NBIP DDoS data report

1st half year 2019

NBIP nationale beheersorganisatie internet providers

Colophon

The NBIP DDos data report: first half year 2019 is published by the Dutch National Internet Providers Management Organization.

Date of publication
September 2019, year 1

Chief editor
Octavia de Weerdt (NBIP)

Text
Gerald Schaapman (NBIP)

Editing
Stefan Penders (Splend)

Marketing and Design
Sam Zondervan (Splend)
Michiel Cazemier (Splend)

Format
This report is available in PDF format at nbip.nl

Contents

Preface

DDoS attacks are increasingly common. They are no longer the terrain of hardened cyber criminals, but can be easily bought by anyone with malicious intent. And favoured targets are no longer just major commercial companies, but banks and government agencies as well. With the pervasive threat of DDoS, an effective DDoS protection should be as common as fire insurance.

We are the Dutch National Internet Providers Management Organization, or the NBIP for short. We are a non-profit foundation, established by Dutch internet service providers back in 2002. With our members joining their resources and knowledge, we can provide a more effective defense against DDoS.

Beyond the protection of our members through our multi-vendor scrubbing center, we also attach great importance to the sharing of knowledge and expertise. Resulting in our bi-annual DDoS Data Reports, the fourth edition of which is currently lying before you. The news is not particularly pleasant: yet again we have to conclude that the number of attacks is on the rise, as is their intensity and sophistication.

But there is a silver lining. In the Netherlands, the national government has joined forces with banks, companies, research institutes and organizations such as the NBIP to combat DDoS more effectively. Similar projects are under way in Germany and the United Kingdom.

The NBIP believes in international cooperation. DDoS attacks do not stop at national borders and nor should DDoS protection. That is why we have expanded our anti-DDoS services to European internet service providers. With the same non-profit, cooperative mindset. Interested in the topic of DDoS or our anti-DDoS services? You will find more information on our website, or you can subscribe to our monthly English newsletter, ‘NBIP Notes’. For now, I wish you an enjoyable and informative read.

Octavia de Weerdt
General director NBIP
octavia@nbip.nl

Introduction

The Dutch National Internet Providers Management Organization (NBIP) is a non-profit foundation set up by Dutch internet service providers in 2002. As a response to the growing threat of DDoS attacks, the members of the foundation decided on the creation of a 'National Scrubbing Center against DDoS attacks' (NaWas). The scrubbing center is financed by the joint contributions of members and, like the NBIP, operates on a non-profit basis. Since 2018, NaWas services have also been made available to internet service providers outside the Netherlands.

DDoS attacks, short for Distributed Denial-of-Service attack, computers flood a website with access requests. The website is unable to cope with the high volume of traffic and as a result slows down significantly or goes offline.

The NaWas ensures that DDoS attacks are stopped before they can cause damage. By passing the data traffic to a given website through our scrubbing center, we ensure that only 'clean' access requests are passed through. The data we collect about incoming attacks gives us insight into the methods used by criminals and other malicious forces, as well as changing trends in the field of DDoS. In this report we provide you with an insight into the developments for the first half of 2019. We use technical terminology and assume some prior knowledge of DDoS.

Clearing House

An important development in the first half of 2019 is the participation of the NBIP in a newly-formed national anti-DDoS coalition. The Dutch national government partnered with banks, companies, research institutes and organizations such as the NBIP as a response to the rising danger of DDoS to the economy and online (public) services.

The NBIP is part of the special taskforce Clearing House, intended to share knowledge of DDos attacks and to gather incriminating data on perpetrators. The technical basis for the taskforce was laid by a joined research project carried out by the NBIP and the University Twente in the past few years. Together we developed a database to keep track of the characteristics of DDoS attacks. With the help of the taskforce Clearing House, the database can be further expanded and professionalized. In practice, this means that we can recognize attacks more quickly and therefore mitigate them better.

NaWas in Europe

Since 2018 our NaWas services have been open to European members. Together we stand strong against DDoS attacks. By exchanging knowledge with European internet service providers we not only further improve the NaWas but also stay one step ahead of DDoS attackers. Currently, the NaWas protects members in Germany, France and the United Kingdom.

Scrubbing clean DDoS data

DDoS attacks come in many shapes and sizes. This includes measures to protect organizations against DDoS attacks.

Most anti-DDoS measures are fairly rigorous. For example, "blackholing" blocks all traffic from a website. Although an extremely effective method, there is one major drawback: innocent visitors can no longer visit the website either. IP-blocking works in a similar way to blackholing, but focuses on regions. The server refuses access to the data traffic coming from a certain geographical location. More accurate than blackholing, but once again innocent visitors are blocked from accessing the website.

