dns_first

2022-03-05

R Markdown

```
library('RSQLite')
library('ggplot2')
library(DBI)
options("scipen"=100, "digits"=4)


db <- dbConnect(RSQLite::SQLite(), dbname="./dnstor_statistics_dns.sqlite")
dns_data <-dbSendQuery(db, "
  SELECT count(*) as countGrouped, year, period, CAST(CAST(year AS text) || CAST(peri
od AS text) as integer) as year_period , qname, qtype, SUM(count) as quantity
    FROM DNS_ANALYSIS
GROUP BY year_period, year, period, qname, qtype
ORDER BY quantity DESC;
")
dns_data_fetched <- fetch(dns_data)
#dns_data_fetched

#str(dns_data_fetched)
#str(dns_data_fetched$payload)
```

```
library(dplyr)
```

```
##
## Attaching package: 'dplyr'
```

```
## The following objects are masked from 'package:stats':
##
##     filter, lag
```

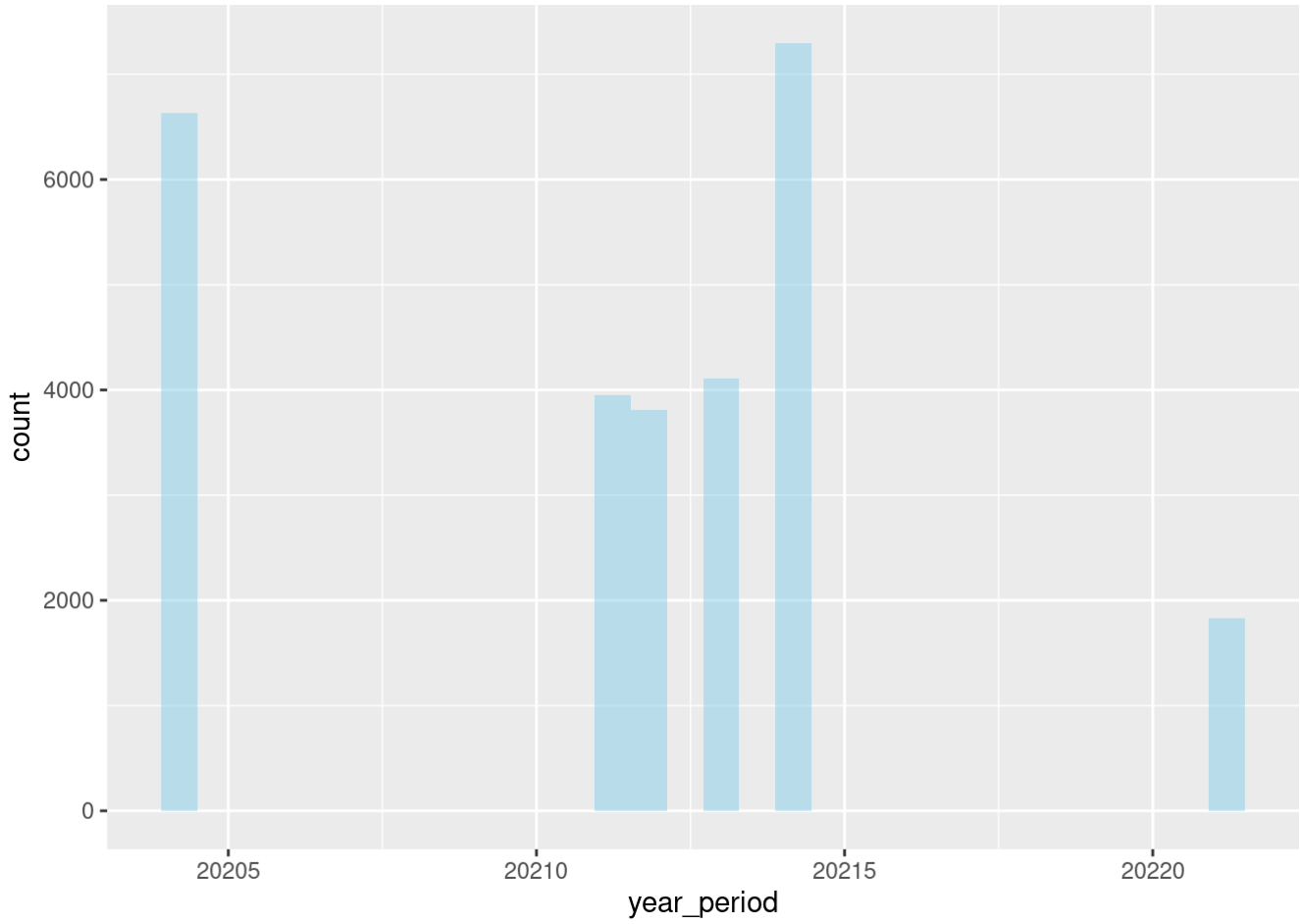
```
## The following objects are masked from 'package:base':
##
##     intersect, setdiff, setequal, union
```

```
library(tibble)

dns_data.year_period.ungrouped <- group_split(dns_data_fetched, year_period)

N = 10
dns_data.topNconsultas <- head(dns_data.year_period.ungrouped[[1]], N)
dns_data.year_period.ungrouped.len = length(dns_data.year_period.ungrouped)

for (i in c(2:dns_data.year_period.ungrouped.len)) {
  dns_data.topNconsultas <- rbind(dns_data.topNconsultas, head(dns_data.year_period.u
ngrouped[[i]], N))
}

#dns_data.year_period.ungrouped[[1]]
#ggplot(dns_data.year_period.ungrouped[[1]], aes(x=qname, y=quantity), ) + geom_histo
gram(fill="skyblue", alpha=0.5)
