

ThreatQuotient



VirusTotal Collections CDF User Guide

Version 1.0.1

July 08, 2023

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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping.....	10
VirusTotal Collections Data.....	10
GET Requests.....	12
IP Addresses.....	13
Domains.....	18
URLs.....	23
Files.....	27
Average Feed Run.....	32
VirusTotal Collections.....	32
Change Log	33

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 © 2023 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.

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 1.0.1

**Compatible with ThreatQ
Versions** $\geq 4.49.0$

Support Tier ThreatQ Supported

Introduction

The VirusTotal Collections feed allows a user to ingest all IoCs (IP Address, Domains, URLs, and Hashes) and related attributes from one or multiple VirusTotal collections.

The integration provides the following endpoint:

- **VirusTotal Collections** - GET `https://www.virustotal.com/api/v3/collections/{collection_id}`

Based on the response of the collection, the integration will then execute four additional GET requests:

- **IP Address** - GET `https://www.virustotal.com/api/v3/collections/{collection_id}/ip_addresses`
- **Domains** - GET `https://www.virustotal.com/api/v3/collections/{collection_id}/domains`
- **URLs** - GET `https://www.virustotal.com/api/v3/collections/{collection_id}/urls`
- **Files** - GET `https://www.virustotal.com/api/v3/collections/{collection_id}/files`

The CDF ingests indicators and indicator attributes.

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 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 parameters under the **Configuration** tab:

PARAMETER

DESCRIPTION

API Key

Your VirusTotal API Key.

Collection IDs

A comma-delimited list of the collections to ingest data from.



The number and size of the collections can affect the performance of the integration. A large number of collections or large collection sizes can extend the amount of time to ingest all data.

< VirusTotal Collections



Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



VirusTotal API key to authenticate with

Collection IDs



Comma-delimited list of the collections we want to ingest data from

How frequent should we pull information from this feed?

Every Day



Set indicator status to...

Active



☒ Send a notification when this feed encounters issues.

Save

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

VirusTotal Collections Data

GET https://www.virustotal.com/api/v3/collections/{collection_id}

Sample Response:

```
{
  "data": {
    "attributes": {
      "alt_names": [
        "Geodo",
        "Heodo"
      ],
      "autogenerated_tags": [
        "cve-2018-20250",
        "cve-2017-11882",
        "upx",
      ],
      "creation_date": 1612569600,
      "description": "While [i]Emotet[/i] historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.\r\nIt is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.",
      "description_html": "While <em>Emotet</em> historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.\r\nIt is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.",
      "domains_count": 0,
      "files_count": 3688,
      "ip_addresses_count": 0,
      "last_modification_date": 1613148085,
      "link": "https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet",
      "name": "Emotet",
      "references_count": 129,
```

```

    "status": "COMPUTED",
    "tags": [
      "upx"
    ],
    "targeted_countries": ["United States"],
    "targeted_industries": ["Finance"],
    "tlp": "WHITE",
    "top_icon_md5": [
      "647ca034cb6c763363b636269047a4c0",
      "da87510c3aabe7851c7c5d0493dbb14a",
      "d2d15e1e362ef2edda7238e165376112"
    ],
    "urls_count": 0
  },
  "id": "malpedia_win_emotet",
  "links": {
    "self": "https://virustotal.com/api/v3/collections/malpedia_win_emotet"
  },
  "type": "collection"
}

```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data.id	Indicator.Attribute	VirusTotal Collection ID	malpedia_win_emotet	N/A
.data.attributes.name	Indicator.Attribute	VirusTotal Collection Name	Emotet	N/A
.data.attributes.creation_date	Indicator.Attribute	VirusTotal Collection Creation Date	2021-02-06 12:00:00-00:00	Uses timestamp to convert from datetime to standardized
.data.attributes.targeted_countries[]	Indicator.Attribute	Targeted Country	United States	One attribute for each country
.data.attributes.targeted_industries[]	Indicator.Attribute	Targeted Industry	Finance	One attribute for each industry
.data.attributes.tags[]	Indicator.Tag	N/A	upx	N/A
.data.attributes.autogenerated_tags[]	Indicator.Tag	N/A	cve-2018-20250	N/A
.data.attributes.tlp	Indicator.TLP	N/A	WHITE	N/A

These attributes and tags are then added to each IoC ingested into ThreatQ. See the [GET Requests](#) section for more details.