A centralized 'car wash' against DDoS attacks is a big step forward. Data traffic is passed through specialized equipment and - in the event of a DDoS attack - scrubbed clean. A scrubbing center stops DDoS attacks while allowing innocent data traffic to pass through freely, in contrast to blackholing and IP-blocking. The main disadvantage of a scrubbing center is the large capacity required to use it effectively. For individual internet service providers, the cost of maintaining that capacity is very high.

> A "scrubbing centre" stands for sophisticated DDoS mitigation

This is why the members of the NBIP agreed to set up the NaWas in 2014. Instead of individual service providers arranging their own protection, the participants of the NaWas work together. They share the costs of purchasing and maintaining the necessary equipment. And they share knowledge about DDoS attacks, so that the NaWas remains up to date.

How we collect our data

DDoS attacks are constantly changing in intensity, size and composition. New forms of DDoS attacks appear regularly. We collect data in order to effectively repel DDoS attacks, now and in the future. The data gathered from DDoS attacks on our members ends up in a registration system, which we use for purposes of research and analysis.

The members of the NaWas consist largely of internet service providers, but banks and insurance companies also participate. Not every member has to contend with DDoS attacks, and the intensity of the attacks varies from member to member. For security reasons, privacy considerations and contractual obligations towards our members, we do not make any statements about the number of attacks per member. Nor do we publish the names of the organizations affected.

The data in this report has been collected for the period of January to June 2019. The figures and analyses in this report have been compiled on the basis of data from 70 participants. These figures only show the DDoS attacks recorded by the NaWas, not the total amount of DDoS attacks on Dutch organizations. Given our large group of participants and the large number of attacks measured, we do however believe that our data is representative of broader trends in the field of DDoS attacks.

Representative for the Netherlands

Although the NaWas does not protect all companies and organisations in the Netherlands against DDoS attacks, the figures in the report are representative. This is partly due to the large number of .nl domain names that are protected by the NaWas: almost 50%

DDoS: numbers and statistics

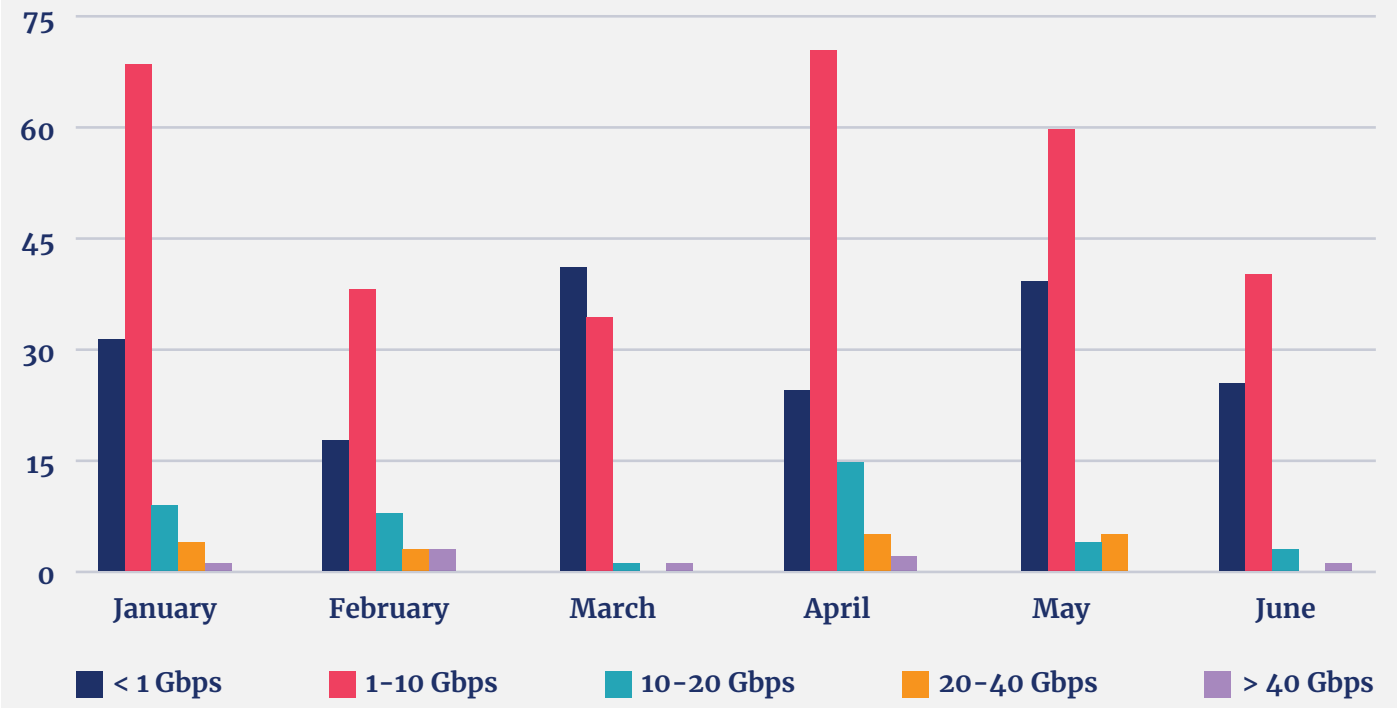
The number of DDoS attacks is on the rise, according to the figures for the first half of 2019. During the year 2018 we recorded 938 attacks, or about 2.6 attacks per day. By mid-2019, the counter had already reached 572, an average of 3.2 attacks per day. It is difficult to predict whether this upward trend will continue into the second half of 2019. However, based on data from 2017 and 2018, it is unlikely that the number of DDoS attacks will decrease in the coming months.

