

Package: virustotal (via r-universe)

September 13, 2024

Title R Client for the VirusTotal API

Version 0.2.2

Maintainer Gaurav Sood <gsood07@gmail.com>

Description Use VirusTotal, a Google service that analyzes files and URLs for viruses, worms, trojans etc., provides category of the content hosted by a domain from a variety of prominent services, provides passive DNS information, among other things. See <<http://www.virustotal.com>> for more information.

URL <https://github.com/themains/virustotal>

BugReports <https://github.com/themains/virustotal/issues>

Depends R (>= 3.3.0)

License MIT + file LICENSE

LazyData false

VignetteBuilder knitr

Imports httr, plyr

Suggests knitr, rmarkdown, testthat, lintr

RoxygenNote 7.1.2

Repository <https://themains.r-universe.dev>

RemoteUrl <https://github.com/themains/virustotal>

RemoteRef HEAD

RemoteSha 1d6c87dd1145f57d3442fa0c8f5607de3edca261

Contents

virustotal-package	2
add_comments	3
domain_report	4
file_report	5
get_domain_comments	6
get_domain_info	7

get_domain_relationship	8
get_domain_votes	9
get_ip_comments	10
get_ip_info	11
get_ip_votes	12
ip_report	13
post_domain_comments	14
post_domain_votes	15
post_ip_comments	16
post_ip_votes	17
rate_limit	18
rescan_file	18
scan_file	19
scan_url	20
set_key	21
url_report	21
virustotal2_GET	22
virustotal2_POST	23
virustotal_check	24
virustotal_GET	24
virustotal_POST	25

Index	26
--------------	-----------

virustotal-package *virustotal: Access Virustotal API*

Description

Access virustotal API. See <https://www.virustotal.com/>. Details about results of calls to the API can be found at <https://developers.virustotal.com/v2.0/reference>.

You will need credentials to use this application. If you haven't already, get the API Key at <https://www.virustotal.com/>.

Author(s)

Gaurav Sood

add_comments	<i>Add comments on Files and URLs</i>
--------------	---------------------------------------

Description

Add comments on files and URLs. For instance, flagging false positives, adding details about malware, instructions for cleaning malware, etc.

Usage

```
add_comments(hash = NULL, comment = NULL, ...)
```

Arguments

hash	hash for the resource you want to comment on; Required; String
comment	review; Required; String
...	Additional arguments passed to virustotal2_POST .

Value

data.frame with 2 columns: response_code, verbose_msg

- If the hash is incorrect or a duplicate comment is posted, response_code will be 0
- If the hash is incorrect, verbose_msg will be 'Invalid resource'
- If a duplicate comment is posted, verbose_msg will be 'Duplicate comment'
- If a comment is posted successfully, response_code will be 1 and verbose_msg will be 'Your comment was successfully posted'

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
add_comments(hash='99017f6eebbac24f351415dd410d522d', comment="This is great.")  
  
## End(Not run)
```

`domain_report`*Get Domain Report*

Description

Retrieves report on a given domain, including passive DNS, urls detected by at least one url scanner. Gives category of the domain from bitdefender.

Usage

```
domain_report(domain = NULL, ...)
```

Arguments

<code>domain</code>	domain name. String. Required.
<code>...</code>	Additional arguments passed to virustotal2_GET .

Value

named list with the following possible items: ``BitDefender category``, `undetected_referrer_samples`, `whois_timestamp`, `detected_downloaded_samples`, `detected_referrer_samples`, ``Webutation domain info``, ``Alexa category``, `undetected_downloaded_samples`, `resolutions`, `detected_communicating_samples`, ``Opera domain info``, ``TrendMicro category``, `categories`, `domain_siblings`, ``BitDefender domain info``, `whois`, ``Alexa domain info``, `response_code`, `verbose_msg`, ``Websense ThreatSeeker category``, `subdomains`, ``WOT domain info``, `detected_urls`, ``Alexa rank``, `undetected_communicating_samples`, ``Dr.Web category``, `pcaps`

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:

# Before calling the function, set the API key using set_key('api_key_here')

domain_report("http://www.google.com")
domain_report("http://www.goodsfwr fw.com") # Domain not found

## End(Not run)
```

file_report	<i>Get File Scan Report</i>
-------------	-----------------------------

Description

Get File Scan Report

Usage

```
file_report(hash = NULL, ...)
```

Arguments

hash	Hash for the scan
...	Additional arguments passed to virustotal_GET .

