DDoS data report 2020

Attacks in 2020: more powerful, more complex and lasting longer

NBIP nationale beheersorganisatie internet providers

Colophon

The NBIP DDoS data report 2020 is a publication of Stichting Nationale Beheersorganisatie Internet Providers.

Publication date
April 2021, year 4

Editor-in-chief
Octavia de Weerdt (NBIP)

Editor
Gerald Schaapman (NBIP)

Contributions
NaWas operationeel team

Final editing
Marc Boersma (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

Vorm
This report was created in PDF format

Summary
In 2020, DDoS attacks continue to be a persistent problem that can severely disrupt social and economic life. In 2020, DDoS attacks were more powerful, more complex, and lasted longer compared to previous years. Deployment of NaWas is required more than ever to continue to face DDoS attacks.

Table of contents

Summary

DDoS attacks are still a major social problem. Because they are able to bring systems down, they disrupt economic life for short periods of time. As a result of mass home working due to the outbreak of corona, we are even more dependent than before on digital systems running in the cloud. This makes us even more vulnerable to DDoS attacks.

In 2020, we saw a number of notable developments. DDoS attacks became more complex, more powerful, and most importantly, lasted a lot longer compared to the attacks in 2019.

In the third quarter, NBIP observed 307 attacks. On average, these were four attacks per day. The strongest attack had a power of 200 Gbps. In total, the NaWas recorded 38 attacks that lasted longer than four hours. By comparison, in the first quarter we saw 11 attacks lasting longer than four hours. In the third quarter, there were 16 attacks that lasted longer than four hours, and in the fourth quarter of 2020, there were 21. The most common attacks were DNS Amplification and LDAP Amplification. They were particularly powerful and largely targeted ISPs and large enterprises in Europe.

In the last three months of 2020, we saw an increase in more technically complex attacks: so-called carpet bombing. In August, powerful attacks began on the infrastructures of ISPs that continued. These were extremely powerful attacks up to a capacity of 167 Gbit per second and lasted longer than four hours. In the last four months we also saw DDoS attacks after working hours and the average number of attacks was four per day.

This trend will continue this year as well. In the first quarter of 2021, we have already observed more attacks than in all of 2020, with the most powerful attack reaching 300 Gbps.

Download infographic

Foreword

This is the already the foruth annual review with DDoS data collected in 2020 by the Nationale DDoS Wasstraat (NaWas) of the Stichting Nationale Beheersorganisatie Internet Providers (NBIP). This report provides an overview of all the figures and trends surrounding DDoS attacks on the Dutch part of the internet. In total, NaWas now protects 2.5 million .nl domain names.

The NaWas

The collective DDoS scrubbing center called 'NaWas' (loosely derived from the Dutch word for 'washing') has been operational since 2014 and automatically mitigates DDoS attacks for connected participants 24/7. By jointly procuring capacity, technology and knowledge and expertise, a highly effective mitigation of DDoS attacks is possible. The NaWas 'washes' the DDoS traffic clean and only sends clean traffic back to the NaWas participant via a separate VLAN. In this way, systems and services remain available and the DDoS attack is rendered harmless.

The NBIP and this report

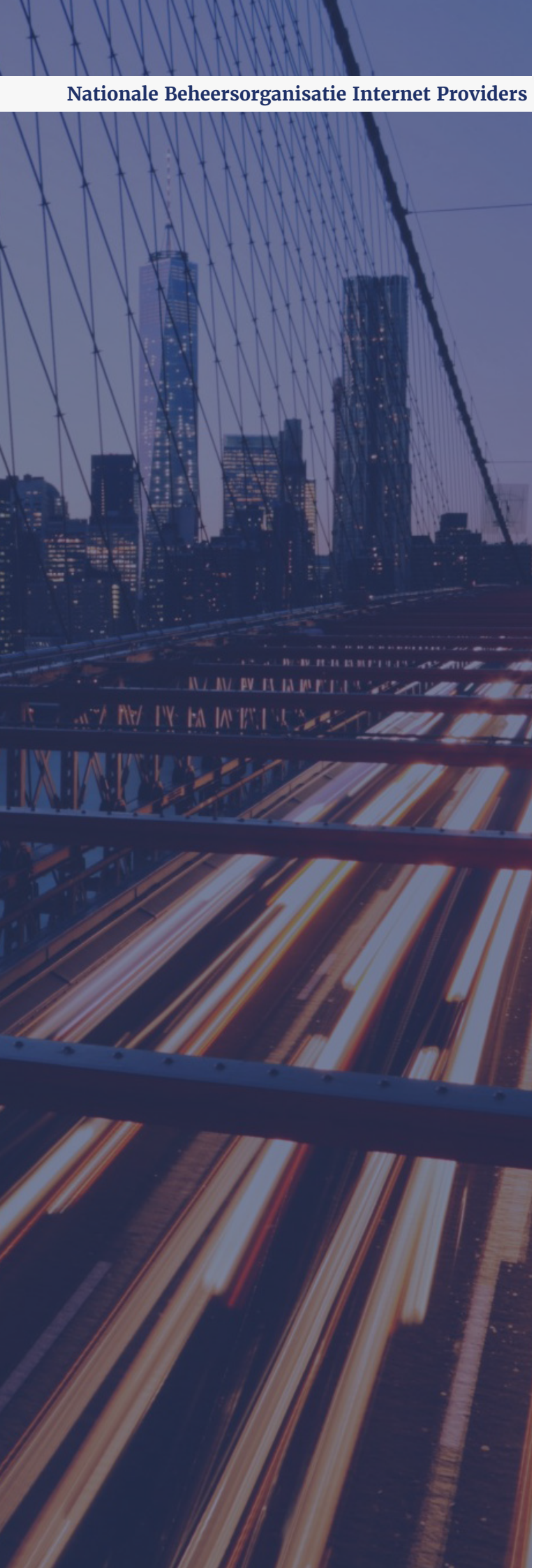
IIn 2017 the NBIP started to publish (semi) annual reports with extensive information about DDoS attacks. The reports provide an overview of the number of DDoS attacks, the magnitude of the attacks, the duration of the attacks, the types of attacks and the trends observed in the NaWas. Incidentally, NBIP does much more than just clean up malicious Internet traffic: together with industry peers, we facilitate the detection and combating of online abuse such as malware, spam, unlawful content and child abuse material. The NBIP also executes wiretapping requests by Dutch authorities so providers can comply with the Dutch Telecommunications Act, which requires them to ensure that their services can be tapped.

With this DDoS Data Report 2020, we want to share as much knowledge and background information as possible about DDoS attacks with our participants, stakeholders and interested parties. There is a lot of in-depth knowledge on this subject within our organization. In order to deal with the increasing number of DDoS attacks in the coming years, a joint approach from all stakeholders is necessary. DDoS attacks are now a common and permanent threat to a secure and stable Internet and this is not expected to change. With this report, NBIP shares knowledge about DDoS attacks and related risks and methods for prevention and mitigation. This report provides insight into the trends and developments of the past year.

