

# ThreatQuotient



## VirusTotal LiveHunt CDF Guide

**Version 1.0.0**

November 24, 2020

**ThreatQuotient**

11400 Commerce Park Dr., Suite 200  
Reston, VA 20191

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# 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 © 2020 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.

# Contents

- Versioning ..... 4
- Introduction ..... 5
- Installation ..... 6
- Configuration ..... 7
- ThreatQ Mapping ..... 8
  - VirusTotal LiveHunt ..... 8
  - VirusTotal LiveHunt Details (Supplemental)..... 14
- Average Feed Run ..... 16
- Change Log ..... 17

# Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions  $\geq$  4.43.0

# Introduction

The VirusTotal LiveHunt Feed must be used in conjunction with VirusTotal LiveHunt Operation. The Operation will push YARA Signatures from ThreatQ to VirusTotal LiveHunt and the CDF will ingest data related to each signature pushed to VirusTotal Livehunt back into ThreatQ.

# Installation

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration 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



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.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

# Configuration



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

To configure the feed:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** tab (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

| PARAMETER      | DESCRIPTION                                                                     |
|----------------|---------------------------------------------------------------------------------|
| <b>API Key</b> | VirusTotal LiveHunt API Key to be used in HTTP headers for accessing feed data. |

5. Review the **Settings** configuration, 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

## VirusTotal LiveHunt

This feed enriches previously pushed YARA Signatures. The data sample and mapping are below:

GET [https://www.virustotal.com/api/v3/intelligence/hunting\\_notification\\_files](https://www.virustotal.com/api/v3/intelligence/hunting_notification_files)

