ThreatQuotient

VirusTotal Operation Implementation Guide

Version 2.2.1

Monday, June 15, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: 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.

Last Updated: Monday, June 15, 2020

Contents

Versioning

- **Operation Version**: 2.2.1
- **Minimum ThreatQ Version**: 4.22.0

Introduction

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

Installation

Perform the following steps to install or upgrade the VirusTotal operation.

1. Log into https://marketplace.threatq.com.
2. Locate and download the VirusTotal operation file.
3. Navigate to your ThreatQ instance.
4. From the ThreatQ navigation menu, choose the **Settings** icon > **Operations Management**.
5. Click on the **Install Operation** button.
6. Perform one of the following options:
   - Drag and drop the operation file into the dialog box.
   - Select **Click to browse** to locate the operation file on your local machine.

   

   If the operation already exists on the platform, ThreatQ will inform you that the operation already exists on the platform and will require confirmation to continue with the installation process.

   The Operation will appear in your list of installed operations once the installation process has completed. You will still need to configure and then enable the operation.

Operation 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 VirusTotal Operation:

1. Click on the **Settings** icon and select **Operations Management**
2. Locate the **VirusTotal** operation and click on **Operation Settings**.
3. Enter the following configuration parameters:

Parameter	Description
API Key	The private or public VirusTotal API key.
Auto Enrichment	If checked, indicator attributes are added automatically.

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Actions

Action	Description	Object Type	Object Subtype
submit_ip	Submits IP for analysis	Indicator	IP
submit_domain	Submits domain for analysis	Indicator	FQDN
submit_url	Submits URL for analysis	Indicator	URL, FQDN
submit_file	Submits file for analysis	ThreatFile	
submit_hash	Submits hash for analysis	Indicator	MD5, SHA-1, SHA-256

submit_ip

Uses the https://www.virustotal.com/vtapi/v2/ip-address/report endpoint

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Related Indicators	N/A	`undetected_downloaded_samples[].sha256`, `detected_downloaded_samples[].sha256`, `detected_referrer_samples[].sha256`, `undetected_referrer_samples[].sha256`, `detected_communicating_samples[].sha256`, `undetected_com`-	SHA-256