Intensive collaboration provides new insights and opportunities

As more and more organizations and sectors are aware that DDoS attacks are a permanent threat, more intensive collaborations are also emerging to combat them. For example, in 2018 a start was made with the anti-DDoS coalition, a collaboration between now 18 organizations including telecom providers, financial institutions, government organizations, police and the digital sector.

Through the DDoS clearinghouse, for which a proof of concept is currently running, collaborating parties share relevant information about DDoS attacks. They are also conducting real-life simulations, in which organizations carry out DDoS attacks on each other with the aim of increasing their knowledge and experience in this area. In this way, they learn



how to recognize and mitigate an attack and how employees of organizations should respond to it.

The NaWas in 2020

Due to the corona crisis, we experienced an exceptional year in 2020. The attacks last year lasted a lot longer - sometimes up to four hours in a row - and were a lot more powerful and complex in their design. We can also see this in the first quarter of 2021, in which we have already measured more attacks than in the whole of 2020. These developments show that NBIP should not remain idle and develop a strong policy in the years to come to counter the DDoS attacks with NaWas.

Despite the increase in the number, duration and complexity of DDoS attacks in the past year, we in the Netherlands are not performing that badly compared to other countries. With the NaWas, we are very well able to effectively counter even very powerful and complex DDoS attacks. We have been able to limit the economic damage because companies and home workers have been able to continue working without interruption.

The NaWas was founded with the idea ‘stronger together’. At the moment of writing, this mentality is needed more than ever, and we will continue to carry out our mission with great dedication.

With kind regards,

Octavia de Weerdt

Managing Director NBIP

1. Introduction

DDoS attacks in the news

There was no shortage of news about DDoS attacks in 2020. Citizens, consumers, students, pupils and businesses were affected by DDoS attacks in different ways in 2020. A small sample of the news from the past year:

- In February, the Dutch Tweede Kamer debated whether the law offers sufficient possibilities to combat online ordering of DDoS attacks.
- In March and again in April, a widely used online learning environment for secondary schools was overloaded by DDoS attacks for a long time.
- In October, five servers driving a botnet were taken offline in Amsterdam.
- In December 2020, Radboud University Nijmegen had to cancel an exam due to repeated DDoS attacks.

Because no one is immune to DDoS attacks, it is necessary to take precautions. At the NaWas, we have been doing just that as a non-profit collective since 2014. Since then, the NaWas has neutralized many thousands of DDoS attacks. We also saw the increase in the number of DDoS attacks in the first quarter of 2021, where there were already more than DDoS attacks than in the year 2020.

Annual reporting

The NaWas records many hundreds of DDoS attacks each year, providing insight into how DDoS attacks are evolving. NBIP shares these insights with the goal of making the Internet safer for everyone. That's why NBIP publishes the DDoS Data report every year. We see trends emerging or may find that some developments are not trends at all. It will hopefully provide the reader with some valuable insights into how DDoS attacks work, how they evolve and which precautions could be made.

This report was written with a reader with some basic knowledge about DDoS attacks and how they work in mind. Those who are still unfamiliar with certain terms can consult the appendix of this report.

2. DDoS - the basics

In order to understand the impact of a DDoS attack, it is necessary to know exactly how such an attack works, what can happen during and after a DDoS attack and how to counteract it.

How does a DDoS attack work?

What's a DDoS attack? DDoS stands for Distributed Denial of Service. To carry out a DDoS attack, an attacker has several options. The most common is to infect a large number of computers or other Internet-connected devices.

This is done for example with malware or via e-mail attachments. In this way a botnet, a network of infected devices, is created. Subsequently, this network commands data to the target's server for the purpose of overloading that server. If the server can no longer handle the traffic, and thus users can no longer access the servers, the attack is successful.

However, the most common way to set up a DDoS attack is not via botnets, but via so-called 'amplification'. In this case, servers are not infected, but they are 'abused' to set up a DDoS attack. In addition, a DDoS attack does not always have to be aimed at overloading servers, but an attempt can be made overload the bandwidth a server has available for incoming traffic, which means the server is no longer accessible.

Anyone who wants to carry out a DDoS attack does not need to have any technical knowledge. DDoS attacks can be purchased on special websites (there are thousands of them), and not just on the darkweb. It is also possible to setup an attack yourself with relatively little knowledge. Manuals for setting up your own botnet are easy to find and knowledge for attacks with other tactics is also readily available.

> Those who want to carry out a DDoS attack do not need to have technical knowledge.

Why are DDoS attacks so popular?

A DDoS attack is still the most obvious way to disrupt a website or online services. But there is more to it than that. There are some factors that maintain the convenience and attractiveness of this type of attack.

Firstly, the increasing number of DDoS services provided from the cloud makes it easier to launch an attack. Hosting is cheap and so are ever higher volumes of bandwidth. Buying malicious services on the Internet is therefore becoming increasingly simple and affordable. These services are purchased via so-called 'stressers' or 'booters'. The vast majority of DDoS attacks are conducted through such intermediaries.

Booters also benefit from attractive business models aimed at quick profits. Attacks purchased via booters are not even very advanced, and that's not in the interests of the booter service provider. Because they want to

make money as quickly as possible with as little effort as possible, booters disappear just as quickly as they appeared.

Because attacks are so easy to purchase, it also means that more people with less technical knowledge can carry out a DDoS attack. And because it is easy to cause disruption with little effort, or to evade your homework, a DDoS attack is a popular crime.

In addition, the Internet of Things (IoT) is a development that should not be underestimated, as it's maintaining the frequency and simplicity of DDoS attacks. More and more devices are connected to the internet. From baby cameras to toasters: many have wifi and in the future there will only be more. These are often devices with poor (or no) standard security. And so IoT devices are an easy target to serve as pawns in a botnet. Gartner estimates that more than 20 billion such devices will circulate in the year 2020.

Consequences of a DDoS attack

The consequences of a DDoS attack are diverse. From minor irritation to major disruptions, it's all possible. One person can be bothered by an attack (his or her personal blog, for example, is down), or a large part of the population (banking via Internet does not work).

In 2018, NBIP and Stichting Internet Domeinregistratie Nederland (SIDN) studied the financial damages a DDoS attack causes. The report 'Impact of DDoS attacks in the Netherlands' shows that the economic impact is enormous: the companies and organisations investigated by NBIP and SIDN missed out on 425 million euros in 2018. If you involve the entirety of businesses in the Netherlands, the damage is at least one billion euros.

This research also showed that there is a lot of collateral damage. Especially if a company has a shared hosting solution with an ISP, where several websites are hosted on one server. For example, a website can fall to a DDoS attack, while it is not the target, simply because the attack is aimed at another target on the same server.

Methods of DDoS mitigation

Various types of measures can be taken to prevent DDoS attacks. These range from extreme and rigorous to refined and subtle. "Blackholing" or channelling of traffic is a rather extreme method of DDoS mitigation. In order to avert a DDoS attack, no more traffic is allowed. Because of this it is not possible for anyone to visit the website.

A somewhat more subtle form of mitigation is geographical IP blocking, where all traffic outside a certain geographical location is blocked in full. This is a reasonably effective way, but also rigorous. After all, many visitors are still excluded.