GET Requests

Based on the response from the collection, the integration will then execute 4 other GET requests for the IoC data:

- [IP Addresses](#)
- [Domains](#)
- [URLs](#)
- [Files](#)

IP Addresses

GET https://www.virustotal.com/api/v3/collections/{collection_id}/ip_addresses

Sample Response:

```
{
  "meta": {
    "count": 300,
    "cursor": "eyJsaW1pdCI6IDIsICJvZmZzZXQiOiAyfQ=="
  },
  "data": [
    {
      "attributes": {
        "as_owner": "Strato AG",
        "asn": 6724,
        "continent": "EU",
        "country": "DE",
        "jarm":
"27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d",
        "last_analysis_results": {
          "ADMINUSLabs": {
            "category": "harmless",
            "engine_name": "ADMINUSLabs",
            "method": "blacklist",
            "result": "clean"
          },
          "AegisLab WebGuard": {
            "category": "harmless",
            "engine_name": "AegisLab WebGuard",
            "method": "blacklist",
            "result": "clean"
          },
          "AlienVault": {
            "category": "harmless",
            "engine_name": "AlienVault",
            "method": "blacklist",
            "result": "clean"
          },
          "Antiy-AVL": {
            "category": "harmless",
            "engine_name": "Antiy-AVL",
            "method": "blacklist",
            "result": "clean"
          },
          "AutoShun": {
            "category": "harmless",
            "engine_name": "AutoShun",
            "method": "blacklist",
            "result": "clean"
          }
        }
      }
    }
  ]
}
```

```

    }
  },
  "last_analysis_stats": {
    "harmless": 5,
    "malicious": 0,
    "suspicious": 0,
    "timeout": 0,
    "undetected": 0
  },
  "last_https_certificate": {
    "cert_signature": {
      "signature":
"97ef5af5e6e898ba4ec4b04644954ed60ba16b82e6f9c56967b90b5abc9a559bc3a912af382a10
73c4793d75749035597b341efec1073c17bd8b5e03714781c6e9f11b1ce39ecc74afcb8319b9f6f
1d9f6c484400bd58374fc0addf7d05f743cdba94a21ebee3d4ea074282a7662eec26171092a69fd
60158cd72dd647146de7eb8ae2b5db6257588acc98429eb40f6b393fcbad71139ba11671370d41c
bb5f6ca6a18506fccf26d05c3c555377d03946d9e01cdefedbd55c66f34276113885a77babb64cc
ea9fe16bfac6f2be823bce6d698aed09c3cc02c2c39127d6418c21dbacd723d8f5fa465ce72a877
8eee58bf5603a8f42d4afc4c10b0470cef4b244",
      "signature_algorithm": "sha256RSA"
    },
    "extensions": {
      "1.3.6.1.4.1.11129.2.4.2":
"0481f300f1007700e2694bae26e8e94009e8861bb63b83d43ee7fe7488fba48f",
      "CA": true,
      "authority_key_identifier": {
        "keyid": "a84a6a63047dddbae6d139b7a64565eff3a8eca1"
      },
      "ca_information_access": {
        "CA Issuers": "http://cert.int-x3.letsencrypt.org/",
        "OCSP": "http://ocsp.int-x3.letsencrypt.org"
      },
      "certificate_policies": [
        "2.23.140.1.2.1",
        "1.3.6.1.4.1.44947.1.1.1"
      ],
      "extended_key_usage": [
        "serverAuth",
        "clientAuth"
      ],
      "key_usage": [
        "ff"
      ],
      "subject_alternative_name": [
        "www.ufos-hosting.de"
      ],
      "subject_key_identifier":
"f522cd9c9a4ccdf5d1ec3f925013bf1185e0bc0c"
    },
    "issuer": {

```

```

        "C": "US",
        "CN": "Let's Encrypt Authority X3",
        "O": "Let's Encrypt"
    },
    "public_key": {
        "algorithm": "RSA",
        "rsa": {
            "exponent": "010001",
            "key_size": 2048,
            "modulus":
"00d1722efe2a2605072f27013b4f9371f1926464dc1c4285f38138a523dc09f0b9ae8578aa7093
4141bf14893921a2b754a5747a7c71ef9a29501f839a2fe3d052b1434a2fbd0d3149eb1bbe4eef1
4583791ea7cde3bee2babc5f7114a0fe1ab0c5c5f07701330056b510e020154cca0385a93955684
d4d99b74904a44e1ad93f035ebe02bd6e9721285855cbe8f6ce4aaf83ade044b6bc8bd8424ce41f
21cf72a1d4ce42ae539fb202efcc791ef810fa49e1c791d4edf4fb83f468cc78b76b5f703332806
81f034b80613438f1b0a387e3bdb0dd324e63905d96d1dc810498d5d157d12fc87d4dee9b2abc26
4b5b6bd7b1e00b838735270e614e15c2c72babb99"
        }
    },
    "serial_number": "36feb381e87e4ed9b5ee53c76bdaccfab0",
    "signature_algorithm": "sha256RSA",
    "size": 1379,
    "subject": {
        "CN": "www.ufos-hosting.de"
    },
    "thumbprint": "b796e1d3210edcf97290e147d1245cfc9a78132c",
    "thumbprint_sha256":
"988858e7387a90af438c9d1edad64fa01e0e85666ebf88ae458b1ceb553c5760",
    "validity": {
        "not_after": "2019-10-10 14:36:27",
        "not_before": "2019-07-12 14:36:27"
    },
    "version": "V3"
},
"last_https_certificate_date": 1566463571,
"last_modification_date": 1591890478,
"network": "81.169.128.0/17",
"regional_internet_registry": "RIPE NCC",
"reputation": 0,
"tags": [],
"total_votes": {
    "harmless": 0,
    "malicious": 0
},
"whois": "NetRange: 31.0.0.0 - 31.255.255.255\nCIDR:
31.0.0.0/8\nNetName: 31-RIPE\nNetHandle: NET-31-0-0-1\nParent: ()\nNetType:
Allocated to RIPE NCC\nOriginAS: \nOrganization: RIPE Network Coordination
Centre (RIPE)\nRegDate: \nUpdated: 2009-03-25\nComment: These addresses have
been further assigned to users in\nComment: the RIPE NCC region. Contact
information can be found in\nComment: the RIPE database at http://www.ripe.net/

