People 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 People API allows administrators to identify which users in their organizations were most attacked or are the top clickers during a specified period.

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 endpoint 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	The request was successful. The body of the response contains the requested information in JSON format.
400	Bad Request	The request is missing a mandatory request parameter or a parameter contains data which is incorrectly formatted.
401	Unauthorized	There is no authorization information included in the request, the authorization information is incorrect, or the user is not authorized
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/people/vap	50 per 24 hours
/v2/people/top-clickers	50 per 24 hours

Available Endpoints

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

/v2/people/vap

Fetch the identities and attack index breakdown of Very Attacked People within your organization for a given period.

Parameters

Required Parameters

window

An integer indicating how many days the data should be retrieved for. Accepted values are 14, 30 and 90.

Optional Parameters

size

The maximum number of VAPs to produce in the response. The *attackIndex* value determine the order of results. Defaults to 1000.

page

The page of results to return, in multiples of the specified size (or 1000, 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/people/vap?window=90" --user "$PRINCIPAL:$SECRET" -s
```

Results Format

The results object format is a JSON structure that contains nested objects.

Top-level Structure

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

```
{
   "users: [ list<Users> ], // an array of User objects
   "totalVapUsers": integer, // an integer describing the total number of VAP users for the interval
   "interval": "string", // an  ISO8601-formatted interval showing what time the response was calculated for
   "averageAttackIndex": integer, // the average attack index value for users during the interval
   "vapAttackIndexThreshold": integer // this interval's attack index threshold, past which a user is considered a
VAP
}
```

USER OBJECTS

A user object contains information about the user's identity and statistics about the threats the user was sent. Detailed Identity information is obtained by synchronizing from a directory.

```
{
   "identity": {
      "guid": "string", // a unique identifier within Proofpoint's system
      "customerUserId": "string", // [Unsupported] a identifier associated with the user which was provided by the
customer, usually from their directory
      "emails": ["string"], // a list of email addresses associated with the user
      "name": "string", // the name of the user, if known, or null
      "department": "string", // the department of the user, if known, or null
      "location": "string", // the location of the user, if known, or null
      "title": "string", // the name of the user, if known, or null
      "vip": false // whether the user has been identified as a VIP
   },
   "threatStatistics": {
      "attackIndex": integer, // the attack index value for this user during the selected interval
      "families": [
            {
               "name": "string", // name of the threat family
               "score": integer // summation of threat scores under this particular threat family
            },
            {
               "name": "string",
               "score": integer
            }
```

```
        ]
    }
}
```

* Note that in the "*threatStatistics*" section, the scores in the "*families*" field will NOT add up to the value in the "*attackIndex*" field. This is because "*attackIndex*" is a weighted aggregate of threats from each threat family, whereas each score in the family breakdown is a pure summation without weights.

EXAMPLE OUTPUT


```
{
    "users": [{
            "identity": {
                "guid": "dc8766cd-39b2-c5a0-b008-849502c50323",
                "customerUserId": "01232336319812225987",
                "emails": ["bruce.wayne@waynetech.net"],
                "name": "Bruce Wayne",
                "department": "Office of the CEO",
                "location": "Gotham City HQ",
                "title": "CEO",
                "vip": true
            },
            "threatStatistics": {
                "attackIndex": 18558,
                "families": [
                    {
                        "name": "phishing",
                        "score": 2619
                    },
                    {
                        "name": "spam",
                        "score": 87
                    },
                    {
                        "name": "APT Malware Financial",
                        "score": 1710
                    },
                    {
                        "name": "APT Malware State",
                        "score": 1007
                    }
                ]
            }
        }, {
            "identity": {
                "guid": "dcdc2104-cf45-9c1d-d358-4f5fbef93ff9",
                "customerUserId": "12225987012323363198",
                "emails": ["clark.kent@dailyplanet.com"],
                "name": "Clark Kent",
                "department": "News Desk",
```

