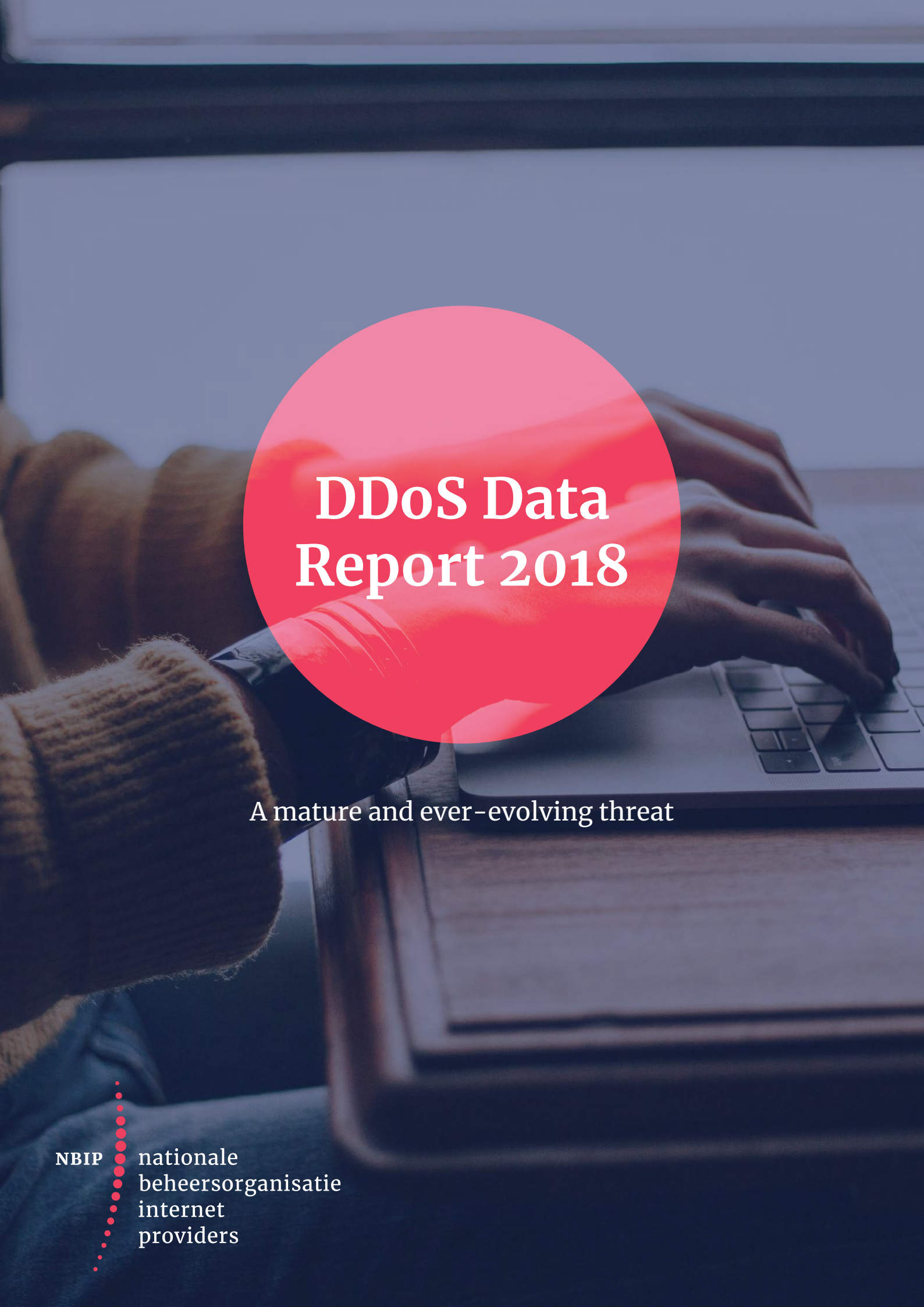


DDoS Data Report 2018

A mature and ever-evolving threat

NBIP nationale beheersorganisatie internet providers

Colophon

The NBIP DDoS Data Report 2018 is published by the Dutch National Internet Providers Management Organisation (Nationale Beheersorganisatie Internet Providers - NBIP).

Publication date
March 2019, year 2

Editor-in-chief
Octavia de Weerdt (NBIP)

Editor
Gerald Schaapman (NBIP)

Contributions
Bureau NBIP

Final editing
Lorenz van Gool (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

Form
This report was made in the PDF format

Summary
The phenomenon ‘DDoS attack’ is well established in our society. DDoS attacks remain complex and the types of attacks are constantly changing. This makes them difficult to combat. A DDoS attack is now a mature threat that needs to be taken seriously.

Table of contents

Preface 4

1. Introduction 6

2. DDoS - the basics 7

3. Research method 9
Data collection 9
Accountability 10

4. Research results 11
4.1 Number of DDoS attacks 11
4.2 Size of a DDoS attack 11
4.3 Duration of a DDoS attack 14
4.4 Types of DDoS attacks 16
4.5 Notable DDoS attacks 19
4.6 New types of DDoS attacks 19

5. Trends 20

6. Conclusion 21
DDoS: a mature threat 21

Appendix Type of DDoS-attacks 22
Main categories 22
Amplification 22
Floods 24

Preface

In the 2018 annual DDoS report, the National Management Organisation for Internet Providers (NBIP) shares figures and trends concerning the DDoS attacks that have been seen, analysed and mitigated by NaWas ('Nationale Wasstraat' - National Scrubbing Centre). This 'scrubbing centre' of 'dirty' internet traffic has been operational since 2014 and has become a household name in the Dutch internet sector in a very short time.