TQ	TQ Attribute Name	VirusTotal	Indicator Type
		municating_samples[].sha256	
Related Indicator Attributes	Positives	undetected_downloaded_samples[].positives, detected_downloaded_samples[].positives, detected_referrer_samples[].positives, undetected_referrer_samples[].positives, detected_communicating_samples[].positives, undetected_communicating_samples[].positives, detected_urls[].positives	N/A
Related Indicator Attributes	Total	undetected_downloaded_samples[].total, detected_downloaded_samples[].total , detected_referrer_samples[].total , undetected_referrer_samples[].total , detected_communicating_samples[].total , undetected_communicating_samples[].total , detected_urls[].total	N/A
Related Indicator Attributes	Date	undetected_downloaded_samples[].date, detected_downloaded_samples[].date , detected_referrer_samples[].date , detected_communicating_samples[].date , undetected_communicating_samples[].date , detected_urls[].scan_date	N/A
Related Indicators	N/A	resolutions[].hostname	FQDN
Related Indicator Attributes	Last Resolved	resolutions[].last_resolved	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Related Indicators	N/A	`detected_urls[].url`	URL
Indicator Attribute	VirusTotal AS Owner	`as_owner`	N/A
Indicator Attribute	VirusTotal ASN	`asn`	N/A
Indicator Attribute	VirusTotal Whois	`whois`	N/A
Indicator Attribute	VirusTotal Country	`country`	N/A
Indicator Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
Indicator Attribute	VirusTotal Undetected Urls	`undetected_urls`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicator Attribute	VirusTotal Continent	`continent`	N/A
Indicator Attribute	VirusTotal Whois Timestamp	`whois_timestamp`	N/A
Indicator Attribute	VirusTotal Network	`network`	N/A
Indicator Attribute	VirusTotal: HTTPS Certificate Date	`https_certificate_date`	N/A
Indicator Attribute	Public Key Algorithm	`last_https_certificate.public_key.algorithm`	N/A
Indicator Attribute	Public Key RSA	`last_https_certificate.public_key.rsa`	N/A
Indicator Attribute	Public Key EC	`last_https_certificate.public_key.ec`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Related Indicator	N/A	`last_https_certificate.thumbprint_sha256`	SHA-256
Indicator Attribute	Tag	`last_https_certificate.tags`	N/A
Indicator Attribute	Signature Algorithm	`last_https_certificate.signature_algorithm`	N/A
Indicator Attribute	Certificate Subject	`last_https_certificate.subject`	N/A
Indicator Attribute	Certificate Validity	`last_https_certificate.validity`	N/A
Indicator Attribute	Certificate Version	`last_https_certificate.version`	N/A
Indicator Attribute	Certificate Policies	`last_https_certificate.extensions.certificate_policies`	N/A
Indicator Attribute	Extended Key Usage	`last_https_certificate.extensions.extended_key_usage`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicator Attribute	Subject Alternative Name	`last_https_certificate.extensions.subject_alternative_name`	N/A
Indicator Attribute	Tag	`last_https_certificate.extensions.tags`	N/A
Indicator Attribute	Certificate Subject Key Identifier	`last_https_certificate.extensions.subject_key_identifier`	N/A
Indicator Attribute	CRL Distribution Points	`last_https_certificate.extensions.crl_distribution_points`	N/A
Indicator Attribute	Key Usage	`last_https_certificate.extensions.key_usage`	N/A
Indicator Attribute	CA	`last_https_certificate.extensions.CA`	N/A
Indicator	CA Inform-	`last_https_certificate.extensions.ca_information_access`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Attribute	ation Access		
Indicator Attribute	Certificate Signature	`last_https_certificate.cert_signature`	N/A
Indicator Attribute	Certificate Serial Number	`last_https_certificate.serial_number`	N/A
Indicator Attribute	Certificate Thumbprint	`last_https_certificate.thumbprint`	N/A
Indicator Attribute	Certificate Issuer	`last_https_certificate.issuer`	N/A
Indicator Attribute	Certificate Size	`last_https_certificate.size`	N/A

submit_domain

Uses the https://www.virustotal.com/vtapi/v2/domain/report endpoint.

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Related Indicators	N/A	`detected_downloaded_samples[].sha256`, `undetected_referrer_samples[].sha256`, `undetected_downloaded_samples[].sha256`, `detected_referrer_samples[].sha256`, `undetected_communicating_samples[].sha256`, `detected_communicating_samples[].sha256`	SHA-256
Related Indicator Attributes	Positives	`detected_downloaded_samples[].positives`, `undetected_referrer_samples[].positives`, `undetected_downloaded_samples[].positives`, `detected_referrer_samples[].positives`, `undetected_communicating_samples[].positives`, `detected_communicating_samples[].positives`, `detected_urls[].positives`	N/A
Related Indicator Attributes	Total	`detected_downloaded_samples[].total`, `undetected_referrer_samples[].total`, `undetected_downloaded_samples[].total`, `detected_referrer_samples[].total`, `undetected_communicating_samples[].total`, `detected_communicating_samples[].total`, `detected_urls[].total`	N/A
Related Indicator Attributes	Date	`detected_downloaded_samples[].date`, `undetected_referrer_samples[].date`, `undetected_downloaded_samples[].date`, `detected_referrer_samples[].date`, `undetected_communicating_samples[].date detected_communicating_samples[].date` `detected_urls[].scan_date`	N/A
Related	N/A	`resolutions[].ip_address`	IP