The concept of a "scrubbing center" is currently one of the most sophisticated and intelligent ways of mitigation. This involves malicious traffic passing through anti-DDoS equipment, after which the traffic is sent back 'clean' (scrubbing).

3. Research method

This chapter discusses the research method. Which data collection methods were used, which data were analysed, and why were certain research choices made?

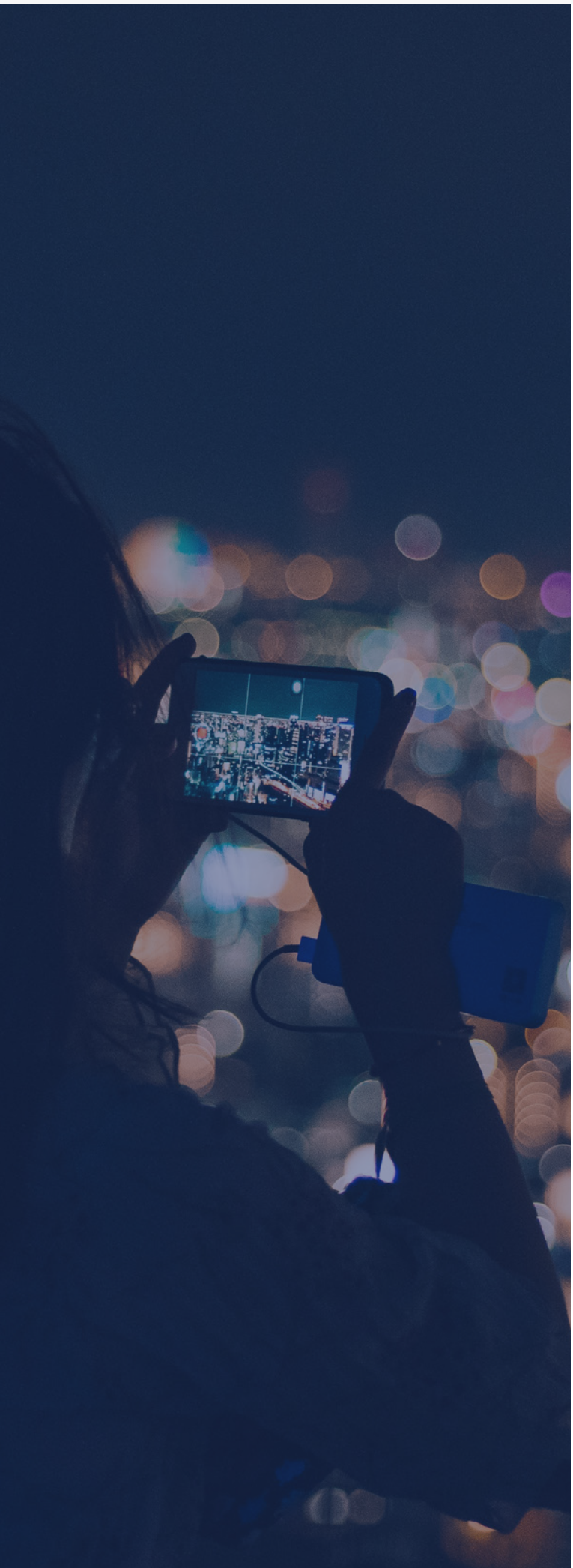
Data collection

In the previous chapter, the principle of a ‘scrubbing center’ like the NaWas, was explained. NBIP has a recording system that stores all types of DDoS attacks that have occurred against NaWas participants. The registration of a type of DDoS attack in that recording system is procedurally documented within the operational team of the NaWas. Data was then selected from this registration system for reporting purposes.

The data originated from attacks on participants of the NaWas. It should be noted that not every participant had to deal with a DDoS attack. Due to security and privacy measures for these participants and NBIP’s contractual obligation towards its participants, it has not been disclosed how often a particular ISP has been attacked or even which ones have been attacked. Data from participants in the NaWas was analysed for this study.

For this study, data from participants in the NaWas was analyzed. At the end of 2020, this involved data from 97 members. At the end of 2020, the NaWas had 97 members.

These participants consist largely of Internet service providers (ISPs). In this study, ISP refers to a company or organisation that offers online services and/or access to the Internet to its customers. In the case of NaWas participants, these are mainly companies that offer cloud and hosting services. There are about 1500 of such companies in the Netherlands (as researched by The METISfiles).



The NaWas has a large share in the Dutch Internet sector. The impact study with SIDN shows that NBIP protects 43% of all .nl domains against DDoS attacks. This means that at least 2.5 million domains can count on DDoS mitigation from NaWas. The figures in this report will never give a complete picture of the situation in the Netherlands, but they do offer a highly representative insight.

Of course, participants of the NaWas are not limited to ISPs. There are also a number of large organisations that participate, such as banks and insurers. Participants can be small as well as large.

Accountability

For this study, it was decided to measure the size of the attacks in Gbps (gigabit per second). An explanation of the terms and types of attacks is included in an appendix. This report is based on readers with some knowledge of the facts. In a few graphs it was decided to create a top 10 instead of a complete overview, for the sake of clarification and to make the results as clear as possible for the reader.

4. Research results

In this report we present the numbers, size and duration of DDoS attacks in 2020. We also pay attention to:

- Types of DDoS attacks
- Notable DDoS attacks in 2020
- New types of DDoS attacks in 2020
- Trends that can be derived from the data

4.1 Number of DDoS Attacks

In the year 2020, as many as 1,610 DDoS attacks were recorded by the NaWas.

Converted, this is 4.4 DDoS attacks per day. In 2019, 919 DDoS attacks were recorded. This represents a whopping 75% increase over 2019, based on absolute numbers due to an increase of NaWas participants.

We saw the most attacks in the month of November. In that month, the NaWas processed 213 attacks. December 2020 was the second busiest month with 190 DDoS attacks.

June, July and August 2020 were relatively the quietest with 94, 87 and 67 attacks respectively. After the summer, the number of attacks increased again: in September and November, there were 153 and 137 attacks, respectively. In January of 2020, 133 attacks were recorded, followed by 118 attacks in February. In March, we saw another increase in the number of attacks: as many as 158 were registered this month. In April and May, the numbers decreased slightly with 121 and 94 attacks registered respectively.

