

ThreatQuotient



VirusTotal Operation User Guide

Version 3.1.0

February 06, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 9

 search_ip, search_domain, submit_url, search_hash 10

 search_url..... 11

 IoC Type Mapping..... 16

 Supplemental calls..... 17

 Relationships Mapping 21

 Action Parameters 23

Change Log 25

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 © 2024 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 3.1.0

**Compatible with ThreatQ
Versions** $\geq 4.47.0$

Support Tier ThreatQ Supported

Introduction

The VirusTotal operation enriches ThreatQ objects with context obtained from the VirusTotal API.

The operation provides the following actions:

- **search_ip** - submits IP for analysis.
- **search_domain** - submits domain for analysis.
- **submit_url** - submits URL for analysis.
- **search_url** - retrieves the VirusTotal report for a URL.
- **search_hash** - submits hash for analysis.

The operation is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256
- FQDN
- IP Address
- URL

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 .whl 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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure](#) and then [enable](#) the operation.

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 **Operation** option from the *Type* dropdown (optional).
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 private or public VirusTotal API Key.
Automatically Add Attributes	If checked, indicator attributes are added automatically.
Automatically Add Indicators	If checked, related indicators, along with their attributes, are added automatically. If not checked, the user can select which indicators to be added (without their attributes).

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.

Actions

The VirusTotal operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
search_ip	Submits IP for analysis.	Indicator	IP
search_domain	Submits domain for analysis.	Indicator	FQDN
submit_url	Submits URL for analysis.	Indicator	URL
search_url	Retrieves the VirusTotal report for a URL.	Indicator	URL
submit_hash	Submits hash for analysis.	Indicator	MD5, SHA-1, SHA-256

search_ip, search_domain, submit_url, search_hash

These actions first call VirusTotal Scan and then retrieves the VirusTotal Report.

search_url

The search_url action retrieves the VirusTotal report if a VirusTotal Scan ID attribute exists for the URL object.

GET https://www.virustotal.com/api/v3/{vt_collection_name}/{ioc_value}



vt_collection_name represents the plural form of the object type as it appears in VirusTotal, while ioc_value represents the actual value of the objects for all indicators except for URLs. The URLs are first encoded to Base64.

Sample Response:

```
{
  "data": {
    "attributes": {
      "type_description": "DOS EXE",
      "tlsh":
"T178445B4972A43CF9ECA7C239C657461BEFF27C664630D35F03641A9A4F233A1622E752",
      "exiftool": {
        "MIMEType": "application/octet-stream",
        "FileType": "DOS EXE",
        "FileTypeExtension": "exe"
      },
      "trid": [
        {
          "file_type": "DOS Executable Generic",
          "probability": 100
        }
      ],
      "crowdsourced_yara_results": [
        {
          "description": "Detects Meterpreter Beacon - file K5om.dll",
          "source": "https://github.com/Neo23x0/signature-base",
          "author": "Florian Roth",
          "ruleset_name": "apt_apt19",
          "rule_name": "Beacon_K5om",
          "ruleset_id": "000f28467c"
        }
      ],
      "names": [
        "e2f6cdade9be842ebd160634c30f1e16.virus"
      ],
      "last_modification_date": 1654841377,
      "type_tag": "mz",
      "times_submitted": 1,
      "total_votes": {
        "harmless": 0,
        "malicious": 0
      }
    }
  }
}
```

```

    },
    "size": 263358,
    "popular_threat_classification": {
      "suggested_threat_label": "trojan.cobaltstrike",
      "popular_threat_category": [
        {
          "count": 4,
          "value": "trojan"
        }
      ],
    },
    "popular_threat_name": [
      {
        "count": 4,
        "value": "cobaltstrike"
      }
    ]
  },
  "last_submission_date": 1653524502,
  "last_analysis_results": {
    "ClamAV": {
      "category": "malicious",
      "engine_name": "ClamAV",
      "engine_version": "0.105.0.0",
      "result": "Win.Trojan.CobaltStrike-8091534-0",
      "method": "blacklist",
      "engine_update": "20220609"
    },
    "FireEye": {
      "category": "undetected",
      "engine_name": "FireEye",
      "engine_version": "35.24.1.0",
      "result": null,
      "method": "blacklist",
      "engine_update": "20220610"
    }
  },
  "downloadable": true,
  "sha256":
"56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23",
  "type_extension": "exe",
  "tags": [
    "mz"
  ],
  "last_analysis_date": 1654834036,
  "unique_sources": 1,
  "first_submission_date": 1653524502,
  "ssdeep": "3072:3sYckn3Xzq4IDwSK2Mbn/
gprEJwJNJsCwQTIfXouPru00TR09BQYJerCo2e:3sYwjwIGIprEJweGTIDjh0TRqQ8I",
  "md5": "e2f6cdade9be842ebd160634c30f1e16",
  "sha1": "ccbbc621afe012b358ed2e13875f1581b944dd25",