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicators			Address
Related Indicator Attributes	Last Resolved	`resolutions[].last_resolved`	N/A
Related Indicators	N/A	`domain_siblings[]`	FQDN
Related Indicators	N/A	`subdomains[]`	FQDN
Related Indicators	N/A	`detected_urls[].url`	URL
Indicator Attribute	VirusTotal Category	`categories`	N/A
Indicator Attribute	VirusTotal Whois Timestamp	`whois_timestamp`	N/A
Indicator	VirusTotal	`whois`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Attribute	Whois		
Indicator Attribute	VirusTotal BitDefender category	`BitDefender category`	N/A
Indicator Attribute	VirusTotal Dr.Web category	`Dr.Web category`	N/A
Indicator Attribute	VirusTotal Opera domain info	`Opera domain info`	N/A
Indicator Attribute	VirusTotal Websense ThreatSeeker category	`Websense ThreatSeeker category`	N/A
Indicator Attribute	VirusTotal Webutation Domain Info	`Webutation Domain Info.Safety score`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
	Safety score		
Indicator Attribute	VirusTotal Webutation Domain Info Adult content	`Webutation Domain Info.Adult content`	N/A
Indicator Attribute	VirusTotal Webutation Domain Info Verdict	`Webutation Domain Info.Verdict`	N/A
Indicator Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
Indicator Attribute	VirusTotal Alexa Cat-egory	`Alexa category`	N/A
Indicator Attribute	VirusTotal Undetected	`undetected_urls`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
	Urls		
Indicator Attribute	VirusTotal Dns Records Date	`dns_records_date`	N/A
Indicator Attribute	Public Key Algorithm	`last_https_certificate.public_key.algorithm`	N/A
Indicator Attribute	Public Key RSA	`last_https_certificate.public_key.rsa`	N/A
Indicator Attribute	Public Key EC	`last_https_certificate.public_key.ec`	N/A
Related Indicator	N/A	`last_https_certificate.thumbprint_sha256`	SHA-256
Indicator Attribute	Tag	`last_https_certificate.tags`	N/A
Indicator Attribute	Signature Algorithm	`last_https_certificate.signature_algorithm`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicator Attribute	Certificate Subject	`last_https_certificate.subject`	N/A
Indicator Attribute	Certificate Validity	`last_https_certificate.validity`	N/A
Indicator Attribute	Certificate Version	`last_https_certificate.version`	N/A
Indicator Attribute	Certificate Policies	`last_https_certificate.extensions.certificate_policies`	N/A
Indicator Attribute	Extended Key Usage	`last_https_certificate.extensions.extended_key_usage`	N/A
Indicator Attribute	Subject Alternative Name	`last_https_certificate.extensions.subject_alternative_name`	N/A
Indicator Attribute	Tag	`last_https_certificate.extensions.tags`	N/A
Indicator	Certificate	`last_https_certificate.extensions.subject_key_identifier`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Attribute	Subject Key Identifier		
Indicator Attribute	CRL Dis-tribution Points	`last_https_certificate.extensions.crl_distribution_points`	N/A
Indicator Attribute	Key Usage	`last_https_certificate.extensions.key_usage`	N/A
Indicator Attribute	CA	`last_https_certificate.extensions.CA`	N/A
Indicator Attribute	CA Inform-ation Access	`last_https_certificate.extensions.ca_information_access`	N/A
Indicator Attribute	Certificate Signature	`last_https_certificate.cert_signature`	N/A
Indicator Attribute	Certificate Serial Num-ber	`last_https_certificate.serial_number`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicator Attribute	Certificate Thumbprint	`last_https_certificate.thumbprint`	N/A
Indicator Attribute	Certificate Issuer	`last_https_certificate.issuer`	N/A
Indicator Attribute	Certificate Size	`last_https_certificate.size`	N/A
Indicator Attribute	VirusTotal Wot Domain Info	`WOT domain info`	N/A
Indicator Attribute	Websense ThreatSeeker Category	`Websense ThreatSeeker Category`	N/A
Indicator Attribute	VirusTotal HTTPS Certificate Date	`https_certificate_date`	N/A
Indicator Attribute	VirusTotal Alexa	`Alexa Domain Info`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
	Domain Info		
Indicator Attribute	VirusTotal Bit-defender Domain Info	`BitDefender domain info`	N/A
Indicator Attribute	VirusTotal Forcepoint Threatseeker Category	`Forcepoint ThreatSeeker category`	N/A
Indicator Attribute	VirusTotal Favicon	`favicon`	N/A
Indicator Attribute	VirusTotal Trendmicro Category	`TrendMicro category`	N/A
Indicator and Report Attribute	Majestic Rank	`popularity_ranks.Majestic.rank`	N/A