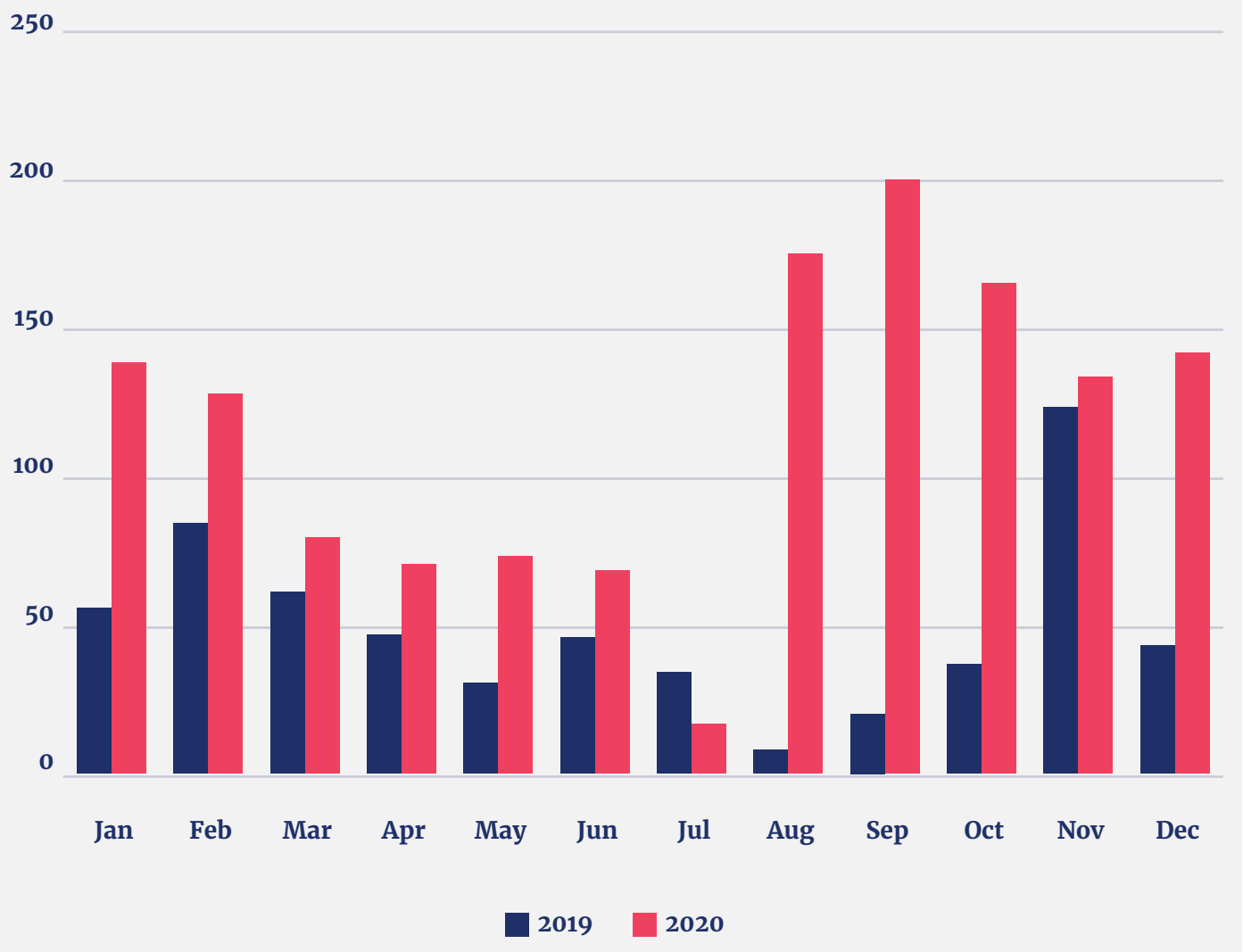
4.2 Size of DDoS attacks

We express the size of a DDoS attack in gigabits per second, or Gbps. In the graph below, the number of DDoS attacks is divided into five categories: smaller than 1 Gbps, between 1-10 Gbps, between 10-20 Gbps, between 20-40 Gbps and larger than 40 Gbps. To also provide insight into the development of DDoS attacks in recent years, we have also included the tables for 2019.

2020	Quarter 1	Quarter 2	Quarter 3	Quarter 4
< 1 Gbps	89	116	120	182
1 - 10 Gbps	265	201	141	257
10 - 20 Gbps	33	15	21	56
20 - 40 Gbps	11	11	6	22
> 40 Gbps	11	11	19	23

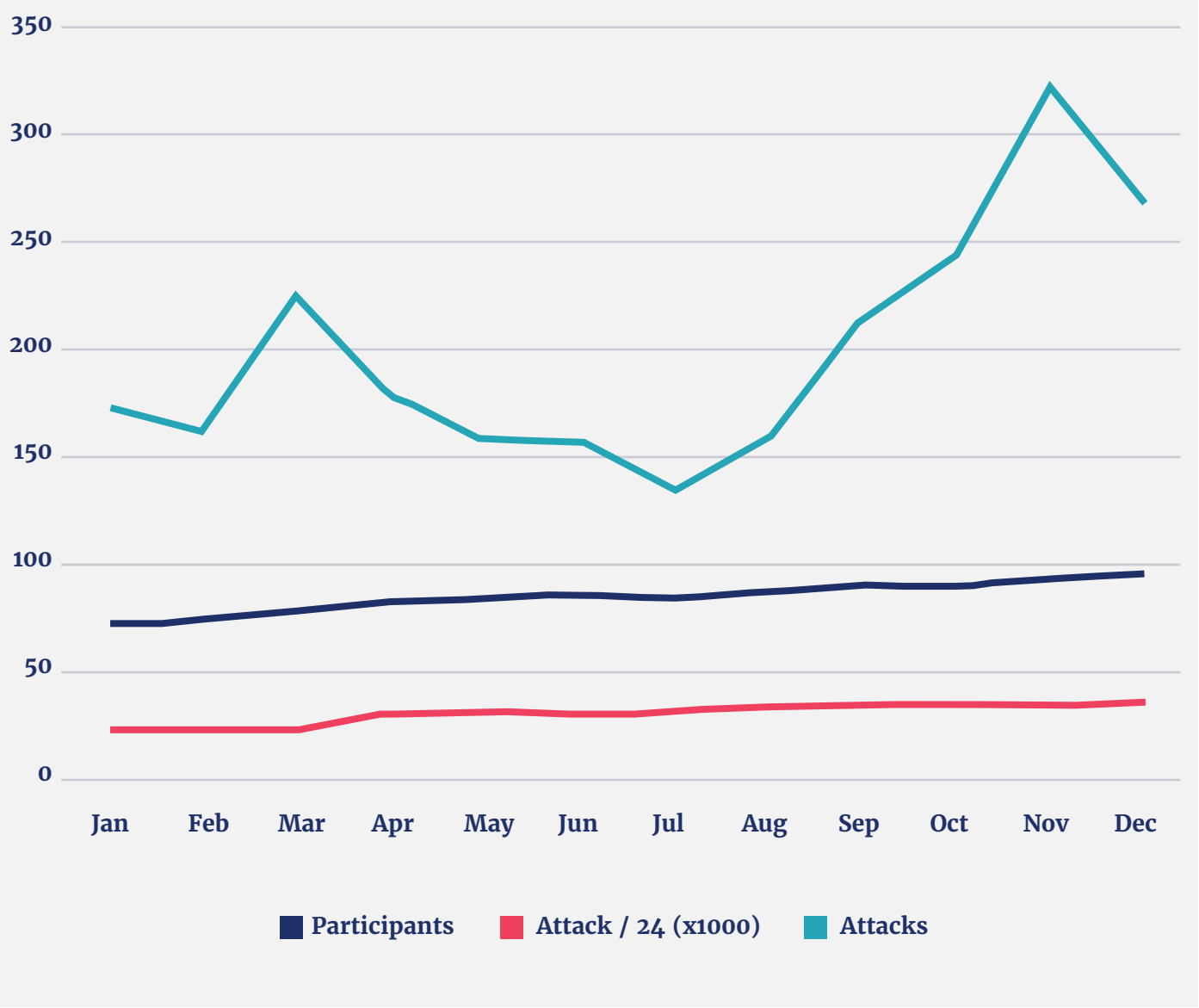
2019	Quarter 1	Quarter 2	Quarter 3	Quarter 4
< 1 Gbps	92	91	43	47
1 - 10 Gbps	144	174	91	140
10 - 20 Gbps	18	22	5	16
20 - 40 Gbps	7	10	2	6
> 40 Gbps	5	3	0	3