```

```

whois\nRef: https://rdap.arin.net/registry/ip/31.0.0.0\nResourceLink: https://
apps.db.ripe.net/search/query.html\nResourceLink: whois.ripe.net\nOrgName: RIPE
Network Coordination Centre\nOrgId: RIPE\nAddress: P.O. Box 10096\nCity:
Amsterdam\nStateProv: \nPostalCode: 1001EB\nCountry: NL\nRegDate: \nUpdated:
2013-07-29\nRef: https://rdap.arin.net/registry/entity/RIPE\nReferralServer:
whois://whois.ripe.net\nResourceLink: https://apps.db.ripe.net/search/
query.html\nOrgTechHandle: RN029-ARIN\nOrgTechName: RIPE NCC
Operations\nOrgTechPhone: +31 20 535 4444 \nOrgTechEmail:
hostmaster@ripe.net\nOrgTechRef: https://rdap.arin.net/registry/entity/RN029-
ARIN\nOrgAbuseHandle: ABUSE3850-ARIN\nOrgAbuseName: Abuse
Contact\nOrgAbusePhone: +31205354444 \nOrgAbuseEmail:
abuse@ripe.net\nOrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3850-
ARIN\ninetnum: 31.139.365.0 - 31.139.365.255\nnetname: STRATO-RZG-DED\norg:
ORG-SRA1-RIPE\ndescr: Strato Rechenzentrum, Berlin\ncountry: DE\nadmin-c: SRDS-
RIPE\ntech-c: SRDS-RIPE\nremarks:
*****\nremarks: * Please
send abuse complaints to abuse-server@strato.de *\nremarks: * or fax
+49-30-88615-755 ONLY. *\nremarks: * Abuse reports to other e-mail addresses
will be ignored. *\nremarks:
*****\nstatus: ASSIGNED
PA\nmnt-by: STRATO-RZG-MNT\ncreated: 2004-02-03T18:37:52Z\nlast-modified:
2013-07-06T09:34:25Z\nsource: RIPE\norganisation: ORG-SRA1-RIPE\norg-name:
Strato AG\norg-type: LIR\naddress: Pascalstrasse 10\naddress: 10587\naddress:
Berlin\naddress: GERMANY\nphone: +4930398020\nfax-no: +493039802222\nadmin-c:
CM265-RIPE\nabuse-c: SRAC-RIPE\nmnt-ref: RIPE-NCC-HM-MNT\nmnt-ref: STRATO-RZG-
MNT\nmnt-by: RIPE-NCC-HM-MNT\nmnt-by: STRATO-RZG-MNT\ncreated:
2004-04-17T11:12:39Z\nlast-modified: 2019-02-06T12:46:35Z\nsource: RIPE #
Filtered\nrole: RIPE contact Dedicated Server\naddress: STRATO AG\naddress:
Pascalstr. 10\naddress: D-10587 Berlin\naddress: Germany\nphone: +49 30
39802-0\norg: ORG-SRA1-RIPE\nabuse-mailbox: abuse-server@strato.de\nadmin-c:
XX1-RIPE\ntech-c: XX1-RIPE\nnic-hdl: SRDS-RIPE\nremarks:
*****\nremarks: * Please
send abuse complaints to abuse-server@strato.de *\nremarks: * or fax
+49-30-88615-755 ONLY. *\nremarks: * Abuse reports to other e-mail addresses
will be ignored. *\nremarks: * *\nremarks: * For peering requests or
operational issues please look *\nremarks: * at the information in the AS6724
RIPE database object. *\nremarks:
*****\nmnt-by: STRATO-
RZG-MNT\ncreated: 2010-01-15T08:35:31Z\nlast-modified:
2019-02-06T12:47:52Z\nsource: RIPE # Filtered\nroute: 81.169.165.0/24\ndescr:
STRATO AG\ndescr: prefix only advertised in case of DDoS\norigin: AS6724\nmnt-
by: STRATO-RZG-MNT\ncreated: 2014-02-18T16:19:05Z\nlast-modified:
2014-02-18T16:19:05Z\nsource: RIPE\n",
    "whois_date": 1565760528
  },
  "id": "31.139.365.245",
  "links": {
    "self": "https://www.virustotal.com/api/v3/ip_addresses/
31.139.365.245"
  },
  "type": "ip_address"

