apresentacao_ssdp_coap_cldap

Rafilx

2022-11-16

```
##
## 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

## Loading required package: gridExtra

##
## Attaching package: 'gridExtra'

## The following object is masked from 'package:dplyr':
##
##     combine

## Loading required package: viridisLite

##
## Attaching package: 'lubridate'

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

##
## Attaching package: 'scales'

## The following object is masked from 'package:viridis':
##
##     viridis_pal
```

```
db_ssdp <- dbConnect(RSQLite::SQLite(), dbname="../../db/database-2022-05-11/dnstor_statistics_ssdp.sqli

data_ssdp_unfetch <-dbSendQuery(db_ssdp, "
  SELECT ip AS vitima_ip, count AS requests_per_attack, CAST(CAST(year AS text) || CAST(period AS text)
    FROM (
      SELECT *,  strftime(\"%Y\", tempoInicio) as year, ((strftime(\"%m\", tempoFinal) - 1) / 3) + 1 AS
        FROM SSDP_MEMORY_DICT
    )
   WHERE year_period >= 20183
")
data_ssdp <- fetch(data_ssdp_unfetch)

dbDisconnect(db_ssdp)
```

```
## Warning in connection_release(conn@ptr): There are 1 result in use. The
## connection will be released when they are closed
```

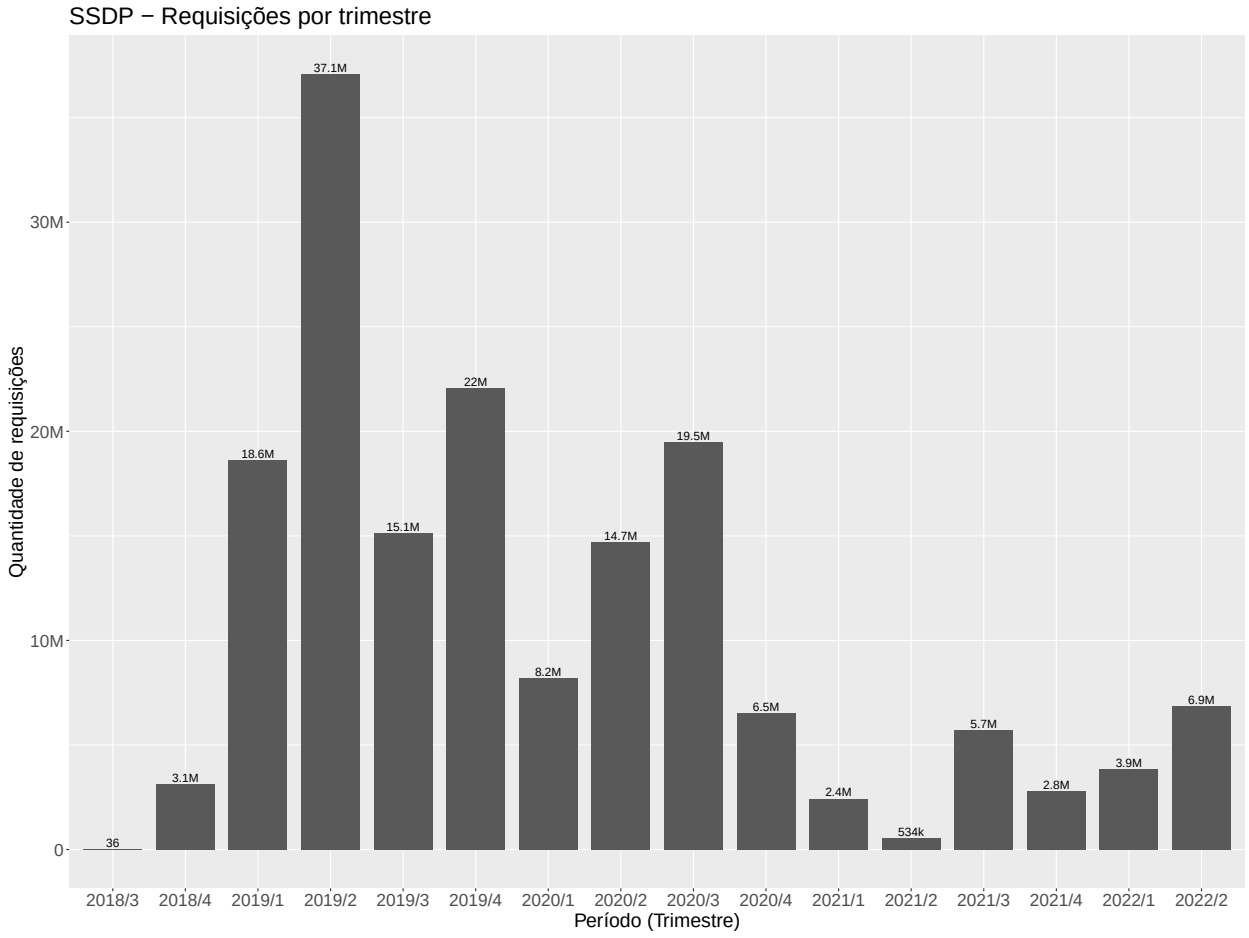
```
data_ssdp_period = data_ssdp %>%
  group_by(year_period) %>%
  summarise(sum_requests_per_attack = sum(requests_per_attack),
            number_of_attacks = n(),
            count_victim = n_distinct(vitima_ip))

print(data_ssdp_period, n=16)
```

```
## # A tibble: 16 x 4
##    year_period sum_requests_per_attack number_of_attacks count_victim
##          <int>                   <int>             <int>        <int>
##  1       20183                      36                28           19
##  2       20184                 3132937             32611         4369
##  3       20191                18637532             40363        15255
##  4       20192                37083647            143977        54087
##  5       20193                15137603             13249         2330
##  6       20194                22049275              3251         1667
##  7       20201                 8209352              4314         1189
##  8       20202                14685242             13610         1910
##  9       20203                19488680             14636         1195
## 10       20204                 6519036             40282         5039
## 11       20211                 2436283              1980          824
## 12       20212                  534279              1331          563
## 13       20213                 5712324              1771          566
## 14       20214                 2793950              7549         4886
## 15       20221                 3864966             31402         9702
## 16       20222                 6863372             30130         7914
```