Max Gbps per month



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Deelnemers	74	77	80	84	86	87	86	89	91	91	94	97
Aantal / 24	24,5	24,7	24,7	31,9	32,4	32,5	32,5	34,3	34,7	34,7	34,8	34,9
(x1000)	54	8	96	69	49	81	14	44	25	25	38	15
Aanvallen	175	164	228	181	160	159	138	161	217	246	324	269

Participants versus attacks and protected prefixes



Compared to 2019, we see a clear increase in the number of attacks smaller than 1 Gbps. In the third quarter of 2020, we saw 120 attacks with this power, compared to 43 attacks in 2019. The same was true for the fourth quarter of 2020. In the fourth quarter of 2020, 182 attacks with a strength of 1 Gbps were recorded. In the fourth quarter of 2019, there were 47.

For attacks with a power between 1 and 10 Gbps, we also see a clear increase in 2020. In the fourth quarter of 200, there were 257, compared to 140 in the same period of 2019. This increase was also seen in the first quarter of 2020. At that time, there were 265 attacks with this strength. In 2019, there were 144 in the first quarter.

Measured in absolute numbers, there were not as many attacks with a power between 10 and 20 Gbps. In the first quarter, there were 33. Looking at the first quarter of 2019, there were 18. In the last quarter of 2020, there were 56, compared to 16 in the same period in 2019.

For attacks with a power between 20 and 40 Gbps, we saw increase in 2020 compared to the previous year. In the third quarter of 2020, there were 19, while in 2019 we saw only two attacks of this kind. The fourth quarter of 2020 saw 23 attacks with this power, compared to six attacks in 2019.

Attacks larger than 40 Gbps also saw a significant increase in 2020 compared to 2019. In the last quarter, the NaWas recorded 23 attacks, compared to three attacks in 2019. In the third quarter of 2020, there were 19 compared to zero in the third quarter of 2019.

4.3 Duration of DDoS attacks

With respect to the maximum duration of a DDoS attack than we see a clear increase compared to previous years. In 2018, the maximum duration of a DDoS attack was 1 day and 5 hours. The following year we saw an increase in the total duration to 1 day and 12 minutes. A clear increase can be seen in 2020: the maximum duration of a DDoS attack lasts a whopping 20 days and 6 hours.

If we look at the duration of DDoS attacks over the different months of 2020, we see a clear peak in the months of September and October. In September the longest attack lasted no less than 20 days and 6 hours. For the month of October, this duration is 13 days and 14 hours. In the other months of that year, DDoS attacks last between one and seven days.

4.4 Types of DDoS attacks

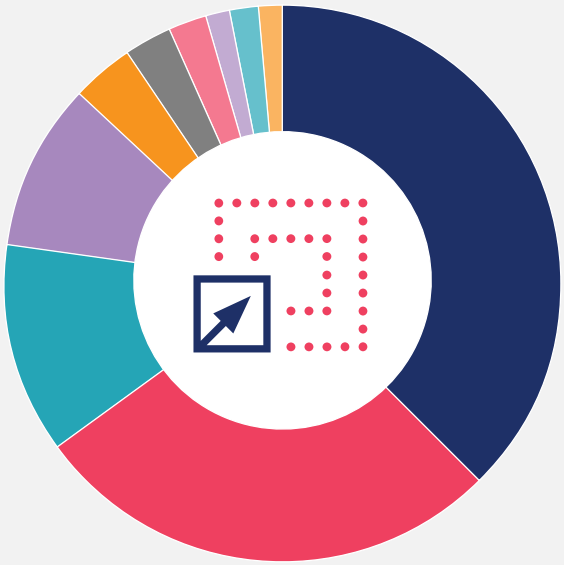
In 2019, we observed 49 types of DDoS attacks. In 2020, this number dropped to 34 types of attacks. In this regard, the NBIP distinguishes between three DDoS main types with several subtypes under them: TCP flood, UDP flood and UDP amplification.

Compared to the year 2019, in 2020 we see an increase in the attack type UDP amplification and a decrease in the TCP flood type. These percentages were still 50% and 32% respectively in 2019, where in 2020 it was 71% and 12%. Compared to the figures of 2018 and 2019, we see a clear decreasing trend of TCP flood in 2020. Looking at UDP amplification we see a clear upward trend in 2020 from the years 2018. The percentage of UDP flood has remained more or less stable in the last three years. Compared to 2019, the top three most common types of DDoS attacks have remained the same in 2020: DNS amplification, LDAP amplification and UDP flood. The share of DNS amplification has almost doubled 2020 compared to 2019 (16.6%) with a percentage of 32.12%.

For LDAP amplification, we see a significant increase in 2020 to 23.57%, compared to 13.8% in 2019. In third place of most common type of DDoS attacks in 2020 is UDP flood with 10.45%. In 2019, this percentage was 10.3%, which means that the share of this type of attack has remained almost the same. In the fourth place with most common type of DDoS attacks is NTP amplifcation with 8.38%. In 2019 this percentage was 8.6% and this means that the share is about the same as in 2020.

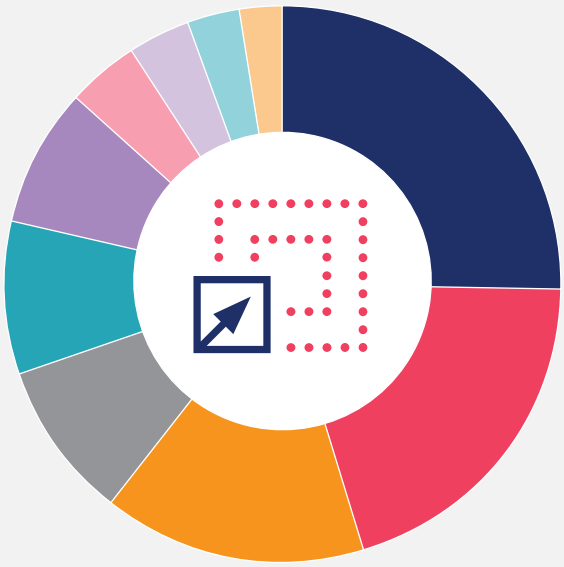
Jaar	< 15 min	15-60 min	1-4 uur	> 4 uur
2017	37,4%	41,2%	18,3%	3,4%
2018	34,4%	45,9%	16,6%	3,1%
2019	44,1%	41,2%	11,6%	3,2%
2020	47,40%	40,20	9%	3,30