```

```

    },
    ...
  ]
}

```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.as_owner	Indicator.Attribute	As Owner	Strato AG	N/A
.data[].attributes.asn	Indicator.Attribute	ASN	6724	N/A
.data[].attributes.continent	Indicator.Attribute	Continent	EU	N/A
.data[].attributes.country	Indicator.Attribute	Country	DE	N/A
.data[].attributes.network	Indicator.Attribute	Network	81.169.128.0/17	N/A
.data[].attributes.regional_internet_registry	Indicator.Attribute	Regional Internet Registry	RIPE NCC	N/A
.data[].attributes.reputation	Indicator.Attribute	Reputation	0	N/A
.data[].attributes.whois	Indicator.Attribute	WHOIS	NetRange: 31.0.0.0 - 31.255.255. 255\nCIDR: 31.0.0.0/8\ ...	N/A
.data[].attributes.tags	Indicator.Tag	N/A		N/A
.data[].id	Indicator	IP Address	31.139.365.245	N/A

Domains

GET https://www.virustotal.com/api/v3/collections/{collection_id}/domains

Sample Response:

```
{
  "meta": {
    "count": 6,
    "cursor": "eyJsaW1pdCI6IDIsICJvZmZzZXQiOiAyfQ=="
  },
  "data": [
    {
      "attributes": {
        "categories": {
          "Dr.Web": "known infection source",
          "Forcepoint ThreatSeeker": "bot networks. parked domain"
        },
        "creation_date": 1106675546,
        "favicon": {
          "dhash": "71f0cc989386ba80",
          "raw_md5": "01625852ea10d9fa44p676b1g2ff1df3"
        },
        "jarm":
"27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d",
        "last_analysis_results": {
          "ADMINUSLabs": {
            "category": "harmless",
            "engine_name": "ADMINUSLabs",
            "method": "blacklist",
            "result": "clean"
          },
          "AegisLab WebGuard": {
            "category": "harmless",
            "engine_name": "AegisLab WebGuard",
            "method": "blacklist",
            "result": "clean"
          },
          "AlienVault": {
            "category": "harmless",
            "engine_name": "AlienVault",
            "method": "blacklist",
            "result": "clean"
          }
        },
        "last_analysis_stats": {
          "harmless": 3,
          "malicious": 0,
          "suspicious": 0,
          "timeout": 0,

```

```

        "undetected": 0
    },
    "last_dns_records": [
        {
            "expire": 1814400,
            "minimum": 600,
            "refresh": 3600,
            "retry": 300,
            "rname": "hostmaster.foo-inc.com",
            "serial": 2020061203,
            "ttl": 1799,
            "type": "SOA",
            "value": "ns1.foo.com"
        },
        {
            "ttl": 1162,
            "type": "A",
            "value": "91.117.116.8"
        },
        {
            "ttl": 299,
            "type": "AAAA",
            "value": "2430:2fb0:f0b1:ca3b::6f"
        },
        {
            "priority": 1,
            "ttl": 1545,
            "type": "MX",
            "value": "mta6.am0.foodns.net"
        },
        {
            "flag": 0,
            "tag": "issue",
            "ttl": 1799,
            "type": "CAA",
            "value": "globalsign.com"
        }
    ],
    "last_dns_records_date": 1591833767,
    "last_https_certificate": {
        "cert_signature": {
            "signature":
"9e788e906bca93be8996f3051bc5c1cbb9305a7a02bccd6f4a132555f0487f7f96f767ef66becc
91d1e22704b1ec383a9d44237c3ecf28833bef44a7105186237750301371d45049e9809f1afd433
1c6f0ebc077c16d86558f43a893e8871226132a677db3d2089c6300f4e1881eaed447ee3623a12c
be0552a0f8b73d29f195135c4f25bp700f035080afe87f2e54fd8c8fa1a505535ee3320ef04f90d
e13222fa476e27ed66fcbddd64e36ea77cbfb602d1f93f7f58ce84af5435096906aa9ad60e8d86c
d7c05207e5d7d47186831e14d5940648e02d407c82be1accb2343725578005020c61980fe341367
05ce8f81cf3202429cc058f405130c4dacfa13e",
            "signature_algorithm": "sha256RSA"
        }
    }
}

