Package 'cymruservices'

September 18, 2018

Title Query 'Team Cymru' 'IP' Address, Autonomous System Number ('ASN'), Border Gateway Protocol ('BGP'), Bogon and 'Malware' Hash Data Services

Version 0.5.0

Description A toolkit for querying 'Team Cymru' <http://team-cymru.org> 'IP' address, Autonomous System Number ('ASN'), Border Gateway Protocol ('BGP'), Bogon and 'Malware' Hash Data Services.

Depends R (>= 3.2.0)

License MIT + file LICENSE

Suggests testthat

Imports utils, stringi, memoise, pingr

Encoding UTF-8

RoxygenNote 6.0.1.9000

NeedsCompilation no

Author Bob Rudis [aut, cre] (<https://orcid.org/0000-0001-5670-2640>)

Maintainer Bob Rudis <bob@rud.is>

Repository CRAN

Date/Publication 2018-09-18 20:40:12 UTC

R topics documented:

bulk_origin *Retrieves BGP Origin ASN info for a list of IPv4 addresses*

Description

Retrieves BGP Origin ASN info for a list of IPv4 addresses

Usage

```
bulk_origin(ips, timeout = getOption("timeout"))
```

Arguments

ips	vector of IPv4 address (character - dotted-decimal)
timeout	numeric: the timeout (in seconds) to be used for this connection. Beware that some OSes may treat very large values as zero: however the POSIX standard requires values up to 31 days to be supported.

Value

data frame of BGP Origin ASN lookup results

- as - AS #
- ip - IPv4 (passed in)
- bgp_refix - BGP CIDR
- cc - Country code
- registry - Registry it falls under
- allocated - date it was allocated
- as_ame - AS name

If a socket connection cannot be made (i.e. a network problem on your end or a service/network problem on their end), all columns will be NA.

Note

The Team Cymru's service is NOT a GeoIP service! Do not use this function for that as your results will not be accurate. Data is updated every 4 hours. Also, A direct connection to TCP Port 43 (WHOIS) is required for most of these API functions to work properly.

See Also

http://www.team-cymru.org/IP-ASN-mapping.html

Examples

```
## Not run:
bulk_origin(c("68.22.187.5", "207.229.165.18", "198.6.1.65"))

## End(Not run)
```

`bulk_origin_asn` *Retrieves BGP Origin ASN info for a list of ASN ids*

Description

Retrieves BGP Origin ASN info for a list of ASN ids

Usage

```
bulk_origin_asn(asns, timeout = getOption("timeout"))
```

Arguments

`asns`	character vector of ASN ids (character)
`timeout`	numeric: the timeout (in seconds) to be used for this connection. Beware that some OSes may treat very large values as zero: however the POSIX standard requires values up to 31 days to be supported.

Value

data frame of BGP Origin ASN lookup results

- `as` - AS #
- `cc` - Country code
- `registry` - registry it falls under
- `allocated` - when it was allocated
- `as_name` - name associated with the allocation

If a socket connection cannot be made (i.e. a network problem on your end or a service/network problem on their end), all columns will be `NA`.

Note

The Team Cymru's service is NOT a GeoIP service! Do not use this function for that as your results will not be accurate. Data is updated every 4 hours. Also, A direct connection to TCP Port 43 (WHOIS) is required for most of these API functions to work properly.

See Also

http://www.team-cymru.org/IP-ASN-mapping.html

Examples

```
## Not run:
bulk_origin_asn(c(22822, 1273, 2381, 2603, 2914, 3257, 3356, 11164,
                  174, 286, 1299, 2914, 3257, 3356, 3549, 22822))

## End(Not run)
```

`bulk_peer` *Retrieves BGP Peer ASN info for a list of IPv4 addresses*

Description

Retrieves BGP Peer ASN info for a list of IPv4 addresses

Usage

```
bulk_peer(ips, timeout = getOption("timeout"))
```

Arguments

`ips`	vector of IPv4 address (character - dotted-decimal)
`timeout`	numeric: the timeout (in seconds) to be used for this connection. Beware that some OSes may treat very large values as zero: however the POSIX standard requires values up to 31 days to be supported.