DDoS-type (top 10) 2020



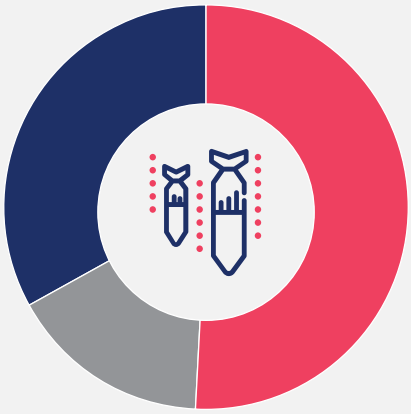
- 37,6% DNS amplification
- 27,6% LDAP amplification
- 12,2% UDP flood
- 9,8% NTP amplification
- 3,6% TCP/SYN flood
- 2,6% TCP/ACK flood
- 2,2% UDP memcached
- 1,6% SNMP amplification
- 1,5% TCP/SYN/ACK
- 1,3% WS-Discovery amplification

DDoS-type (top 10) 2019



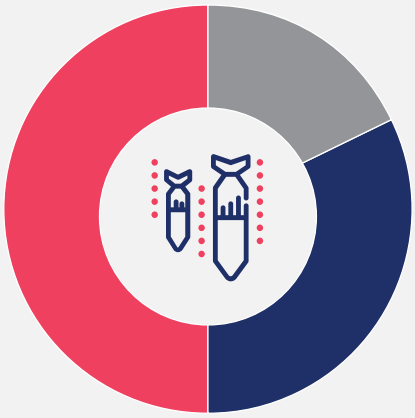
- 25,3% DNS amplification
- 20,2% LDAP amplification
- 15,2% TCP/SYN flood
- 9,2% TCP/ACK flood
- 8,7% UDP flood
- 8,2% NTP amplification
- 4,2% UDP flood 2
- 3,5% GRE flood
- 3,0% TCP/RST flood
- 2,4% TCP/ACK flood; flags AP

DDoS type main group distribution 2018



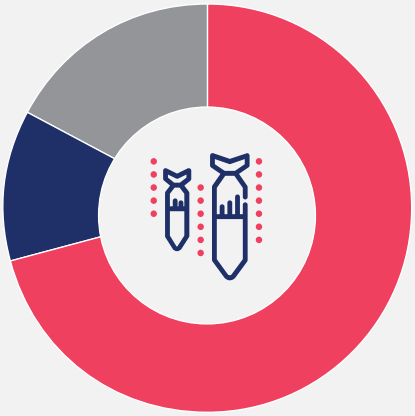
33% TCP flood
51% UDP amplification
16% UDP flood

DDoS type main group distribution 2019

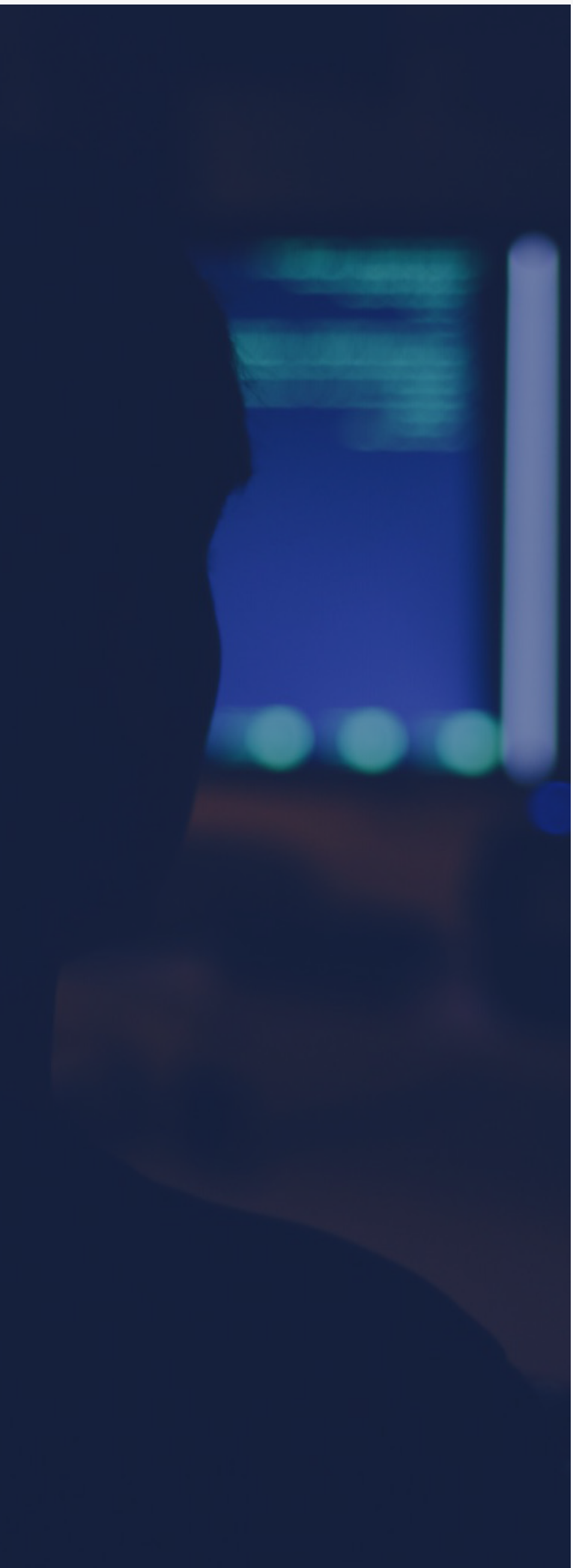


32% TCP flood
50% UDP amplification
18% UDP flood

DDoS type main group distribution 2020



12% TCP flood
71% UDP amplification
17% UDP flood



4.5 Multi-vector attacks

Multivector attacks continue to be popular in 2020. This involves multiple attack types being bundled together. It can involve both a "simple", heavy attack type accompanied by a small, advanced type of attack but also two "simple" attacks that are relatively easy to set up. The most complex attack observed in the NaWas used as many as 30 different vectors, although in the aggregate this is an exception. Attacks with 11, 12 or 13 vectors were also observed with some regularity in 2020.

4.6 Notable DDoS attacks

DNS water torture involves attacks on non-existent subdomains of an existing domain name. These subdomains are created randomly and automatically by the attacker. Due to the querying of random subdomains, the highest authority server cannot fulfill these requests because this information is not cached. The result is that the authority server goes down.

4.7 Newly observed DDoS attacks

Cybercriminals are constantly looking for new protocols and/or services that they can deploy for DDoS attacks. In particular, these are protocols and/or service that can provide a multiplier. In 2020, the protocols Microsoft Remote Desktop protocol, 4talk amplification and Quote of the Day (QOTD) were used.