```

```

"magic": "MS-DOS executable, MZ for MS-DOS",
"last_analysis_stats": {
  "harmless": 0,
  "type-unsupported": 11,
  "suspicious": 0,
  "confirmed-timeout": 0,
  "timeout": 0,
  "failure": 2,
  "malicious": 5,
  "undetected": 54
},
"meaningful_name": "e2f6cdade9be842ebd160634c30f1e16.virus",
"reputation": 0
},
"type": "file",
"id": "56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23",
"links": {
  "self": "https://www.virustotal.com/api/v3/files/
56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23"
}
}
}

```

ThreatQuotient provides the following default mapping for these actions:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious Count	.attributes.creation_date or .attributes.first_submission_date	10	If Malicious Count user option is checked. For all indicator types.
.attributes.last_analysis_stats.harmless	Indicator.Attribute	Harmless Count	.attributes.creation_date or .attributes.first_submission_date	23	If Harmless Count user option is checked. For all indicator types.
.attributes.last_analysis_stats.suspicious	Indicator.Attribute	Suspicious Count	.attributes.creation_date or .attributes.first_submission_date	8	If Suspicious Count user option is checked. For all indicator types.
.attributes.last_analysis_stats.undetected	Indicator.Attribute	Undetected Count	.attributes.creation_date or .attributes.first_submission_date	0	If Undetected Count user option is checked. For all indicator types.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.reputation	Indicator.Attribute	Reputation	.attributes.creation_date or .attributes.first_submission_date	0	If Basic Properties or Reputation user option is checked. For all indicator types.
.attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious	.attributes.creation_date or .attributes.first_submission_date	True	If .attributes.last_analysis_stats.malicious is greater or equal then the Malicious Verdict Threshold value.
.attributes.type_description	Indicator.Attribute	File Type	.attributes.creation_date or .attributes.first_submission_date	DOS EXE	For File Hashes. If Basic Properties user option is checked
.attributes.first_submission_date	Indicator.Attribute	First Published Date	.attributes.creation_date or .attributes.first_submission_date	1581118958	For File Hashes. If Basic Properties user option is checked
.attributes.first_submission_date	Indicator.Attribute	First Submission Date	.attributes.creation_date or .attributes.first_submission_date	1581118958	For URLs. If Basic Properties user option is checked
.attributes.last_analysis_results.result	Indicator.Attribute	Last Analysis Result	.attributes.creation_date or .attributes.first_submission_date	0	For File Hashes. If Basic Properties user option is checked.
.attributes.meaningful_name	Indicator.Attribute	Meaningful Name	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16.virus	For File Hashes. If Basic Properties user option is checked
.attributes.md5	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16	For File Hashes. If MD5 user option is checked

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.md5	Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16	For File Hashes. If MD5 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.md5}
.attributes.sha1	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	ccbbc621afe012b358ed2e13875f1581b944dd25	For File Hashes. If SHA-1 user option is checked
.attributes.sha1	Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	ccbbc621afe012b358ed2e13875f1581b944dd25	For File Hashes. If SHA-1 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.sha1}
.attributes.sha256	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23	For File Hashes. If SHA-256 user option is checked
.attributes.sha256	Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23	For File Hashes. If SHA-256 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.sha256}
.attributes.names[]	Indicator.Attribute	Name	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16.virus	For File Hashes. If Names user option is checked
.attributes.asn	Related Indicator	ASN	.attributes.creation_date or .attributes.first_submission_date	39798	For IP Addresses. If Basic Properties

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					user option is checked
.attributes.as_owner	Indicator.Attribute	AS Owner	.attributes.creation_date or .attributes.first_submission_date	MivoCloud SRL	For IP Addresses. If Basic Properties user option is checked
.attributes.last_https_certificate	Indicator.Attribute	Last SSL certificate	.attributes.creation_date or .attributes.first_submission_date	1581118958	For IP Addresses. If Last SSL certificate user option is checked

IoC Type Mapping

The following tables provides ThreatQ to VirusTotal Collection Name IoC type mapping.