```

```

    },
    "extensions": {
      "1.3.6.1.4.1.11129.2.4.2":
"0481f300f1007700vbea773f9df56c0e7b536487dd049e0327a919a0c84a11212",
      "CA": true,
      "authority_key_identifier": {
        "keyid": "98d1f86e10ebcf9bec6089918901ba0eb7d09fd2b"
      },
      "ca_information_access": {
        "CA Issuers": "http://pki.goog/gsr2/GTS101.crt",
        "OCSP": "http://ocsp.pki.goog/gts101"
      },
      "certificate_policies": [
        "2.23.140.1.2.2",
        "1.3.6.1.4.1.11129.2.5.3"
      ],
      "crl_distribution_points": [
        "http://crl.pki.goog/GTS101.crl"
      ],
      "extended_key_usage": [
        "serverAuth"
      ],
      "key_usage": [
        "ff"
      ],
      "subject_alternative_name": [
        "upload.video.foo.com",
        "*.clients.foo.com",
        "*.docs.foo.com"
      ],
      "subject_key_identifier":
"9da1b782caaad70a2c9480ac488aca8316ad7790",
      "tags": []
    },
    "issuer": {
      "C": "US",
      "CN": "GTS CA 101",
      "O": "Google Trust Services"
    },
    "public_key": {
      "algorithm": "EC",
      "ec": {
        "oid": "secp256r1",
        "pub":
"04139a8a6a96066c0c62b5358b863147314b402ea9b079cd00361c9099d23cb3db2d937e9cfed2
b3826f5ea7f64074a038acd7f33d37c7f897fe95d544c25c8dfc"
      }
    },
    "serial_number": "a7670522413cc18d0800000000420d4f",
    "signature_algorithm": "sha256RSA",

```

```

        "size": 1506,
        "subject": {
            "C": "US",
            "CN": "upload.video.foo.com",
            "L": "Mountain View",
            "O": "Google LLC",
            "ST": "California"
        },
        "tags": [],
        "thumbprint": "ea2fe94b45d4c2929d3c2fd84292086820bd86ad",
        "thumbprint_sha256":
"24c386d0829cae13b3c923bfc5c337d156c11c6ea6136b02e5c0a48634328e83",
        "validity": {
            "not_after": "2020-08-12 12:07:40",
            "not_before": "2020-05-20 12:07:40"
        },
        "version": "V3"
    },
    "last_https_certificate_date": 1591833767,
    "last_modification_date": 1591889814,
    "last_update_date": 1577183919,
    "popularity_ranks": {
        "Alexa": {
            "rank": 47288,
            "timestamp": 1591630561
        },
        "Cisco Umbrella": {
            "rank": 338,
            "timestamp": 1591803361
        },
        "Majestic": {
            "rank": 36741,
            "timestamp": 1585496163
        },
        "Statvoo": {
            "rank": 24060,
            "timestamp": 1591889764
        }
    },
    "registrar": "MarkMonitor Inc.",
    "reputation": 0,
    "tags": [
        "dga"
    ],
    "total_votes": {
        "harmless": 0,
        "malicious": 0
    },
    "whois": "Creation Date: 2005-01-25T17:52:26Z\nDNSSEC:
unsigned\nDomain Name: FOOAPIS.COM\nDomain Status: clientDeleteProhibited