5. Trends

In 2020, we see some clear trends compared to previous years. First, we see a clear increase in the number of attacks. That's 1,610 in 2020 compared to 919 and 928 in 2019 and 2018, respectively. Also, DDoS attacks are becoming more powerful: 200 Gbps in 2020, while in the two previous years they were 124 Gbps (2019) and 68 Gbps (2018). Looking at the duration of the attacks, an upward trend is also visible: the longest attack lasted a whopping 20 days and 6 hours in 2020. In 2018 (1 day and 4 hours) and 2019 (1 day and 12 hours), these attacks lasted a lot shorter. With a power of 200 Gbps, the largest attack took place November 2020. In 2019, the largest attack was 124 Gbps. The smallest attack of 18.1 Gbps was seen in July 2019.

In 2020, 763 attacks were observed to last less than 20 minutes. In 2019, that number was 405 attacks. The number of attacks that lasted between 15 and 60 minutes also increased, totaling 648 attacks. In 2019, there were 378. Looking at the number of attacks that lasted between one and four hours, there were 146. A year earlier, there were 107. In 2020, the NaWas observed 53 attacks that lasted longer than four hours. In 2019, there were only 23: that means more than double the number of seizures lasting longer than four hours in 2020.

Raising the threshold

Before the corona era, the NaWas used a certain threshold value. If this value exceeds a certain level, the anti-DDos equipment checks if it is an attack. As working from home has increased, it also means more traffic on the ports. There have been occasions when thousands of workstations were seen to be under some sort of DDoS attack. This resulted in more filtering, which was not the intention. The NaWas had to raise the threshold values to ensure that the increasing traffic on ports was no longer seen as an attack.

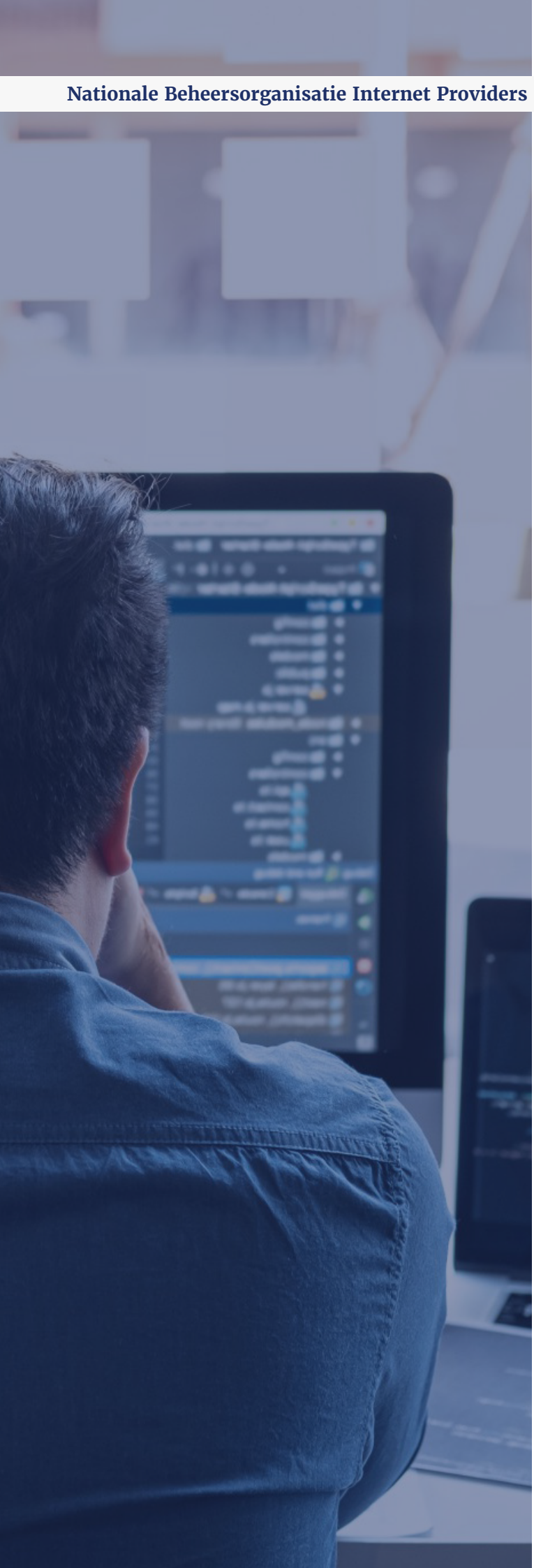
> First, we see a marked increase in the number of attacks in 2020.

Attacks on Internet service providers

In 2020, we saw attacks on the infrastructures of Internet service providers in the months of August and September. The DDoS attacks targeted routers and DNS infrastructures of the DNS amplification, LDAP amplification and NTP amplification types. The attacks were very intense, up to 260 Gbit per second, and when one attack was repelled, the next one started half an hour later.

The attacks were particularly powerful (up to 260 Gbit per second) and sometimes lasted longer than four hours. They were aimed at Internet service providers in the Benelux. The attacks can be divided into four different categories: LDAP amplification, DNS amplification, NTP amplification and DNS request flood. Measurements by NBIP have shown the following breakdown: LDAP amplification (37%), DNS amplification (37%), NTP amplification (18%) and DNS request flood (10%).

The DDoS attacks were aimed at Caiway, among others. On Tuesday morning, 1 September, the provider suffered a major DDoS attack. There was also a major attack on Signet on Tuesday afternoon. Signet also manages the infrastructure for TransIP and their customers also suffered disruptions due to that attack. The forum of the Belgian ISP EDPNet even talks about attacks of up to 200 Gbit per



second. This provider has already had DDoS attacks for five days in a row.

Companies outside of the Benelux were also attacked and had to deal with Internet service disruptions. NaWas was able to connect several new participants in a short period of time to combat DDoS and make the Internet safer. Recently, NaWas expanded its presence to London on the London Internet Exchange (LINX), Italy with the connection of IT.Gate to Top-IX and the Vienna Internet Exchange (VIX).

Profiles for participants

For participants, NaWas has developed a number of profiles depending on the type of attack that can be used in different situations. In this way, a particular type of DDoS attack can be quickly blocked and it is not necessary to make ad hoc settings.

In the case of a DDoS attack, the NaWas is activated by a command. The NaWas does this by setting a prefix. Participants who are more affected by DDoS attacks leave the prefixes, also called routes through the NaWas, in place longer. They leave the prefixes in place because they fear new attacks. This is because more DDoS attacks are carried out in a row.

We are also seeing the increase in attacks in the first quarter of 2021, where we have already observed more attacks than in all of 2020. The most powerful attack had a power of 300 Gbps.

6. Conclusion

Based on the research results for the year 2020, the NBIP draws a number of conclusions: more attacks, lasting longer and at the same time being more powerful and complex.

If we examine the figures for 2020, the first thing we see is a significant increase in the number of attacks. There were no less than 1610 in 2020 compared to 919 and 928 in 2019 and 2018. We have not investigated the cause of this increase. In any case, the increase can be called striking.

With regard to the strength of the attacks, we also see a clear increase in 2020 compared to previous years. The most powerful attack in 2020 had a size of 200 Gbps. In comparison, in 2018 and 2019, the most powerful attacks were 68 Gbps and 124 Gbps in size, respectively.

