DDoS data report 2019

A closer look at the DDoS arms race

NBIP
nationale
beheersorganisatie
internet
providers

Colophon

The NBIP DDoS data report 2019 is a publication of Stichting Nationale Beheersorganisatie Internet Providers.

Publication date
June 2020, year 3

Editor-in-chief
Octavia de Weerdt (NBIP)

Editor
Gerald Schaapman (NBIP)

Contributions
NaWas operational team

Final editing
Wouter Pegtel (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

This report was created in PDF format

Summary
DDoS attacks remain a persistent problem with a major social and economic impact. In 2019, attacks were once again larger and more complex than the previous year, a trend that seems to be holding up. Vigilance remains necessary.

Table of contents

Foreword

This is the third annual review with DDoS data collected in 2019 by the Nationale DDoS Wasstraat (NaWas) of the Stichting Nationale Beheersorganisatie Internet Providers (NBIP). Here you can read all about the figures and trends regarding DDoS attacks on a significant part of the 'Dutch Internet'. The NaWas protects almost 2.5 million .nl domains.

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

In 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

The aim of this report is to share as much knowledge as possible about DDoS attacks with our participants, stakeholders and interested parties. Only by means of a collective approach to combat DDoS attacks will we be able to meet the challenge. One thing is certain: DDoS attacks are a permanent threat to a secure and stable Internet and there is no reason to expect this to change within a few years. The NBIP therefore wants to share its knowledge about DDoS attacks, the risks associated with these types of attacks and ways of mitigation and prevention with affiliated parties, stakeholders and interested parties. We strongly believe insight into the trends and developments of the past year will help readers to take the right precautions.

Intensive collaboration provides new insights and possibilities

As more and more organizations and sectors recognize DDoS attacks are a permanent threat that also affects them, more intensive cooperation in combating these attacks becomes possible. In 2018, for example, a start was made with the anti-DDoS coalition, a collaboration between 18 organizations including telecom providers, financial institutions, government organizations, the Dutch national police and the digital industry.

Recently, the first proof of concept for a DDoS clearing house has been completed, in which cooperating parties share a lot of information about DDoS attacks. Lifelike simulations are also carried out, in which one organization literally carries out a DDoS attack on another. In this way we were able to gain a lot of valuable knowledge and experience on how to recognize and mitigate DDoS attacks, and how organizations and their employees can deal with an attack.

The NaWas in 2020

2020 is already an exceptional year due to the coronacrisis and all its consequences for our societies. Behind the scenes, the NBIP shares knowledge where possible and offers help when needed. We offer our services to hospitals and other healthcare institutions if the need arises. We are constantly researching how the NaWas can contribute to the enormous effort we are making as a society to overcome this crisis.

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

Not so long ago, it took a lot of knowledge and patience to carry out a DDoS attack. Nowadays, this is no longer the case: with a few mouse clicks and a credit card, you can buy illegal DDoS attacks on the darkweb or the regular Internet. You would think that due to this ease of use, the number of DDoS attacks would rise dramatically. This is not the case: the number of DDoS attacks handled by the NaWas decreased slightly in 2019.

> Anyone who wants to carry out a DDoS attack does not need to have any technical knowledge.

DDoS attacks nevertheless remain a serious problem that can lead to major disruption. Although major attacks with a major impact, such as those that occurred in January 2018 in the Netherlands, did not occur in 2019, we must remain vigilant.

DDoS attacks in the news

There was no lack of news about DDoS attacks in 2019. Citizens, consumers, students, pupils and companies in the Netherlands have suffered from DDoS attacks in various ways in 2019. A small selection:

In February, the Lower House debated whether the law offers sufficient possibilities to combat the sale of DDoS attacks. In March and also in April, a widely used online learning environment for secondary schools was unavailable due to DDoS attacks. The Dutch-language Wikipedia was inaccessible for hours in September 2019 due to a global DDoS attack. In October, five servers operating a botnet in Amsterdam were taken offline. And at the beginning of December, Radboud University Nijmegen had to cancel an exam due to repeated DDoS attacks.

If it weren't for DDoS mitigation, we would see an enormous number of news reports about disrupted online services. The fact this is not the case means there is a growing awareness that no one is immune to DDoS attacks and that it is therefore necessary to take precautions. At the NaWas, we have been doing this as a not-for-profit collective since 2014. Since its founding, the NaWas has neutralized many thousands of DDoS attacks.

Annual reporting

The NaWas detects many hundreds of DDoS attacks every year. These observations provide insight into how DDoS attacks evolve. NBIP shares these insights to make the Internet safer for everyone. That is why NBIP publishes the DDoS data report every year. We see trends emerging, or we 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.

> It has become very easy to launch a DDoS attack due to the increasing number of cloud based DDoS-as-a-service.

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.