In addition to the number of attacks, the maximum size of attacks is also growing. The first half of 2019 saw a new record, with a DDoS attack peaking at 71 Gbps. The previous record dates from 2018, when we measured an attack of 68 Gbps. It should be noted that the majority of attacks are far more limited in size, less than 10Gbps. Malicious parties evidently find it more useful to employ attacks that are just big enough to make a server or service unreachable.

> A DDoS attack of 71 Gbps was the largest attack observed and mitigated in the first half of 2019

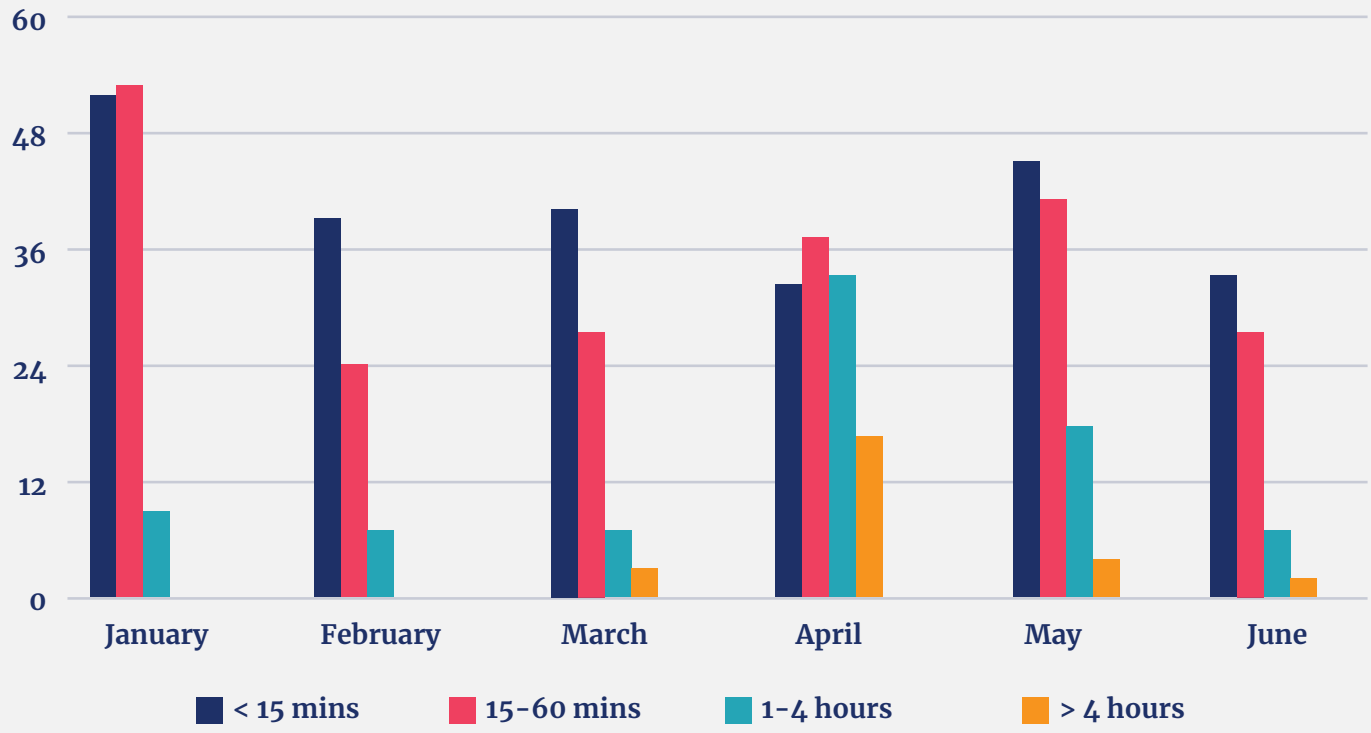
Finally, the duration of attacks is also on the rise. In 2019, we recorded 23 attacks lasting more than four hours. In contrast with 2018, when ‘only’ 22 such long-term attacks took place throughout the year.