```

```
https://icann.org/epp#clientDeleteProhibited\nDomain Status:
clientTransferProhibited https://icann.org/epp#clientTransferProhibited\nDomain
Status: clientUpdateProhibited https://icann.org/
epp#clientUpdateProhibited\nDomain Status: serverDeleteProhibited https://
icann.org/epp#serverDeleteProhibited\nDomain Status: serverTransferProhibited
https://icann.org/epp#serverTransferProhibited\nDomain Status:
serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited\nName
Server: NS1.FOO.COM\nName Server: NS2.FOO.COM\nName Server: NS3.FOO.COM\nName
Server: NS4.FOO.COM\nRegistrar Abuse Contact Email:
abusecomplaints@markmonitor.com\nRegistrar Abuse Contact Phone:
+1.2083895740\nRegistrar IANA ID: 292\nRegistrar URL: http://
www.markmonitor.com\nRegistrar WHOIS Server: whois.markmonitor.com\nRegistrar:
MarkMonitor Inc.\nRegistry Domain ID: 140496530_DOMAIN_COM-VRSN\nRegistry
Expiry Date: 2021-01-25T17:52:26Z\nUpdated Date: 2019-12-24T10:38:39Z"
    },
    "id": "foo.fooapis.com",
    "links": {
      "self": "https://www.virustotal.com/api/v3/domains/foo.fooapis.com"
    },
    "type": "domain"
  },
  ...
]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.creation_date	Indicator.Attribute	Creation Date	2005-01-25 17:52:26-00:00	Uses timestamp to convert from datetime to standardized
.data[].attributes.jarm	Indicator.Attribute	JARM	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d	N/A
.data[].attributes.registrar	Indicator.Attribute	Registrar	MarkMonitor Inc.	N/A
.data[].attributes.reputation	Indicator.Attribute	Reputation	0	N/A
.data[].attributes.whois	Indicator.Attribute	WHOIS	Creation Date: 2005-01-25T17:52:26Z\nDNSSEC: unsigned\nDomain Name: ...	N/A
.data[].attributes.tags	Indicator.Tag	N/A	dga	N/A
.data[].id	Indicator	FQDN	foo.fooapis.com	N/A

URLs

GET https://www.virustotal.com/api/v3/collections/{collection_id}/urls

Sample Response:

```
{
  "meta": {
    "count": 6,
    "cursor": "eyJsaW1pdCI6IDIsICJvZmZzZXQiOiAyfQ=="
  },
  "data": [
    {
      "attributes": {
        "categories": {
          "BitDefender": "business",
          "Forcepoint ThreatSeeker": "web hosting"
        },
        "favicon": {
          "dhash": "30d6d6dec869b6a6",
          "raw_md5": "f6c933a8a01167c2bfgb5fg65183781"
        },
        "first_submission_date": 1591711462,
        "has_content": true,
        "html_meta": {
          "description": [
            kv\u0017cwego"
            ],
            "sessid": [
              "6555835"
            ],
            "viewport": [
              "width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no"
            ]
          },
          "last_analysis_date": 1591715484,
          "last_analysis_results": {
            "ADMINUSLabs": {
              "category": "harmless",
              "engine_name": "ADMINUSLabs",
              "method": "blacklist",
              "result": "clean"
            },
            "AegisLab WebGuard": {
              "category": "harmless",
              "engine_name": "AegisLab WebGuard",
              "method": "blacklist",
              "result": "clean"
            }
          }
        }
      }
    }
  ]
}
```

```

    },
    "AlienVault": {
      "category": "harmless",
      "engine_name": "AlienVault",
      "method": "blacklist",
      "result": "clean"
    },
    "Antiy-AVL": {
      "category": "harmless",
      "engine_name": "Antiy-AVL",
      "method": "blacklist",
      "result": "clean"
    },
    "Artists Against 419": {
      "category": "harmless",
      "engine_name": "Artists Against 419",
      "method": "blacklist",
      "result": "clean"
    }
  },
  "last_analysis_stats": {
    "harmless": 64,
    "malicious": 7,
    "suspicious": 0,
    "timeout": 0,
    "undetected": 9
  },
  "last_final_url": "http://pocvttpalok.net/qwlotnvsc8090067532",
  "last_http_response_code": 200,
  "last_http_response_content_length": 28195,
  "last_http_response_content_sha256":
"45b81b2d4c58ada2c13q503hb56daf440ec1b9b69f3737df4cf460a080c0ab63",
  "last_http_response_cookies": {
    "PHPSESSID": "5aivcogdl1tjp2b4kbfbm5551mo0",
    "SameSite": "Lax,",
    "__cfduid": "d84e7486e1p2cc5a7ff3vd85d128183624591715485",
    "sessid": "494429474"
  },
  "last_http_response_headers": {
    "cache-control": "no-store, no-cache, must-revalidate, post-
check=0, pre-check=0",
    "cf-cache-status": "DYNAMIC",
    "cf-ray": "5a0b78f576668hch-0hD",
    "cf-request-id": "03hb3befhc00h083h9dh9c820h0h0h01",
    "connection": "keep-alive",
    "content-type": "text/html; charset=UTF-8",
    "date": "Tue, 09 Jun 2020 15:11:25 GMT",
    "expires": "Thu, 19 Nov 1981 08:52:00 GMT",
    "pragma": "no-cache",
    "server": "cloudflare",

```