#ggplot(data = dns_data.year_period.ungrouped[[1]], aes(x = qname, y = quantity)) +
 #geom_boxplot()

#dns_data.topNconsultas

#dns_data.year_period.ungrouped

#dns_data_fetched[order(dns_data_fetched$year, dns_data_fetched$period, -dns_data_fet
ched$quantity),]

#dns_data_fetched

# ggplot(request, aes(x=rt, fill=Type)) + geom_density(alpha=0.4) + scale_x_log10() +
xlab("Number Request (log 10)") + ylab("Density") + ggtitle("Request per DRDoS Attack
s")
# barplot
#  ggplot(nlme::Oxboys, aes(age, height))

# Top N consultas por período N = 10
head(dns_data.topNconsultas)
```

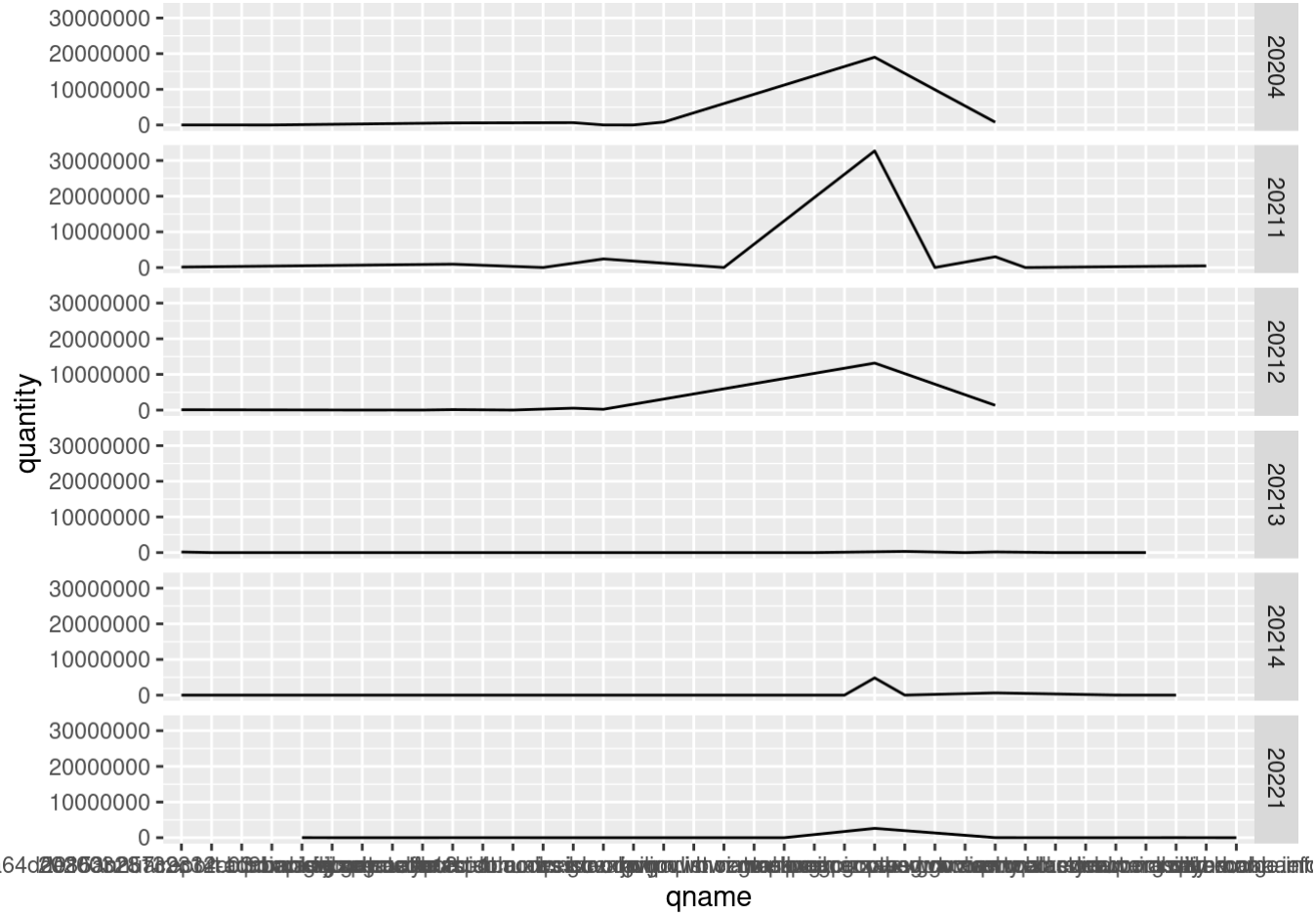
```
## # A tibble: 6 × 7
##   countGrouped  year period year_period qname           qtype quantity
##          <int> <int>  <int>       <int> <chr>           <chr>    <int>
## 1        23891  2020      4       20204 peacecorps.gov. ANY   19005578
## 2        49615  2020      4       20204 lavrov.in.      ANY     816242
## 3          777  2020      4       20204 sl.             ANY     779892
## 4        45508  2020      4       20204 irs.gov.        ANY     652325
## 5         1336  2020      4       20204 fe18.ru.        ANY     569411
## 6          354  2020      4       20204 .               ANY      12296
```

```
ggplot(dns_data_fetched, aes(x=year_period), ) + geom_histogram(fill="skyblue", alpha
=0.5)
```

```
## `stat_bin()` using `bins = 30`. Pick better value with `binwidth`.
```



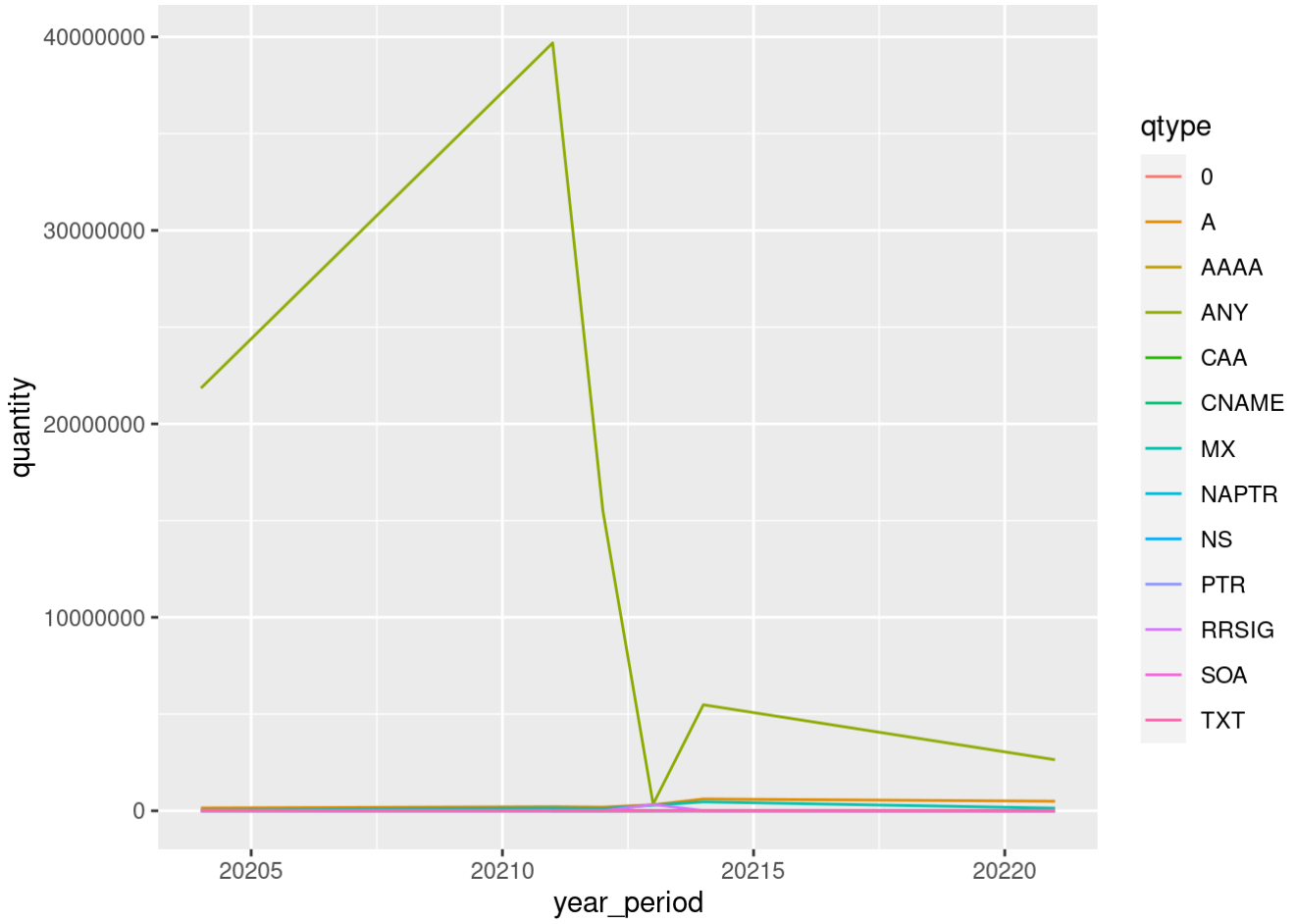

```
ggplot(dns_data.topNconsultas, aes(qname,quantity, group = 1)) + geom_line() + facet_