TQ	TQ Attribute Name	VirusTotal	Indicator Type
Indicator and Report Attribute	Statvoo Ranks	`popularity_ranks.Statvoo.rank`	N/A
Indicator and Report Attribute	Alexa Ranks	`popularity_ranks.Alexa.rank`	N/A
Indicator and Report Attribute	Cisco Umbrella Ranks	`popularity_ranks.Cisco Umbrella.rank`	N/A
Indicator and Report Attribute	Quantcast Ranks	`popularity_ranks.Quantcast.rank`	N/A
Indicator Attribute	DNS Records	`dns_records`	N/A

submit_url

Uses the https://www.virustotal.com/vtapi/v2/url/scan and https://www.virustotal.com/vtapi/v2/url/report endpoints.

scan

By running the action the first time on an indicator, the 'scan' endpoint is used to send the url to VirusTotal for analysis, returning a scan ID that will be used in the report endpoint in order to retrieve the analysis report.

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Indicator Attribute	VirusTotal Permanent Link	`permalink`	N/A
Indicator Attribute	VirusTotal Scan ID	`scan_id`	N/A

report

The second time the action is executed on the indicator that has a 'VirusTotal Scan ID' attribute, the 'report' endpoint is used.

All the related indicators are related to the enriched indicator and the report object.

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #1	N/A	`md5`	MD5
Related Indicator #1	N/A	`sha1`	SHA-1
Related Indicator #1	N/A	`sha256`	SHA-256
Related Indicator #1	N/A	`ssdeep`	Fuzzy Hash
Related Indicator #1	N/A	`authentihash`	Fuzzy Hash
Related Indicator `authen-tihash` Attribute	Authenticode Hash: "Yes"	N/A	N/A
Report	"VirusTotal Report for `ThreatFile.title`"	N/A	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal File Type	`type`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Unique Sources	`unique_sources`	N/A
ThreatFile, Related Indicator #1	Published at	`first_seen`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Attribute			
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Number of Positives	`positives`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Community Reputation	`community_reputation`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Harmless Votes	`harmless_votes`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Malicious Votes	`malicious_votes`	N/A
Report Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal PermaLink	`permalink`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Scan Date	`scan_date`	N/A
Related Indicator #2	N/A	`submission_names`	FilePath / FileName

TQ	TQAttribute Name	VirusTotal	Indicator Type
Report Attributes	`scans[].dict_key` Scan: `(if scans.detected)` `scans.result` Detected on `scans.update` with version `scans.version` `(else if not scans.detected)` `scans.version` NOT Detected on `scans.update`	`scans`	N/A
Report Attributes	Portable Executable Timestamp	`additional_info.pe-timestamp`	N/A
Report Attributes	`additional_info.exiftool.dict_key` ExifTool	`additional_info.exiftool`	N/A
Related Indicator #3	N/A	`additional_info.pe-imphash`	MD5
Related Indicator `additional_info.pe-imphash` Attribute	Import Hash: 'Yes'	N/A	N/A
Report Attributes	Portable Executable `additional_info.pe-resource-langs.dict_key` Lang	`additional_info.pe-resource-langs`	N/A
Report Attributes	DeepGuard	`additional_info.deepguard`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Report Attributes	Sigcheck `additional_info.sigcheck`	`additional_info.sigcheck`	N/A
Report Attributes	Positives Delta	`additional_info.positives_delta`	N/A
Report Attributes	Portable Executable Machine Type	`additional_info.pe-machine-type`	N/A
Report Attributes	TrID	`additional_info.trid`	N/A
Report Attributes	VirusTotal Private API Magic	`additional_info.magic`	N/A
Related Indicator #3	N/A	`additional_info.main_icon-.raw_md5`	MD5
Related Indicator `additional_info.main_icon.raw_md5` Attribute	Main Icon: 'Yes'	N/A	N/A
Related Indicator #3 Attribute	Main Icon DHash	`additional_info.main_icon-.dhash`	N/A
Report Attribute	Process Name	`additional_info.behaviour-v1.process.tree.name`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Report Attribute	Runtime DLL: Successfully Run / Failed to Run `(if additional_info.behaviour-v1.runtime-dlls.success) additional_info.behaviour-v1.runtime-dlls.file`	`additional_info.behaviour-v1.runtime-dlls`	N/A
Related Indicator #4	N/A	`additional_info.behaviour-v1.mutex.opened`	Mutex
Related Indicator `additional_info.behaviour-v1.mutex.opened` Attribute	`additional_info.behaviour-v1.mutex.opened.mutex`: Opened Mutex	N/A	N/A
Related Indicator #4	N/A	`additional_info.behaviour-v1.created`	Mutex
Related Indicator `additional_info.behaviour-v1.created` Attribute	`additional_info.behaviour-v1.created.mutex`: Created Mutex	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.opened`	FilePath