- SSDP Plot Requisições

```
data_ssdp_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=sum_requests_per_attack)) +
```

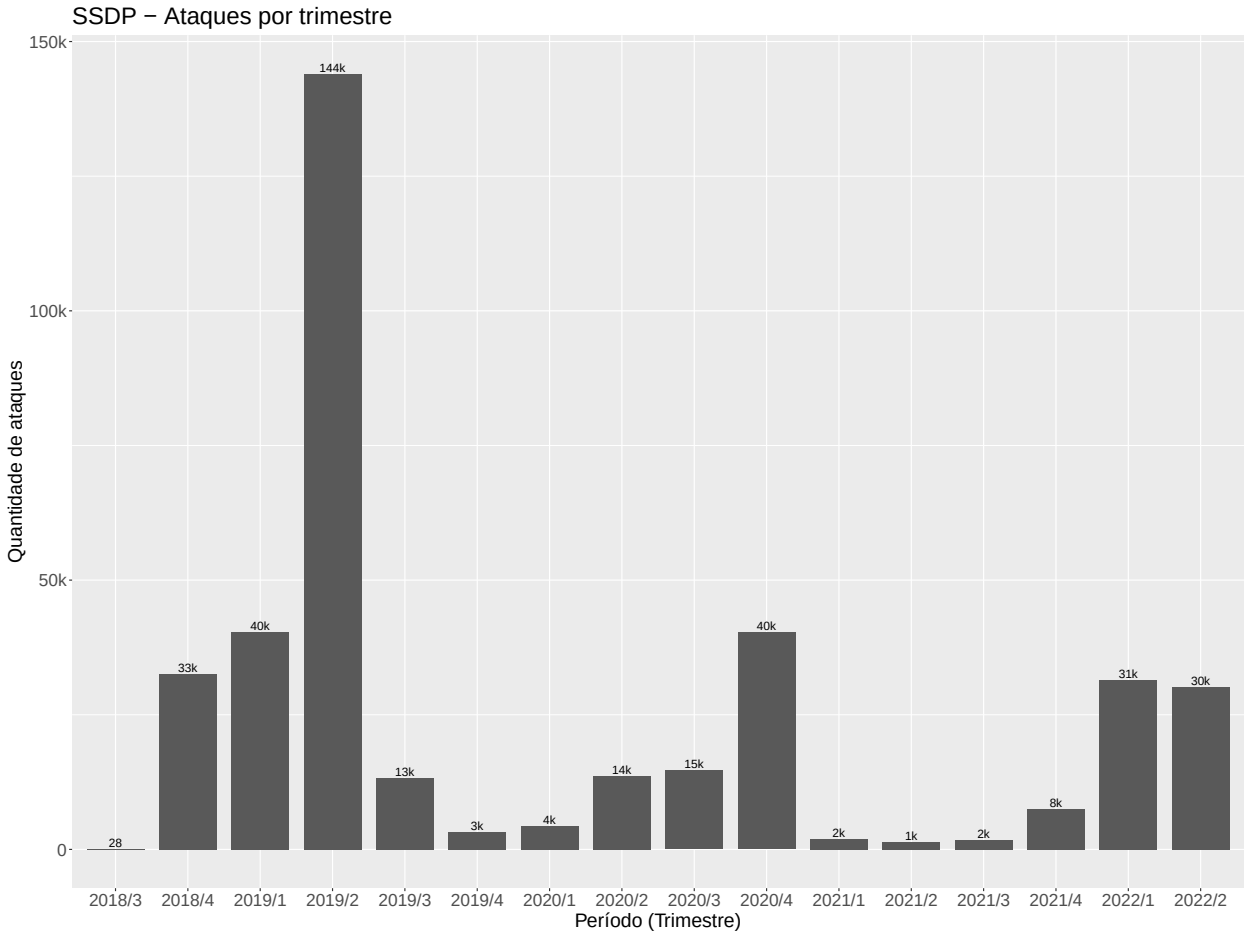
```
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(sum_requests_per_attack),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de requisições") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("SSDP - Requisições por trimestre")
```



- SSDP Plot Ataques

```
data_ssdp_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
```

```
ggplot( aes(x=year_period, y=number_of_attacks)) +
  geom_bar(stat="identity", width = 0.8, position="dodge") +
  geom_text(aes(label = addUnits(number_of_attacks),  vjust = -0.25)) +
  scale_fill_viridis(discrete=TRUE) +
  scale_y_continuous(labels = addUnits) +
  ylab("Quantidade de ataques") +
  xlab("Período (Trimestre)") +
  theme(
    plot.title = element_text(size = 22),
    axis.title = element_text(size = 18),
    legend.position="none",
    strip.text = element_text(size = 16),
    axis.text.x = element_text(size = 16),
    axis.text.y = element_text(size = 16),
  ) +
  ggtitle("SSDP - Ataques por trimestre")
```