grid(year_period ~ .)
```



```
#ggplot(data = dns_data.topNconsultas) +
 # geom_point(mapping = aes(x = year_period, y = quantity)) +
  #facet_wrap(~ class, nrow = 2)

#ggplot(data = dns_data.topNconsultas) +
 # geom_bar(mapping = aes(x = year_period, y = count, fill = year_period), position =
"fill")


## ------------ Quantos ataques com cada tipo de qtype foi utilizado, por trimestre ?
------------
#dns_data_fetched

dns_data_fetched.quarter_type_quantity = select(dns_data_fetched, c('year_period', 'q
type', 'quantity'))

#dns_data_fetched.quarter_type_quantity
#typeof(dns_data_fetched$year_period)
#dns_data_fetched$year_period

#dns_data_fetched.quarter_type_quantity[order(dns_data_fetched.quarter_type_quantity
$year_period),]

dns_data_fetched.sum_attacks_quarterly = dns_data_fetched.quarter_type_quantity %>%
  group_by(qtype, year_period) %>%
  summarise(quantity = sum(quantity))
```

```
## `summarise()` has grouped output by 'qtype'. You can override using the
## `.groups` argument.
```

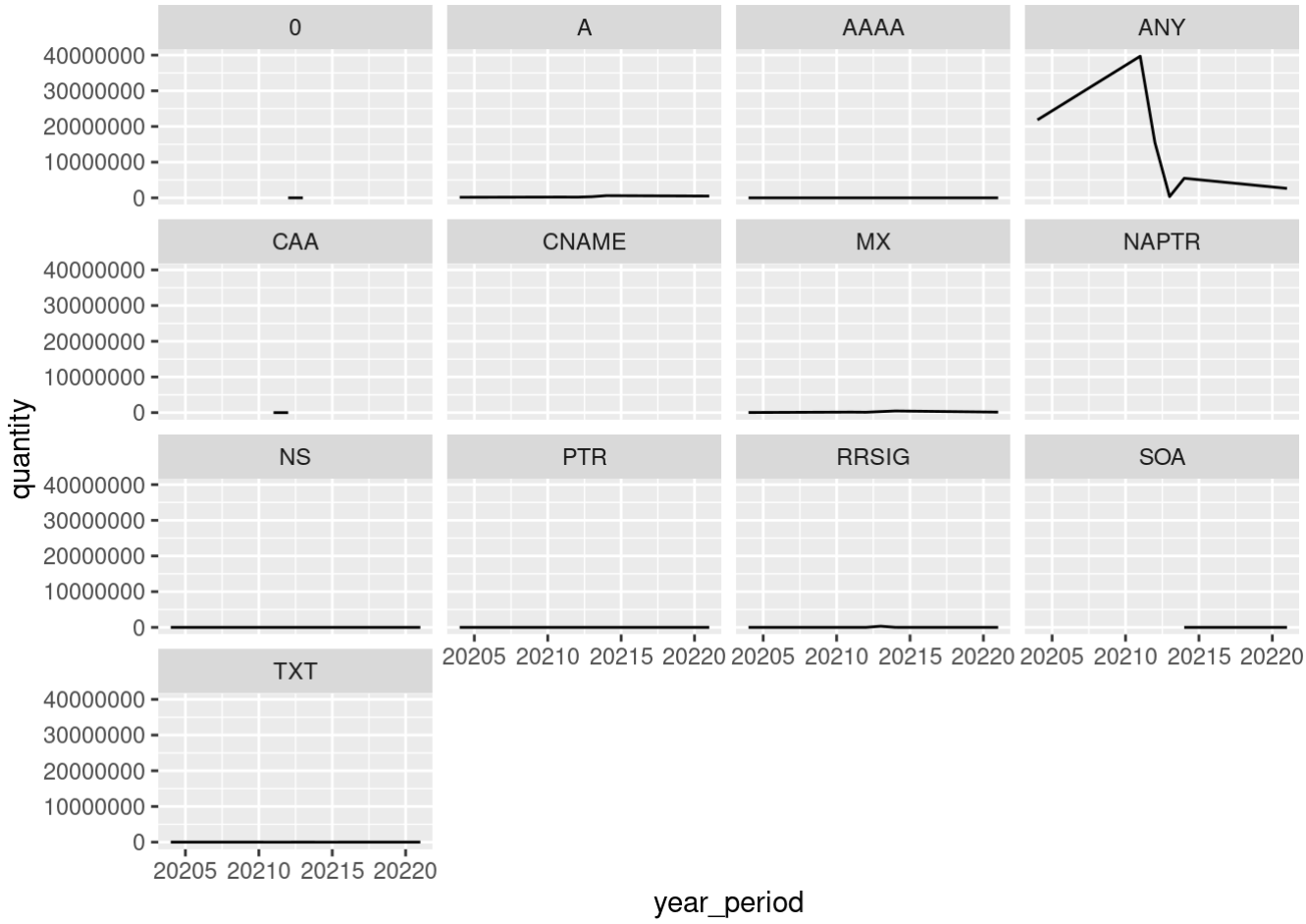
```
#dns_data_fetched.sum_attacks_quarterly[order(-dns_data_fetched.sum_attacks_quarterly
$quantity, dns_data_fetched.sum_attacks_quarterly$year_period),]

ggplot(data = dns_data_fetched.sum_attacks_quarterly, aes(x = year_period, y = quanti
ty, color = qtype)) +
    geom_line()
```




```
ggplot(data = dns_data_fetched.sum_attacks_quarterly, aes(x = year_period, y = quanti
ty)) +
    geom_line() +
    facet_wrap(facets = vars(qtype))
```

