ThreatQuotient

ThreatFabric CDF User Guide

Version 1.0.0

March 12, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

ThreatFabric enables safe and frictionless online customer journeys by integrating industry-leading threat intel, behavioral analytics, malware threat detection, advanced device fingerprinting, and 10.000+ adaptive fraud indicators. ThreatFabric's Fraud Risk Suite provides banks with omni-channel (web and mobile) fraud visibility creating peace of mind in an age of ever-changing fraud.

The integration provides the following feeds:

- **ThreatFabric Samples** - returns information about the analysis of the different malware samples analyzed by ThreatFabric.
- **ThreatFabric Malware Families** - returns information about the different malware families tracked by ThreatFabric.
- **ThreatFabric Malware Variants** - returns information about the different malware variants tracked by ThreatFabric.

The integration ingests the following system objects:

- Indicators
- Malware

Prerequisites

The following is required to run the integration:

- A ThreatFabric API Key

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
6. Select the feeds to install, when prompted, and click **Install**. The feed(s) will be added to the integrations page.

   > 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.

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 integration-related credentials.

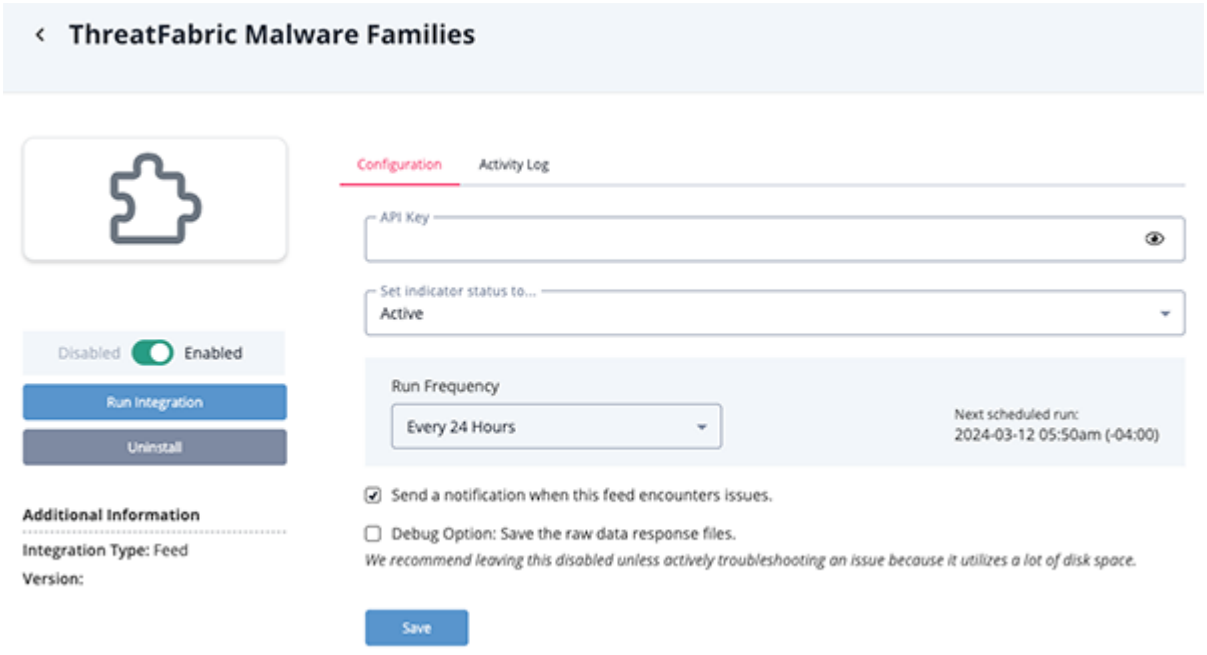
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
API Key	Your ThreatFabric API Key.



5. Review any additional settings, 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

ThreatFabric Samples

The ThreatFabric Samples feed returns information about the analysis of the different malware samples analyzed by ThreatFabric.