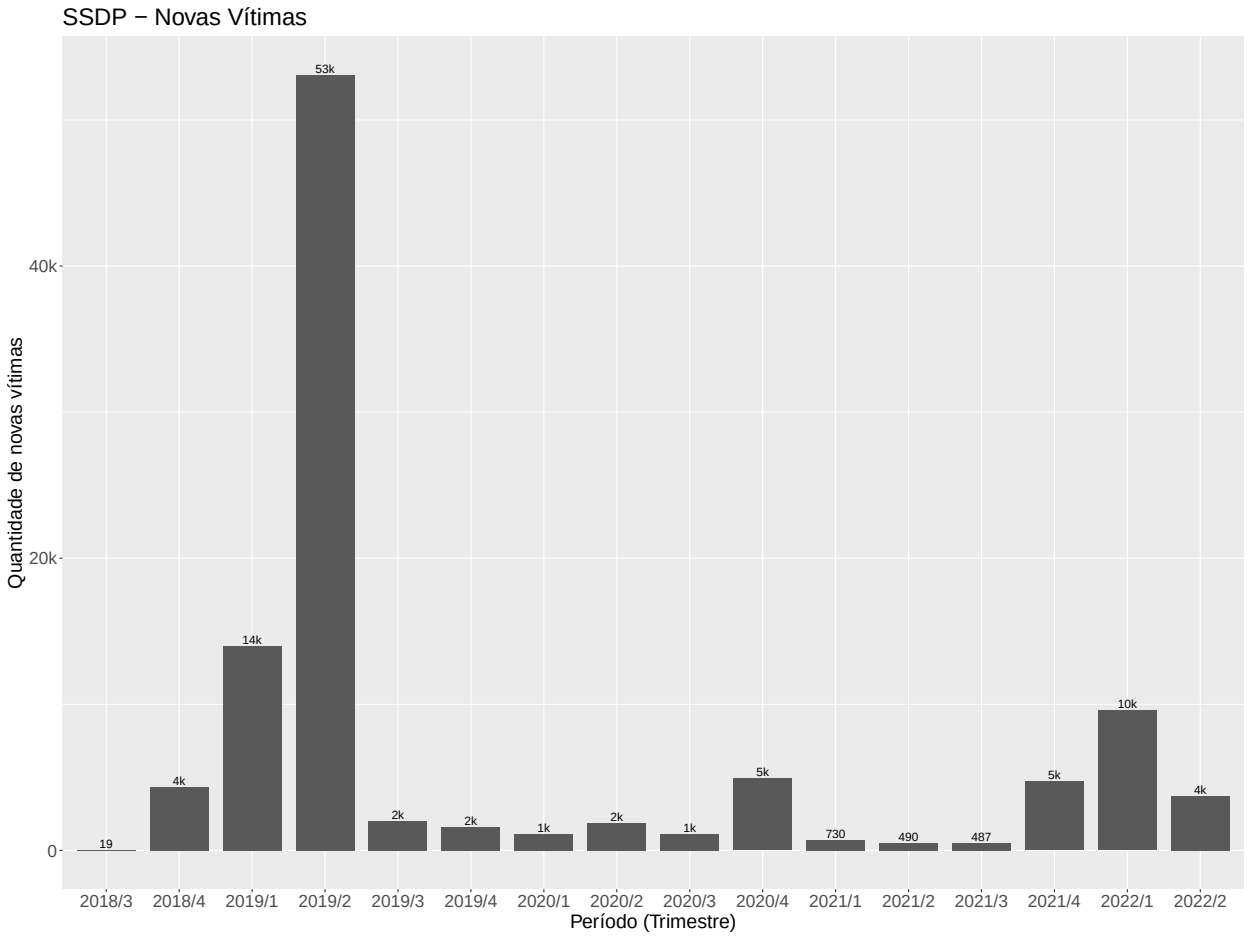


- Pergunta, alguma suposição do motivo de tantas requisições/ataques em 2019/2
- SSDP Novas Vítimas

```
data_ssdp_period_new_victim = data_ssdp %>%
  ungroup() %>%
  group_by(vitima_ip) %>%
  summarise(year_period = min(year_period)) %>%
  ungroup() %>%
  group_by(year_period) %>%
  summarise(new_victims = n_distinct(vitima_ip)) %>%
  mutate(year_period=as.factor(year_period))
```

- SSDP Plot Novas Vítimas

```
ssdp_plot_new_victim = data_ssdp_period_new_victim %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=new_victims)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(new_victims),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de novas vítimas") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("SSDP - Novas Vítimas")
#
# pdf(paste(plots_path, "/ssdp.pdf", sep=""), width = 16, height = 10, pointsize=16)
# print(ssdp_plot_new_victim)
# dev.off()

ssdp_plot_new_victim
```



COAP

```
db_coap <- dbConnect(RSQLite::SQLite(), dbname="../../db/database-2022-05-11/dnstor_statistics_coap.sqli

data_coap_unfetch <-dbSendQuery(db_coap, "
  SELECT ip AS vitima_ip, count AS requests_per_attack, CAST(CAST(year AS text) || CAST(period AS text)
    FROM (
      SELECT *,  strftime(\"%Y\", tempoInicio) as year, ((strftime(\"%m\", tempoFinal) - 1) / 3) + 1 AS
        FROM COAP_MEMORY_DICT
    )
   WHERE year_period >= 20183
")
data_coap <- fetch(data_coap_unfetch)

dbDisconnect(db_coap)
```

```
## Warning in connection_release(conn@ptr): There are 1 result in use. The
## connection will be released when they are closed
```