```
## geom_path: Each group consists of only one observation. Do you need to adjust
## the group aesthetic?
```

```
## geom_path: Each group consists of only one observation. Do you need to adjust
## the group aesthetic?
```


0
A
AAAA
ANY
CAA
CNAME
MX
NAPTR
NS
PTR
RRSIG
SOA
TXT
quantity
40000000
30000000
20000000
10000000
0
20205 20210 20215 20220
year_period

```
#aggregate(x = dns_data_fetched.quarter_type_quantity, FUN = "sum", drop = TRUE)

# ------------ Quantos qtypes novos aprecem em cada trimestre ------------
# > Diferenças percentuais são mais relevantes que absolutas

quarter_qtype_aux = dns_data.year_period.ungrouped[[1]] %>%
  group_by(qtype) %>%
  summarise(quantity = sum(quantity))

#quarter_qtype_2 = dns_data.year_period.ungrouped[[2]] %>%
#  group_by(qtype) %>%
#  summarise(quantity = sum(quantity))

#quarter_qtype_2
#merged = merge(x = quarter_qtype_aux, y = quarter_qtype_2, by = "qtype", all = TRUE)
#merged.new_quantity = merged$quantity.x - merged$quantity.y
#merged




quarter_new_qtype = data.frame()



for (i in c(2:dns_data.year_period.ungrouped.len)) {
  quarter_qtype = dns_data.year_period.ungrouped[[i]] %>%
    group_by(qtype) %>%
    summarise(quantity = sum(quantity))

  merged = merge(x = quarter_qtype_aux, y = quarter_qtype, by = "qtype", all = TRUE)
  merged.new_quantity = merged$quantity.x - merged$quantity.y

  perio_to_period = paste(head(dns_data.year_period.ungrouped[[i - 1]]['year'], 1),
'.',  head(dns_data.year_period.ungrouped[[i - 1]]['period'], 1), '->' , head(dns_dat
a.year_period.ungrouped[[i]]['year'], 1), '.', head(dns_data.year_period.ungrouped
[[i]]['period'], 1))
  quarter_new_qtype <- rbind(quarter_new_qtype, data.frame(quarter_to_quarter=perio_t
o_period, merged$qtype, sum_quantity=merged$quantity.y - merged$quantity.x, quantity_
percentage=(((merged$quantity.y - merged$quantity.x)*100)/merged$quantity.x), merged
$quantity.x, merged$quantity.y))

  quarter_qtype_aux = quarter_qtype
}

#quarter_new_qtype
head(na.omit(quarter_new_qtype[order(-quarter_new_qtype$quantity_percentage),]))
```

```
##      quarter_to_quarter merged.qtype sum_quantity quantity_percentage
## 30 2021 . 2 -> 2021 . 3        RRSIG       325120             26803.0
## 18 2021 . 1 -> 2021 . 2           NS          119              2975.0
## 35 2021 . 3 -> 2021 . 4          ANY      5133467              1480.4
## 24 2021 . 2 -> 2021 . 3         AAAA          195               367.9
## 6  2020 . 4 -> 2021 . 1           MX       111066               336.9
## 46 2021 . 4 -> 2022 . 1           NS            2               200.0
##    merged.quantity.x merged.quantity.y
## 30              1213            326333
## 18                 4               123
## 35            346754           5480221
## 24                53               248
## 6              32964            144030
## 46                 1                 3
```