JSON response sample:

```
{
  "data": [
    {
      "attributes": {
        "androguard": {
          "Activities": [

            "com.google.android.gms.auth.api.signin.internal.SignInHubActivity",
            "com.google.android.gms.common.api.GoogleApiActivity"

          ],
          "AndroguardVersion": "3.0-dev",
          "AndroidApplication": 1,
          "AndroidApplicationError": false,
          "AndroidApplicationInfo": "APK",
          "AndroidVersionCode": "71000222",
          "AndroidVersionName": "3.41.1",
          "Libraries": [
            "org.apache.http.legacy"
          ],
          "MinSdkVersion": "17",
          "Package": "com.b2w.soubarato",
          "Providers": [
            "com.b2w.main.providers.SoubAutoCompleteSuggestionProvider",
            "com.imagepicker.FileProvider"
          ],
          "Receivers": [
            "com.facebook.CurrentAccessTokenExpirationBroadcastReceiver",
            "com.google.android.gms.measurement.AppMeasurementReceiver",

            "com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver"

          ],
          "RiskIndicator": {
            "APK": {
              "DEX": 3
            },
            "PERM": {
              "DANGEROUS": 3,
              "INTERNET": 1,
              "NORMAL": 9,
              "PRIVACY": 3,
              "SIGNATURE": 1
            }
          }
        }
      },
    },
  ],
}
```

```
"Services": [
  "com.google.android.datatransport.runtime.backends.TransportBackendDiscovery",
  "com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService"
],
"StringsInformation": [
  "http://",

  "https://www.example.com/"
],
"TargetSdkVersion": "29",
"VTAndroidInfo": 1.41,
"certificate": {
  "Issuer": {
    "C": "55",
    "CN": "Francisco Cavedon",
    "DN": "C:55, CN:Francisco Cavedon, L:Rio de Janeiro, O:Ideais, ST:RJ, OU:Mobile",
    "L": "Rio de Janeiro",
    "O": "Ideais",
    "OU": "Mobile",
    "ST": "RJ"
  },
  "Subject": {
    "C": "55",
    "CN": "Francisco Cavedon",
    "DN": "C:55, CN:Francisco Cavedon, L:Rio de Janeiro, O:Ideais, ST:RJ, OU:Mobile",
    "L": "Rio de Janeiro",
    "O": "Ideais",
    "OU": "Mobile",
    "ST": "RJ"
  },
  "serialnumber": "737736f4",
  "thumbprint": "486454815aa53bd3182797f507ed6f58fe9af772",
  "validfrom": "2014-02-05 13:37:21",
  "validto": "2039-01-30 13:37:21"
},
"intent_filters": {
  "Activities": {
    "com.b2w.main.activity.account.manager.MyAccountActivity": {
      "action": [
        "android.intent.action.VIEW"
      ],
      "category": [
        "android.intent.category.DEFAULT",
        "android.intent.category.BROWSABLE"
      ]
    },
    "com.facebook.CustomTabActivity": {
      "action": [
        "android.intent.action.VIEW"
      ],
      "category": [
        "android.intent.category.DEFAULT",
        "android.intent.category.BROWSABLE"
      ]
    }
  },
  "Receivers": {
    "com.pushio.manager.PushIOBroadcastReceiver": {
      "action": [
        "com.google.android.c2dm.intent.RECEIVE",
        "com.google.android.c2dm.intent.REGISTRATION"
      ],
      "category": [
```

```
        "com.b2w.soubarato"
      ]
    },
    "Services": {
      "com.b2w.main.push.SoubaratoFCMService": {
        "action": [
          "com.google.firebase.MESSAGING_EVENT"
        ]
      },
      "com.pushio.manager.PIOFCMIntentService": {
        "action": [
          "com.google.firebase.MESSAGING_EVENT",
          "com.google.firebase.INSTANCE_ID_EVENT"
        ]
      }
    }
  },
  "main_activity": "com.b2w.main.activity.MainActivity",
  "permission_details": {
    "me.everything.badger.permission.BADGE_COUNT_READ": {
      "full_description": "Unknown permission from android reference",
      "permission_type": "normal",
      "short_description": "Unknown permission from android reference"
    },
    "me.everything.badger.permission.BADGE_COUNT_WRITE": {
      "full_description": "Unknown permission from android reference",
      "permission_type": "normal",
      "short_description": "Unknown permission from android reference"
    }
  }
},
"bundle_info": {
  "extensions": {
    "bin": 1,
    "cer": 1,
    "crt": 1,
    "dex": 3,
    "gz": 1,
    "jpg": 3,
    "js": 1,
    "otf": 1,
    "png": 255,
    "ttf": 2,
    "txt": 1,
    "xml": 592
  },
  "file_types": {
    "DEX": 3,
    "JPG": 4,
    "Java Bytecode": 1,
    "PNG": 255,
    "XML": 592,
    "unknown": 145
  },
  "highest_datetime": "1980-00-00 00:00:00",
  "lowest_datetime": "1980-00-00 00:00:00",
  "num_children": 1238,
  "type": "APK",
  "uncompressed_size": 45875567
},
"capabilities_tags": [],
"downloadable": true,
```

```
"exiftool": {
  "FileType": "ZIP",
  "FileTypeExtension": "zip",
  "MIMEType": "application/zip",
  "ZipBitFlag": "0",
  "ZipCRC": "0x0f0d5329",
  "ZipCompressedSize": "11703",
  "ZipCompression": "Deflated",
  "ZipFileName": "AndroidManifest.xml",
  "ZipModifyDate": "1980:00:00 00:00:00",
  "ZipRequiredVersion": "0",
  "ZipUncompressedSize": "70984"
},
"first_submission_date": 1601777166,
"last_analysis_date": 1604478567,
"last_analysis_results": {
  "ALYac": {
    "category": "undetected",
    "engine_name": "ALYac",
    "engine_update": "20201104",
    "engine_version": "1.1.1.5",
    "method": "blacklist",
    "result": null
  },
  "APEX": {
    "category": "type-unsupported",
    "engine_name": "APEX",
    "engine_update": "20201104",
    "engine_version": "6.94",
    "method": "blacklist",
    "result": null
  },
  "eGambit": {
    "category": "type-unsupported",
    "engine_name": "eGambit",
    "engine_update": "20201104",
    "engine_version": null,
    "method": "blacklist",
    "result": null
  },
  "Bkav": {
    "category": "malicious",
    "engine_name": "Bkav",
    "engine_update": "20201117",
    "engine_version": "1.3.0.9899",
    "method": "blacklist",
    "result": "W32.AIDetectVM.malware2"
  },
  "Cylance": {
    "category": "malicious",
    "engine_name": "Cylance",
    "engine_update": "20201124",
    "engine_version": "2.3.1.101",
    "method": "blacklist",
    "result": "Unsafe"
  }
},
"last_analysis_stats": {
  "confirmed-timeout": 0,
  "failure": 1,
  "harmless": 0,
  "malicious": 0,
  "suspicious": 0,
```

```
    "timeout": 3,
    "type-unsupported": 12,
    "undetected": 60
  },
  "last_modification_date": 1604478749,
  "last_submission_date": 1604478567,
  "magic": "Zip archive data",
  "main_icon": {
    "dhash": "d4c8e8e8e8e8b2cc",
    "raw_md5": "76b13404cbc08c06a46cf6b1c1c9e937"
  },
  "md5": "0a33341ab24baddf443a890f8b815e0f",
  "meaningful_name": "com.b2w.soubarato",
  "names": [
    "yMNMxqjSgnmm55zzyax120201004-118624-sxoqgo"
  ],
  "reputation": 0,
  "sha1": "f4b1f470b1cee686d97602e7d6e51d43d6bef1de",
  "sha256": "c3e6aa52d926d0d00e89d8ba09fa21ef95c63fba9cfbf3d4217891fa27230394",
  "size": 18080108,
  "ssdeep":
"393216:JaqZ7bmEMETsf7AdB4KICa5ZicJZ6+HgDjvTYv5NBbRJSMqcg8gdrv3JZh7:cqhmED8famCajicH6+HgDjvs5N4yg88j",
  "tags": [
    "apk",
    "android"
  ],
  "times_submitted": 2,
  "tlsh": "T15B073394F368E41BC9BBA43399A6036226421D8585C2EF532558F34CAEF7E844F59FCC",
  "total_votes": {
    "harmless": 0,
    "malicious": 0
  },
  "trid": [
    {
      "file_type": "VYM Mind Map",
      "probability": 9.0
    }
  ],
  "type_description": "Android",
  "type_tag": "android",
  "unique_sources": 2,
  "vhash": "edafd3c0e528684be1d6409852ab8eb3"
},
"context_attributes": {
  "match_in_subfile": false,
  "notification_date": 1604478761,
  "notification_id": "1695784045420398-5121460817657856-9ce413deb7042fede0817960b939fa4b",
  "notification_snippet": "16 41 4C 54 45 52 41 52 20 45 4D 41 49 4C 20 4F .ALTERAR EMAIL",
  "notification_source_country": "LU",