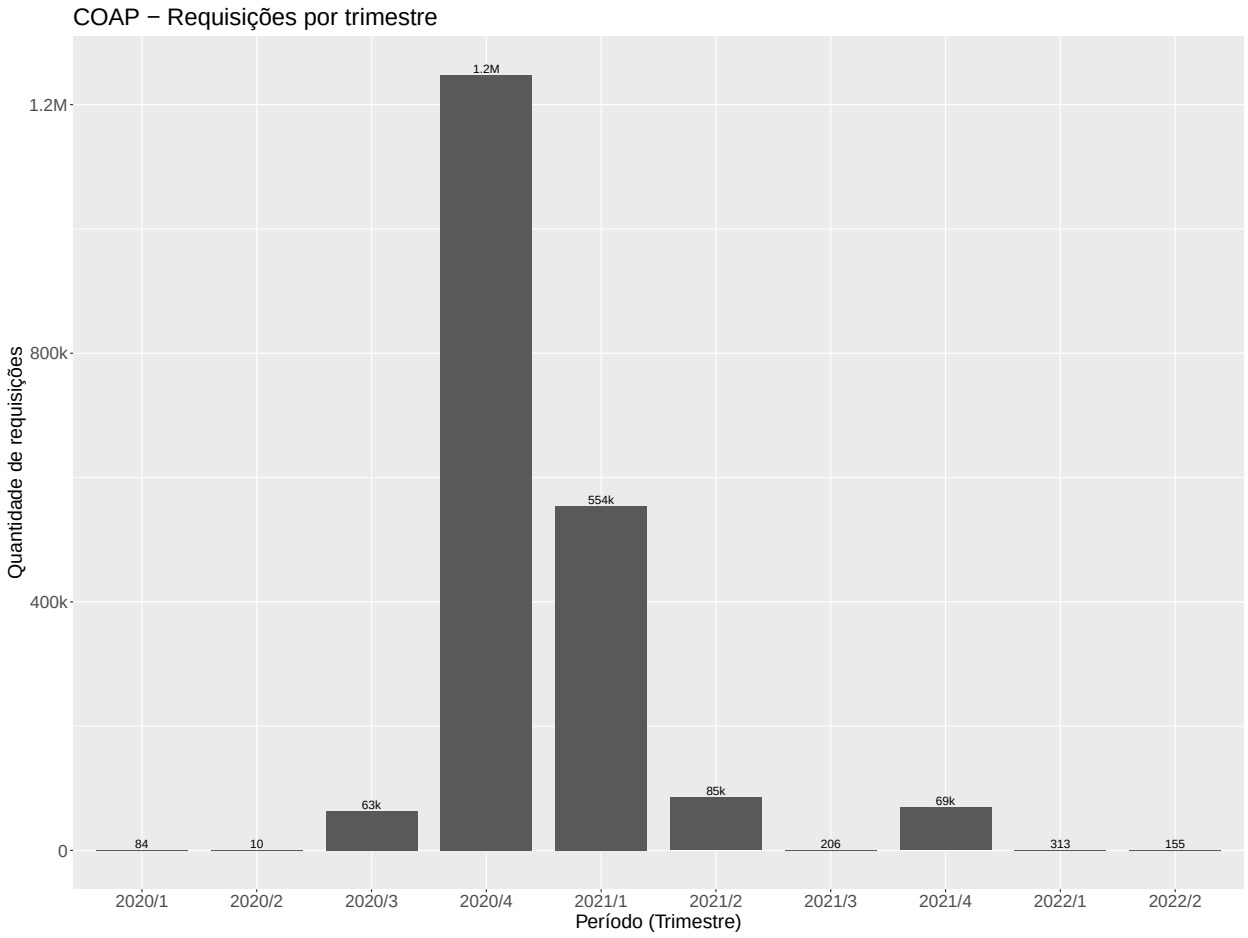
```
data_coap_period = data_coap %>%
  group_by(year_period) %>%
```

```
  summarise(sum_requests_per_attack = sum(requests_per_attack),
            number_of_attacks = n(),
            count_victim = n_distinct(vitima_ip))

print(data_coap_period, n=16)
```

```
## # A tibble: 10 x 4
##    year_period sum_requests_per_attack number_of_attacks count_victim
##          <int>                   <int>             <int>        <int>
##  1       20201                      84                64           28
##  2       20202                      10                 7            7
##  3       20203                   62984               240           95
##  4       20204                 1247687               973          625
##  5       20211                  553510               641          448
##  6       20212                   85067               335          238
##  7       20213                     206               191           88
##  8       20214                   69172              3115         2934
##  9       20221                     313               291          161
## 10       20222                     155               145          101
```