```
# ------------ Quantos qname novos aprecem em cada trimestre ------------

quarter_qname_aux = dns_data.year_period.ungrouped[[1]] %>%
  group_by(qname) %>%
  summarise(quantity = sum(quantity))

quarter_new_qname = data.frame()
for (i in c(2:dns_data.year_period.ungrouped.len)) {
  quarter_qname = dns_data.year_period.ungrouped[[i]] %>%
    group_by(qname) %>%
    summarise(quantity = sum(quantity))

  merged = merge(x = quarter_qname_aux, y = quarter_qname, by = "qname", all = TRUE)
  merged.new_quantity = merged$quantity.x - merged$quantity.y

  period_to_period = paste(head(dns_data.year_period.ungrouped[[i - 1]]['year'], 1),
'.',  head(dns_data.year_period.ungrouped[[i - 1]]['period'], 1), '->' , ... = head(d
ns_data.year_period.ungrouped[[i]]['year'], 1), '.', head(dns_data.year_period.ungrou
ped[[i]]['period'], 1))
  quarter_new_qname <- rbind(quarter_new_qname, data.frame(quarter_to_quarter=period_
to_period, merged$qname, sum_quantity=(merged$quantity.y - merged$quantity.x), quanti
ty_percentage_diff=(((merged$quantity.y - merged$quantity.x)*100)/merged$quantity.x),
merged$quantity.x, merged$quantity.y))

  quarter_qname_aux = quarter_qname
}
#quarter_new_qname
head(na.omit(quarter_new_qname[-order(quarter_new_qname$quantity_percentage_diff),]))
```

```
## [1] quarter_to_quarter       merged.qname             sum_quantity
## [4] quantity_percentage_diff merged.quantity.x        merged.quantity.y
## <0 rows> (or 0-length row.names)
```

```
# @todo
#1- olhar a longo prazo, o timelapse dos qnames
#2- qual a frequencia d qnames novos nesses períodos
 #   2.1 olhar em detalhes as variações dos qnames (pq geralmente eles acabam sendo u
m grupo)
```

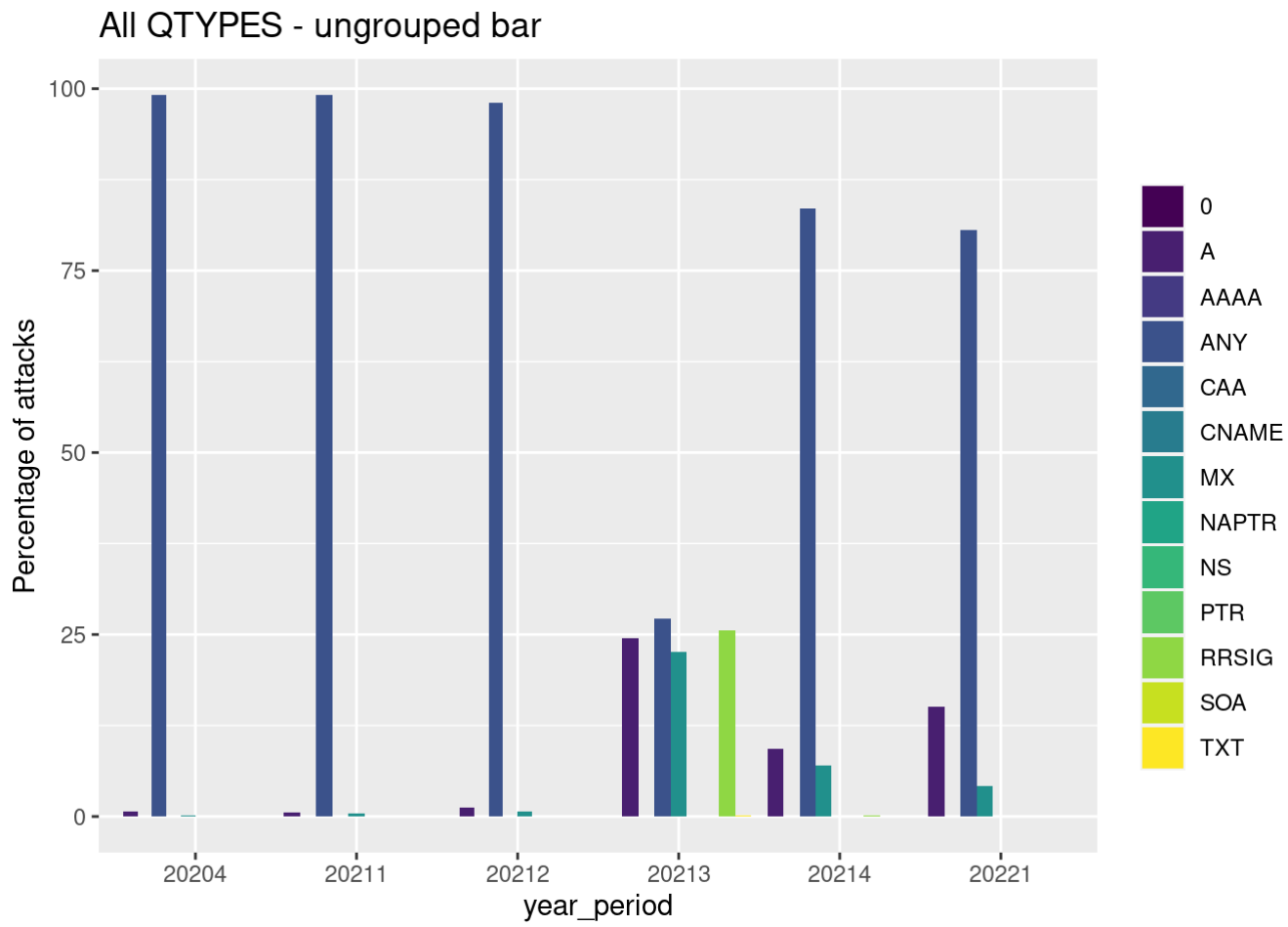
```
# Vale um gráfico de barras (dois, um agrupado e outro empilhado) da porcentagem de Q
TYPEs por período
# https://www.data-to-viz.com/graph/barplot.html
# Libraries
#library(tidyverse)
#library(hrbrthemes)
library(viridis)
```

```
## Loading required package: viridisLite
```

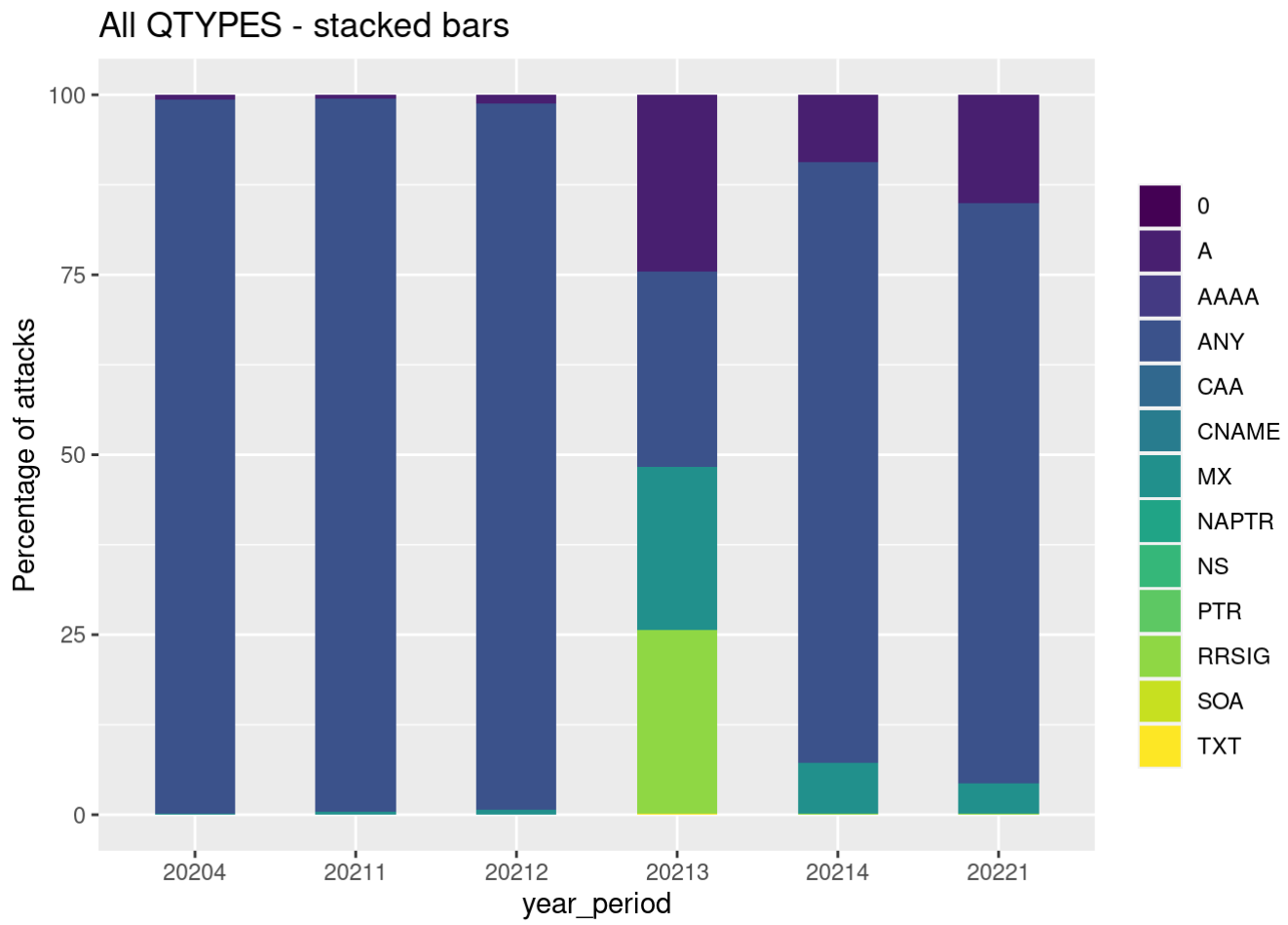
```
dns_data_fetched.sum_attacks_quarterly.quantity_percentage = dns_data_fetched.sum_att
acks_quarterly$quantity / 2
#dns_data_fetched.sum_attacks_quarterly

dns_data_fetched.sum_attacks_quarterly.sum_period = dns_data_fetched.sum_attacks_quar
terly %>%
  group_by(year_period) %>%
  summarise(period_quantity = sum(quantity), qtype=qtype, quantity=quantity)
```