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator `additional_info.behaviour-v1.-filesystem.opened` Attribute	`additional_info.behaviour-v1.-filesystem.opened.path`: File Successfully Opened	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.read`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.read` Attribute	`additional_info.behaviour-v1.-filesystem.read.path`: File Successfully Read	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.moved`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.moved` Attribute	`additional_info.behaviour-v1.-filesystem.read.moved`: File Successfully Moved	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.downloaded`	FilePath
Related Indicator `additional_info.behaviour-v1.-`	`additional_info.behaviour-v1.-filesystem.read.downloaded`: File Suc-	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
`filesystem.downloaded` Attribute	cessfully Downloaded		
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.written`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.written` Attribute	`additional_info.behaviour-v1.-filesystem.read.written`: File Successfully Written	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.replaced`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.replaced` Attribute	`additional_info.behaviour-v1.-filesystem.read.replaced`: File Successfully Replaced	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.deleted`	FilePath
Related Indicator `additional_`	`additional_info.behaviour-v1.-`	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
`info.behaviour-v1.-filesystem.deleted` Attribute	`filesystem.read.deleted`: File Successfully Deleted		
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.copied`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.copied` Attribute	`additional_info.behaviour-v1.-filesystem.read.copied`: File Successfully Copied	N/A	N/A
Report Attribute	Portable Executable Resource Type `additional_info.pe-resource-types.dict_key`	`additional_info.pe-resource-types`	N/A
Related Indicator #4	N/A	`additional_info.network_infrastructure`	URL
Report Attribute	Portable Executable Entry Point	`additional_info.pe-entry-point`	N/A
Related Indicator #5	N/A	`additional_info.pe-resource-detail[].sha256`	SHA-256

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #5 Attribute	Portable Executable Language"	`additional_info.pe-resource-detail[].lang`	N/A
Related Indicator #5 Attribute	Portable Executable Chi Squared"	`additional_info.pe-resource-detail[].chi2`	N/A
Related Indicator #5 Attribute	Portable Executable File Type"	`additional_info.pe-resource-detail[].filetype`	N/A
Related Indicator #5 Attribute	Portable Executable Entropy"	`additional_info.pe-resource-detail[].entropy`	N/A
Related Indicator #5 Attribute	Portable Executable Type"	`additional_info.pe-resource-detail[].type`	N/A
Related Indicator #6	N/A	`additional_info.contacted_domains`	FQDN
Related Indicator `additional_info.contacted_domains` Attribute	Malware Contacted Domain: Yes	N/A	N/A
ThreatFile, Related Indicator #1	Officecheck Document Summary Info `addi`-	`additional_info.of`-	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Attribute	`tional_info.officecheck.document_summary_info.dict_hey`	`ficecheck.document_summary_info`	
ThreatFile, Related Indicator #1 Attribute	Officecheck Summary Info `additional_info.officecheck.summary_info.dict_hey`	`additional_info.officecheck.summary_info`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	Library imported from `additional_info.imports.dict_hey`	`additional_info.imports`	N/A

submit_file

Uses the https://www.virustotal.com/vtapi/v2/file/report and https://www.virustotal.com/vtapi/v2/file/scan endpoints.

scan

By running the action the first time on an indicator, the 'scan' endpoint is used to send the file to VirusTotal for analysis, returning a scan ID that will be used in the report endpoint in order to retrieve the analysis report.