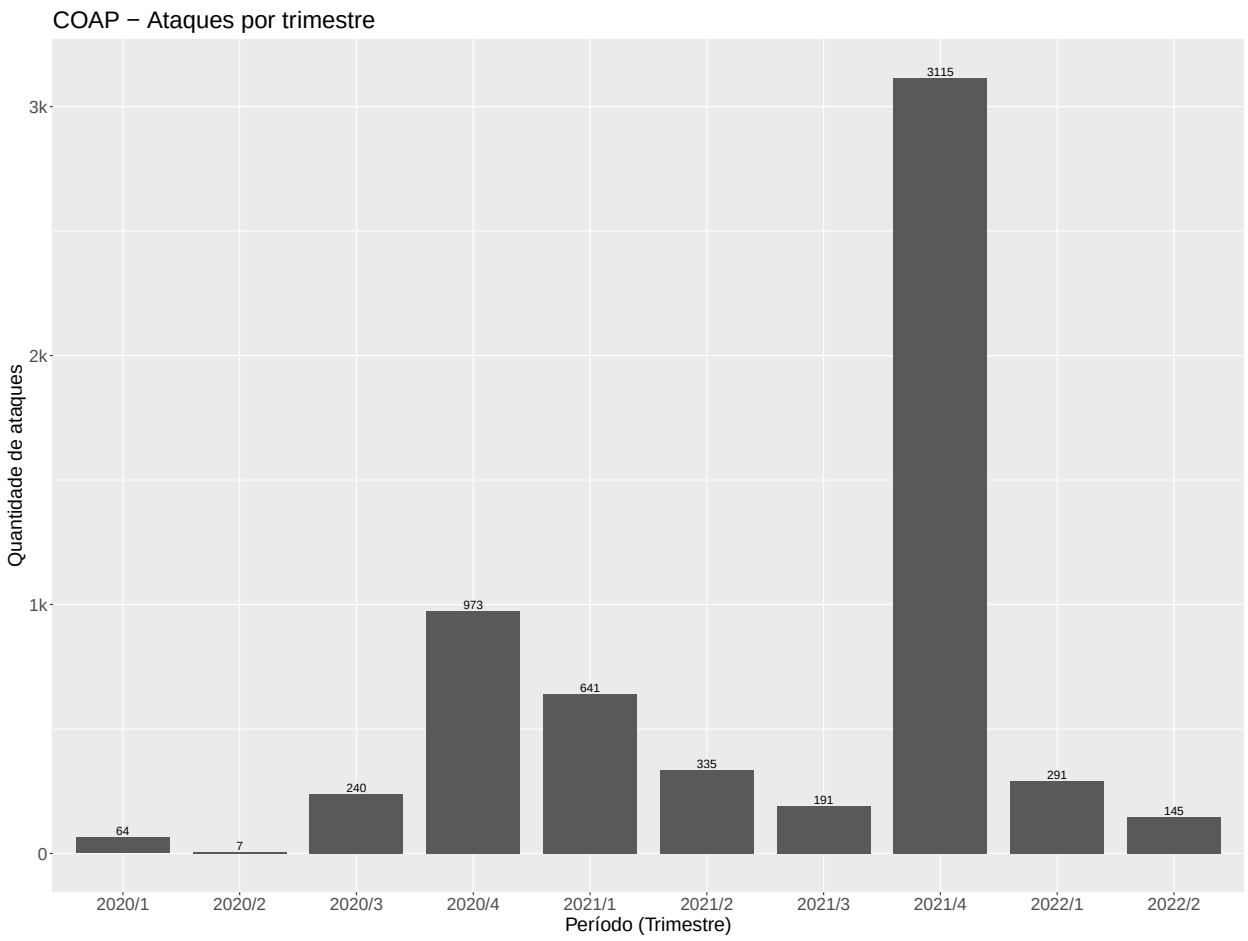
- COAP Plot Requisições

```
data_coap_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=sum_requests_per_attack)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(sum_requests_per_attack),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de requisições") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("COAP - Requisições por trimestre")
```



- COAP Plot Ataques

```
data_coap_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=number_of_attacks)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = number_of_attacks,  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de ataques") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("COAP - Ataques por trimestre")
```



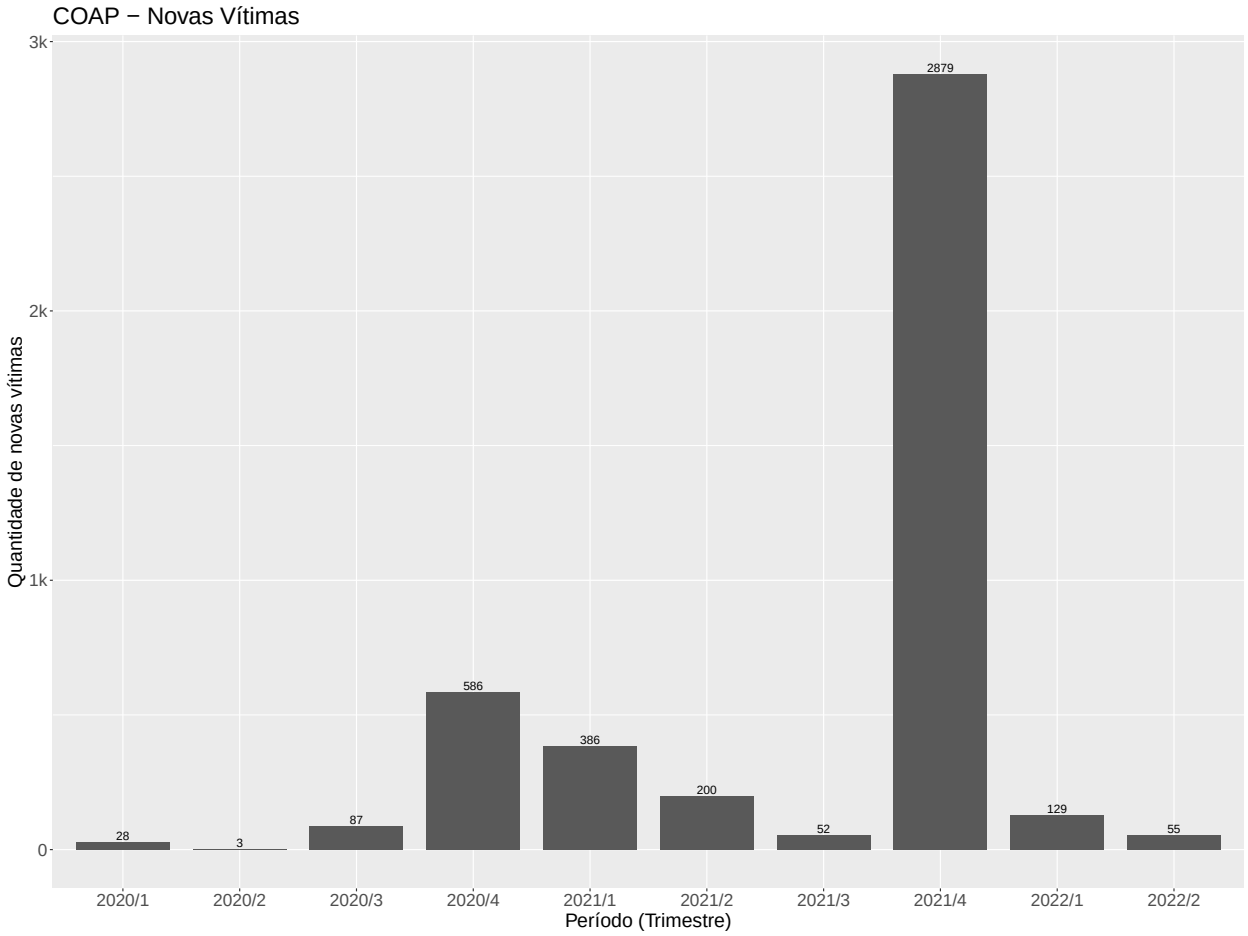
- Ataques com muitas requisições em 2020/4
- Muitos ataques com "poucas" requisições em 2021/4, resultando em várias novas vítimas
- COAP Novas Vítimas

```
data_coap_period_new_victim = data_coap %>%
  ungroup() %>%
  group_by(vitima_ip) %>%
  summarise(year_period = min(year_period)) %>%
  ungroup() %>%
  group_by(year_period) %>%
  summarise(new_victims = n_distinct(vitima_ip)) %>%
  mutate(year_period=as.factor(year_period))
```