  "notification_source_key": "83276777",
  "notification_tags": [
    "c3e6aa52d926d0d00e89d8ba09fa21ef95c63fba9cfbf3d4217891fa27230394",
    "banbra",
    "banker"
  ],
  "rule_name": "banbra",
  "rule_tags": [
    "banker"
  ],
  "ruleset_id": "5121460817657856",
  "ruleset_name": "banbra"
},
"id": "c3e6aa52d926d0d00e89d8ba09fa21ef95c63fba9cfbf3d4217891fa27230394",
```

```
{
  "links": {
    "self": "https://www.virustotal.com/api/v3/files/c3e6aa52d926d0d00e89d8ba09fa21ef95c63fba9cfbf3d4217891fa27230394"
  },
  "type": "file"
},
{
  "links": {
    "self": "https://www.virustotal.com/api/v3/users/tis.threatq/hunting_notification_files?limit=10"
  },
  "meta": {
    "count": 1
  }
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH                                             | THREATQ ENTITY            | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                           | NOTES                                                                                                                                                  |
|------------------------------------------------------------|---------------------------|--------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| .data[].context_attributes.ruleset_name                    | Signature.Attribute       | Ruleset Name                         | 'banker'                           |                                                                                                                                                        |
| .data[].context_attributes.notification_source_country     | Signature.Attribute       | Source Country                       | 'US'                               |                                                                                                                                                        |
| .data[].attributes.magic                                   | Signature.Attribute       | Magic                                | 'Dalvik dex file version 035'      |                                                                                                                                                        |
| .data[].attributes.meaningful_name                         | Signature.Attribute       | Meaningful Name                      | 'classes.dex'                      |                                                                                                                                                        |
| .data[].attributes.reputation                              | Signature.Attribute       | Reputation                           | '0'                                |                                                                                                                                                        |
| .data[].attributes.trid.file_type                          | Signature.Attribute       | File Type                            | 'Dalvik Dex class'                 |                                                                                                                                                        |
| .data[].attributes.trid.probability                        | Signature.Attribute       | Probability                          | '100'                              |                                                                                                                                                        |
| .data[].attributes.type_description                        | Signature.Attribute       | Description Type                     | 'Android'                          |                                                                                                                                                        |
| .data[].attributes.type_tag                                | Signature.Attribute       | Tag Type                             | 'android'                          |                                                                                                                                                        |
| .data[].attributes.exiftool.FileTypeExtension              | Signature.Attribute       | File Extension                       | 'DEX'                              |                                                                                                                                                        |
| .data[].attributes.last_analysis_results.(key).result      | Signature.Attribute       | (key) Analysis Result                | 'Unsafe'                           | The name of this attribute is dynamically set with the value found on (key). We only add this attribute if the value is not null.                      |
| .data[].attributes.last_analysis_results.(key).result      | Related.Malware           | N/A                                  | 'W32.AIDetectVM.malware2'          | If the value corresponds to a type of malware, then a Malware object is ingested instead of ingesting the '(key) Analysis Result' signature attribute. |
| .data[].attributes.last_analysis_results.(key).engine_name | Related.Malware.Attribute | Analysis Engine                      | 'Bkav'                             |                                                                                                                                                        |
| .data[].attributes.md5                                     | Related.Indicator         | MD5                                  | '52c5d34ffcf797f5d8de9fb8ae9120c8' |                                                                                                                                                        |
| .data[].attributes.sha1                                    | Related.Indicator         | SHA-1                                | '552eb372553ee115b8871'            |                                                                                                                                                        |

| FEED DATA PATH                           | THREATQ ENTITY    | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                                                                                                  | NOTES |
|------------------------------------------|-------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------|-------|
|                                          |                   |                                      | 4180513da44<br>cce748da'                                                                                  |       |
| .data[].attributes.sha256                | Related.Indicator | SHA-256                              | '8775216e22c<br>6501fc65042c<br>8c3a984fce0c<br>20b27bdd17c<br>28493c2318d<br>7bb5cc9'                    |       |
| .data[].attributes.ssdeep                | Related.Indicator | Fuzzy Hash                           | '49152:vaMqT<br>ZeWWZsKWQf<br>g+sbwUt1pdV/<br>eTETEmvHNgy<br>jkGKeQU6/7kn<br>E5KS:iMooTsA<br>mMoHe7beQES' |       |
| .data[].context_attributes.<br>rule_name | Signature.Name    | YARA                                 | 'banbra'                                                                                                  |       |

## VirusTotal LiveHunt Details (Supplemental)

The supplemental feed is used to fetch the previously pushed signature value. The JSON Key from the previous feed '.data[].context\_attributes.ruleset\_id' is used to call the supplemental feed.

GET [https://www.virustotal.com/api/v3/intelligence/hunting\\_rulesets/{ruleset\\_id}](https://www.virustotal.com/api/v3/intelligence/hunting_rulesets/{ruleset_id})

JSON response sample:

```
{
  "data": {
    "attributes": {
      "creation_date": 1604476073,
      "enabled": true,
      "limit": 100,
      "modification_date": 1604476073,
      "name": "banbra",
      "notification_emails": [
        "test@test.com"
      ],
      "number_of_rules": 1,
      "rule_names": [
        "banbra"
      ],
      "rules": "rule banbra : banker {\n\tstrings: \n $a = \"senha\" fullword nocase\ncondition:\n #a > 3}\n",
    },
    "id": "5121460817657856",
    "links": {
      "self": "https://www.virustotal.com/api/v3/intelligence/hunting_rulesets/5121460817657856"
    },
    "type": "hunting_ruleset"
  }
}
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH         | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | EXAMPLES                                                                                        |
|------------------------|-----------------|--------------------------------------|-------------------------------------------------------------------------------------------------|
| .data.attributes.rules | Signature.Value | YARA                                 | 'rule banbra : banker {\n\tstrings: \n\$a = "senha" fullword<br>nocase\ncondition:\n #a > 3}\n' |

# Average Feed Run

Average Feed Run results for VirusTotal LiveHunt:

| METRIC               | RESULT    |
|----------------------|-----------|
| Run Time             | 2 minutes |
| Signatures           | 1         |
| Signature Attributes | 333       |
| Indicators           | 6         |



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.

# Change Log

- **Version 1.0.0**
  - Initial release