`GET https://api.mti.threatfabric.net/v0/samples`

Sample Response:


```
{
  "before":
"eyJ0eXBlIjowLCJib3VuZGFyeSI6IjIwMjQtMDItMjdUMDg6NDk6NTguMjYxWiIsIm9yaWdpbmFsUX
VlcnkiOnsiZnJvbURhdGUiOiIyMDI0LTAxLTAxVDAwOjAwOjAwLjAwMFoiLCJwYWdlU2l6ZSI6NTAsI
nNvcnRPcmRlciI6ImRlc2MiLCJzb3J0RmllbGQiOiJ1cGxvYWREYXRlIn19",
  "after":
"eyJ0eXBlIjoxLCJib3VuZGFyeSI6IjIwMjQtMDItMjdUMDI6NTI6NDcuMzYxWiIsIm9yaWdpbmFsUX
VlcnkiOnsiZnJvbURhdGUiOiIyMDI0LTAxLTAxVDAwOjAwOjAwLjAwMFoiLCJwYWdlU2l6ZSI6NTAsI
nNvcnRPcmRlciI6ImRlc2MiLCJzb3J0RmllbGQiOiJ1cGxvYWREYXRlIn19",
  "hasBefore": false,
  "hasAfter": true,
  "results": [
    {
      "id": "35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
      "data": {
        "_id":
"35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
        "hashes": {
          "md5": "5fcd17472765f46d1693da1f8eb35e70",
          "sha1": "9f3fddc26443d62b5464dbde3d2fc611d49f5bcb",
          "sha256":
"35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
          "ssdeep": "196608:6TNAru3rW7zkxUTHHaG1duJ4TCPP9ab/
5Ki7Bh6PXahsb6f3w:cW67yOZGzueAP9u1ydbqw"
        },
        "uploadDate": "2024-02-27T07:19:09.323Z",
        "lastModifiedDate": "2024-02-27T07:20:13.456Z",
        "analysis": {
          "static": {
            "estimatedBuildDate": "2024-02-27T06:13:44.000Z"
          }
        }
      }
    }
  ]
}
```

Samples Get Details (Supplemental)