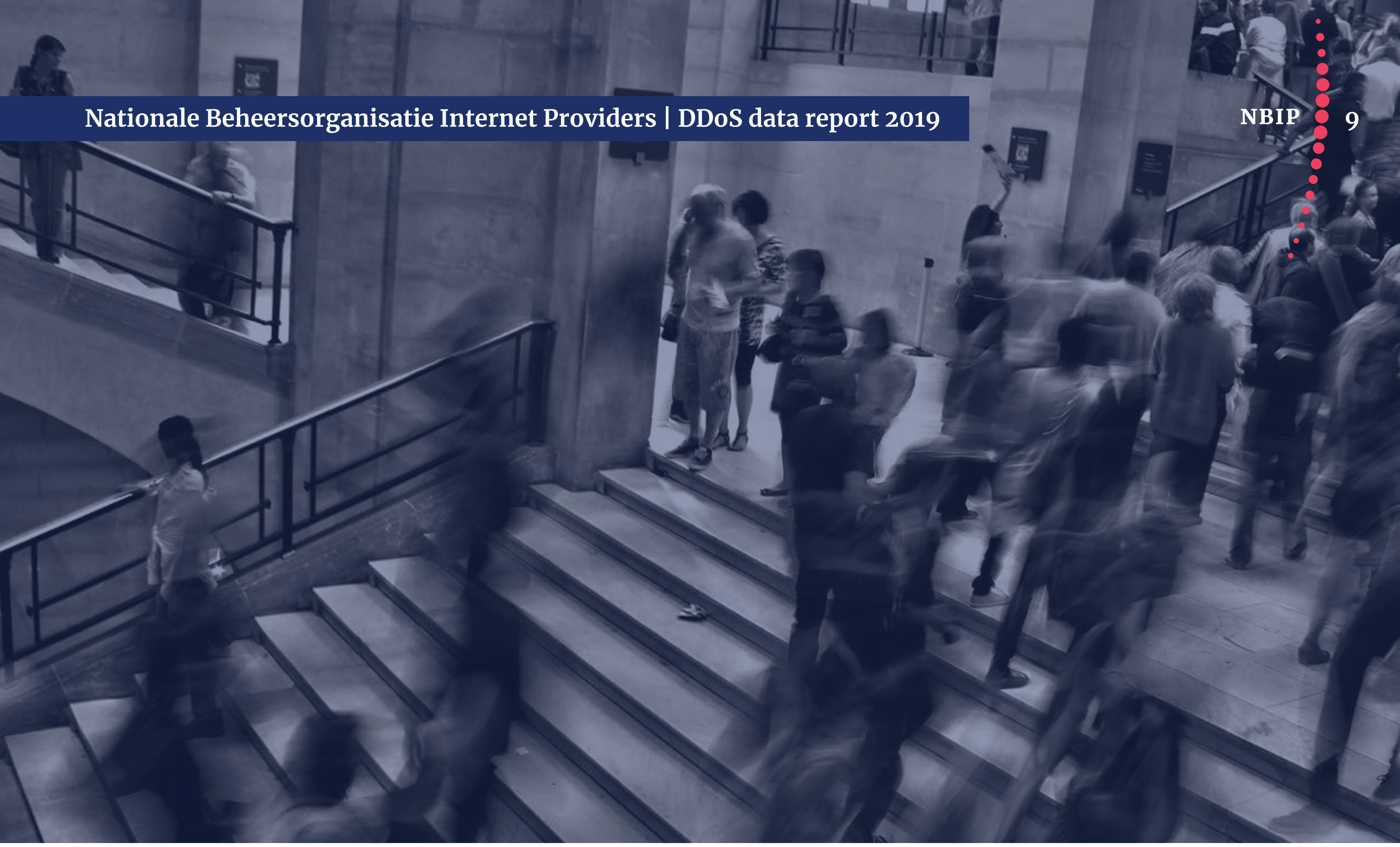
This research also showed that there is a lot of collateral damage. Especially if a company has a shared hosting solution with an ISP, where several websites are hosted on one server. For example, a website can fall to a DDoS attack, while it is not the target, simply because the attack is aimed at another 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. At the end of 2017, the number of participants was 56. At the end of 2018, the data of 68 participants was analysed. 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

VFor 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 make an present the number, size and duration of DDoS attacks in 2019. We also pay attention to:

- Types of DDoS attacks
- Notable DDoS attacks in 2019
- New types of DDoS attacks in 2019
- Trends that can be derived from the data

4.1 Number of DDoS attacks

In the year 2019, 919 DDoS attacks were registered by the NaWas. These are on average 2.5 DDoS attacks per day. In 2018, 938 DDoS attacks were registered. This represents a slight decrease of 2% in 2019 compared to the previous year, based on absolute numbers, while the number of participants in the NaWas grew by almost 10%. It could therefore be possible that the decrease in the number of DDoS attacks in 2019 is greater than two percent. In any case, it is certain that the substantial growth that was visible from 2017 to 2018 has not continued in 2019.

This observation in itself is surprising, because in the half-year report for 2019 we cautiously expressed the expectation that the number of DDoS attacks in 2019 will exceed the number of attacks we registered in 2018. We based this statement on the fact that we observed 572 attacks in the first six months of 2019, well in excess of the number of DDoS attacks in the first half of 2018. As we can now see, that growth levelled off as early as June 2019.

In no month after June the number of attacks exceeded 100, while in the first half of 2019 in both January, April and May more than 100 attacks were mitigated by the NaWas. In 2018 we saw an almost similar pattern: most attacks per month were observed in March and April.

The quietest month was August 2019 with only 19 registered attacks. In August 2018 49 attacks were registered. This is a drop of over 61%. The month with the fewest attacks in 2018 was October, when 38 attacks were registered. Looking at the month of October 2019, we see 66 DDoS attacks: an increase of 73%.

4.2 Size of DDoS attacks

We express the size of DDoS attacks in gigabit per second, or Gbps. Below is a graph showing how the total number of DDoS attacks is divided over the categories of DDos attacks smaller than 1 Gbps, between 1-10 Gbps, between 10-20 Gbps, between 20-40 Gbps, greater than 40 Gbps and the total.

To provide insight into how DDoS attacks develop over the longer term, the tables for 2017 and 2018 have also been included.

months	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	total
Jan-2017	12	53	4	1	0	70
Feb-2017	11	16	6	4	0	37
Mar-2017	34	37	9	3	0	83
Apr-2017	20	29	8	0	0	57
May-2017	22	58	7	2	0	89
Jun-2017	34	41	8	1	0	84
Jul-2017	17	17	2	0	0	36
Aug-2017	12	16	2	1	0	31
Sep-2017	14	33	6	1	0	54
Oct-2017	44	50	9	6	0	109
Nov-2017	34	31	5	4	0	74
Dec-2017	40	56	5	1	0	102
Final total	**294**	**437**	**71**	**24**	**0**	**826**

