ntp_monlist

Rafilx

2022-06-01

```
##
## 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: viridisLite

##
## Attaching package: 'lubridate'

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

R Markdown

NT1. NTP: incidência de monlist

Resultados esperados: Historicamente os ataques DRDoS com NTP fazem uso do comando monlist. Analisar a porcentagem de monlist por período, para ver se ela se mantém consistentemente acima de 99% ou houve alteração

Resultados esperados:

- tabela/gráfico de barras com a %monlist por período

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

data_unfetch <-dbSendQuery(db, "
  SELECT *, CAST(CAST(year AS text) || CAST(period AS text) as integer) as year_period
    FROM NTP_ANALYSIS
")
data <- fetch(data_unfetch)

dbDisconnect(db)
```

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

- Calculado a porcentagem de "ntp_type" por período
  - Existem apenas dois tipos em "ntp_type" = {"Monlist", "Outros"}
  - Além disso o "ntp_type" é definido da seguinte forma

```
def get_ntp_type(ntp_payload):
  ntp_data_pattern = b'\x17\x00\x03\x2a\x00\x00\x00\x00'
  if ntp_data_pattern == ntp_payload:
    return "Monlist"
  return "Other"
```

- Agrupamento realizado:

```
data['tempo_final_cast'] = as.POSIXct(data[['tempo_final']], format = "%Y-%m-%d %H:%M:%S")
data['tempo_inicio_cast'] = as.POSIXct(data[['tempo_inicio']], format = "%Y-%m-%d %H:%M:%S")

data_grouped_period_ntp_type = data %>%
  mutate(year_period = as.factor(year_period)) %>%
  group_by(year_period, ntp_type) %>%
  summarise(sum_requests_per_attack = sum(requests_per_attack), number_of_attacks = n())
```

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

```
data_grouped_period_ntp_type_percentage = data_grouped_period_ntp_type %>%
  group_by(year_period) %>%
  summarise(ntp_type = ntp_type, number_of_attacks = number_of_attacks,
            sum_period_number_of_attacks = sum(number_of_attacks),
            sum_period_requests_per_attack = sum(sum_requests_per_attack),
            sum_requests_per_attack = sum_requests_per_attack) %>%
  mutate(number_of_attacks_percentage = (number_of_attacks / sum_period_number_of_attacks) * 100,
         number_of_requests_percentage = (sum_requests_per_attack / sum_period_requests_per_attack) * 1
```

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

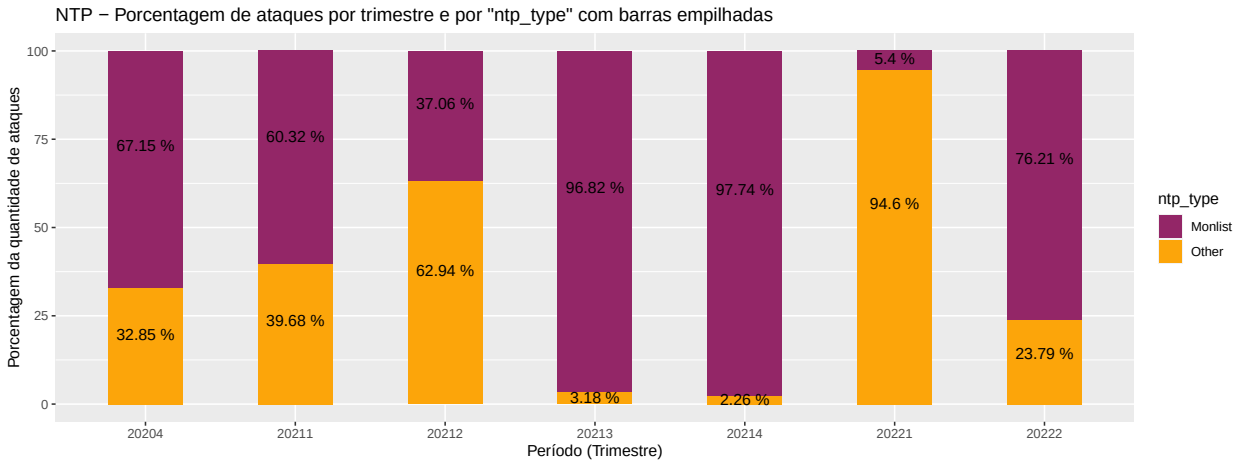
```
data_grouped_period_ntp_type_percentage %>%
  select(year_period, ntp_type, number_of_attacks_percentage, number_of_attacks) %>%
  print(n=14)
```

```
## # A tibble: 14 x 4
## # Groups:   year_period [7]
##    year_period ntp_type number_of_attacks_percentage number_of_attacks
##    <fct>       <chr>                           <dbl>             <int>
##  1 20204       Monlist                          67.1             20427
##  2 20204       Other                            32.9              9994
##  3 20211       Monlist                          60.3             11335
##  4 20211       Other                            39.7              7456
##  5 20212       Monlist                          37.1              1391
```

```
##  6 20212       Other                  62.9              2362
##  7 20213       Monlist                96.8             81451
##  8 20213       Other                   3.18             2677
##  9 20214       Monlist                97.7             79406
## 10 20214       Other                   2.26             1840
## 11 20221       Monlist                 5.40             1125
## 12 20221       Other                  94.6              19725
## 13 20222       Monlist                76.2              2226
## 14 20222       Other                  23.8               695
```