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Related Indicator	N/A	`md5`	MD5

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Related Indicator	N/A	`sha1`	SHA-1
Related Indicator	N/A	`sha256`	SHA-256
Indicator Attribute	VirusTotal Permanent Link	`permalink`	N/A
Indicator & Threat File Attribute	VirusTotal Scan ID	`scan_id`	N/A

report

All the related indicators are related to the enriched indicator and the report object.

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #1	N/A	`md5`	MD5
Related Indicator #1	N/A	`sha1`	SHA-1
Related Indicator #1	N/A	`sha256`	SHA-256
Related Indicator #1	N/A	`ssdeep`	Fuzzy Hash
Related Indicator #1	N/A	`authentihash`	Fuzzy Hash

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator `authen-tihash` Attribute	Authenticode Hash: "Yes"	N/A	N/A
Report	"VirusTotal Report for `ThreatFile.title`"	N/A	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal File Type	`type`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Unique Sources	`unique_sources`	N/A
ThreatFile, Related Indicator #1 Attribute	Published at	`first_seen`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Number of Positives	`positives`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Community Reputation	`community_reputation`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Harmless Votes	`harmless_votes`	N/A
ThreatFile, Report, Related Indic-	VirusTotal Malicious Votes	`malicious_votes`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
ator #1 Attribute			
Report Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal PermaLink	`permalink`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Scan Date	`scan_date`	N/A
Related Indicator #2	N/A	`submission_names`	FilePath / FileName
Report Attributes	`scans[].dict_key` Scan: `(if scans.detected)` `scans.result` Detected on `scans.update` with version `scans.version` `(else if not scans.detected)` `scans.version` NOT Detected on `scans.update`	`scans`	N/A
Report Attributes	Portable Executable Timestamp	`additional_info.pe-timestamp`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Report Attributes	`additional_info.exiftool.dict_key` ExifTool	`additional_info.exiftool`	N/A
Related Indicator #3	N/A	`additional_info.pe-imphash`	MD5
Related Indicator `additional_info.pe-imphash` Attribute	Import Hash: 'Yes'	N/A	N/A
Report Attributes	Portable Executable `additional_info.pe-resource-langs.dict_key` Lang	`additional_info.pe-resource-langs`	N/A
Report Attributes	DeepGuard	`additional_info.deepguard`	N/A
Report Attributes	Sigcheck `additional_info.sigcheck`	`additional_info.sigcheck`	N/A
Report Attributes	Positives Delta	`additional_info.positives_delta`	N/A
Report Attributes	Portable Executable Machine Type	`additional_info.pe-machine-type`	N/A
Report Attributes	TrID	`additional_info.trid`	N/A
Report Attributes	VirusTotal Private API Magic	`additional_info.magic`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #3	N/A	`additional_info.main_icon-.raw_md5`	MD5
Related Indicator `additional_info.main_icon.raw_md5` Attribute	Main Icon: 'Yes'	N/A	N/A
Related Indicator #3 Attribute	Main Icon DHash	`additional_info.main_icon-.dhash`	N/A
Report Attribute	Process Name	`additional_info.behaviour-v1.process.tree.name`	N/A
Report Attribute	Runtime DLL: Successfully Run / Failed to Run `(if additional_info.behaviour-v1.runtime-dlls.success) addi-tional_info.behaviour-v1.runtime-dlls.file`	`additional_info.behaviour-v1.runtime-dlls`	N/A
Related Indicator #4	N/A	`additional_info.behaviour-v1.mutex.opened`	Mutex
Related Indicator `additional_`	`additional_info.behaviour-v1.mu-`	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
`info.behaviour-v1.mutex.opened` Attribute	`tex.opened.mutex`: Opened Mutex		
Related Indicator #4	N/A	`additional_info.behaviour-v1.created`	Mutex
Related Indicator `additional_info.behaviour-v1.created` Attribute	`additional_info.behaviour-v1.created.mutex`: Created Mutex	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.opened`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.opened` Attribute	`additional_info.behaviour-v1.filesystem.opened.path`: File Successfully Opened	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.read`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.read` Attribute	`additional_info.behaviour-v1.filesystem.read.path`: File Successfully Read	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.moved`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.moved` Attribute	`additional_info.behaviour-v1.-filesystem.read.moved`: File Successfully Moved	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.downloaded`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.downloaded` Attribute	`additional_info.behaviour-v1.-filesystem.read.downloaded`: File Successfully Downloaded	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.written`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.written` Attribute	`additional_info.behaviour-v1.-filesystem.read.written`: File Successfully Written	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.replaced`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.replaced` Attribute	`additional_info.behaviour-v1.-filesystem.read.replaced`: File Successfully Replaced	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.deleted`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.deleted` Attribute	`additional_info.behaviour-v1.-filesystem.read.deleted`: File Successfully Deleted	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.copied`	FilePath
Related Indicator `additional_info.behaviour-v1.-filesystem.copied` Attribute	`additional_info.behaviour-v1.-filesystem.read.copied`: File Successfully Copied	N/A	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
Report Attribute	Portable Executable Resource Type `additional_info.pe-resource-types.dict_key`	`additional_info.pe-resource-types`	N/A
Related Indicator #4	N/A	`additional_info.network_infrastructure`	URL
Report Attribute	Portable Executable Entry Point	`additional_info.pe-entry-point`	N/A
Related Indicator #5	N/A	`additional_info.pe-resource-detail[].sha256`	SHA-256
Related Indicator #5 Attribute	Portable Executable Language"	`additional_info.pe-resource-detail[].lang`	N/A
Related Indicator #5 Attribute	Portable Executable Chi Squared"	`additional_info.pe-resource-detail[].chi2`	N/A
Related Indicator #5 Attribute	Portable Executable File Type"	`additional_info.pe-resource-detail[].filetype`	N/A
Related Indicator #5 Attribute	Portable Executable Entropy"	`additional_info.pe-`	N/A