```
## `summarise()` has grouped output by 'year_period'. You can override using the
## `.groups` argument.
```

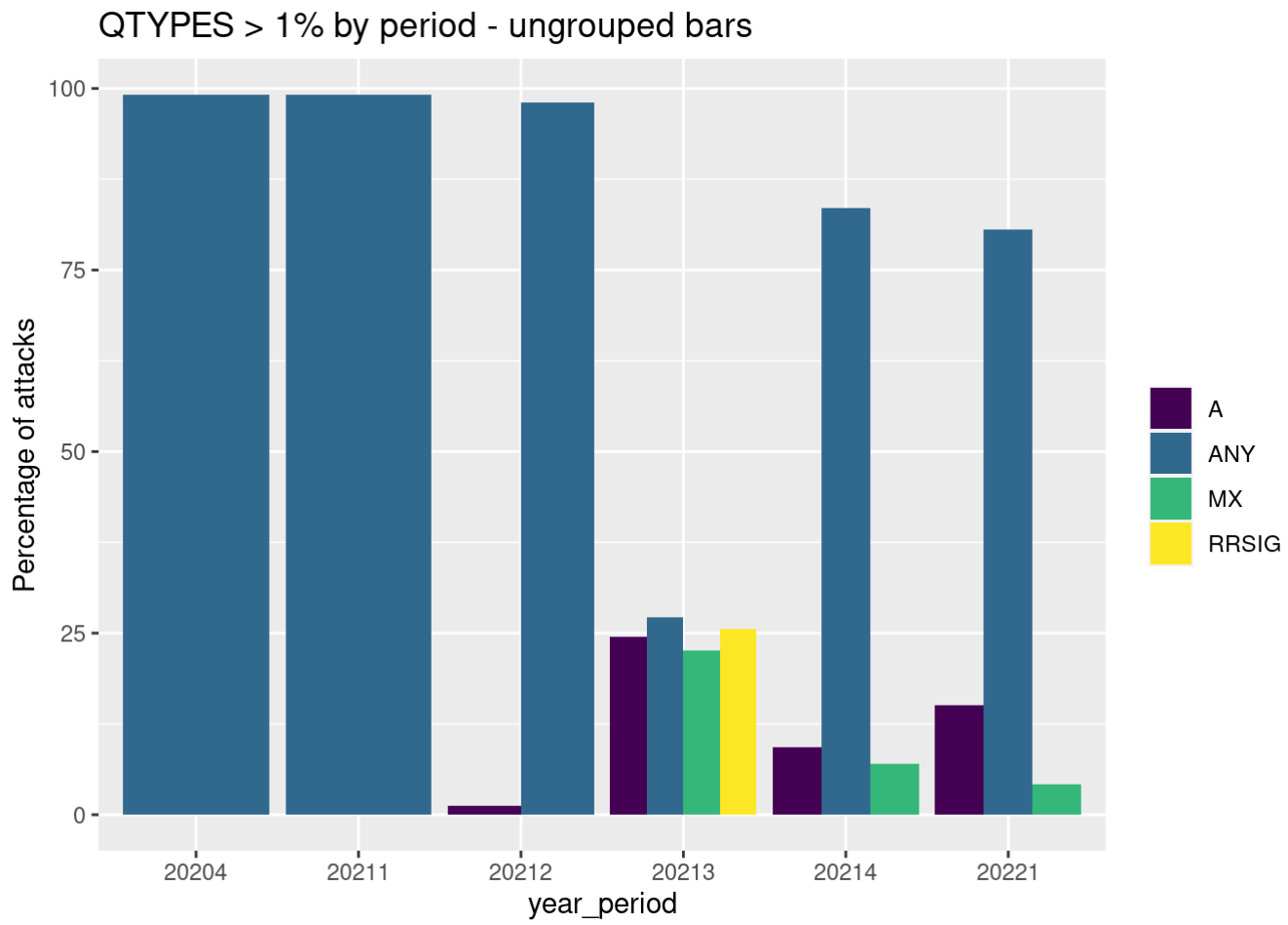
```
dns_data_fetched.sum_attacks_quarterly.sum_period['quantity_percentage'] = (dns_data_
fetched.sum_attacks_quarterly.sum_period$quantity * 100) / dns_data_fetched.sum_attac
ks_quarterly.sum_period$period_quantity

#dns_data_fetched.sum_attacks_quarterly.sum_period


dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", position="dodge") +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("All QTYPES - ungrouped bar")
```



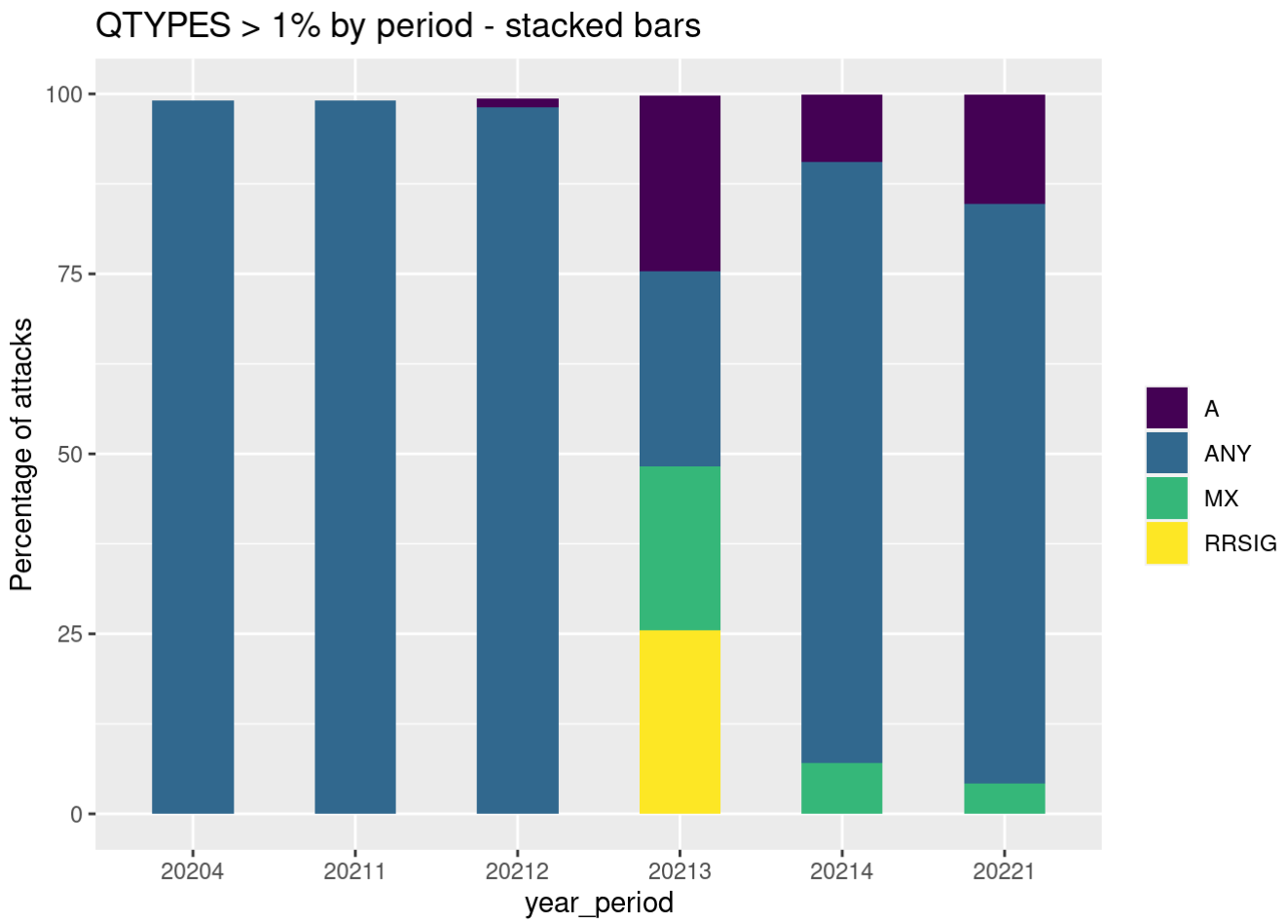

```
dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", width = 0.5) +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("All QTYPES - stacked bars")
```



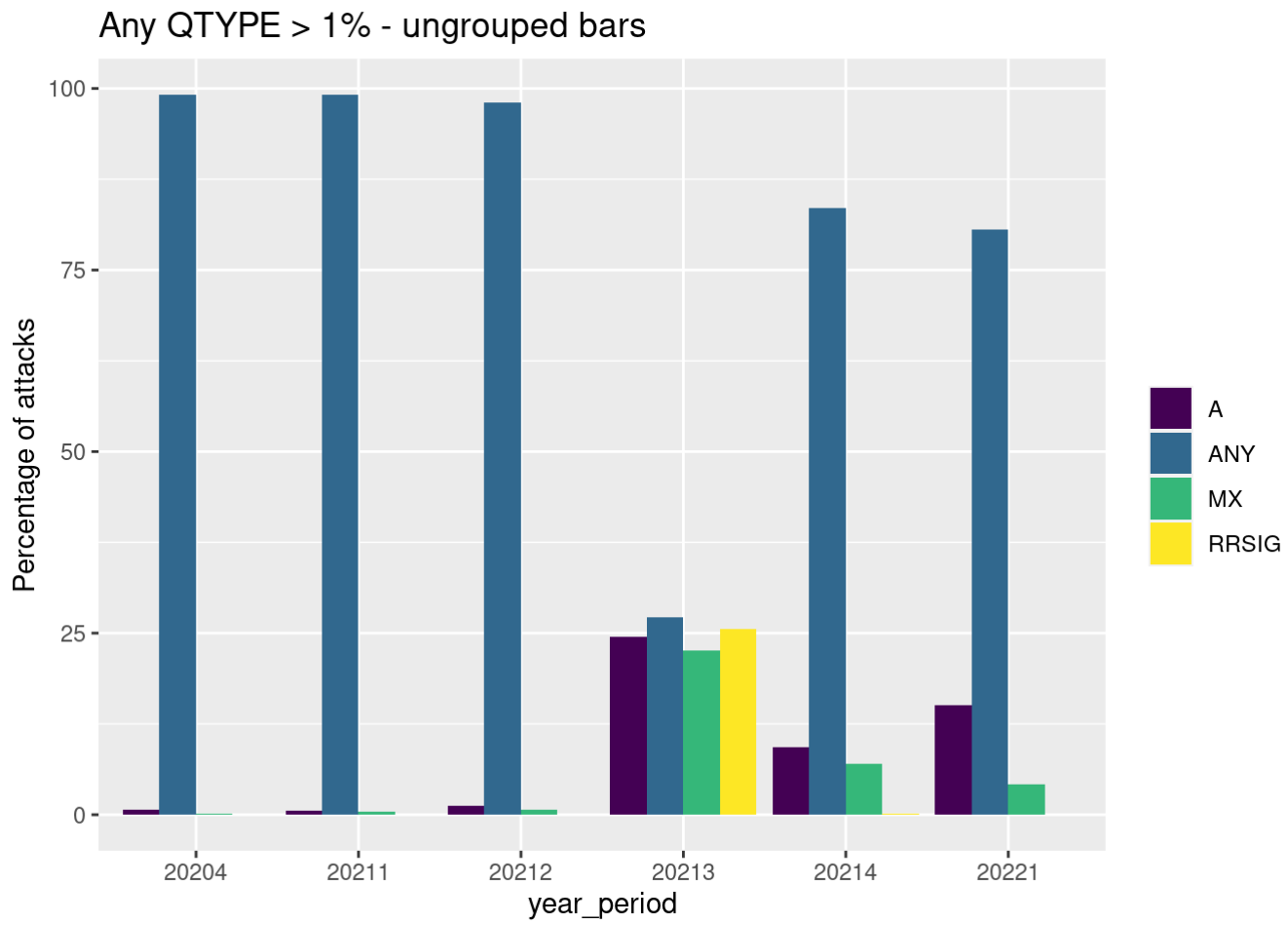

```