```

        "set-cookie":
        "__cfduid=d8ded48de1d2dc1da7df34d85d1bd1d56d1d9d7d5d85; expires=Thu, 09-Jul-20
        15:11:25 GMT; path=/; domain=.fpofztfpflfk.net; HttpOnly; SameSite=Lax,
        PHPSESSID=5afvcfgf1tjs2bakf1mfvfqfo0; path=/, sessid=665627777; expires=Thu,
        09-Jul-2020 15:10:43 GMT; Max-Age=2592000; path=/",
        "transfer-encoding": "chunked"
    },
    "last_modification_date": 1591715488,
    "last_submission_date": 1591715484,
    "outgoing_links": [
        "https://ssl.dgtuww.pl/files/reg2lafif_gttp3w_way.pdf",
        "http://www.dtywpwy.pl/polwtwka-wwikow-wowkiws/"
    ],
    "reputation": -44,
    "redirection_chain": [
        "http://wwwcztapwlwk.net/plafgxc80333067532",
        "http://wwwcztapwlwk.net/step2"
    ],
    "tags": [
        "base64-embedded"
    ],
    "targeted_brand": {
        "Phishtank": "Bank Blablabla"
    },
    "times_submitted": 2,
    "title": "Dwtpww - Bwzpiwczww plwtnew wntwrnewowe wa kwzdego!",
    "total_votes": {
        "harmless": 0,
        "malicious": 1
    },
    "trackers": {
        "Google Tag Manager": [
            {
                "id": "UA-162655555-1",
                "timestamp": 1603372118,
                "url": "https://www.googletagmanager.com/gtag/js?
id=UA-162655555-1"
            }
        ]
    },
    "url": "http://wwwcztapwlwk.net/plafgxc80333067532"
},
"id":
"661q6ceqa60e4qaf1998qa8aa8q6d8daq4c51qc2qfqc5fcd6d885700c0acee3b",
"links": {
    "self": "https://www.virustotal.com/ui/urls/
661q6ceqa60e4qaf1998qa8aa8q6d8daq4c51qc2qfqc5fcd6d885700c0acee3b"
},
"type": "url"
},

```

```

    ...
  ]
}

```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.reputation	Indicator.Attribute	Reputation	-44	N/A
.data[].attributes.times_submitted	Indicator.Attribute	Times Submitted	2	N/A
.data[].attributes.title	Indicator.Attribute	Title	Dwtpww - Bwzpiwcwww plwtntwww wntwrnewowe wa kwzdego!	N/A
.data[].attributes.tags	Indicator.Tag	N/A	base64-embedded	N/A
.data[].attributes.url	Indicator	URL	http://wwwcztapwlwk.net/ plafgxc80333067532	N/A

Files

GET https://www.virustotal.com/api/v3/collections/{collection_id}/files

Sample Response:

```
{
  "meta": {
    "count": 6,
    "cursor": "eyJsaW1pdCI6IDIsICJvZmZzZXQiOiAyfQ=="
  },
  "data": [
    {
      "attributes": {
        "capabilities_tags": [
          "str_win32_internet_api",
          "cred_ff",
          "win_mutex",
          "keylogger",
          "str_win32_winsock2_library",
          "sniff_audio",
          "network_dropper",
          "ldpreload",
          "win_files_operation",
          "str_win32_wininet_library",
          "inject_thread"
        ],
        "creation_date": 1589251011,
        "crowdsourced_ids_results": [
          {
            "alert_context": [
              {
                "proto": "TCP",
                "src_ip": "152.126.25.42",
                "src_port": 80
              }
            ],
            "alert_severity": "high",
            "rule_category": "Potential Corporate Privacy Violation",
            "rule_id": "32481",
            "rule_msg": "POLICY-OTHER Remote non-JavaScript file found in script tag src attribute",
            "rule_source": "snort"
          }
        ],
        "crowdsourced_ids_stats": {
          "high": 1,
          "info": 0,
          "low": 0,
          "medium": 0
        }
      }
    }
  ]
}
```

```

},
"crowdsourced_yara_results": [
  {
    "description": "Detects a very evil attack",
    "match_in_subfile": true,
    "rule_name": "evil_a_b",
    "ruleset_id": "000abc43",
    "ruleset_name": "evilness",
    "source": "https://example.com/evil/ruleset"
  }
],
"downloadable": true,
"first_submission_date": 1592134853,
"last_analysis_date": 1592141610,
"last_analysis_results": {
  "ALYac": {
    "category": "malicious",
    "engine_name": "ALYac",
    "engine_update": "20200614",
    "engine_version": "1.1.1.5",
    "method": "blacklist",
    "result": "Trojan.GenericKDZ.67102"
  },
  "APEX": {
    "category": "malicious",
    "engine_name": "APEX",
    "engine_update": "20200613",
    "engine_version": "6.36",
    "method": "blacklist",
    "result": "Malicious"
  },
  "AVG": {
    "category": "malicious",
    "engine_name": "AVG",
    "engine_update": "20200614",
    "engine_version": "18.4.3895.0",
    "method": "blacklist",
    "result": "Win32:PWSX-gen [Trj]"
  },
  "Acronis": {
    "category": "undetected",
    "engine_name": "Acronis",
    "engine_update": "20200603",
    "engine_version": "1.1.1.76",
    "method": "blacklist",
    "result": null
  }
},
"last_analysis_stats": {
  "confirmed-timeout": 0,

```