Value

data frame of BGP Peer ASN lookup results

- `peer_as` - peer AS #
- `ip` - IPv4 (passsed in)
- `bgp_prefix` - BGP CIDR block
- `cc` - Country code
- `registry` - Registry it falls under
- `allocated` - date allocated
- `peer_as_name` - peer name

If a socket connection cannot be made (i.e. a network problem on your end or a service/network problem on their end), all columns will be `NA`.

Note

The Team Cymru's service is NOT a GeoIP service! Do not use this function for that as your results will not be accurate. Data is updated every 4 hours. Also, A direct connection to TCP Port 43 (WHOIS) is required for most of these API functions to work properly.

See Also

http://www.team-cymru.org/IP-ASN-mapping.html

Examples

```
## Not run:
bulk_peer(c("68.22.187.5", "207.229.165.18", "198.6.1.65"))

## End(Not run)
```

`cymruservices` *cymruservices is an R package that provides interfaces to various* R*hrefhttp://www.team-cymru.org/services.htmlTeam Cymru Services including The Bogon Refrerence, The IP to ASN Mapping Project and The Malware Hash Registry*

Description

cymruservices is an R package that provides interfaces to various Team Cymru Services including The Bogon Refrerence, The IP to ASN Mapping Project and The Malware Hash Registry

Note

A direct connection to TCP Port 43 (WHOIS) is required for most of these API functions to work properly.

Author(s)

Bob Rudis (bob@rud.is)

`cymru_active` *Check to see if Team Cymru WHOIS servers are up*

Description

Check to see if Team Cymru WHOIS servers are up

Usage

```
cymru_active(timeout = 1, count = 3L, verbose = TRUE)
```

Arguments

`timeout`	how long to wait for a response (seconds). Default is one second.
`count`	number of pings to issue. Default is three pings.
`verbose`	be verbose in output? Default `FALSE`.

Examples

```
cymru_active()
```

`flush` *Flush cached results*

Description

Within a given R session, it will be highly unlikely that API responses to calls to Team Cymru services will change if the parameters have not varied (i.e. you use the same vector of IP addresses again). To respect the resources that have beeen freely provided, all the API functions cache their results.

It may be advantageous or necessary to invalidate one or more of these caches. This function allows for the invalidation of one or more (or all) caches.

Usage

```
flush(..., quiet = TRUE)
```

Arguments

`...`	strings naming cached results to flush. Can be any of "`origin`", "`peer`", "`asn`", "`v4_bogons`", "`v6_bogons`" or "`hash`". If no parameters are specified all caches will be flushed.
`quiet`	if `TRUE` no diagnostic or informative messages will be displayed. If `FALSE` warnings for unknown cache names and invalidation progress for valid caches will be displayed if the session is interactive.

Note

Invalid cache names will be ignored. If `quiet` is `FALSE` and `flush` was called from an interactive session invalid cache names will be noted.

Also, you will still need to `force` the reloading of bogon lists if you are within the 4 hour window even if you invalided the memoised cache.

Examples

```
## Not run:
flush("peer", "origin")
flush()

## End(Not run)
```

`ipv4_bogons` *Retrieve list of IPv4 "full bogons" from Team Cymru webservice*

Description

The traditional bogon prefixes (IPV4), plus prefixes that have been allocated to RIRs but not yet assigned by those RIRs to ISPs, end-users, etc. Updated every four hours.

Usage

```
ipv4_bogons(force = FALSE, cached_bogons = NA)
```

Arguments

`force`	force a refresh even if the time-frame (4-hours) is not up
`cached_bogons`	if you pass in the previous result of a call to `ipv4_bogoons` it will be returned if the refresh time constraint has not been met, otherwise `NA` will be returned.

Details

Bogons are defined as Martians (private and reserved addresses defined by RFC 1918, RFC 5735, and RFC 6598) and netblocks that have not been allocated to a regional internet registry (RIR) by the Internet Assigned Numbers Authority.