`GET https://api.mti.threatfabric.net/v0/samples/{{id}}/details`

Sample Response:


```
{
   "id":"35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
   "data":{
      "_id":"35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
      "hashes":{
         "md5":"5fcd17472765f46d1693da1f8eb35e70",
         "sha1":"9f3fddc26443d62b5464dbde3d2fc611d49f5bcb",

"sha256":"35a572736e9984c4110f6e93d3b2098cce518617b16d209f22ea2a534d8f6733",
         "ssdeep":"196608:6TNAru3rW7zkxUTHHaG1duJ4TCPP9ab/
5Ki7Bh6PXahsb6f3w:cW67yOZGzueAP9u1ydbqw"
      },
      "size":9572693,
      "uploadDate":"2024-02-27T07:19:09.323Z",
      "lastModifiedDate":"2024-02-28T00:08:19.206Z",
      "manifest":{
         "versionCode":7942516,
         "versionName":"7.94.25.16",
         "package":"surfing.destiny.differential",
         "platformBuildVersionCode":30,
         "platformBuildVersionName":"11",
         "usesPermissions":[
            {
               "name":"android.permission.SEND_SMS"
            },
            {
               "name":"android.permission.SET_WALLPAPER"
            }
         ],
         "usesPermissionsSdk23":[
         ],
         "permissions":[
         ],
         "permissionTrees":[
         ],
         "permissionGroups":[
         ],
         "metaData":[
         ],
         "instrumentation":null,
         "usesSdk":{
            "minSdkVersion":21,
            "targetSdkVersion":29
         },
         "usesConfigurations":[
```

```
         ],
         "usesFeatures":[
         ],
         "supportsScreens":null,
         "compatibleScreens":[
         ],
         "supportsGlTextures":[
         ],
         "protectedBroadcasts":[
         ],
         "application":{
            "hardwareAccelerated":true,
            "icon":"resources.arsc/drawable/variousg70.png",
            "largeHeap":true,
            "label":"Data Entry App",

"name":"surfing.destiny.zrbyeyumuscgbzggtyacyogdwfvdxkajuwirucnlqojbwatybv2.vya
iifodglriyasmwodajlwgwlzjsfzqjvctndhfmmjbgazenj6GmXfz89",
            "requestLegacyExternalStorage":true,
            "supportsRtl":true,
            "theme":"@android:style/Theme.Translucent.NoTitleBar",
            "usesCleartextTraffic":true,
            "activities":[
               {

"name":"surfing.destiny.zrbyeyumuscgbzggtyacyogdwfvdxkajuwirucnlqojbwatybv2.vya
iifodglriyasmwodajlwgwlzjsfzqjvctndhfmmjbgazenj6SJTMB87",
                  "intentFilters":[
                     {
                        "actions":[
                           {
                              "name":"android.intent.action.MAIN"
                           }
                        ],
                        "categories":[
                           {
                              "name":"android.intent.category.LAUNCHER"
                           }
                        ],
                        "data":[
                        ]
                     }
                  ],
                  "metaData":[
                  ],
                  "layouts":[
                  ],
                  "configChanges":"0xfb0",
                  "enabled":true,
                  "exported":true,
```

```
                  "hardwareAccelerated":true,
                  "icon":"classes.dex/drawable/skinicon.png",
                  "label":"Data Entry App",
                  "screenOrientation":"4",
                  "taskAffinity":"app.one",
                  "theme":"@android:style/Theme.Translucent.NoTitleBar"
               }
            ],
            "activityAliases":[
            ],
            "services":[
