fragment of the threat
    "type" : "url", // the type of the threat: attachment or url
    "subType" : "string", // the sub-type of the threat: ATTACHMENT, COMPLETE_URL, NORMALIZED_URL, HOSTNAME, or DOMAIN
    "threatTime" : "string" // an  ISO8601-formatted datetime corresponding to the the threat variant was first recognized as malicious
}
```

CampaignFamily Objects

The *CampaignFamily* object shows the specific category and type of campaign used by malicious actors.

```
{
    "name" : "string", // the name of the campaign family
    "id" : "string" // the campaign family identifier
}
```