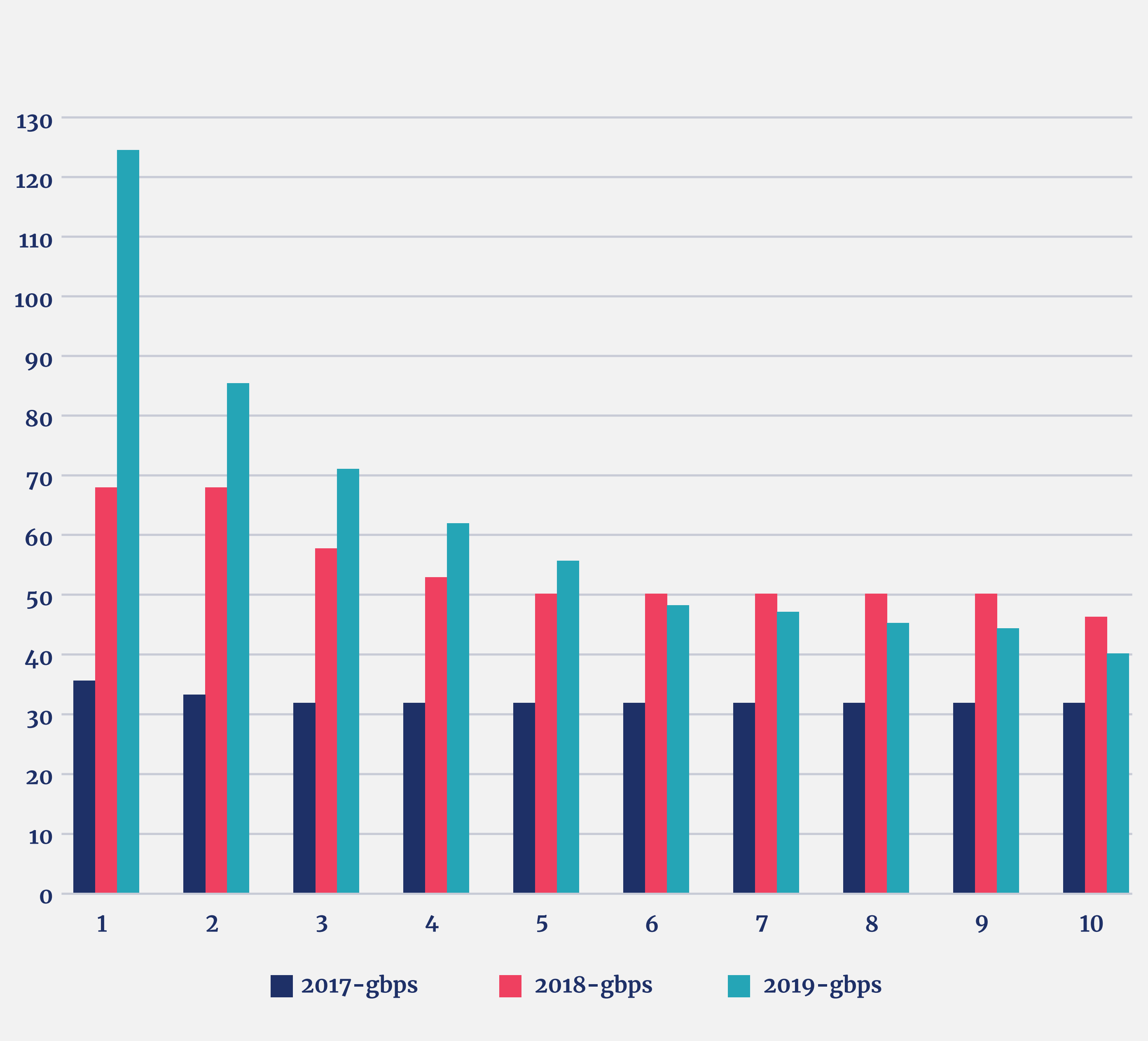
months	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	total
Jan-2018	26	55	3	14	1	99
Feb-2018	34	42	4	1	2	83
Mar-2018	33	57	20	3	0	113
Apr-2018	44	55	9	2	0	110
May-2018	43	22	5	0	0	70
Jun-2018	32	43	4	0	1	80
Jul-2018	18	32	2	3	1	56
Aug-2018	22	20	2	4	1	49
Sep-2018	33	38	3	4	1	79
Oct-2018	10	27	0	1	0	38
Nov-2018	32	53	6	2	3	96
Dec-2018	35	25	4	0	1	65
Final total	**362**	**469**	**62**	**34**	**11**	**938**

months	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	total
Jan-2019	32	70	9	4	1	116
Feb-2019	18	39	8	3	3	71
Mar-2019	42	35	1	0	1	79
Apr-2019	25	72	15	5	2	119
May-2019	40	61	4	5	0	110
Jun-2019	26	41	3	0	1	71
Jul-2019	12	25	2	1	0	40
Aug-2019	7	9	0	0	0	16
Sep-2019	24	57	3	1	0	85
Oct-2019	13	49	2	2	0	66
Nov-2019	14	51	5	1	2	73
Dec-2019	20	40	9	3	1	73
Final total	**273**	**549**	**61**	**25**	**11**	**919**

year	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps
2017	35,6%	52,9%	8,6%	2,9%	0%
2018	38,6%	50%	6,6%	3,6%	1,2%
2019	29,7%	59,7%	6,6%	2,7%	1,2%

Compared to 2018, in 2019 we have seen a decrease in the proportion of attacks smaller than 1 Gbps, but there is a significant increase in the percentage of attacks between 1 and 10 Gbps. The share in the total number of attacks between 10 and 20 Gbps remains the same as 2018. There has been a small drop is the share of attacks with a size between 20-40 Gbps in 2019. The share of large attacks of 40 Gbps or greater remained the same.

2017 - 2019 top 10 Gbps



4.3 Duration of DDoS attacks

Compared to 2018, we see the number of attacks shorter than 15 minutes increase from 323 to 405 in 2019. The number of attacks with a duration of between 15 and 60 minutes decreases in the same period from 430 to 378. The number of attacks with a duration of between 1 and 4 hours decreases from 156 to 107. In 2019, as in 2018, 29 attacks lasting more than 4 hours were registered.