               {

"name":"surfing.destiny.zrbyeyumuscgbzggtyacyogdwfvdxkajuwirucnlqojbwatybv2.vya
iifodglriyasmwodajlwgwlzjsfzqjvctndhfmmjbgazenj6aEgDk72",
                  "intentFilters":[
                  ],
                  "metaData":[
                  ],
                  "enabled":true,
                  "label":"Data Entry App"
               }
            ],
            "receivers":[
               {

"name":"surfing.destiny.zrbyeyumuscgbzggtyacyogdwfvdxkajuwirucnlqojbwatybv2.vya
iifodglriyasmwodajlwgwlzjsfzqjvctndhfmmjbgazenj6gcmZn57",
                  "intentFilters":[
                     {
                        "actions":[
                           {

"name":"surfing.destiny.differential.RestartSensor"
                           }
                        ],
                        "categories":[
                        ],
                        "data":[
                        ]
                     }
                  ],
                  "metaData":[
                  ],
                  "enabled":true,
                  "exported":true
               }
            ],
            "providers":[
               {
```

```
                  "name":"androidx.core.content.FileProvider",
                  "metaData":[
                     {
                        "name":"android.support.FILE_PROVIDER_PATHS",
                        "resource":"AndroidManifest.xml/xml/prov_path.xml"
                     }
                  ],
                  "grantUriPermissions":[
                  ],
                  "pathPermissions":[
                  ],
                  "authorities":"surfing.destiny.differential.provider",
                  "exported":false
               }
            ],
            "metaData":[
               {
                  "name":"com.google.android.maps.v2.API_KEY",

"value":"vyaiifodglriyasmwodajlwgwlzjsfzqjvctndhfmmjbgazenj69"
               }
            ],
            "usesLibraries":[
            ]
         }
      },
      "icons":[
         {
            "hashes":{
               "md5":"53ad69983adb2f80043e74b2fccb005b",
               "sha1":"7366095f4e6d625b44f3e7044a0ec44806130cac",

"sha256":"caf6967857b507af851673df0bed433a249d037d8a72dc82e2d80de09b9ccb9a"
            },
            "filePath":"resources.arsc/drawable/variousg70.png",

"base64":"iVBORw0KGgoAAAANSUhEUgAAAJAAAACQCAYAAADnRuK4AAAPfUlEQVR42u2de3BUVx3HP
+c+9pVNNiEJrwqmIBjLS0G0HSilxQGFKWqtCrTWoTMg1VrQP6oiausojjA6oCIz1YHOVEBnrCimHexY
UoFBRaRAhdpHpigICSEhJJvs6957/ONuNgkE2EBIuHvPdyaTZB93d89+7u9x7u/
8jkilUotM05ybTqdRUuqLAoEAhpTyXiHE0mAwqEZEqc8ypJTtAKlUSo2GUp8UDAbR1DAo3YgUQEoKIC
UFkJICSEkBpKSACkpgJQQgMwEEkJgQBaLJZ7fZlOu7crgG5xSYkIhQDI7NtH
audOrL/
9DfvUKUgmBw6goiL0qirMGTMIfupTGFOngpQuSIV0niYSiR+HQqGvFEpNtAgGcRobia9aRXL7diQgBp
NnQDMMwl/
4AkXr1iEiEeRAgXyTVXA10SIYxD55kpbZs0ls347IZgliEH80AMuifdMmLs6bh9Pc7FrIAnFnBQOQME
1kSwsXFywgc+LELffBNCC1fz+tDz7oxmKGoQC6pbIsTaPti1+8JeHpAVFtLe1r1qAZRkG4sYIASDNNU
jU1JHbsuOU/kAZ0rF9P+p//RAQCCqBBl64jLYuONWvwyvnsSEnH00/
nphsUQIP5AQyD1K5dpI8e9QxAGpD64x/J/
P3vnrdC3gZI05BAYtMmvHYeSyC5eTNej4I8DZAwTazXXyezd6/
```

```
nvggBpHbtwm5sBNNUAA3Wl5CuqcGxLE+
+d+fCBTIvv4ymaQqggf8GBBLI7N7tWTcggfTu3cqFDYpME+fcOTKHD3sWIAFkDhzASaU8O7HoWYCEEF
gnTrhX2T0MkP3OO9jvvIPQdQXQgA/+0aN4/YqStCzsEyeUCxsMWcePD2i84mR/9/
dxrePHPeuGvel4swG0XVd30wfewb1UEpwyBW3YMOwzZ0i/
+qpbptFPr2HX1XnWknrTAmkaMpPBOXv2plocNI3ixx9n2JEjVP7jH5TX1DD08GEq//IXgh/
6EP1RrCoA59Sp3ImhABoI6TqyrQ3Z3HzTrI5RVUXFyy9T+tOfYtxxR4/7g7NmUVlbS2jmzH6BSJ4/
j7RtBdBAZmCyrQ0Zj/e7C3OAwKRJVO7dS3D27Cu/
h0iEIdu3o8diN+x+nNZWZCLhlqUogAYoqG1vd0tD+xueceOoeOkl9FGjrm0IR42iePXqG49f4nFQAA0