THREATQ IOC TYPE	VIRUSTOTAL COLLECTION NAME
FQDN	domain
IP Address	ip_addresses
URL	urls
MD5, SHA-1, SHA-256	files

Supplemental calls

VirusTotal objects contain relationships with other objects in the dataset that can be retrieved using the following endpoint:

GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/{{ioc_value}}/{{relationship}}

Sample Response:

```
{
  "meta": {
    "count": 1
  },
  "data": [
    {
      "attributes": {
        "last_dns_records": [
          {
            "type": "CNAME",
            "value": "rigpriv.com",
            "ttl": 599
          },
          {
            "type": "NS",
            "value": "jm2.dns.com",
            "ttl": 21600
          }
        ],
        "jarm":
"28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88",
        "whois": "Creation Date: 2022-06-29T16:00:00Z\nCreation Date:
2022-06-30T02:32:32Z\nDNSSEC: unsigned\nDomain Name: RIGPRIV.COM\nDomain
Status: ok https://icann.org/epp#ok\nName Server: JM1.DNS.COM\nName Server:
JM2.DNS.COM\nRegistrant City: 7145b6c7c70448a6\nRegistrant Country:
CN\nRegistrant Email: 5c0a26a8248bb13fs@\nRegistrant State/Province:
4f3a9c87b8ed6c6a\nRegistrar Abuse Contact Email: domainabuse@35.cn\nRegistrar
Abuse Contact Phone: +86.4001353511\nRegistrar Abuse Contact Phone:
+86.4006003535\nRegistrar IANA ID: 1316\nRegistrar Registration Expiration
Date: 2023-06-30T04:00:00Z\nRegistrar URL: http://www.35.com\nRegistrar WHOIS
Server: whois.35.com\nRegistrar: Xiamen 35.Com Technology Co., Ltd\nRegistrar:
Xiamen 35.Com Technology Co., Ltd.\nRegistry Domain ID: 2707568686_DOMAIN_COM-
VRSN\nRegistry Expiry Date: 2023-06-30T02:32:32Z\nRegistry Registrant ID: Not
Available From Registry\nUpdated Date: 2022-06-30T02:43:05Z\nUpdated Date:
2022-08-21T16:00:00Z",
        "last_https_certificate_date": 1660080390,
        "tags": [],
        "popularity_ranks": {},
        "last_dns_records_date": 1660080390,
        "last_analysis_stats": {
```

```

        "harmless": 86,
        "malicious": 0,
        "suspicious": 0,
        "undetected": 8,
        "timeout": 0
    },
    "creation_date": 1656556352,
    "reputation": 0,
    "registrar": "Xiamen 35.Com Technology Co., Ltd",
    "last_analysis_results": {
        "CMC Threat Intelligence": {
            "category": "harmless",
            "result": "clean",
            "method": "blacklist",
            "engine_name": "CMC Threat Intelligence"
        }
    },
    "last_update_date": 1661097600,
    "last_modification_date": 1660080390,
    "last_https_certificate": {
        "size": 1159,
        "public_key": {
            "ec": {
                "oid": "secp256r1",
                "pub":
"0481596f6c64661fffb6a79fce6cba763d9ee961778b6e21f93eca791db1bb8fa401bbda5b35fc3
874e05774448520d600e5f041b35257c4d7b428390afac0d514e"
            },
            "algorithm": "EC"
        },
        "thumbprint_sha256":
"2a676d52b302af217fd08e64dca3a5635bd8eea0d19ad91a50c518da2e26acc4",
        "tags": [],
        "cert_signature": {
            "signature":
"6902093866e2a299575f2c04f852aaf3c2789cf53687873d4e6f599ea9140101e9be50dd8774f0
1b30115ca721561416a4d03d316b146844a3b819ec235346bb2ddc7cf3a17592a142c6b303080b1
8cd801d28bf7738fffb3e513059d8c0664783bc7edaf3711c1e6062eb20abedada8c0c8f5b2a1be2
0519b3056422f3c92b02c4190f649189ea4ed07d2f9e3e87839bb180afe9a81e36f28a826400eee
290775b2035bb37b681424d8224e5c8955d5ce21ecf0475a7670f772fe16e5133176fd6dc0cc538
c3d459faa72f7ffec06c4c1f9f2578cb168f82c56e10a0ffa77365db3378f6f55fbb1144465011a
0cadb2d72658fc59b54958b0f34a89de56d640c",
            "signature_algorithm": "sha256RSA"
        },
        "validity": {
            "not_after": "2022-10-20 12:54:43",
            "not_before": "2022-07-22 12:54:44"
        },
        "version": "V3",
        "extensions": {