Value

data.frame with 16 columns: service, detected, version, update, result, scan_id, sha1, resource, response_code, scan_date, permalink, verbose_msg, total, positives, sha256, md5

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
file_report(hash='99017f6eebbac24f351415dd410d522d')  
  
## End(Not run)
```

get_domain_comments *Retrieve comments for an Internet domain*

Description

Retrieve comments for an Internet domain

Usage

```
get_domain_comments(domain = NULL, limit = limit, cursor = cursor, ...)
```

Arguments

domain	domain name. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list with the following possible items: `BitDefender category`, undetected_referrer_samples, whois_timestamp, detected_downloaded_samples, detected_referrer_samples, `Webutation domain info`, `Alexa category`, undetected_downloaded_samples, resolutions, detected_communicating_samples, `Opera domain info`, `TrendMicro category`, categories, domain_siblings, `BitDefender domain info`, whois, `Alexa domain info`, response_code, verbose_msg, `Websense ThreatSeeker category`, subdomains, `WOT domain info`, detected_urls, `Alexa rank`, undetected_communicating_samples, `Dr.Web category`, pcaps

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:

# Before calling the function, set the API key using set_key('api_key_here')

get_domain_comments("http://www.google.com")
get_domain_comments("http://www.goodsfwrw.com") # Domain not found

## End(Not run)
```

get_domain_info	<i>Retrieve information about an Internet domain</i>
-----------------	--

Description

Retrieve information about an Internet domain

Usage

```
get_domain_info(domain = NULL, limit = NULL, cursor = NULL, ...)
```

Arguments

domain	domain name. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
get_domain_info("http://www.google.com")  
get_domain_info("http://www.goodsfwrw.com") # Domain not found  
  
## End(Not run)
```

`get_domain_relationship`*Retrieve related objects to an Internet domain*

Description

Retrieve related objects to an Internet domain

Usage

```
get_domain_relationship(  
    domain = NULL,  
    relationship = "subdomains",  
    limit = NULL,  
    cursor = NULL,  
    ...  
)
```

Arguments

<code>domain</code>	domain name. String. Required.
<code>relationship</code>	relationship name. String. Required. Default is subdomains. For all the options see https://developers.virustotal.com/v3.0/reference#domains-relationships
<code>limit</code>	Number of entries. Integer. Optional. Default is 10.
<code>cursor</code>	String. Optional.
<code>...</code>	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
get_domain_relationship("https://www.google.com")  
get_domain_relationship("https://www.goodsfwrfw.com") # Domain not found
```



```
## End(Not run)
```

get_domain_votes	<i>Retrieve votes for an Internet domain</i>
------------------	--

Description

Retrieve votes for an Internet domain

Usage

```
get_domain_votes(domain = NULL, limit = NULL, cursor = NULL, ...)
```

Arguments

domain	domain name. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
get_domain_votes("http://www.google.com")  
get_domain_votes("http://www.goodsfwrfw.com") # Domain not found  
  
## End(Not run)
```

get_ip_comments	<i>Retrieve comments for an IP address</i>
-----------------	--

Description

Retrieve comments for an IP address

Usage

```
get_ip_comments(ip = NULL, limit = NULL, cursor = NULL, ...)
```

Arguments

ip	IP Address. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
get_ip_comments("64.233.160.0")  
  
## End(Not run)
```

get_ip_info	<i>Retrieve information about an IP address</i>
-------------	---

Description

Retrieves report on a given domain, including passive DNS, urls detected by at least one url scanner. Gives category of the domain from bitdefender.

Usage

```
get_ip_info(ip = NULL, limit = NULL, cursor = NULL, ...)
```

Arguments

ip	IP address. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
get_ip_info("64.233.160.0")  
  
## End(Not run)
```

get_ip_votes	<i>Retrieve votes for an IP address</i>
--------------	---

Description

Retrieve votes for an IP address

Usage

```
get_ip_votes(ip = NULL, limit = NULL, cursor = NULL, ...)
```

Arguments

ip	IP address. String. Required.
limit	Number of entries. Integer. Optional. Default is 10.
cursor	String. Optional.
...	Additional arguments passed to virustotal_GET .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
get_ip_votes("64.233.160.0")  
  
## End(Not run)
```

`ip_report`*Get IP Report*

Description

Get passive DNS data and URLs detected by URL scanners

Usage

```
ip_report(ip = NULL, ...)
```

Arguments

<code>ip</code>	a valid IPv4 address in dotted quad notation; String; Required
<code>...</code>	Additional arguments passed to virustotal2_GET .