wQB0d7rKZfox59LIyymtq0IcPz/t50ccew6iouG6IBCBTKWQyiVAubACVSPR75jLkV7/CGD+
+bwAUFxN+4IEbei+dAKksbCDVjxdQHaDkW98iNH/+dT0/
tHDhDebxdr9+HgVQPmdtPw24AwSnTaPkqaeu+xiBadPQIxEFkB8lhKB006YbCmC14cMxxoxB+nD8fA2
QA0Q++UkCH/7wDR9LHz1aAeQ76wNEv/rV/
hnIPmRuCqACkAQCkycTmDGjfwYyFlMA+Q2g8Gc+0+fnZY4dw2lquvwOw1AA+e2D9yVtly0tNC9ZQsP7
30/jXXdhNzTctGkFBZAHrI/x7ndjTpyYX7BdX0/
jnDnEd+xASEnqrbfo2LKl5zHb2hRAvgJo8uS8ltPIeJzzCxaQOnwYvVvwnd6/
vydkN6kyQAF0i8p473vzelzzww+TOny4x0AJuMyF2fX1CiA/
SR8x4pqPaX3qKTr+8IfeB6l7Qy7Lwjl7FqEA8pGusc156k9/
ovXpp688QN2eb585g33mjLJAvoqDLl684n322bM0P/
LIVWMovby8ywC9+SZOKqUskJ+UOXr0CimXw4WHHsI6d+6qQOhVVbm/
O4vslQXyiQSQ+vOfL1+UaNs0L1lCorb2mgNjTpnSBdCBA76NBHwLkNXcTMuXvpRru5v5179onDuX9t/
85pqDIgAzewFWJpNunx+/ZrN+PnM6tm8nc+QIemUl6b/
+FTudviY8EjBGj8acNMkF79AhLJ9mYL4GqNOSZE6cIJ0FqhMep9v9oheAQh/
5SK6zWGLXrkHvRa1c2CBDpF0CSPGKFZRt2IBWXNxrcBx68MFs+mWR/
N3vfAuP7y3QZQlYFp7SzZtduHSd5i9/OQeIBMzRownedx8AqT17SNfV+fosVNs9dYdj1ChiP/
pRl6VZuBCt2/
UyCUQeeQSRnUSMb9rk+3FTAHWDI7pyJaJbcbwIhRCBQM6N6aEQRcuXu97r9ddJvvCC7wdQAZSFR49Ei
Dz0UI/
b7dOncTo63AYIQOThh3MrVtvWrsXpx4WNKgbyOECBGTMuq2vu2LYNmd0URQsGKV692k3dX3uNdg90xV
cWaAAVnDOnp/
Wpr6f9l79Ey1qf6OOPo99+OwCtTz7pdtNQUgB1pvKB6dN73BZfuxa7tdUNrocPp3jNGgCSO3fSsXu3G
jgFULdBME2MMWNy/1snTxJ/5pncdpWlGzaglZYiW1tpWbnS1/
M+CqBe4h9RXo5WUdFlfdatw0ml3MxsyRLCn/
0sAC2rVpE5dUoBpAC6xIWFw7kCMaelhcSvf40EglOnUvrMMwAktm0jvnWrGjAFUC/qtj239e9/
k75wgeCECZTX1CCKisgcP07zihXK8iiAepfT1ITM1gbpw4dT+o1vUPnKK+gjRuA0N9P0wAM4N6GdngK
oQDIwp72dzBtvuABVVRFbuxatogIZj9P08Y+TefNNNVAKoKsH0h3PPtvjNquujvPz5pHcv18N0lWkZq
KzZ1H7s89ijBtHYMYM0rW1xH/
yE6zmZgWPAihPVyYlLatX5+Z+hDLPCqDr9ecqWFYxkJICaOADaSUF0PXFP5EIxu23K4gUQH2XA8TWrW
Poq6+iDxvWK0Sde4XlezypAPLRAGgawY99DC0WI3Dnnb1+
+XpFBZH58xHR6NUtWShEZN48X1kz5cIAke0RLXrpFS2B8p07KX/
hBUQ4fEUwHCC6ahXlu3djvu99CiDfuDDHIbVvHzKTIX3wYK8pvFZe7lYgXqMPoigrc6Hr3jtIAVRYmZ
bTzWJ0DkDLY4/RMHYs1v/+lwOoM5aRZLdVcJwezRhkb7GRDxttan6CR6+sZMjmzVQePEjsm9/
MuRlRUkJw1qyuIFrXKf3ud6nct4/
i5cuRFy4gdJ2yrVsxbrsNBwjdey8Vu3ZR+v3vg0e37O4PGX6BRyspoWLPnlxn1sD06VhvvEHbb3/
LsJ//nNAnPkH9e96D09BAxS9+QWTpUsBtnuC0tYGmEfn852lbtw49maR81y5ENEro/
vtxWlpoWb9epfEFGyQDpNPoo0djvfUW6X37AChavty9Lxs8y+ZmIrNnu/
BYFqk9e0js2JFbbOg0NeE0NVG0dCkiGs11Zi1ascIdSB+u1PCPC0smaXn0Uc5Nncq5WbNw6usxp0xBA
2Qm4z4mnSZw990AXHzySRrmzCF18KBbG2RZNE6fjt3QQGTxYmQiwbmpU0m+
+CLGmDEYsZivgmdfBtHtzz+PHY8jAeu//
0UbMsTdZrLTcggBnQ2nXnutKyOTEqTEOn0aLRjEnDSJ9MGDJP7zH1IvveTOFY0enQNRxUAFGgcZQ4dS
8u1vo48di1Fd7e6UfIV9SkUo1Ot8kTZ8OJgmWjRK8eLFmNn1ZFplpS9dmH/
KOXSd8uefJzBzZtcc0PnzfYPQtnO78pjTplGxfXuXKY/
```

```
FcoX5CqACkwOE776bwMyZyHSaxM6dhObMybVpyZ8gmbNMTlMT9smTbgpvGDgtLeg+3LHHNzFQ575g8Q
0baFy0COvtt3u0cskvnRO5NfHJ3/+e+g9+kHMf+ADnJk1yO7uWliqACtaDZTtvpGtr3eDYMNzguC/
8aFquQbkIh3sFTLmwQg2iu2da0Ld4RUo3W8Pd1gDbRh87Nhecd/
lK95h+ysY8a4FEHls1dZf19tuuK7vnHvf5kUjelyCcixfBMDCqq7E7OsgcPYo5dSqB8eNB0yj+
+tcxKipwsjv2mBMm9PE0NvLaekoB1K+2M3/
jKbKuC9w2diMOHcKcOBG7vt5tIHWVLb8lYB07BkB5TQ16WRkdzz2HME0qamsZduQIsR/
8gMD06aQPHgQgtn49kYUL8y5CE4aB8GgA7l2AIpG8V08IIHX8uHtZIhTCnDYNgIsrV2JLiTZkSM69dc
Y2nX2gBdC+dasbR40ahXHbbcS3bMFpaEAfORJz0iTshgaskydJHzqEVVeHKCrCrK7uQ4QfgN5iKhUD3
UQXFom4VijPEgoBXFi2DPvsWbRhw+jYsoXEnj3o2cwsWVODTCZJvvgiMpEgc/RortF4+vBhzs+dS/C+
+3AaG3FaWzk/dy7Rr30N2d5O2w9/
SKauDgE0zZ9P0bJlpPbuzQtwCWiRiFusJr1XhiYSicSPQ6HQV1Ieuo4jgkHs06e5MGECsrU1/1i4W9D
bvQt95+1at78v7VLf/TH5HKu3LvdXek/
G2LGUHTvmtpjxUE1RMBj0pguTjoMoLkaUlPSpdLRztal2yZfbfRWq6OX+Sx+Tz7H6ktCLWMx1nR6cyf
ZmDGTbiGi0K3bxeio8dKg7veBBF+ZNgKRE6Drau97l/
fkpQKuqci2WAmgAAQL0ceMKYvWDPn68d62npwd+4kTPN0IQgHHHHZ49ETwLkASMyZM9D5AWDqP3Zc5I
AdR/mZheXY02cqRnz14J6NXV6KNGuUuHFEADqEwGvaQE8667PB1Am/
fc466I9Wg1o+fLOQILFnjWAgkgMH+