```

```

        "certificate_policies": [
            "2.23.140.1.2.1",
            "1.3.6.1.4.1.44947.1.1.1"
        ],
        "extended_key_usage": [
            "serverAuth",
            "clientAuth"
        ],
        "authority_key_identifier": {
            "keyid": "142eb317b75856cbae500940e61faf9d8b14c2c6"
        },
        "subject_alternative_name": [
            "m.rigpriv.com",
            "rigpriv.com",
            "wap.rigpriv.com",
            "www.rigpriv.com"
        ],
        "tags": [],
        "subject_key_identifier":
"48a87063dd6dc4462b432889e1615c2ce20f118d",
        "key_usage": [
            "ff"
        ],
        "1.3.6.1.4.1.11129.2.4.2":
"0481f100ef007500dfa55eab68824f1f6cadeeb85f4e3e5aeacda212a46a5e8e",
        "CA": true,
        "ca_information_access": {
            "CA Issuers": "http://r3.i.lencr.org/",
            "OCSP": "http://r3.o.lencr.org"
        }
    },
    "signature_algorithm": "sha256RSA",
    "serial_number": "044be080e3027b8cbf43952e34f00ce03492",
    "thumbprint": "de1cabd8d7c8b5e3b9ef2d8899b2f148390fa3d2",
    "issuer": {
        "C": "US",
        "CN": "R3",
        "O": "Let's Encrypt"
    },
    "subject": {
        "CN": "m.rigpriv.com"
    }
},
"categories": {},
"total_votes": {
    "harmless": 0,
    "malicious": 0
}
},
"type": "domain",

```

```

        "id": "wap.rigpriv.com",
        "links": {
            "self": "https://www.virustotal.com/api/v3/domains/
wap.rigpriv.com"
        }
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/domains/rigpriv.com/
subdomains?limit=10"
    }
}

```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.url	Related Indicator.Value	N/A	N/A	www.rigpriv.com/ upload	For URLs relationships
.attributes.md5	Related Indicator.Value	N/A	N/A	e2f6cdade9be842 ebd160634c30f1e 16	For Referrer MD5 relationship
.attributes.sha1	Related Indicator.Value	N/A	N/A	ccb6c621afe012b3 58ed2e13875f1581 b944dd25	For Referrer SHA-1 relationship
.attributes.sha256	Related Indicator.Value	N/A	N/A	56e784268807ee23 7adebd98046f0090c eecdfe6d2e1326af d3670e4e3ffd23	For Referrer SHA-256 relationship
.context_attributes.first_seen_date	Indicator.Attribute	Historical SSL certificate	N/A	1591571057	For Historical SSL certificate relationship
.id	Related Indicator.Value	View the Relationships table above	N/A	www.rigpriv.com	For all other relationships
.attributes.last_dns_records	Related Indicator.Value	IP Address	N/A	N/A	For domains relationships

Relationships Mapping

The available relationships are shown in the following table:

VIRUSTOTAL COLLECTION NAME	VIRUSTOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
domains	ns_records	FQDNs	VT Premium users only
domains	soa_records	FQDNs	VT Premium users only
domains	mx_records	FQDNs	VT Premium users only
domains	urls	Immediate Parent	Everyone
domains	parent	Parent	Everyone
domains	siblings	Siblings	Everyone
domains	immediate_parent	Immediate Parent	Everyone
domains	subdomains	Subdomains	Everyone
domains	urls	URLs	VT Premium users only
ip_addresses	historical_ssl_certificates	Historical SSL certificates	Everyone
ip_addresses	urls	URLs	VT Premium users only

VIRUSTOTAL COLLECTION NAME	VIRUSTOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
urls	contacted_domains	Contacted Domains	VT Premium users only
urls	redirecting_urls	Redirecting URLs	VT Premium users only
urls	referrer_files	Referrer Files	VT Premium users only
urls	referrer_urls	Referrer URLs	VT Premium users only

Action Parameters

Each action provides the offers the following configuration parameters:

PARAMETER	DESCRIPTION
API Key	Private or public VirusTotal API key.
Automatically add attributes	If checked, Indicator attributes are added automatically.
Automatically add indicators	If checked, Indicator are added automatically.
Malicious Verdict Threshold	The minimum number of AV scans reporting the IOC as malicious. Passing this threshold will result in an attribute of "Malicious: True" to be added.
AV Scan Information	Number of reports from URL scanners marking it as harmless, suspicious, malicious or undetected
Supporting Context (for File Hash Submission)	Extra information to fetch, File Type, First Published Date, Meaningful Name, Names and VirusTotal Link
Synonymous Hashes (for File Hash Submission)	Which indicator type should be ingested into ThreatQ for File Hash Submission (MD5, SHA-256, SHA-1)
Set synonymous hash status to...	The status of the ingested IOCs.
Supporting Context (for FQDN Submission)	Which data should be used to enrich the IOC for FQDN Submission.
Relationships (for FQDN Submission)	The Relationships data to be retrieved from VirusTotal (for FQDN Submission).
Set related indicator status to...	The status of the related indicators (for FQDN, IP Address and URL Submission)

PARAMETER	DESCRIPTION
Supporting Context (for IP Address Submission)	Which data should be used to enrich the IOC for IP Address Submission.
Relationships (for IP Address Submission)	The Relationships data to be retrieved from VirusTotal (for IP Address Submission).
Supporting Context (for URL Submission)	Which data should be used to enrich the IOC for URL Submission.
Relationships (for URL Submission)	The Relationships data to be retrieved from VirusTotal (for URL Submission).

Change Log

- **Version 3.1.0**
 - Resolved an issue where URLs were ingested instead of the proper IoC types for the FQDN's related IoC.
 - Updated the following action names:
 - **submit_ip** is now **search_ip**
 - **submit_domain** is now **search_domain**
 - **submit_hash** is now **search_hash**
 - Added a new action: **search_url**. This action retrieves the VirusTotal report for a URL.
 - Updated the Referrer URL attribute name.
- **Version 3.0.2**
 - Resolved the following issues:
 - no results would be returned for non-malicious IOCs.
 - If supporting context endpoints are not licensed, no enrichment would be returned at all.
 - (UX issue) when submitting URLs, it would only show the raw response.
 - Attribute names for Related Files are now displayed as Related <hash type>.
 - Attribute Redirecting URL now includes the URL value rather than its ID.
 - Added an info block when malicious count > 0, but the malicious threshold was not met.
 - Renamed attributes to better illustrate what they represent.
 - Added support for the Reputation attribute.
- **Version 3.0.1**
 - Updated the operation for improved reentrancy.
- **Version 3.0.0**
 - Updated the API to match VirusTotal API V3.
 - Performed functionality improvements to the actions.
 - Performed UI enhancements.
- **Version 2.3.0**
 - Submit URL - FQDN indicators can't be submitted through this action anymore
 - Submit IP - .asn attribute ingested as ASN indicator
 - Minor tweaking for ingested attributes
- **Version 2.2.2**
 - Minor UI Enhancements
 - Improved error handling
 - Removed .undetected_urls parsing for IPs and FQDNs
 - Added Automatically add attributes and Automatically add indicators user fields
- **Version 2.2.1**
 - Improved enrichment attributes UI formatting
- **Version 2.2.0**
 - Improve UI messages, add new user field, mapping changes
- **Version 1.0.0**
 - Initial release