- SSDP Plot Novas Vítimas

```
data_coap_period_new_victim %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=new_victims)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
```

```
    geom_text(aes(label = new_victims,  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de novas vítimas") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("COAP - Novas Vítimas")
```



CLDAP

```
db_cldap <- dbConnect(RSQLite::SQLite(), dbname="../../db/database-2022-05-11/dnstor_statistics_cldap.s

data_cldap_unfetch <-dbSendQuery(db_cldap, "
  SELECT ip AS vitima_ip, count AS requests_per_attack, CAST(CAST(year AS text) || CAST(period AS text)
```

```
    FROM (
      SELECT *,  strftime(\"%Y\", tempoInicio) as year, ((strftime(\"%m\", tempoFinal) - 1) / 3) + 1 AS
        FROM CLDAP_MEMORY_DICT
    )
   WHERE year_period >= 20183
")
data_cldap <- fetch(data_cldap_unfetch)

dbDisconnect(db_cldap)
```

```
## Warning in connection_release(conn@ptr): There are 1 result in use. The
## connection will be released when they are closed
```

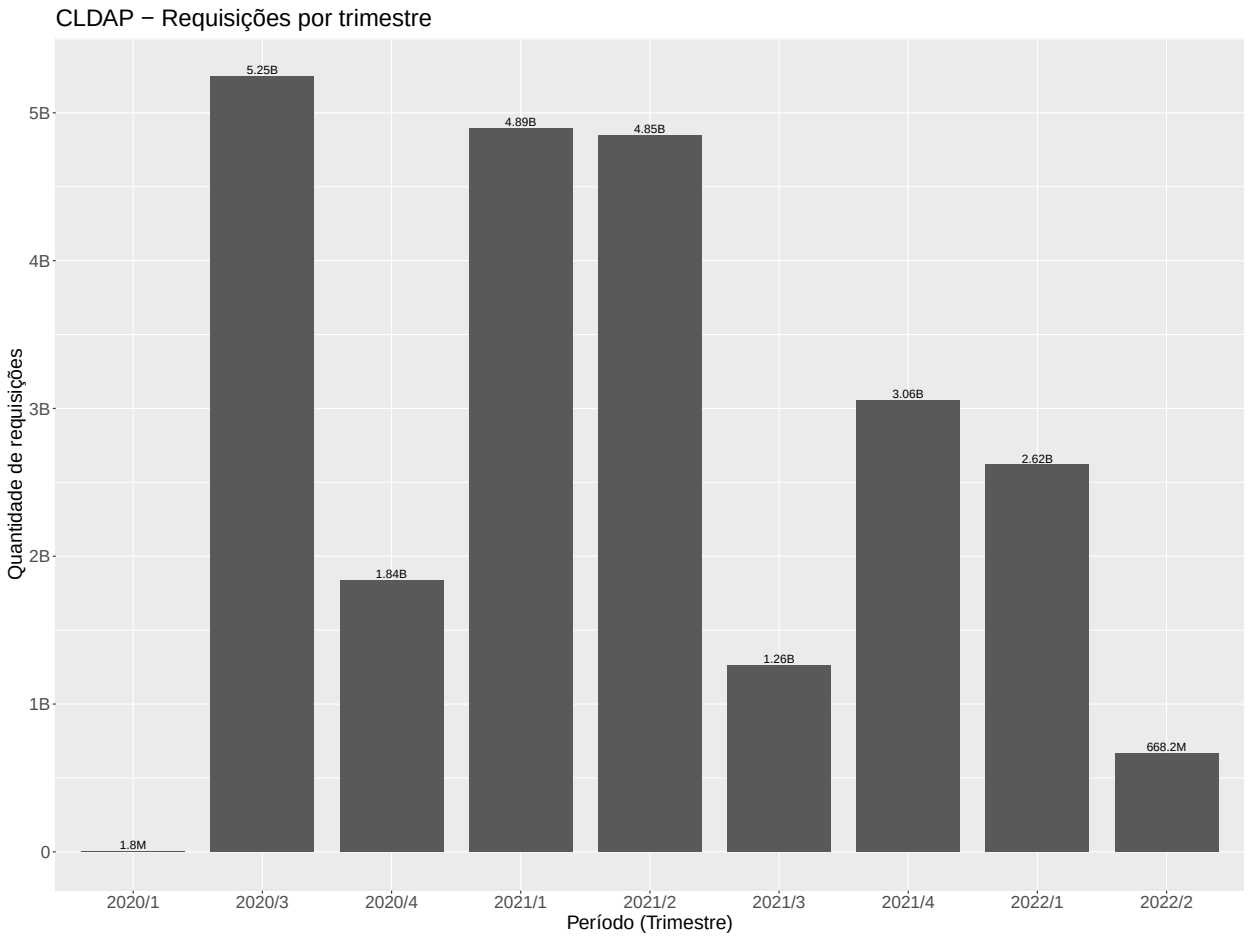
```
data_cldap_period = data_cldap %>%
  group_by(year_period) %>%
  summarise(sum_requests_per_attack = sum(requests_per_attack),
            number_of_attacks = n(),
            count_victim = n_distinct(vitima_ip))

print(data_cldap_period, n=16)
```

```
## # A tibble: 9 x 4
##   year_period sum_requests_per_attack number_of_attacks count_victim
##         <int>                   <dbl>             <int>        <int>
## 1       20201                 1829217                88           88
## 2       20203              5246353138            235269       130130
## 3       20204              1838363621            387658       227865
## 4       20211              4894059510            141788        87468
## 5       20212              4848786180           1072311       119097
## 6       20213              1263796087           1093882        52911
## 7       20214              3057673029           1115518        89845
## 8       20221              2619080183           1873084        57023
## 9       20222               668244857            682052        68421
```