+pxMBTwMkpcT86EfRi4u9GcNVVWHOnOnpjVu8DVA6jTFiBIH778fxIEDBxYvRwmFPL4n2vAuTQLjbvq
Zeyr5Cy5Z58gJqYQGUTmPeeSdBD1khBwg/+qjbRyi7Dk0BNHiBEABF3/
semgeKsiSgl5URXr0aWQDLgAqiqF6mUpiTJ1P0ne/c8lZIAtGNG9FHjiyI2umCWZXhWBaRNWsIf/
rTtyxEDlD0xBOEP/
c5z7uuggMI2wYpKX7uOcKLFt1SzS47i8yKnniC6MaNOJblySvvhQ1Q1pWJQICSHTso+dnP3IYHXNJtb
AB/Ol/XqK6mZNs2ohs3unM+BbSG3pMlrdeUrqMZBnZTE5lXXiFz4AB2XR0yHu+1kWa/g+w4iFgMY/
x4zJkz3csV0ajrtmThtN8MBoMFClCnAgGEELkNVAb87Oy0Rnk06PQqQIW9MjWd7ip+H4Rlx1IWfrNf/
7STkGojAxVEKymAlBRASkoKICUFkJICSEkBpKQAUlJSACkpgJQUQEoKICUlBZCSAkhJAaSkAFJSupoM
KWURuOWJSkp91f8Bn1ihY9ITPbMAAAAASUVORK5CYII=",
            "default":true
         }
      ],
      "signerCertificates":[
         {
            "hashes":{
               "md5":"1900bbfba756edd3419022576f3814ff",
               "sha1":"b79df4a82e90b57ea76525ab7037ab238a42f5d3",

"sha256":"465983f7791f2abeb43ea2cbdc7f21a8260b72bc08a55c839fc1a43bc741a81e"
            },
            "publicKey":{
               "md5":"351c600fb6eff769319191988892596f",
               "sha1":"1089ed3e98120f39920711b17c857969a7b6cea7",

"sha256":"091377d6fd00e4e217b750571d45cbe1a32c7fa74075138fc529fdf162b5416f"
            },
            "issuerDN":{
               "C":"US",
               "CN":"Android",
               "E":"android@android.com",
               "L":"Mountain View",
               "O":"Android",
               "OU":"Android",
               "ST":"California"
```

```
            },
            "subjectDN":{
               "C":"US",
               "CN":"Android",
               "E":"android@android.com",
               "L":"Mountain View",
               "O":"Android",
               "OU":"Android",
               "ST":"California"
            },
            "serial":"00f2b98e6123572c4e",
            "signatureAlgorithm":"MD5withRSA",
            "notBefore":"2008-04-15T23:40:57.000Z",
            "notAfter":"2035-09-01T23:40:57.000Z"
         }
      ],
      "analysis":{
         "static":{
            "estimatedBuildDate":"2024-02-27T06:13:44.000Z",
            "targets":[
            ]
         },
         "classification":{
            "startDate":"2024-02-27T07:20:10.438Z",
            "endDate":"2024-02-27T07:20:12.406Z",
            "match":{
               "id":"6329b55a64071624c467306a",
               "updatedAt":"2024-01-25T14:13:03.633Z",
               "objectType":"Variant",
               "name":"SpyNote.D",
               "report":"64fb32e56251ddbdee137039",
               "aliases":[
                  "CraxsRat"
               ],
               "types":[
                  "RAT",
                  "Spyware"
               ],
               "family":"SpyNote",
               "familyAliases":[
               ],
               "capabilities":[
                  "Remote access",
                  "Updatable",
                  "Emulation detection",
                  "App termination",
                  "Preventing removal",
                  "Accessibility actions",
                  "Application listing",
                  "Contact list collection",
```

```
                  "Device info collection",
                  "Picture making",
                  "SMS listing",
                  "Sound recording",
                  "Screenshots grabbing",
                  "Keylogging"
               ],
               "firstSeen":"2022-09-19T12:43:00.000Z"
            }
         },
         "host":{
            "hosts":[
               {
                  "startDate":"2024-02-27T07:19:27.211Z",
                  "endDate":"2024-02-27T07:20:07.631Z",
                  "name":"paytm.com",