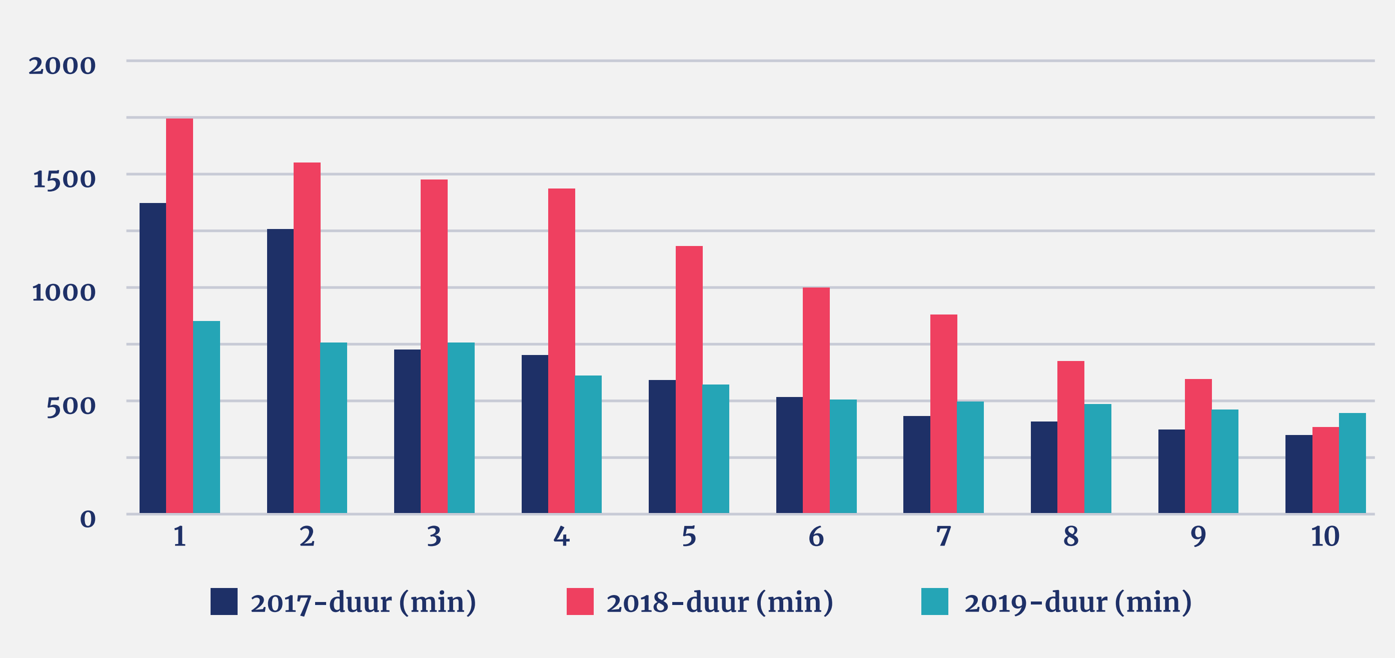
months	< 15 min	15-60 min	1-4 hours	> 4 hours	total
Jan-2017	29	29	7	5	70
Feb-2017	18	9	7	3	37
Mar-2017	34	23	21	5	83
Apr-2017	28	24	4	1	57
May-2017	46	28	14	1	89
Jun-2017	36	36	9	3	84
Jul-2017	12	14	8	2	36
Aug-2017	12	12	7	0	31
Sep-2017	15	31	8	0	54
Oct-2017	18	58	32	1	109
Nov-2017	18	34	17	5	74
Dec-2017	43	42	15	2	102
Final total	**309**	**340**	**149**	**28**	**826**

months	< 15 min	15-60 min	1-4 hours	> 4 hours	total
Jan-2018	40	37	20	2	99
Feb-2018	30	41	11	1	83
Mar-2018	44	47	20	2	113
Apr-2018	41	46	19	4	110
May-2018	20	39	9	2	70
Jun-2018	30	38	11	1	80
Jul-2018	15	26	11	4	56
Aug-2018	10	27	9	3	49
Sep-2018	19	44	15	1	79
Oct-2018	12	17	8	1	38
Nov-2018	32	43	17	4	96
Dec-2018	30	25	6	4	65
Final total	**323**	**430**	**156**	**29**	**938**

months	< 15 min	15-60 min	1-4 hours	> 4 hours	total
Jan-2019	53	54	9	0	116
Feb-2019	40	24	7	0	71
Mar-2019	41	28	7	3	79
Apr-2019	33	38	34	14	119
May-2019	46	42	18	4	110
Jun-2019	34	28	7	2	71
Jul-2019	14	24	2	0	40
Aug-2019	10	4	2	0	16
Sep-2019	36	41	7	1	85
Oct-2019	28	33	5	0	66
Nov-2019	37	31	4	1	73
Dec-2019	33	31	5	4	73
Final total	**405**	**378**	**107**	**29**	**919**

year	< 15 min	15-60 min	1-4 hours	> 4 hours
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%

2017 - 2019 top 10 duration (min)



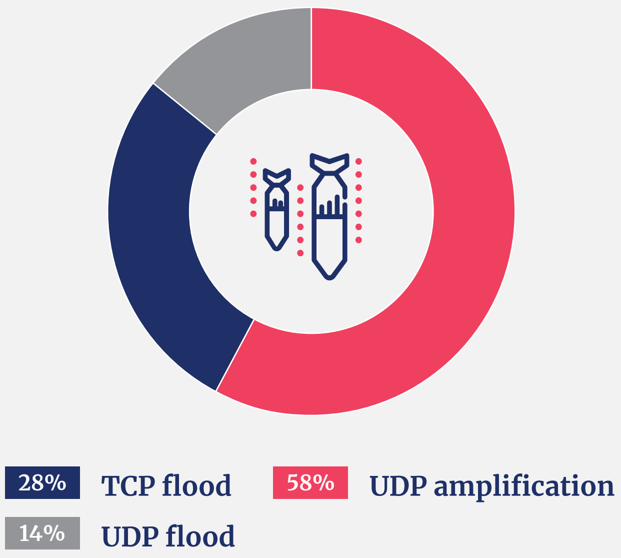
4.4 Types of DDoS attacks

In 2018, we observed 56 types of DDoS attacks. In 2019 this number decreased to 49 types of attacks. In this context, NBIP distinguishes between three main types of DDoS attacks that can be divided in different subtypes. The main categories are TCP flood, UDP flood and UDP amplification.

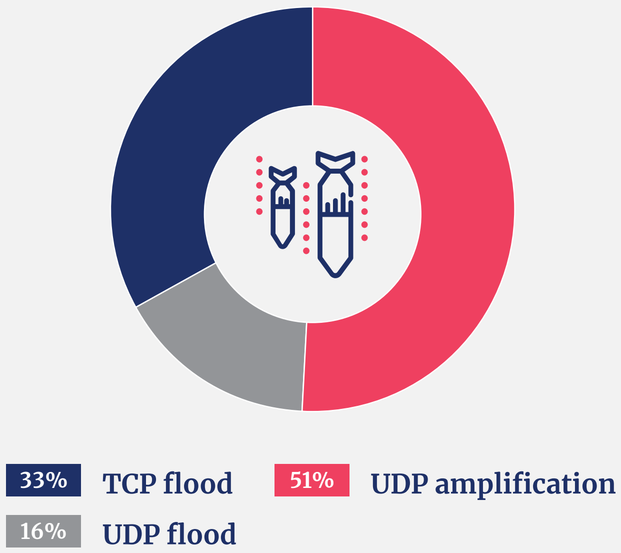
Compared to the year 2018, there was an increase in the attack type UDP amplification and a decrease in the type TCP flood. These percentages were 51% and 33% respectively in 2019 compared to 56% and 28% respectively in 2019. Compared to the figures for 2017, there appears to be a small fluctuation in popularity of UDP amplification and TCP flood attacks, while the proportion of UDP flood attacks fluctuates to a lesser extent year on year.