- CLDAP Plot Requisições

```
data_cldap_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=sum_requests_per_attack)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(sum_requests_per_attack),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de requisições") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
```

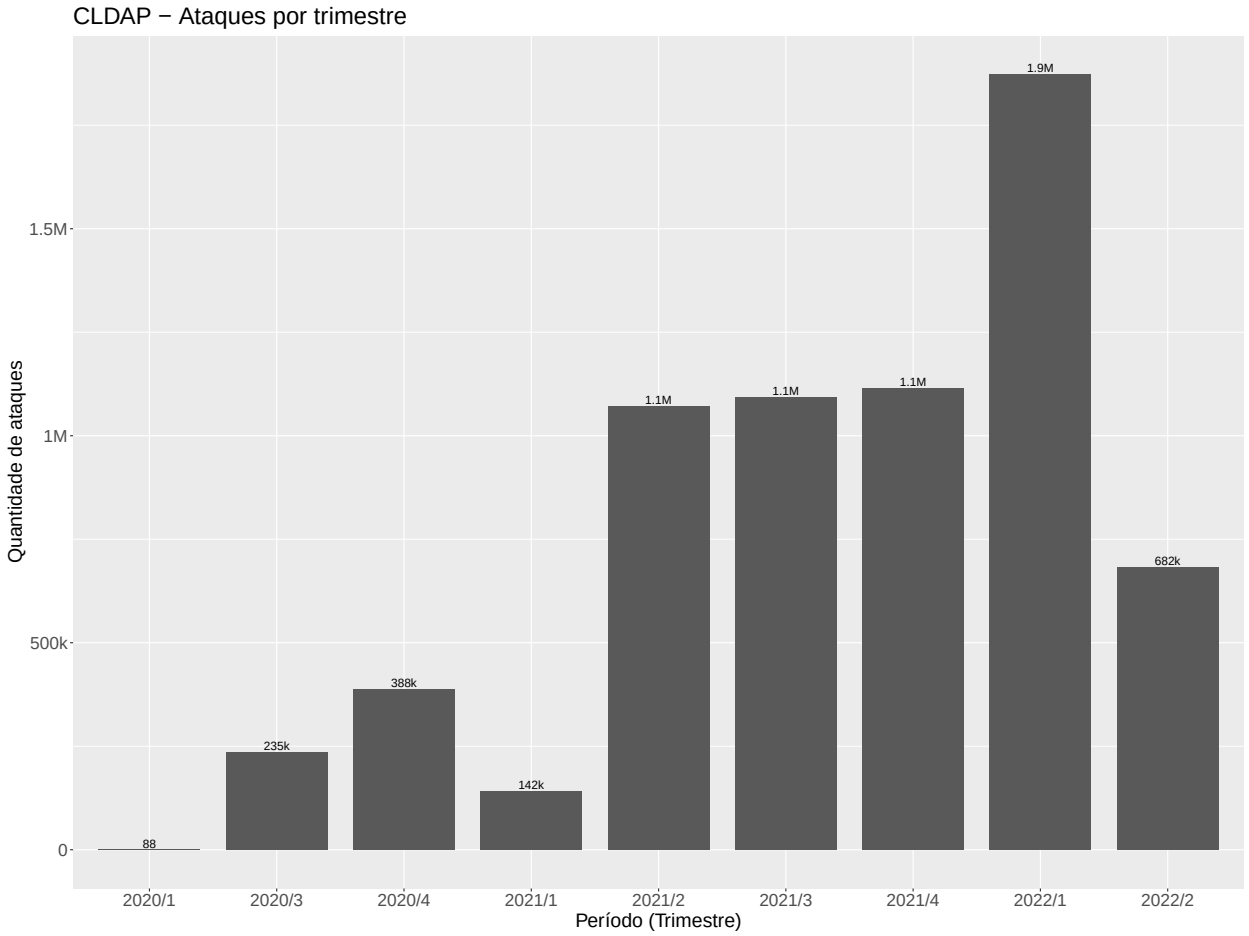
```
    axis.text.x = element_text(size = 16),
    axis.text.y = element_text(size = 16),
  ) +
  ggtitle("CLDAP - Requisições por trimestre")
```