                  "domains":[
                     "paytm.com"
                  ],
                  "ips":[
                     "172.65.64.50",
                     "172.65.64.51"
                  ],
                  "dnsRecords":[
                     {
                        "name":"paytm.com",
                        "type":"A",
                        "ttl":60,
                        "data":"172.65.64.50"
                     }
                  ],
                  "whoisRecord":null,
                  "urls":[
                     "https://paytm.com/%3EBlank%3E!
phonepe%3Ewww.phonepe.com%3EBlank%3E!googlepay%3Ewww.googlepay.com%3EBlank%3E!"
                  ],
                  "isWhitelisted":false,
                  "isC2":false
               }
            ]
         }
      }
   }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result[].hashes.sha256	Indicator.Value	SHA-256	result[].uploadDate	35a572736e9984c41 10f6e93d3b2098cce 518617b16d209f22e a2a534d8f6733	N/A
result[].hashes.md5	Related.Indicator.Value	MD5	result[].uploadDate	5fcd17472765f46d1 693da1f8eb35e70	N/A
result[].hashes.sha1	Related.Indicator.Value	SHA-1	result[].uploadDate	9f3fddc26443d62b54 64dbde3d2fc611d49f 5bcb	N/A
result[].hashes.ssdeep	Related.Indicator.Value	Fuzzy Hash	result[].uploadDate	196608:6TNAru3rW7z kxUTHHaG1duJ4TCPP9 ab/ 5Ki7Bh6PXahsb6f 3w:cW67yOZGzueAP9u 1ydbqw	N/A
result[].analysis.host.hosts[].name	Related.Indicator.Value	FQDN	result[].uploadDate	paytm.com"	N/A
result[].analysis.host.hosts[].isWhitelisted	Related.Indicator.Attribute	Is Whitelisted	result[].uploadDate	False	N/A
result[].analysis.host.hosts[].urls	Related.Indicator.Value	URL	result[].uploadDate	https://paytm.com/%3EBlank%3E! phonepe%3E www.phonepe.com%3EBlank%3E! googlepay%3Eww.googlepay.com%3EBlank%3E!	N/A
result[].analysis.host.hosts[].ips	Related.Indicator.Value	IP Address	result[].uploadDate	172.65.64.50	N/A
result[].analysis.host.hosts[].ips	Related.Indicator.Value	IP Address	result[].uploadDate	172.65.64.50	N/A
result[].manifest.versionName	Indicator.Attribute	Package Version	result[].uploadDate	7.94.25.16	N/A
result[].manifest.package	Indicator.Attribute	Package Name	result[].uploadDate	surfing.destiny.differential	N/A
result[].manifest.usesPermissions[].name	Indicator.Attribute	Uses Permissions	result[].uploadDate	android.permission.SEND_SMS	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result[].manifest.application.label	Indicator.Attribute	Application Label	result[].uploadDate	Data Entry App	N/A
result[].manifest.application.name	Indicator.Attribute	Application Name	result[].uploadDate	surfing.destiny.zrbye yumuscgbzggtyacyogdwf vdxkajuwirucnlqojbwat ybv2.vyaiifodglriyasm wodajlwgwlzjsfzqjvctndhfmmjbgazenj6GmXfz89	N/A
result[].analysis.classification.match.name	Related.Malware	N/A	result[].analysis.classification.match.updatedAt	SpyNote.D	N/A
result[].analysis.classification.match.types	Related.Malware.Attribute	Malware Types	result[].analysis.classification.match.updatedAt	Spyware	N/A
result[].analysis.classification.match.capabilities	Related.Malware.Attribute	Malware Capabilities	result[].analysis.classification.match.updatedAt	Remote access	N/A
result[].analysis.classification.match.family	Related.Malware	N/A	result[].analysis.classification.match.updatedAt	SpyNote	N/A

ThreatFabric Malware Families

The ThreatFabric Malware Families feed returns information about the analysis of the different malware families analysed by ThreatFabric.

`https://api.mti.threatfabric.net/malware/families`

Sample Response:


```
{
   "hasBefore":false,
   "hasAfter":true,
   "after":"W251bGwseyIkb2lkIjoiNjQxMzQzMjRkNjk1NTIyM2JjOGJmZTM3In1d",
   "result":[
      {
         "id":"65d49563b236572ab70c415e",
         "name":"Monitorultra",
         "aliases":[
         ],
         "description":"Commercial Spyware: Monitor-Ultra",
         "createdAt":"2024-02-20T12:04:51.081Z",
         "updatedAt":"2024-02-20T12:04:51.081Z"
      },
      {
         "id":"65cf3e006e1ac29d18b21011",
         "name":"Maqobanko",
         "aliases":[
         ],
         "description":"Fake apps that targets Uzbekistan and Russian users,
that can perform both Spyware and Banker activity.",
         "createdAt":"2024-02-16T10:50:40.716Z",
         "updatedAt":"2024-02-16T10:50:44.905Z"
      }
   ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`result[].name`	Malware.Value	N/A	`result[].createdAt`	`Maqobanko`	N/A
`result[].description`	Malware.Description	N/A	`result[].createdAt`	`Fake apps that targets Uzbekistan and Russian users, that can perform both Spyware and Banker activity.`	N/A

ThreatFabric Malware Variants

High-level summary of what info the feed does

`GET https://api.mti.threatfabric.net/malware/variants`

Sample Response:


```
{
  "hasBefore": false,
  "hasAfter": true,
  "after": "W251bGwseyIkb2lkIjoiNjRhODE0MTQ2NjE4NWRiOTFlMDlhZjQ0In1d",
  "result": [
    {
      "id": "65d88c5693c1aca61cc9621f",
      "name": "Maqobanko.B",
      "aliases": [
      ],
      "description": "Fake Financial and productivity apps with capability to
perform both Spyware and Banker activity targeting Uzbekistan users",
      "family": "65cf3e006e1ac29d18b21011",
      "descendantOf": [
      ],
      "firstSeen": "2024-01-07T15:28:00.000Z",
      "timeline": [
      ],
      "types": [
        "5dbaaa06e324d9591259ddff",
        "5d81e57e784972a76b94b40b"
      ],
      "capabilities": [
        "5f2a8bf53db9c82e50e01412",
        "5f2a8be407fc5a79b61b2b46"
      ],
      "createdAt": "2024-02-23T12:15:18.107Z",
      "updatedAt": "2024-02-23T12:15:18.107Z"
    },
    {
      "id": "65d495d0576b6b0c5e73d2ed",
      "name": "Monitorultra.A",
      "aliases": [
      ],
      "description": "Commercial Spyware: Monitor-Ultra",
      "family": "65d49563b236572ab70c415e",
      "descendantOf": [
      ],
      "firstSeen": "2024-02-17T14:07:00.000Z",
      "timeline": [
      ],
      "types": [
```

```
        "5dbc2142e324d957dc59dee7",
        "5dbaaa06e324d9591259ddff"
      ],
      "capabilities": [
        "5ef1fda44c881025e52413b2",
        "5dbaba6ce324d93e9e59de30"
      ],
      "createdAt": "2024-02-20T12:06:40.564Z",
      "updatedAt": "2024-02-20T12:06:40.564Z"
    }
  ]
}
```

Get Result (Supplemental)

`GET https://api.mti.threatfabric.net/malware/families/{{result[].family}}`

Sample Response:

```
{
   "id":"65cf3e006e1ac29d18b21011",
   "name":"Maqobanko",
   "aliases":[
   ],
   "description":"Fake apps that targets Uzbekistan and Russian users, that can perform both Spyware and Banker activity.",
   "createdAt":"2024-02-16T10:50:40.716Z",
   "updatedAt":"2024-02-16T10:50:44.905Z"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`result[].name`	Malware.Value	N/A	`result[].createdAt`	`Maqobanko.B`	N/A
`result[].description`	Malware.Description	N/A	`result[].createdAt`	`Fake Financial and productivity apps with capability to perform both Spyware and Banker activity targeting Uzbekistan users.`	N/A
`result[].name`	Malware.Attribute	Malware Family	`result[].createdAt`	`Maqobanko`	N/A
`result[].name`	Related.Malware.Value	N/A	`result[].createdAt`	`Maqobanko`	N/A

Average Feed Run

> 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.

ThreatFabric Samples

METRIC	RESULT
Run Time	1 minute
Indicators	959
Indicator Attributes	3,408
Malware	22
Malware Attributes	181

ThreatFabric Malware Families

METRIC	RESULT
Run Time	1 minute
Malware	50

ThreatFabric Malware Variants

METRIC	RESULT
Run Time	1 minute
Malware	88
Malware Attributes	50

Change Log

- **Version 1.0.0**
  - Initial release