Value

named list with the following potential items: `undetected_referrer_samples`, `detected_downloaded_samples`, `detected_referrer_samples`, `undetected_downloaded_samples`, `detected_urls`, `undetected_downloaded_sample`, `response_code`, `as_owner`, `verbose_msg`, `country`, `undetected_referrer_samples`, `detected_communicating_sam`, `resolutions`, `undetected_communicating_samples`, `asn`

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
ip_report(ip="8.8.8.8")  
  
## End(Not run)
```

post_domain_comments *Add a comment to an Internet domain*

Description

Add a comment to an Internet domain

Usage

```
post_domain_comments(domain = NULL, comment = NULL, ...)
```

Arguments

domain	domain name. String. Required.
comment	vote. String. Required. Any word starting with # in your comment's text will be considered a tag, and added to the comment's tag attribute.
...	Additional arguments passed to virustotal_POST .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
post_domain_comments(domain = "https://google.com", comment = "Great!")  
  
## End(Not run)
```

post_domain_votes	<i>Add a vote for a hostname or domain</i>
-------------------	--

Description

Add a vote for a hostname or domain

Usage

```
post_domain_votes(domain = NULL, vote = NULL, ...)
```

Arguments

domain	domain name. String. Required.
vote	vote. String. Required.
...	Additional arguments passed to virustotal_POST .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
post_domain_votes("http://google.com", vote = "malicious")  
  
## End(Not run)
```

post_ip_comments	<i>Add a comment to an IP address</i>
------------------	---------------------------------------

Description

Add a comment to an IP address

Usage

```
post_ip_comments(ip = NULL, comment = NULL, ...)
```

Arguments

ip	IP address. String. Required.
comment	Comment. String. Required.
...	Additional arguments passed to virustotal_POST .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
post_ip_comments(ip = "64.233.160.0", comment = "test")  
  
## End(Not run)
```

post_ip_votes	<i>Add a vote for a IP address</i>
---------------	------------------------------------

Description

Add a vote for a IP address

Usage

```
post_ip_votes(ip = NULL, vote = NULL, ...)
```

Arguments

ip	IP address. String. Required.
vote	vote. String. Required.
...	Additional arguments passed to virustotal_POST .

Value

named list

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
post_ip_votes(ip = "64.233.160.0", vote = "malicious")  
  
## End(Not run)
```

rate_limit	<i>Rate Limits</i>
------------	--------------------

Description

Virustotal requests throttled at 4 per min. The function creates an env. var. that tracks number of requests per minute, and enforces appropriate waiting.

Usage

```
rate_limit()
```

rescan_file	<i>Rescan already submitted files</i>
-------------	---------------------------------------

Description

The function returns a data.frame with a scan_id and sha256, sha1, md5 hashes, all of which can be used to retrieve the report using [file_report](#)

Usage

```
rescan_file(hash = NULL, ...)
```

Arguments

hash	Hash for the scan. String. Required.
...	Additional arguments passed to virustotal2_POST .

Value

data.frame with 12 columns: scans, scan_id, sha1, resource, response_code, scan_date, permalink, verbose_msg, total, positives, sha256, md5 response_code is 0 if the file is not in the database (hash can't be found).

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
rescan_file(hash='99017f6eebbac24f351415dd410d522d')  
rescan_file(hash='99017f6ee51415dd410d522d') # incorrect hash  
  
## End(Not run)
```

scan_file	<i>Submit a file for scanning</i>
-----------	-----------------------------------

Description

Submit a file for scanning

Usage

```
scan_file(file_path = NULL, ...)
```

Arguments

file_path	Required; Path to the document
...	Additional arguments passed to virustotal2_POST .

Value

data.frame with the following columns: scan_id, sha1, resource, response_code, sha256, permalink, md5, verbose_msg

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
scan_file(file_path='path_to_suspicious_file')  
  
## End(Not run)
```

scan_url	<i>Submit URL for scanning</i>
----------	--------------------------------

Description

Submit a URL for scanning. Returns a data.frame with scan_id which can be used to fetch the report using [url_report](#)

Usage

```
scan_url(url = NULL, ...)
```

Arguments

url	url; string; required
...	Additional arguments passed to virustotal_POST .

Value

data.frame with 7 columns: permalink, resource, url, response_code, scan_date, scan_id, verbose_msg

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:  
  
# Before calling the function, set the API key using set_key('api_key_here')  
  
scan_url("http://www.google.com")  
  
## End(Not run)
```

set_key	<i>Set API Key</i>
---------	--------------------

Description

Before anything else, get the API key from <https://www.virustotal.com/en/>. Next, use `set_key` to store the API key in an environment variable `VirustotalToken`. Once you have set the API key, you can use any of the functions.