TQ	TQAttribute Name	VirusTotal	Indicator Type
		`resource-detail[].entropy`	
Related Indicator #5 Attribute	Portable Executable Type"	`additional_info.pe-resource-detail[].type`	N/A
Related Indicator #6	N/A	`additional_info.contacted_domains`	FQDN
Related Indicator `additional_info.contacted_domains` Attribute	Malware Contacted Domain: Yes	N/A	N/A
ThreatFile, Related Indicator #1 Attribute	Officecheck Document Summary Info `additional_info.officecheck.document_summary_info.dict_hey`	`additional_info.officecheck.document_summary_info`	N/A
ThreatFile, Related Indicator #1 Attribute	Officecheck Summary Info `additional_info.officecheck.summary_info.dict_hey`	`additional_info.officecheck.summary_info`	N/A
ThreatFile, Report, Related Indicator #1 Attribute	Library imported from `additional_info.imports.dict_hey`	`additional_info.imports`	N/A

submit_hash

Uses the https://www.virustotal.com/vtapi/v2/file/report endpoint

Mapping is the same as submit_file - report.

Change Log

- **Version 2.2.1**
  - Fixed a details column formatting bug.
- **Version 2.2.0**
  - Added additional attributes that were missing from previous versions.
- **Version 2.1.0**
  - Better Error Handling for finished, queued or pending scans.
  - Create relation between enriched indicator and returned indicators
  - Bug Fix for Internal 5XX errors
- **Version 2.0.0**
  - Initial Release