Package 'virustotal'

May 1, 2017

Title R Client for the VirusTotal API

Version 0.2.1

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 http://github.com/soodoku/virustotal

BugReports http://github.com/soodoku/virustotal/issues

Depends R (>= 3.3.0)

License MIT + file LICENSE

LazyData true

VignetteBuilder knitr

Imports httr, plyr

Suggests knitr, rmarkdown, testthat, lintr

RoxygenNote 6.0.1

NeedsCompilation no

Author Gaurav Sood [aut, cre]

Repository CRAN

Date/Publication 2017-05-01 19:25:07 UTC

R topics documented:

`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://www.virustotal.com/en/documentation/public-api/.

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` *Add comments on Files and URLs*

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 `virustotal_GET`.

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://www.virustotal.com/en/documentation/public-api/

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

`domain`	domain name. String. Required.
`...`	Additional arguments passed to `virustotal_GET`.

Value

named list with the following possible items: `BitDefender category`, undetected_referrer_samples, whois_times

References

https://www.virustotal.com/en/documentation/public-api/

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.goodsfwrfw.com") # Domain not found

## End(Not run)
```

---

file_report *Get File Scan Report*

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_

References

https://www.virustotal.com/en/documentation/public-api/

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)
```

`ip_report` *Get IP Report*

Description

Get passive DNS data and URLs detected by URL scanners

Usage

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

Arguments

`ip`	a valid IPv4 address in dotted quad notation; String; Required
`...`	Additional arguments passed to `virustotal_GET`.

Value

named list with the following potential items: `undetected_referrer_samples, detected_downloaded_samples, detec`

References

https://www.virustotal.com/en/documentation/public-api/

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)
```

rate_limit *Rate Limits*

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 *Rescan already submitted files*

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 `virustotal_POST`.

Value

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

References

https://www.virustotal.com/en/documentation/public-api/

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` *Submit a file for scanning*

Description

Submit a file for scanning

Usage

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

Arguments

`file_path`	Required; Path to the document
`...`	Additional arguments passed to `virustotal_POST`.

Value

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

References

https://www.virustotal.com/en/documentation/public-api/

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 *Submit URL for scanning*

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://www.virustotal.com/en/documentation/public-api/

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 *Set API Key*

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://www.virustotal.com/en/documentation/public-api/

Examples

```
## Not run:

set_key('api_key_here')


## End(Not run)
```

url_report *Get URL Report*

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 virustotal_GET.

Value

data.frame with 13 columns: scan_id, resource, url, response_code, scan_date, permalink, verbose_msg, posi

References

https://www.virustotal.com/en/documentation/public-api/

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)
```

---

virustotal_check *Request Response Verification*

Description

Request Response Verification

Usage

```
virustotal_check(req)
```

Arguments

req	request

Value

in case of failure, a message

virustotal_GET *Base POST AND GET functions. Not exported.*

Description

GET

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 *POST*

Description

POST

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