- Isso significa que no ultimo trimestre de 2020 ("year_period" = 20204) 67% dos ataques realizados foram monlist, e 32% outros tipos
- Gráfico de barras empilhadas apresentando a porcentagem da quantidade de ataques em cada "ntp_type" por período

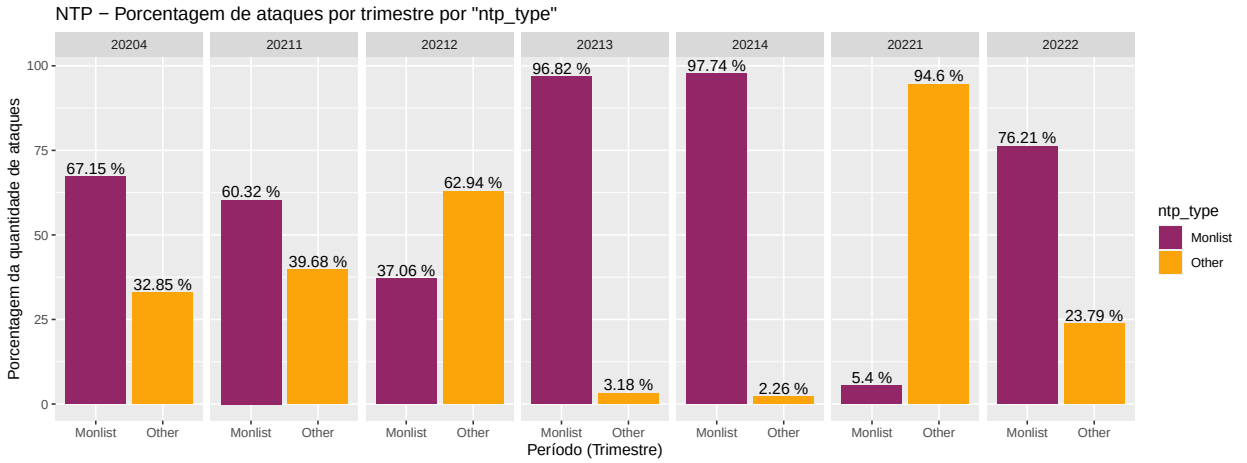
```
data_grouped_period_ntp_type_percentage %>%
  ggplot( aes(x=year_period, y=number_of_attacks_percentage, fill=ntp_type)) +
    geom_bar(stat="identity", width = 0.5) +
    geom_text(aes(label = paste(round(number_of_attacks_percentage, 2), "%")),
              position = position_stack(vjust = 0.6)) +
    scale_fill_viridis(discrete=TRUE, option="inferno", begin = 0.8, end = 0.4, direction = -1) +
    ylab("Porcentagem da quantidade de ataques") +
    xlab("Período (Trimestre)") +
    ggtitle("NTP - Porcentagem de ataques por trimestre e por \"ntp_type\" com barras empilhadas")
```



- Gráfico de barras empilhadas apresentando a porcentagem da quantidade de ataques em cada "ntp_type" por período

```
data_grouped_period_ntp_type_percentage %>%
  ggplot( aes(x=ntp_type, y=number_of_attacks_percentage, fill=ntp_type)) +
    #geom_bar(stat="identity", width = 0.5, prosition = "dodge") +
    geom_bar(stat="identity", position="dodge") +
    geom_text(aes(label = paste(round(number_of_attacks_percentage, 2), "%"),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE, option="inferno", begin = 0.8, end = 0.4, direction = -1) +
    facet_grid(~year_period) +
    ylab("Porcentagem da quantidade de ataques") +
```

```
    xlab("Período (Trimestre)") +
    ggtitle("NTP - Porcentagem de ataques por trimestre por \"ntp_type\"")
```



- Gráfico de barras empilhadas apresentando a porcentagem da quantidade de requisições em cada "ntp_type" por período

```
data_grouped_period_ntp_type_percentage %>%
  ggplot( aes(x=ntp_type, y=number_of_requests_percentage, fill=ntp_type)) +
    #geom_bar(stat="identity", width = 0.5, prosition = "dodge") +
    geom_bar(stat="identity", position="dodge") +
    geom_text(aes(label = paste(round(number_of_requests_percentage, 2), "%"),  vjust = -0.25)) +
    scale_fill_viridis(discrete=TRUE, option="inferno", begin = 0.8, end = 0.4, direction = -1) +
    facet_grid(~year_period) +
    ylab("Porcentagem da quantidade de requisições") +
    xlab("Período (Trimestre)") +
    ggtitle("NTP - Porcentagem de requisições por trimestre por \"ntp_type\"")
```