Threats 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 Threats API allows administrators to pull detailed attributes about individual threats observed in their environment.

It can be used to retrieve more intelligence for threats identified in the SIEM or Campaign API responses.

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.

Throttle Limits

The Threats API currently has no throttle limits.

Available Endpoints

GET /v2/threat/summary/<threatId>

Required Parameters

threatId

A string containing a unique identifier associated with the threat in TAP Dashboard.

The threat ID can be found in SIEM API events or the URL suffix of the TAP Dashboard Threat Detail page as bolded in the example below:

https://threatinsight.proofpoint.com.../threat/
email/**c5480b765318994ea33d297283d7bb256ffefe8738d4d53bacf6ab08f0332b9f**

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/threat/summary/<threatId>" --user "$PRINCIPAL:$SECRET" -s*

Results Format

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

Field	Content	Description
id	String	A unique threat ID.
identifiedAt	DateTime	Proofpoint identified the threat at this time.
name	String	The threat name
type	String	The threat type (*attachment*, *url*, or *message text*).
category	String	The threat category (*impostor*, m*alware*, p*hish*, or *spam*).
status	String	The threat status (*active* or *cleared*)
detectionType	String	New field created called detectionType
severity	Integer	The threat severity score ranges from 0-1000.
attackSpread	Integer	The number of Proofpoint customers that also received this threat.
notable	Boolean	Whether the threat is marked as notable by Proofpoint's Threat Analysts.
verticals	Boolean	Whether the threat is identified as vertically targeted.
geographies	Boolean	Whether the threat is identified as geographically targeted.
actors	Array of objects	The id and name of the actor associated with the threat.
families	Array of objects	The id(s) and name(s) of the threat families associated with the threat.
malware	Array of objects	The id(s) and name(s) of the malware associated with the threat.
techniques	Array of objects	The id(s) and name(s) of the techniques associated with the threat.

brands	Array of objects	The id(s) and name(s) of the brands associated with the threat.

Example Output

```
{
    "id": "029bef505d5de699740a1814cba0b6abb685f46d053dea79fd95ba6769e40a6f",
    "identifiedAt": "2020-07-21T15:30:10.000Z",
    "name": "029bef505d5de699740a1814cba0b6abb685f46d053dea79fd95ba6769e40a6f",
    "type": "attachment",
    "category": "malware",
    "status": "active",
    "severity": 20,
    "attackSpread": 62,
    "notable": false,
    "verticals": false,
    "geographies": false
    "actors": [
        {
            "id": "6e3b86b0-a823-4ed6-8d75-db4d7ead43ba",
            "name": "TA505"
        }
    ],
    "families": [
        {
            "id": "cfd29eb5-544f-4ef4-920c-7c4e428931e0",
            "name": "Banking"
        }
    ],
    "malware": [
        {
            "id": "8faf65ef-0524-45e0-a036-d1b6e261825c",
            "name": "Ursnif"
        }
    ],
    "techniques": [
        {
            "id": "accc60d8-4426-4ba2-b2f5-f9ec2eb4685b",
            "name": "XL4 macros"
        }
    ],
    "brands": [
        {
            "id": "acasd60d8-4426-4ba2-b2f5-f9ec2eb4685b",
            "name": "DocuSign"
        }
    ]
}
```