Introduction

Between 27th and 30th of January 2018, a remarkable number of DDoS attacks have targeted Dutch services of the Public sector. The NaWas (The Dutch National Scrubbing Center) has also closely monitored attacks activity during this period of time. The following report shows the results of the analysis of the DDoS attacks filtered via the NaWas during this period. This is not an analysis of the particular attacks aimed at the Banks or other targets as described in the news and media during this week.

This report is a condensed analysis of the attacks mitigated by NaWas during this period.

Definitions

A DDoS attack is described in this note as follows:

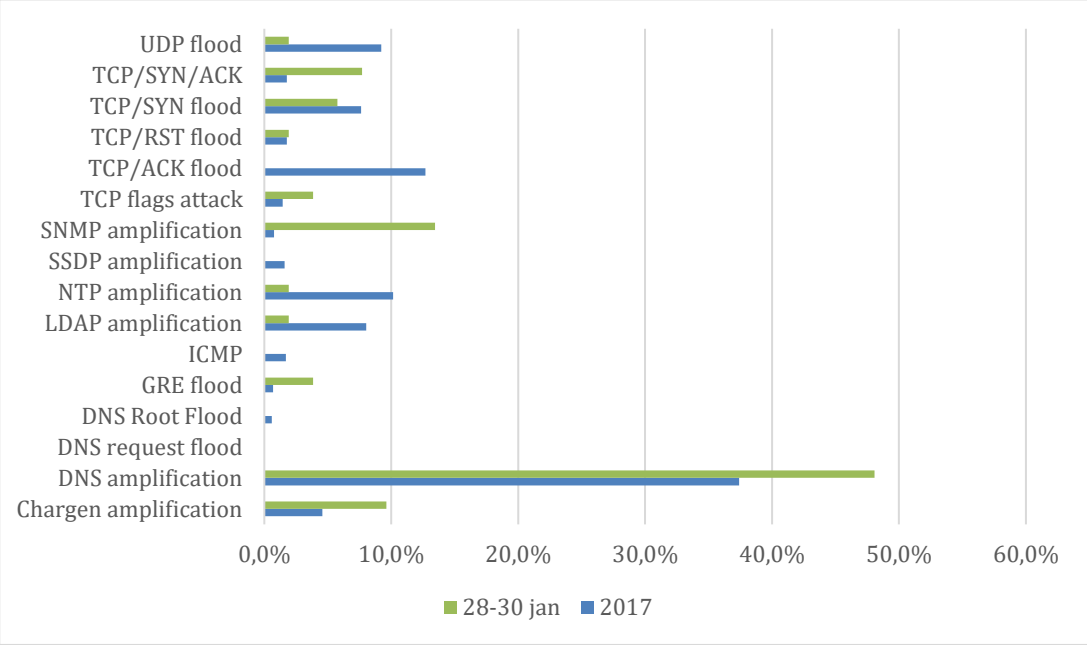
a) DDoS type - the way in which a DDoS is established and / or causes disruption of the target

b) DDoS bps - the maximum number of bits per second during an attack

c) DDoS pps - the maximum reached packets per second during an attack

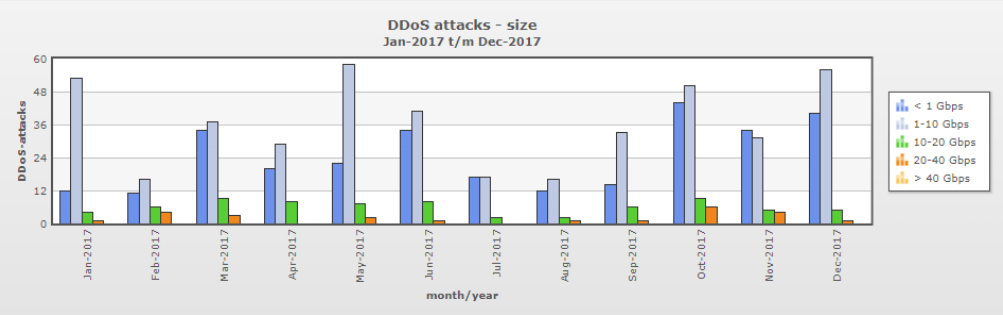
Even though “traffic size” has been repeatedly pinpointed as the most important weapon in a DDoS attack to eliminate a target, this is not correct. A DDoS attack with low DDoS bps (b) but with a high DDoS-pps (c) can also disable the service of a target.

DDoS-types

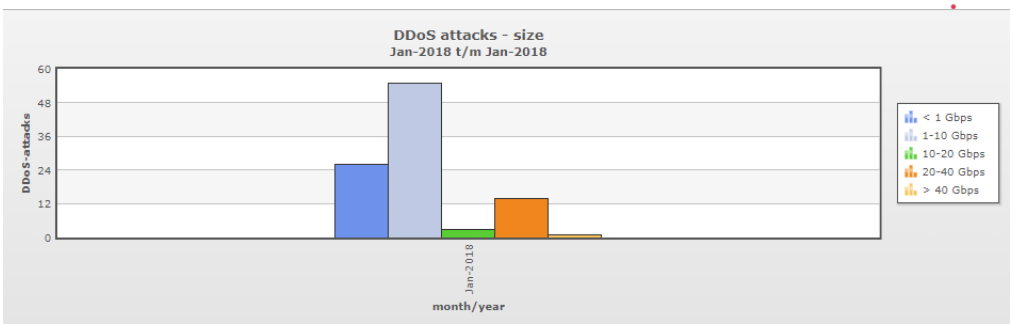


The graphic above shows the percentage type of recorded attacks. We notice a relative large percentage of DNS, SNMP and Chargen amplification attacks in the period 28-30 January compared to 2017.

DDoS-size



The graphic above shows the DDoS attack size mitigated by the NaWas in 2017.



The size of the DDoS attacks in January 2018 is shown above. Striking is the number of DDoS attacks of more than 40 Gbps. There were a number of 50 Gbps DDoS attacks.

DDoS-attacks in numbers

The number of DDoS attacks in January 2018 was not remarkably high for the NAWas. The months September and December of 2017 were busier months.

Conclusion

- The attacks monitored were not more complex than the usual type of attacks mitigated during the last year
- The number of 40-50Gbs attacks was obviously higher than in the same period last year
- The total of mitigated attacks in januari 2018 including the period of 28-30th of January was not unusual high compared with the medium number attacks mitigated by the NaWas

The NBIP would like to refer to the annual reporting of DDoS attacks as observed by the NBIP in 2017. This report does a broad analysis of the DDoS attacks, including more complex DDoS attacks as mitigated by NaWas during 2017. Please follow the publications of the NBIP.