> In 2019 there was a marked increase in UDP amplification attacks compared to the previous year.

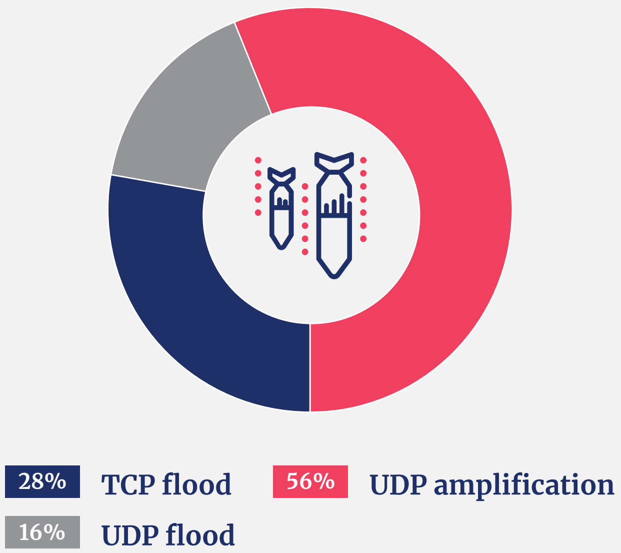
DDoS type main group distribution 2017



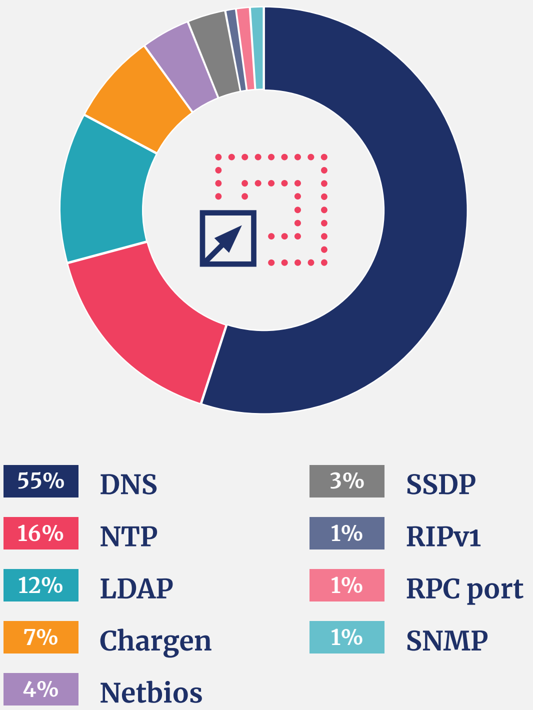
DDoS type main group distribution 2018



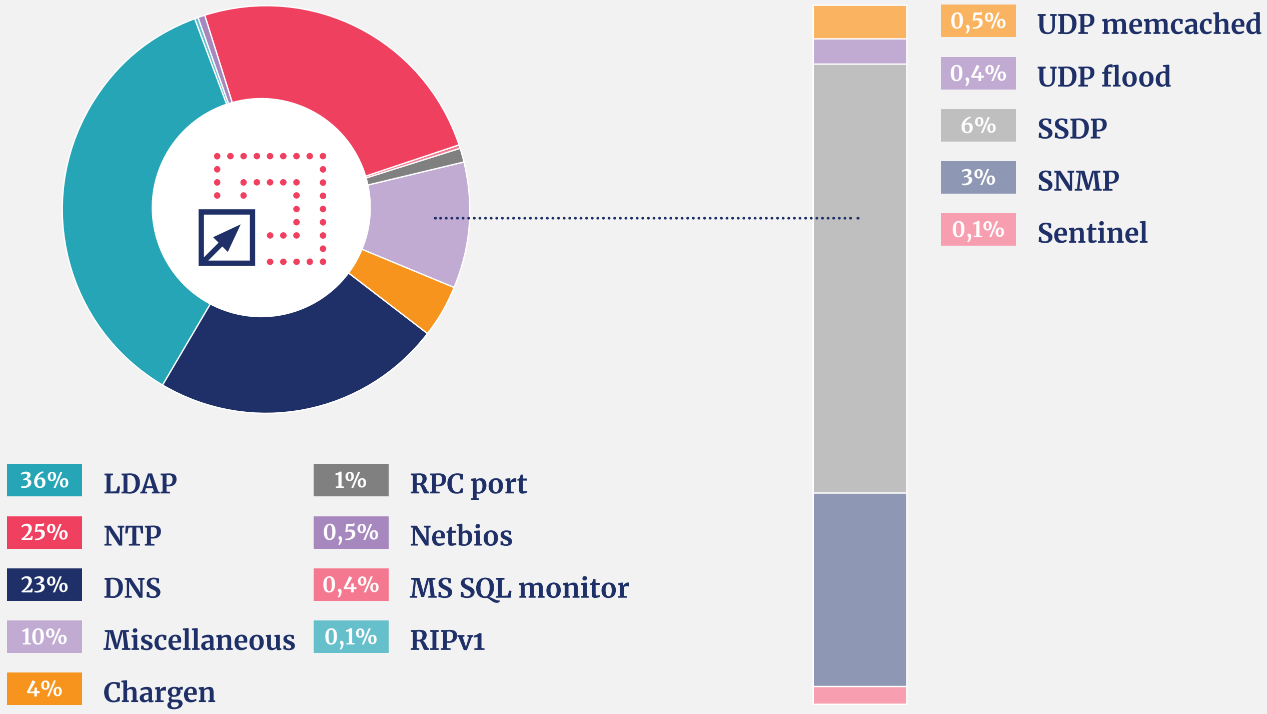
DDoS type main group distribution 2019



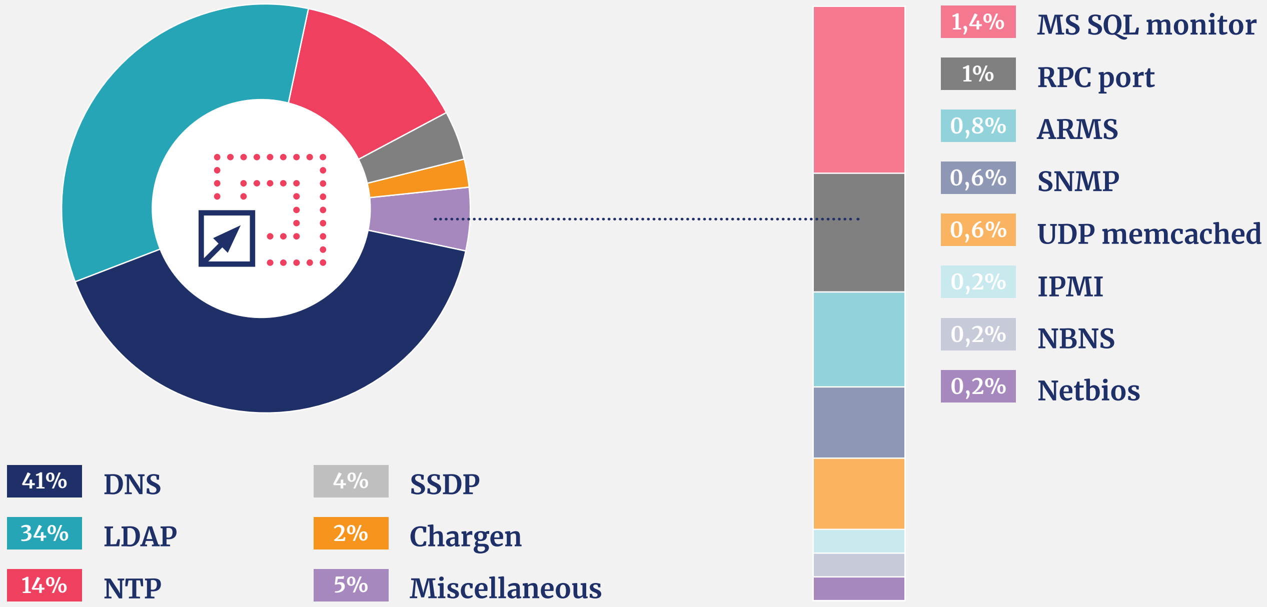