Fullbogons are a larger set which also includes IP space that has been allocated to an RIR, but not assigned by that RIR to an actual ISP or other end-user. IANA maintains a convenient IPv4 summary page listing allocated and reserved netblocks, and each RIR maintains a list of all prefixes that they have assigned to end-users. Our bogon reference pages include additional links and resources to assist those who wish to properly filter bogon prefixes within their networks.

See Also

http://www.team-cymru.org/bogon-reference-http.html

Examples

```
## Not run:
v4_bogons <- ipv4_bogons()
v4_bogons <- ipv4_bogons(cached_bogons=v4_bogons)

## End(Not run)
```

`ipv6_bogons` *Retrieve list of IPv6 "full bogons" from Team Cymru webservice*

Description

IPv6 "fullbogons", all IPv6 prefixes that have not been allocated to RIRs and that have not been assigned by RIRs to ISPs, end-users, etc. Updated every four hours.

Usage

```
ipv6_bogons(force = FALSE, cached_bogons = NA)
```

Arguments

`force`	force a refresh even if the time-frame (4-hours) is not up
`cached_bogons`	if you pass in the previous result of a call to `ipv6_bogoons` it will be returned if the refresh time constraint has not been met, otherwise `NA` will be returned.

Details

Bogons are defined as Martians (private and reserved addresses defined by RFC 1918, RFC 5735, and RFC 6598) and netblocks that have not been allocated to a regional internet registry (RIR) by the Internet Assigned Numbers Authority.

Fullbogons are a larger set which also includes IP space that has been allocated to an RIR, but not assigned by that RIR to an actual ISP or other end-user. IANA maintains a convenient IPv4 summary page listing allocated and reserved netblocks, and each RIR maintains a list of all prefixes that they have assigned to end-users. Our bogon reference pages include additional links and resources to assist those who wish to properly filter bogon prefixes within their networks.

See Also

http://www.team-cymru.org/bogon-reference-http.html

Examples

```
## Not run:
v6_bogons <- ipv6_bogons()
v6_bogons <- ipv6_bogons(cached_bogons=v6_bogons)

## End(Not run)
```

malware_hash *Retrieves malware hash metadata from the Malware Hash Registry*

Description

The Malware Hash Registry (MHR) project is a look-up service similar to the Team Cymru IP address to ASN mapping project. This project differs however, in that you can query the service for a computed MD5 or SHA-1 hash of a file and, if it is malware and the service knows about it, it returns the last time it's seen it along with an approximate anti-virus detection percentage.

Usage

```
malware_hash(hashes, timeout = getOption("timeout"))
```

Arguments

hashes	vector of IPv4 address (character - dotted-decimal)
timeout	numeric: the timeout (in seconds) to be used for this connection. Beware that some OSes may treat very large values as zero: however the POSIX standard requires values up to 31 days to be supported.

Value

data frame of BGP Origin ASN lookup results

- sha1_md5 - hash queried for
- last_known_timestamp - last known GMT timestamp associated with that hash
- detection_pct - detection percentage across a mix of AV packages

If a socket connection cannot be made (i.e. a network problem on your end or a service/network problem on their end), all columns will be NA.

Note

Attempting to enumerate the malware registry via the public service interface is not only impractical, it is also strictly prohibited. Contact Team Cymru if the public interface is insufficient for your needs and we may be able to come up with alternative arrangement. Also, A direct connection to TCP Port 43 (WHOIS) is required for most of these API functions to work properly.

See Also

http://www.team-cymru.org/IP-ASN-mapping.html

Examples

```
## Not run:
malware_hash(c("1250ac278944a0737707cf40a0fbecd4b5a17c9d",
               "7697561ccbbdd1661c25c86762117613",
               "cbed16069043a0bf3c92fff9a99cccdc",
               "e6dc4f4d5061299bc5e76f5cd8d16610",
               "e1112134b6dcc8bed54e0e34d8ac272795e73d74"))

## End(Not run)
```

Index