```
            "location": "Metropolis",
            "title": "Reporter",
            "vip": false
         },
         "threatStatistics": {
            "attackIndex": 17280,
            "families": [
               {
                  "name": "Backdoor",
                  "score": 8856
               },
               {
                  "name": "Banking",
                  "score": 13419
               },
               {
                  "name": "Consumer Credential Phishing",
                  "score": 12682
               }
            ]
         }
      }, {
         "identity": {
            "guid": "dc5410b3-5fa9-a26e-8c34-fca0cb9a01e3",
            "customerUserId": null,
            "emails": ["all-members@jla.org"],
            "name": null,
            "department": null,
            "location": null,
            "title": null,
            "vip": false
         },
         "threatStatistics": {
            "attackIndex": 17259,
            "families": [
               {
                  "name": "Consumer Credential Phishing",
                  "score": 17259
               }
            ]
         }
      }
   ],
   "totalVapUsers": 150,
   "interval": "2019-10-01T00:00:00Z/2019-11-01T00:00:00Z",
   "averageAttackIndex": 371,
   "vapAttackIndexThreshold": 1520
}
```

/v2/people/top-clickers

Fetch the identities and attack index of the top clickers within your organization for a given period. Top clickers are the users who have demonstrated a tendency to click on malicious URLs, regardless of whether the clicks were blocked or not. Knowing who are more susceptible to threats is useful for proactive security approaches such as security training assignments.

Parameters

Required Parameters

window

An integer indicating how many days the data should be retrieved for. Accepted values are 14, 30 and 90.

Optional Parameters

size

The maximum number of top clickers to produce in the response. The *attackIndex* value determine the order of results. 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/people/top-clickers?window=90&page=1&size=100" --user "$PRINCIPAL:$SECRET" -s*

Results Format

The results object format is a JSON structure that contains nested objects.

Top-level Structure

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

> {

```
    "users: [ list<Users> ], // an array of User objects
    "totalTopClickers": integer, // an integer describing the total number of top clickers in the time interval
    "interval": "string", // an  ISO8601-formatted interval showing what time the response was calculated for
}
```

USER OBJECTS

A user object contains information about the user's identity and statistics of the clicking behavior. Detailed Identity information is obtained by synchronizing from a directory.

```
{
    "identity": {
        "guid": "string", // a unique identifier within Proofpoint's system
        "customerUserId": "string", // [Unsupported] a identifier associated with the user which was provided by the customer, usually from their directory
        "emails": ["string"], // a list of email addresses associated with the user
        "name": "string", // the name of the user, if known, or null
        "department": "string", // the department of the user, if known, or null
        "location": "string", // the location of the user, if known, or null
        "title": "string", // the name of the user, if known, or null
        "vip": false // whether the user has been identified as a VIP
    },
    "clickStatistics": {
        "clickCount": 11, // total number of clicks from this user in the time internval
        "families": [
          {
            "name": "Backdoor", // name of the threat family
            "clicks": 3 // total number of clicks on threats belong to this threat family
          },
          {
            "name": "Banking",
            "clicks": 8
          }
        ]
    }
}
```

EXAMPLE OUTPUT

```
{
    "users": [{
            "identity": {
                "guid": "dc8766cd-39b2-c5a0-b008-849502c50323",
                "customerUserId": "01232336319812225987",
                "emails": ["bruce.wayne@waynetech.net"],
                "name": "Bruce Wayne",
                "department": "Office of the CEO",
```

```
            "location": "Gotham City HQ",
            "title": "CEO",
            "vip": true
          },
          "clickStatistics": {
            "clickCount": 15,
            "families": [
              {
                "name": "phishing",
                "clicks": 3
              },
              {
                "name": "spam",
                "clicks": 12
              }
            ]
          }
        },
        {
          "identity": {
            "guid": "dcdc2104-cf45-9c1d-d358-4f5fbef93ff9",
            "customerUserId": "12225987012323363198",
            "emails": ["clark.kent@dailyplanet.com"],
            "name": "Clark Kent",
            "department": "News Desk",
            "location": "Metropolis",
            "title": "Reporter",
            "vip": false
          },
          "threatStatistics": {
            "clickCount": 27,
            "families": [
              {
                "name": "Backdoor",
                "clicks": 16
              },
              {
                "name": "Banking",
                "clicks": 8
              },
              {
                "name": "Consumer Credential Phishing",
                "clicks": 3
              }
            ]
          }
        },
    ],
    "totalTopClickers": 2,
    "interval": "2020-09-01T00:00:00Z/2020-09-01T00:00:00Z",
}
```