UDP amplification DDoS-types 2017



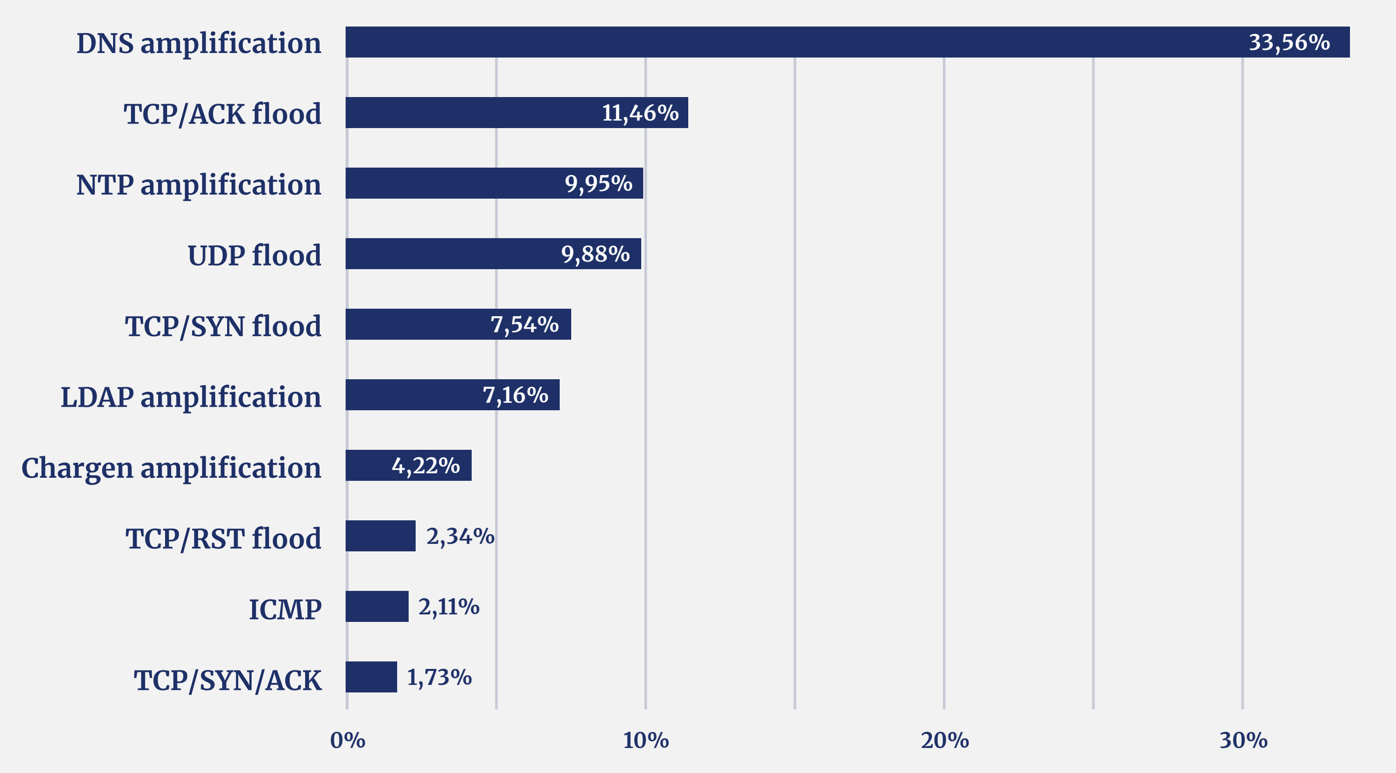
UDP amplification DDoS-types 2018



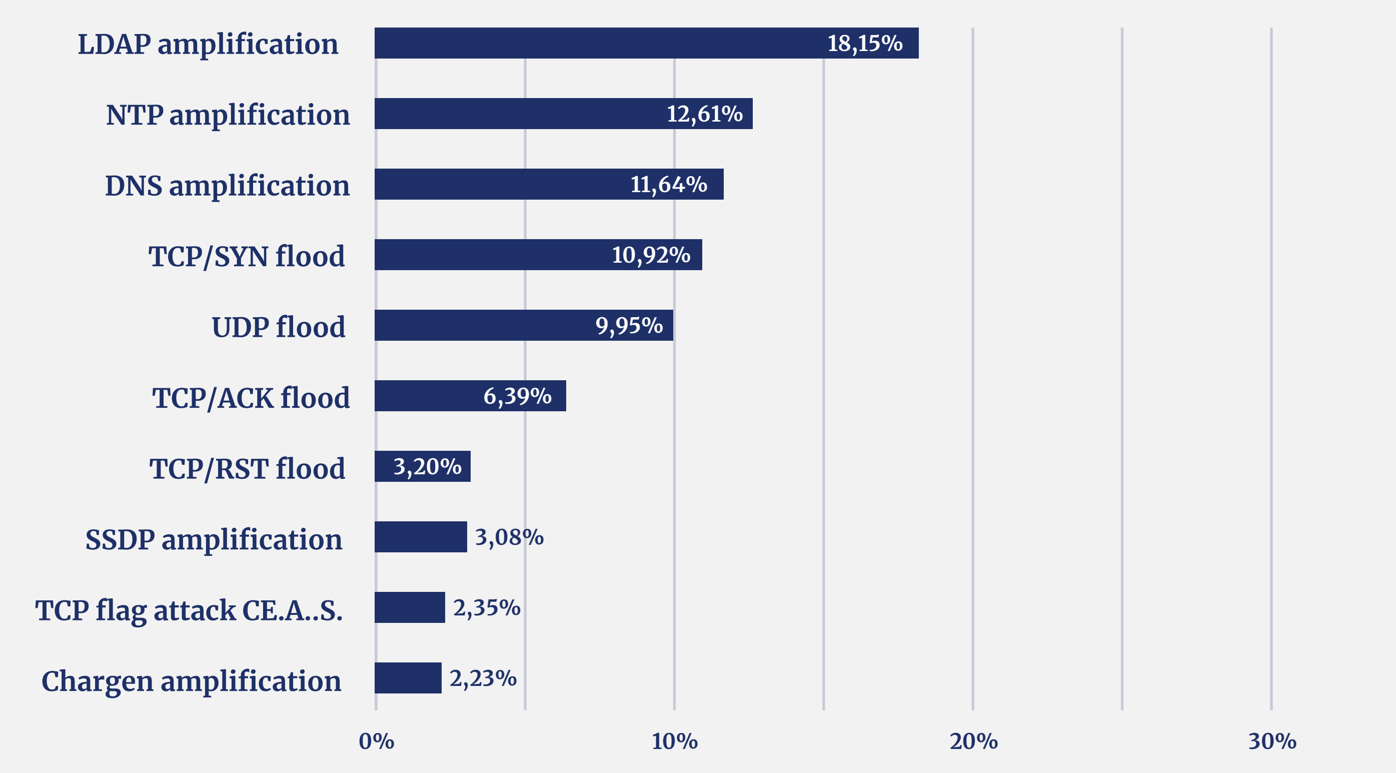
UDP amplification DDoS-types 2019



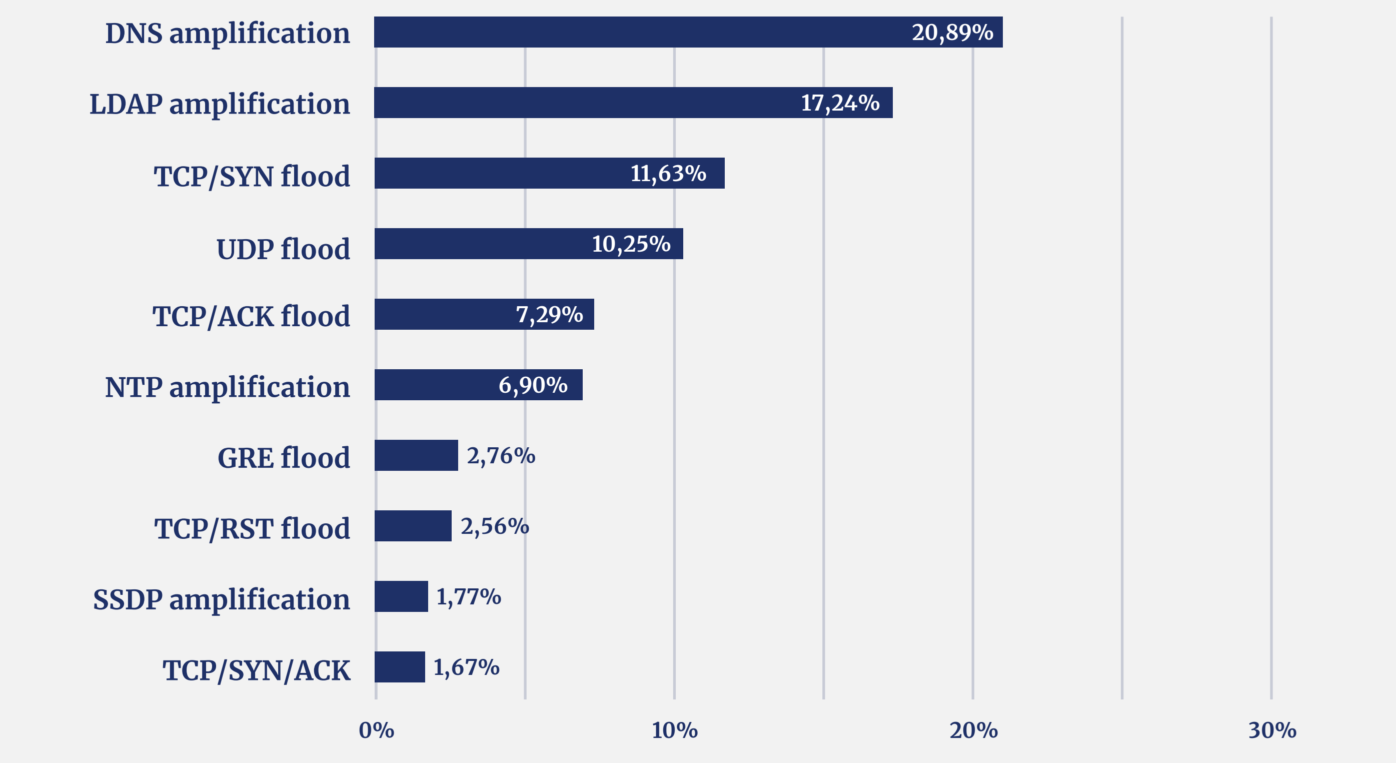
DDoS-type top 10 2017



DDoS-type top 10 2018



DDoS-type top 10 2019



In 2018, LDAP amplification was at the top of the DDoS type top 10 list with a share of 18.15%. In 2019, DNS amplification is the most common DDoS-type attack with a share of over 20%. In 2017, DNS amplification also scored high with a percentage of of 33.56%. LDAP amplification also remains popular. Remarkably, NTP amplification, which was still in second place last year, has fallen significantly: from 12.61% in 2018 to 6.9% in 2019 (6th place).