Usage

```
set_key(api_key = NULL)
```

Arguments

`api_key` API key. String. Required.

References

<https://developers.virustotal.com/v2.0/reference>

Examples

```
## Not run:  
  
set_key('api_key_here')  
  
## End(Not run)
```

url_report	<i>Get URL Report</i>
------------	-----------------------

Description

Retrieve a scan report for a given URL. If no scan report is available, set `scan` to 1 to get a new report.

Usage

```
url_report(url = NULL, scan_id = NULL, scan = 1, ...)
```

Arguments

url	URL. String. url or scan_id must be specified.
scan_id	scan id for a particular url scan. String. url or scan_id must be specified.
scan	String. Optional. Can be 0 or 1. Default is 1. When 1, submits url for scanning if no existing reports are found. When scan is set to 1, the result includes a scan_id field, which can be used again to retrieve the report.
...	Additional arguments passed to virustotal2_GET .

Value

data.frame with 13 columns: scan_id, resource, url, response_code, scan_date, permalink, verbose_msg, positives, total, .id, detected, result, detail

References

<https://developers.virustotal.com/v2.0/reference>

See Also

[set_key](#) for setting the API key

Examples

```
## Not run:

# Before calling the function, set the API key using set_key('api_key_here')

url_report("http://www.google.com")
url_report(scan_id = "ebdd15c397d2b0c6f50c3f2df531357d1201ff5976802316405e60880d6bf5ec-1478786749")

## End(Not run)
```

virustotal2_GET

Base POST AND GET functions. Not exported.

Description

GET for the v2 API

Usage

```
virustotal2_GET(
  query = list(),
  path = path,
  key = Sys.getenv("VirusTotalToken"),
  ...
)
```

Arguments

query	query list
path	path to the specific API service url
key	A character string containing Virustotal API Key. The default is retrieved from <code>Sys.getenv("VirustotalToken")</code> .
...	Additional arguments passed to GET .

Value

list

virustotal2_POST	<i>POST for V2 API</i>
------------------	------------------------

Description

POST for V2 API

Usage

```
virustotal2_POST(
  query = list(),
  path = path,
  body = NULL,
  key = Sys.getenv("VirustotalToken"),
  ...
)
```

Arguments

query	query list
path	path to the specific API service url
body	file
key	A character string containing Virustotal API Key. The default is retrieved from <code>Sys.getenv("VirustotalToken")</code> .
...	Additional arguments passed to POST .

Value

list

virustotal_check	<i>Request Response Verification</i>
------------------	--------------------------------------

Description

Request Response Verification

Usage

```
virustotal_check(req)
```

Arguments

req	request
-----	---------

Value

in case of failure, a message

virustotal_GET	<i>GET for the Current V3 API</i>
----------------	-----------------------------------

Description

GET for the Current V3 API

Usage

```
virustotal_GET(
  query = list(),
  path = path,
  key = Sys.getenv("VirustotalToken"),
  ...
)
```

Arguments

query	query list
path	path to the specific API service url
key	A character string containing Virustotal API Key. The default is retrieved from Sys.getenv("VirustotalToken").
...	Additional arguments passed to GET .

Value

list

virustotal_POST	<i>POST for the Current V3 API</i>
-----------------	------------------------------------

Description

POST for the Current V3 API

Usage

```
virustotal_POST(  
    query = list(),  
    path = path,  
    body = NULL,  
    key = Sys.getenv("VirusTotalToken"),  
    ...  
)
```

Arguments

query	query list
path	path to the specific API service url
body	file
key	A character string containing Virustotal API Key. The default is retrieved from Sys.getenv("VirusTotalToken").
...	Additional arguments passed to POST .

Value

list

Index

add_comments, 3

domain_report, 4

file_report, 5, 18

GET, 23, 24

get_domain_comments, 6

get_domain_info, 7

get_domain_relationship, 8

get_domain_votes, 9

get_ip_comments, 10

get_ip_info, 11

get_ip_votes, 12

ip_report, 13

POST, 23, 25

post_domain_comments, 14

post_domain_votes, 15

post_ip_comments, 16

post_ip_votes, 17

rate_limit, 18

rescan_file, 18

scan_file, 19

scan_url, 20

set_key, 3–21, 21, 22

url_report, 20, 21

virustotal (virustotal-package), 2

virustotal-package, 2

virustotal2_GET, 4, 13, 22, 22

virustotal2_POST, 3, 18, 19, 23

virustotal_check, 24

virustotal_GET, 5–12, 24

virustotal_POST, 14–17, 20, 25