```

        "failure": 0,
        "harmless": 0,
        "malicious": 3,
        "suspicious": 0,
        "timeout": 0,
        "type-unsupported": 0,
        "undetected": 2
    },
    "last_modification_date": 1592141790,
    "last_submission_date": 1592141610,
    "md5": "5a430646b4d3c04f0b43b444ad48443f",
    "meaningful_name": "o4oz44Z4E444.exe",
    "names": [
        "myfile.exe",
        "o4oz44Z4E444.exe"
    ],
    "reputation": 0,
    "sandbox_verdicts": {
        "VirusTotal Jujubox": {
            "category": "malicious",
            "confidence": 70,
            "malware_classification": [
                "MALWARE",
                "TROJAN"
            ],
            "malware_names": [
                "XMRigMiner"
            ],
            "sandbox_name": "VirusTotal Jujubox"
        },
        "sha1": "54fdf53af86f90bf446f0a5fe26f6e4fd5f4c9fd",
        "sha256": "3f6fa13af90cf967f0b5f5d07f413f9d1f39d2fa366f09ff760fcd3fd8bf6fbf",
        "sigma_analysis_stats": {
            "critical": 0,
            "high": 0,
            "low": 2,
            "medium": 0
        },
        "sigma_analysis_summary": {
            "Sigma Integrated Rule Set (GitHub)": {
                "critical": 0,
                "high": 0,
                "low": 2,
                "medium": 0
            }
        },
        "size": 374272,
        "tags": [

```

```

        "peexe",
        "runtime-modules",
        "assembly",
        "direct-cpu-clock-access",
        "detect-debug-environment"
    ],
    "times_submitted": 3,
    "total_votes": {
        "harmless": 0,
        "malicious": 0
    },
    "type_description": "Win32 EXE",
    "type_tag": "exe",
    "type_tag": "peexe",
    "unique_sources": 3,
    "vhash": "2350f6f515f29f93f147f0f0"
},
    "id":
    "3f6fa13af90cf967f0b5f5d07f413f9d1f39d2fa366f09ff760fcd3fd8bf6fbf",
    "links": {
        "self": "https://www.virustotal.com/ui/files/
3f6fa13af90cf967f0b5f5d07f413f9d1f39d2fa366f09ff760fcd3fd8bf6fbf"
    },
    "type": "file"
},
    ...
]
}

```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.creation_date	Indicator.Attribute	Creation Date	2020-05-12 2:36:51-00:00	Uses timestamp to convert from datetime to standardized
.data[].attributes.downloadable	Indicator.Attribute	Downloadable	True	Only available for Premium API users
.data[].attributes.meaningful_name	Indicator.Attribute	Meaningful Name	o4oz44Z4E444.exe	N/A
.data[].attributes.size	Indicator.Attribute	Size	374272	File size in bytes
.data[].attributes.times_submitted	Indicator.Attribute	Times Submitted	3	N/A
.data[].attributes.type_description	Indicator.Attribute	Type Description	Win32 EXE	N/A
.data[].attributes.reputation	Indicator.Attribute	Reputation	0	N/A
.data[].attributes.type_extension	Indicator.Attribute	Type Extension	exe	N/A
.data[].attributes.unique_sources	Indicator.Attribute	Unique Sources	3	N/A
.data[].attributes.capabilities_tags	Indicator.Tag	N/A	str_win32_internet_api	Only available for Premium API users.
.data[].attributes.type_tag	Indicator.Tag	N/A	peexe	N/A
.data[].attributes.tags	Indicator.Tag	N/A	runtime-modules	N/A
.data[].attributes.md5	Indicator	MD5	5a430646b4d3c04f0b43b444ad48443f	N/A
.data[].attributes.sha1	Indicator	SHA-1	54fdf53af86f90bf446f0a5fe26f6e4fd5f4c9fd	N/A
.data[].attributes.sha256	Indicator	SHA-256	3f6fa13af90cf967f0b5f5d07f413f9d1f39d2fa366f09ff760fcd3fd8bf6fbf	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.

VirusTotal Collections

METRIC	RESULT
Run Time	15 minutes
Indicators	1,788
Indicator Attributes	19,719

Change Log

- **Version 1.0.1**
 - Resolved a filter-mapping timeout issue.
- **Version 1.0.0**
 - Initial release