DDoS attacks - size (January - June 2019)



Month (2019)	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	total
January	32	70	9	4	1	116
February	18	39	8	3	3	71
March	42	35	1	0	1	79
April	25	72	15	5	2	119
May	40	61	4	5	0	110
June	26	41	3	0	1	71
Total	**183**	**318**	**40**	**17**	**8**	**566**

DDoS attacks - duration (January - June 2019)



Month (2019)	< 15 mins	15-60 mins	1-4 hours	> 4 hours	total
January	53	54	9	0	116
February	40	24	7	0	71
March	41	28	7	3	79
April	33	38	34	14	119
May	46	42	18	4	110
June	34	28	7	2	71
Total	**247**	**214**	**82**	**23**	**566**

DDoS: types and trends

The first step in successfully mitigating a DDoS attack is timely recognition. Based on data from our participants, the NBIP analyses DDoS trends and collects information on the characteristics of different types of DDoS attacks. Below we share the most important insights for the first half of 2019.

DDoS types

The NBIP keeps track of a top ten of the most common DDoS attacks. During the first half of 2019, DNS amplification proved to be the most common variant. By contrast, the LDAP amplification proved most common in 2018, now finishing second. A striking phenomenon is that only 8% of all DDoS attacks still use NTP amplification. This puts NTP amplification in sixth place. In 2018, 15% of all DDoS attacks used NTP amplification. Although the exact cause of this decrease remains a point of contention, it is likely that the improved security of many NTP services plays a major role.

An eye-catching newcomer to the top ten is the so-called GRE flood. We consider it likely that the emergence of GRE floods is related to the use of GRE tunnels in network nodes. These are a new target for malicious parties. An additional advantage from the point of view of a DDoS attacker is that GRE traffic is encrypted. Because the data cannot be viewed in terms of content, it is more difficult to recognize a DDoS attack in time.

An additional surprise was the so-called DNS water torture attack, which we registered at the beginning of this year. This macabre name refers to an attack on DNS services in which targeted DNS queries are made in the form of '<prefix>.<victim domain>'. In the <prefix>, a random string of sixteen or more characters is included that is constantly randomized. As a result, the authoritative name server must be queried, which then receives so many requests that the name server goes down. If this takes long enough, the domains disappear from the DNS services cache. It is no longer possible to translate to IP, with the result that the domains of the authoritative name server are inaccessible. By clever use of filters, the NaWas was one step ahead of this form of DDoS, allowing us to mitigate the attacks.

Trends

Two major trends in the first half of 2019 were briefly mentioned above: both the number of attacks in general and their maximum size is growing. But the number of large attacks specifically is also increasing. Although the majority of DDoS attacks remain below the 10Gbps limit, there is nevertheless an upward trend in the number of attacks above that limit. Incidentally, this is not a completely new development: in 2018 we also saw a steady increase in the number of large attacks. Nevertheless, these disturbing figures once again point to the growing danger of DDoS.

Conclusions

As noted, the figures in this report only refer to the first half of 2019. The conclusions that can be drawn on the basis of these data are therefore limited. Nevertheless, a number of trends can be identified that are in line with the developments of recent years.

In our annual report for 2018, we had already concluded that the duration, size and complexity of attacks is increasing. These conclusions can be extended to the first half of 2019. The total number of attacks is increasing. On average, more than three attacks occur every day. The attacks have also grown in duration. Attacks of more than four hours are becoming more common. Size is increasing as well, with more and more large attacks of more than 10 Gbps. And although the majority of DDoS attacks can be categorized as 'small', their danger should not be underestimated: even a small attack can take a server or service off the air.

A second important conclusion is that DDoS attacks are getting smarter and smarter. We see that criminal parties react quickly to improvements in security (such as the NTP services) and opt for new attack routes. Weak spots, such as GRE tunnels, can easily be exploited. Clever new DDoS methods, such as GRE floods and DNS water torture, are difficult (but not impossible) to repel. This requires a proactive approach to DDoS protection, one which can react quickly to new types of attacks.

Both developments show that the threat of DDoS is more topical than ever. For some years now, we have seen an upward trend in the number, duration and impact of DDoS attacks. The first figures for 2019 suggest that this is becoming a long-term trend. The emergence of new types of DDoS attacks furthermore point to the need for constant vigilance and innovative research. Reason enough for the NBIP to continue its efforts to protect its members.

NBIP nationale beheersorganisatie internet providers

For more information:

www.nbip.nl