## Filter data using qtype quantity percentage bigger than 1

dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  filter(quantity_percentage > 1) %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", position="dodge") +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("QTYPES > 1% by period - ungrouped bars")
```



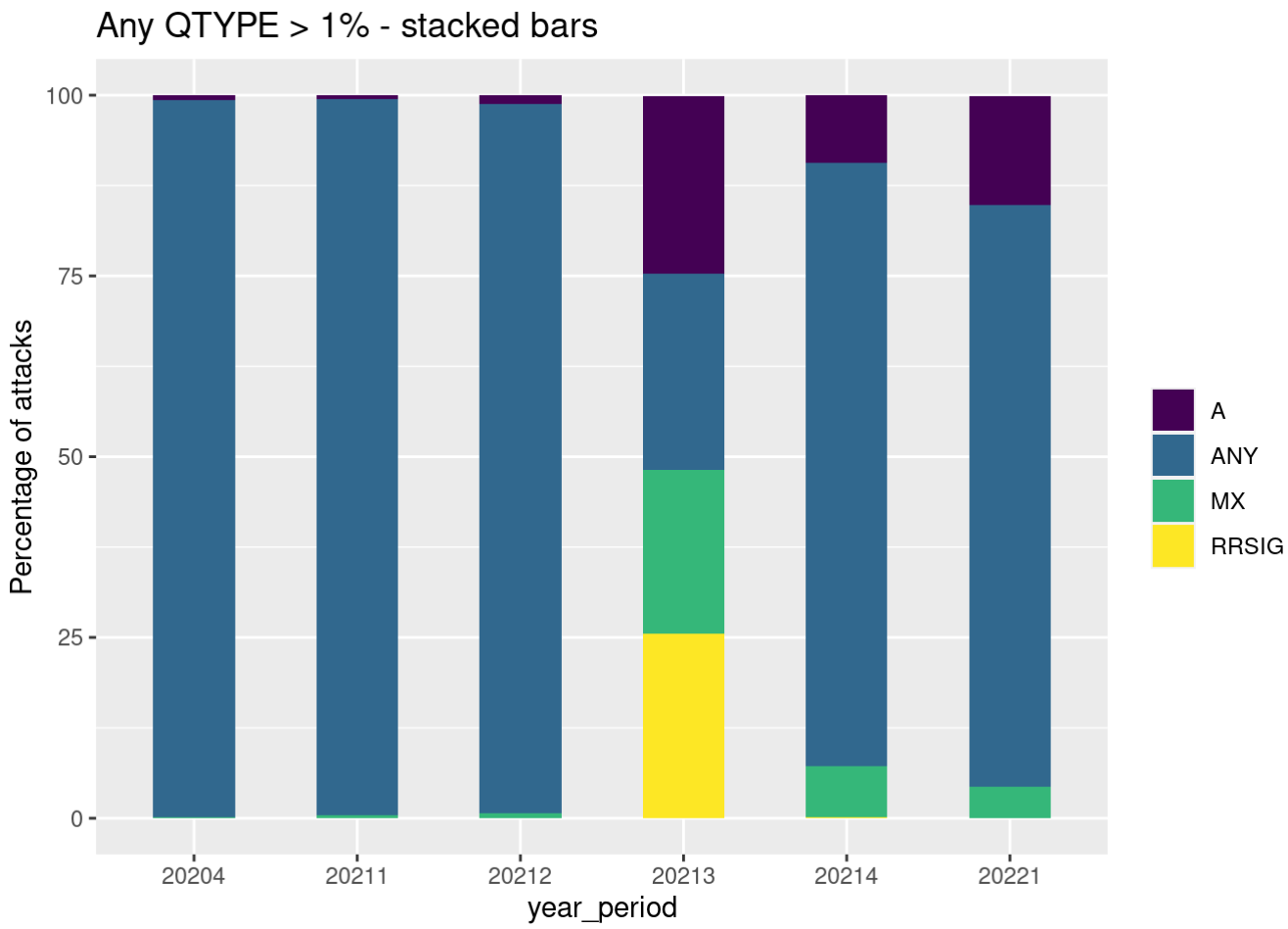

```
dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  filter(quantity_percentage > 1) %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", width = 0.5) +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("QTYPES > 1% by period - stacked bars")
```




```
#dns_data_fetched.sum_attacks_quarterly.sum_period
dns_data_fetched.sum_attacks_quarterly.sum_period.relevant = dns_data_fetched.sum_att
acks_quarterly.sum_period %>%
  filter(quantity_percentage > 1)

#dns_data_fetched.sum_attacks_quarterly.sum_period.relevant$qtype
qtypes_bigger_1 = dns_data_fetched.sum_attacks_quarterly.sum_period.relevant$qtype[!d
uplicated(dns_data_fetched.sum_attacks_quarterly.sum_period.relevant$qtype)]
#qtypes_bigger_1

dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  filter(qtype %in% qtypes_bigger_1) %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", position="dodge") +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("Any QTYPE > 1% - ungrouped bars")
```




```
dns_data_fetched.sum_attacks_quarterly.sum_period %>%
  filter(qtype %in% qtypes_bigger_1) %>%
  mutate(year_period=as.factor(year_period)) %>%
  ggplot( aes(x=year_period, y=quantity_percentage, fill=qtype)) +
    geom_bar(stat="identity", width = 0.5) +
    scale_fill_viridis(discrete=TRUE, name="") +
    ylab("Percentage of attacks") +
    ggtitle("Any QTYPE > 1% - stacked bars")
```


Any QTYPE > 1% - stacked bars
Percentage of attacks
100
75
50
25
0
20204
20211
20212
20213
20214
20221
year_period
A
ANY
MX
RRSIG