- CLDAP Plot Ataques

```
data_cldap_period %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=number_of_attacks)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(number_of_attacks),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de ataques") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
```

```
    strip.text = element_text(size = 16),
    axis.text.x = element_text(size = 16),
    axis.text.y = element_text(size = 16),
  ) +
  ggtitle("CLDAP - Ataques por trimestre")
```

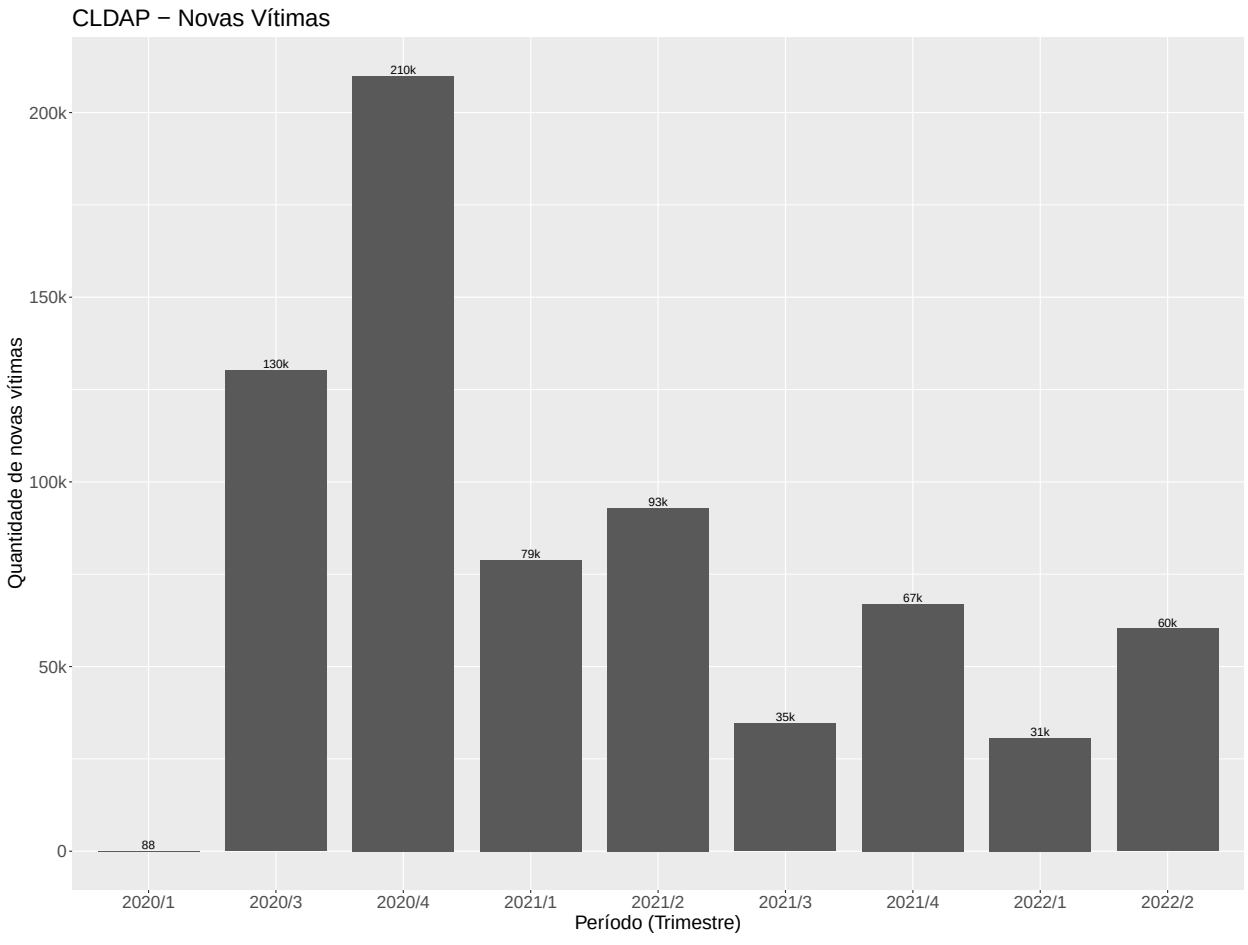


- Ataques com muitas requisições em 2020/3
- CLDAP Novas Vítimas

```
data_cldap_period_new_victim = data_cldap %>%
  ungroup() %>%
  group_by(vitima_ip) %>%
  summarise(year_period = min(year_period)) %>%
  ungroup() %>%
  group_by(year_period) %>%
  summarise(new_victims = n_distinct(vitima_ip)) %>%
  mutate(year_period=as.factor(year_period))
```

- SSDP Plot Novas Vítimas

```
data_cldap_period_new_victim %>%
  mutate(
    year_period = paste(substr(year_period, 0, 4), substr(year_period, 5, 5), sep = "/"),
  ) %>%
  ggplot( aes(x=year_period, y=new_victims)) +
    geom_bar(stat="identity", width = 0.8, position="dodge") +
    geom_text(aes(label = addUnits(new_victims),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE) +
    scale_y_continuous(labels = addUnits) +
    ylab("Quantidade de novas vítimas") +
    xlab("Período (Trimestre)") +
    theme(
      plot.title = element_text(size = 22),
      axis.title = element_text(size = 18),
      legend.position="none",
      strip.text = element_text(size = 16),
      axis.text.x = element_text(size = 16),
      axis.text.y = element_text(size = 16),
    ) +
    ggtitle("CLDAP - Novas Vítimas")
```



- Uma grande quantidade de novas vítimas para 2020/4 em relação a quantidade de ataques/requisições