Despite the increase in the number, duration and complexity of DDoS attacks, we in the Netherlands are not doing too badly compared to other countries. With the advanced anti-DDoS platform NaWas, which was set up together with the participating internet service providers and a number of other large organizations, we are very well able to adequately repel even very powerful and complex DDoS attacks. As a result, we have already been able to limit a great deal of economic damage because companies and home workers have been able to continue working without interruption.

> The attacks last longer while being more powerful and complex.

Appendix
Type of DDoS attacks

Main categories

There are two main categories in DDoS attacks: (UDP-based) amplification en flood.

Amplification (UDP-based)

In case of a DDoS amplification attack, a (non-secured) server is abused. The message being sent is enlarged by a factor X. This allows an attacker with small and simple messages to provide a huge number of messages to a server. In the simple message the sender falsifies (spoofs) the return address to that of the target. The attacker sends a postcard to the post office, as it were, and the target receives back hundreds of bags full with mail.

Flood

In a so-called DDoS flood attack several computers are used at the same time that send packets to a server. Usually, 'half' messages are sent that cause the server to be disturbed. For example, a 'start communication' is sent, but then no follow-up message is sent when the target reacts with 'ok, start the follow-up communication'.

Amplification

In alphabetical order

Charge amplification

Charging is an old protocol exploited for amplification attacks. In such an attack, small packets with a forged IP address sent to a server, via devices with an Internet connection that still use CharGEN. Most printers and copiers connected to the Internet have this old protocol enabled by default. The server then receives to handle a UDP flood. The server gets 'exhausted' and goes offline or does a reboot.

DNS amplification

The attacker sends a DNS look-up request to vulnerable DNS servers with the spoofed IP address. Usually these are DNS servers that support open recursive relay The request is often passed on via a botnet so that the attack is bigger and better hidden. The DNS request is sent using the EDNS0 extension of the DNS protocol, which allows large DNS messages. The request can also abuse the cryptographic function of the DNS security extension (DNSSEC) to make the message larger.

LDAP amplification

LDAP amplification exploits a specific weakness in older LDAP servers that are still in use - the CLDAP protocol. Originally intended to see what services are available on an internal network server, some servers have the UDP port 389 open to the "outside".

MS SQL monitor amplification

This concerns abuse of a Microsoft SQL server environment - an old form, especially popular around 2015. Many SQL servers were

'Internetfacing' making them vulnerable to botnets, among other things. The fact that this attack is back indicates that companies still do not have basic security in order. MS SQL is another older technique.

It is a common practice in DDoS attacks: legacy that has not been updated or patched is vulnerable, so it is checked to see if there is anything to be gained. The well-known 'knocking on the door'.

Netbios amplification
NetBIOS is a protocol used in software to allow applications to communicate with each other over LAN networks. Targets of Netbios amplifications were mainly in the gaming and hosting sector.

NTP amplification
NTP amplification is a type of DDoS attack in which the attacker uses publicly accessible Network Time Protocol servers to bombard the target server with UDP traffic. NTP is one of the oldest network protocols and is used by connected devices to synchronize their clock. Older versions of NTP support a monitoring service that allows administrators to do a traffic count. This command is called monlist and it sends the requester a list of the last 600 hosts that have connected to the server. Since the sender is spoofed, the target of the attack will have to process an enormous amount of data.

RIPv1 amplification
The Routing Information Protocol (RIP), helps small networks to share network route information. It has existed since 1988, but it has also been hopelessly outdated since 1996. Traffic is sent to an IP address that corresponds to an IP address rumored to be on a list of known RIPv1 routers on the Internet. Based on recent attacks, attackers prefer routers that appear to have a suspiciously large number of routes in their RIPv1 routing table.

RPC Portmapper amplification
RPC Portmapper is an Open Network Computing Remote Procedure Call (ONC RPC) service designed to link RPC service numbers to network port numbers. When RPC clients want to connect to the Internet, portmapper tells them which TCP or UDP port to use. When Portmapper is requested, the magnification factor of the response can be up to 20 depending on the RPC services present on the host. Malicious users may use Portmapper requests for DDoS attacks because the service is running on TCP or UDP port 111.

SNMP amplification
An SNMP (Simple Network Management Protocol) amplification attack works just like a CharGEN attack, but then connected devices running SNMP are used. The big difference with a CharGEN attack is that the amplification with SNMP is many times greater.

SSDP
(Simple Service Discovery Protocol) is a network protocol used for discovering network services. SSDP allows universal plug-and-play devices to send and receive information via UDP on port 1900. SSDP is attractive to DDoS attackers due to its open state, which enables spoofing and amplification.

(UDP) memcached
Last year, NBIP saw memcached attacks. These are very small DDoS attacks that also have a very short duration and abuse the memcached protocol. Normally port UDP/11211 not to be open to the Internet, but if this is the case, then the attacks can be greatly increased.

Floods

ESP flood
ESP flood is an attack in which the UDP Encapsulating Security Protocol (ESP) is abused. An Encapsulating Security Payload (ESP) is a protocol for providing authentication, integrity and confidentiality of data and payload network packets in IPv4 and IPv6 networks.

GRE flood
In a GRE flood, a large number of packages from the Generic Routing Encapsulation protocol to a server sent. Normally, a firewall should handle it, but the amount of GRE packets is so high that the server can't handle it. Was mainly used by the well-known Mirai-botnet.

TCP flood
TCP/ACK, TCP/SYN, TCP/RST, TCP/SYN/ACK are one of the oldest but still very popular Denial of Service (DoS)-attacks. The most common attack is sending a large number of SYN packets to the victim. The attack will send the SRC IP spoofing, which means that the answer (a SYN+ACK packet) does not go to the original source, but to the target. In most cases, the purpose of this attack is to overload the firewall.

Servers must open a state for every SYN packet that comes in and this state save in tables of limited size. No matter how large this table is, it is easy to send enough SYN packets. that will fill the table, and once this is done happens the server starts a new request including legitimate requests. In Unlike other TCP attacks, the attacker does not need to use a real IP address; this is perhaps the greatest strength of the attack.

UDP flood
UDP flood is a type of attack in which random ports of a host (the target) are flooded with IP packets containing UDP datagrams. The host checks applications associated with these datagrams - finds nothing - and returns a Destination Unreachable packet.

ICMP flood
Internet Control Message Protocol (ICMP) is a connectionless protocol. In an ICMP flood attack, ICMP packets (especially network latency packets that test ping) are sent, which the server tries to process.

DNS request flood
This version of a UDP attack is one of the best known DDoS attacks. It specifically targets DNS servers to attack other web servers. It is also one of the most difficult attacks to detect and prevent. In order to carry out an attacker a large quantity of spoofed DNS request packets that look no different than real requests. These come from a very large number of IP addresses. This makes it impossible for the target server to distinguish between legitimate DNS requests and DNS requests that appear legitimate. The server gets overloaded trying to handle all requests - all bandwidth is consumed.

NBIP nationale beheersorganisatie internet providers

For more information:
www.nbip.nl/en