4.5 Multi-vector attacks

Multi-vector attacks have been be popular in 2019, just as in 2018 when we observed a notable rise in these types of attacks. Multi-vector attacks involve several types of attacks (vectors) that are bundled together. It can be both a 'simple', large attack type with 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 in 2019 made use of as many as 30 different vectors, although this is an exception. Attacks with 8, 9 or 10 vectors have been observed with some regularity in 2019.

4.6Notable DDoS attacks

SIPvicious attack

SIPvicious is part of a toolset for testing Session Initiation Protocol (SIP) based VoIP systems. Hackers can also abuse this toolset for a flood aimed at these systems in an attempt to shut them down.

SIPvicious is an auditing tool used in attacks targeting IP phones, VoIP phones and PBX systems. It is therefore recommended to place the IP/VoIP devices behind a firewall.

4.7 Newly observed DDoS attacks

WS-Discovery amplification

In 2019 we observed a WS-discovery DDoS attack in the NaWas for the first time. The WS-Discovery protocol is not designed to be 'Internet facing'. Attacks carried out via this protocol are only possible because the device that uses this protocol has been set up incorrectly.

WS-Discovery is intended for local, closed networks where devices can use the protocol to 'discover' which other devices are in the network. These include printers for example, but also IoT-devices. Although it should not be possible for devices outside the network to query devices on an internal network using this protocol, this is often possible because these devices are configured incorrectly and can be found on the Internet. This allows the attacker to 'query' large quantities of devices in a short period of time, sending the actual target address of the DDoS attack as the return address for these devices to respond to. As a result, many thousands of devices potentially send their response to a single target address, causing it to be overloaded.

GRE flood

The Generic Routing Encapsulation (GRE) flood is a type of DDoS attack that encapsulates network packets into large amounts of data. These packets are then sent to the target network, which gets overloaded when the packets are unpacked. There have also been observed GRE floods that only use header information for the packets.

GRE floods became widely known after the attack of 665 Gbps by the Mirai-botnet on a well-known international security specialist in 2016. The type of attack is therefore not new, but was little observed in the NaWas until 2019. The growth of this type of attack is therefore remarkable.

> The most complex attack in 2019 used no less than 30 different vectors.

5. Trends

At first sight, 2019 seems to have a lot in common with 2018 in terms of the number of DDoS attacks observed by the NaWas. However, there are also important differences. For example, there was a decrease in the number of attacks. At the same time, the size of these attacks increased across the board.

The number of attacks decreased in 2019, but their size and complexity increased.

Attacks continue to grow in size rapidly

The largest attack observed in 2019 was almost twice as large as the largest attack in 2018: 124 Gbps in 2019 compared to 68 Gbps in 2018. In 2017 the largest DDoS attack observed was 36 Gbps. In both 2018 and 2019, an attack of 36 Gbps wouldn't even have made it into the top 10 largest attacks.

We observe that the largest DDoS attacks are getting stronger, but these attacks do not account for a larger percentage of the total. The conclusion must therefore be that the largest DDoS attacks observed by the NaWas increase in size year on year, with the attacks in the top 3 being particularly large compared to 2018, but that their number does not increase proportionally.

Also, the number of small (< 1Gbps) attacks is slowly decreasing. The share of attacks with a size between 1 and 10 Gbps remains the highest and has grown considerably compared to 2018.

Duration and timing of DDoS attacks

The duration of DDoS attacks seems to decrease slightly on average. The number of short-term attacks (<15 minutes) increased over the past three years, while the number of attacks with a duration of between 1 and 4 hours decreased over the same period. The yearly number of very prolonged attacks remains about the same in the time period 2017-2019. However, 9 of the top 10 longest attacks in 2019 are (much) shorter than the longest attacks in 2018.

It is striking that, as in 2018, more DDoS attacks are being carried out in the first half of the year than in the second half. It is a matter of conjecture what the reasons are for this trend, if any can be given at all.

It would seem reasonable to assume that the higher frequency in the first half of the year can be related to certain variables that remain unknown for now; in the context of prevention, it might be worth doing research to be able to understand this trend better.

Top 10 types of attacks changes annually

It is noticeable that in 2019 the types of attacks that are 'popular' have again changed compared to 2018. In 2018 LDAP amplification was the most popular type of attack, while in 2019 it was DNS amplification, where this was also the case in 2017. In 2017, for example, TCP/ACK flood took a second place in the top 10, whereas in 2019 it was a fifth place. Another type of attack, chargen amplification, was still in the top 10 of most common attack types in 2017 and 2018, but disappeared from the top 10 in 2019.

6. Conclusion

Based on the research results for the year 2019, the NBIP draws three conclusions.

We see a decrease in the number of DDoS attacks in the year 2019. In 2019, 919 attacks were registered, in 2018 there were 938. The number of participants in the NaWas also grew, which makes the decrease relatively stronger. As the number of DDoS attacks increased in 2018 compared to 2017, it is quite possible that the slight decrease in 2019 will not be a trend. However, it seems that more DDoS attacks are carried out in the first half of each year than in the second half of the year. It will therefore only be possible to assess whether the number of attacks is rising or falling after 2020 has come to an end.

DDoS attacks increased in size in 2019, as they did in 2018. The maximum size of a DDoS attack in 2019 was approx. 124 Gbps, compared to 68 Gbps in 2018. In 2017, no DDoS attack above 40 Gbps has been registered by the NaWas. It is therefore advisable that organizations that have to deal with DDoS attacks prepare for a further increase in the scale of these attacks and take the appropriate measures to protect their systems.

Finally, the data collected by the NaWas in 2019 showed that the popularity of the multi-vector attack, involving multiple types of DDoS attacks combined in one attack, is still growing and that attacks are getting more complex than ever.

> The continuous evolution of DDoS attacks points to an arms race that is unlikely to stop any time soon.

The growth in both size and complexity of DDoS attacks still needs to be anticipated as the continuous evolution of DDoS attacks points to an arms race that is unlikely to stop any time soon. Luckily, through cooperation, we will be able to keep ahead, reducing the impact of DDoS attacks and making the Internet a safer place.

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 'Internet-facing' 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

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

TCP/SYN floods 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