Last year, NBIP started publishing annual and semester reports with data on DDoS attacks. This report provides insight into the number of DDoS attacks, the duration of attacks, the types of DDoS attacks, and trends as seen and analysed by NaWas experts in 2018.

We also have been conducting broader research in collaboration with other parties - such as the DDoS impact study with Stichting Internet Domeinregistratie Nederland (SIDN). This study showed that NaWas protects 43% of all .nl domains in the Netherlands - or more than 2.5 million .nl domains.

NBIP is also involved in the DDoS Clearinghouse, a multiparty initiative to better understand and analyse DDoS attacks. So far, this has resulted in a number of tools and a DDoS database. In addition, research into DDoS attacks in December 2018 was conducted, of which the results were discussed in the Dutch public broadcast news bulletin.

These studies and media outreach are part of our focus to share as much knowledge as possible, not only about DDoS attacks. The NBIP is also very active in abuse control and the execution of lawful interception.

Back to DDoS. Our collective approach of the

NaWas (we buy together and is only used when necessary) is now starting to get attention abroad. We are pleased that NBIP is talking to many interesting parties from all over Europe, on its way to a pan-European anti-DDoS scrubbing centre. We have already taken our first European steps. Because we believe that the more organisations join, the better our service will be. Even across borders.

We hope that you will learn new things by reading this report. We ourselves aren't surprised of anything anymore. That's why we published this report, so you know what's happening in the world of DDoS. We are firmly convinced that mitigating DDoS attacks starts with gaining and sharing knowledge.

We hope you enjoy reading this report,

Octavia de Weerdt,
Managing director NBIP

The NBIP protects more than 2.5 million .nl domains

1. Introduction

At the beginning of 2018, the Netherlands woke up to major DDoS attacks on several big institutions. In one fell swoop, DDoS became a hot topic. On the one hand because of the disruptive effect, and on the other hand because of the ease of the attack. A broadcast of Nieuwsuur with a DDoS 'expert' ensued mass hilarity. The result: a wave of attention for the phenomenon of a DDoS attack. It intrigued both the media and consumers.

It has been found that sharing knowledge is necessary to be able to take the right measures. NRC and BNR, among others, argued for a joint approach to DDoS threats by banks.

Taking action and sharing data to learn from it - that is exactly NBIP's approach with their NaWas initiative. This enabled us to mitigate more than 3200 DDoS attacks since 2014.

For us, DDoS attacks are a daily occurrence - unfortunately. Companies are confronted with them more frequently and an attack is more often in the news. Especially the reason for such an attack is often the subject of discussion. Last year we already showed that the motive ('for fun') is strengthened by the ease with which a DDoS attack can be carried out.

The fact that DDoS is perceived as a threat is shown by the news that the Dutch toy store chain Intertoys even used such an attack as an excuse, even though it was actually a 'normal' overload of its servers that caused an outage.

Despite this ignorance, we are fortunately also seeing more serious reactions to DDoS attacks. How easy it may be to carry out, and how light-hearted an attack like this is taken by companies ("it doesn't happen to me anyway"), it is and remains a crime. It is finally dawning on society that conducting a DDoS attack is serious and a form of cybercrime - with appropriate punishments.

It is therefore necessary to continue investigating DDoS. After all, it starts with awareness and we cannot emphasise this often enough. Despite the ease with which they can be carried out, a DDoS attack itself, how it works, is quite complex. Last year's report already showed this.

This report is made for readers with some expertise. The appendix contains descriptions of all the types of DDoS attacks mentioned in 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 counter it.

How does a DDoS attack work

What is a DDoS attack? DDoS stands for Distributed Denial of Service. In order to carry out a DDoS attack, the attacker infects a large number of computers or other Internet-connected devices. This is done with, for example, malware or via e-mail attachments. This creates a 'botnet', a network of infected devices. This network is then instructed to send data to the target server in order to overload that server. If the server can no longer handle the traffic, and users can no longer access the servers, the attack is successful.

That sounds very simple, and unfortunately it is. A DDoS attack can be carried out with little technical knowledge. DDoS attacks can be bought on special websites (there are thousands of them), and not only on the dark web. It is also possible to create an attack with relatively little knowledge: manuals to set up one's own botnet are easy to find.

Why are DDoS attacks so popular?

This is one of the reasons why 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 a number of factors that maintain the ease and attractiveness of this type of attack.

First, the increasing number of DDoS services in the cloud makes conducting an attack easier. Hosting is cheap and there is more and more bandwidth available. Buying rogue services on the internet is therefore becoming easier and easier. These services are purchased via so-called 'stressers' or 'booters'. The vast majority of DDoS attacks come via such an intermediary.

> The increasing number of DDoS services in the cloud makes conducting an attack easier

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 interest of the booter service provider either. Because these people want to make money as quickly as possible with as little effort as possible, booters disappear just as quickly as they appear.

Because attacks are so easy to purchase, this also means that more people with less technical knowledge can launch a DDoS attack. Because it's relatively easy to make some noise with little effort, or to avoid 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 toothbrushes to thermostats: 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 25 billion of such devices will exist in the year 2021.

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).

Last year, 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.

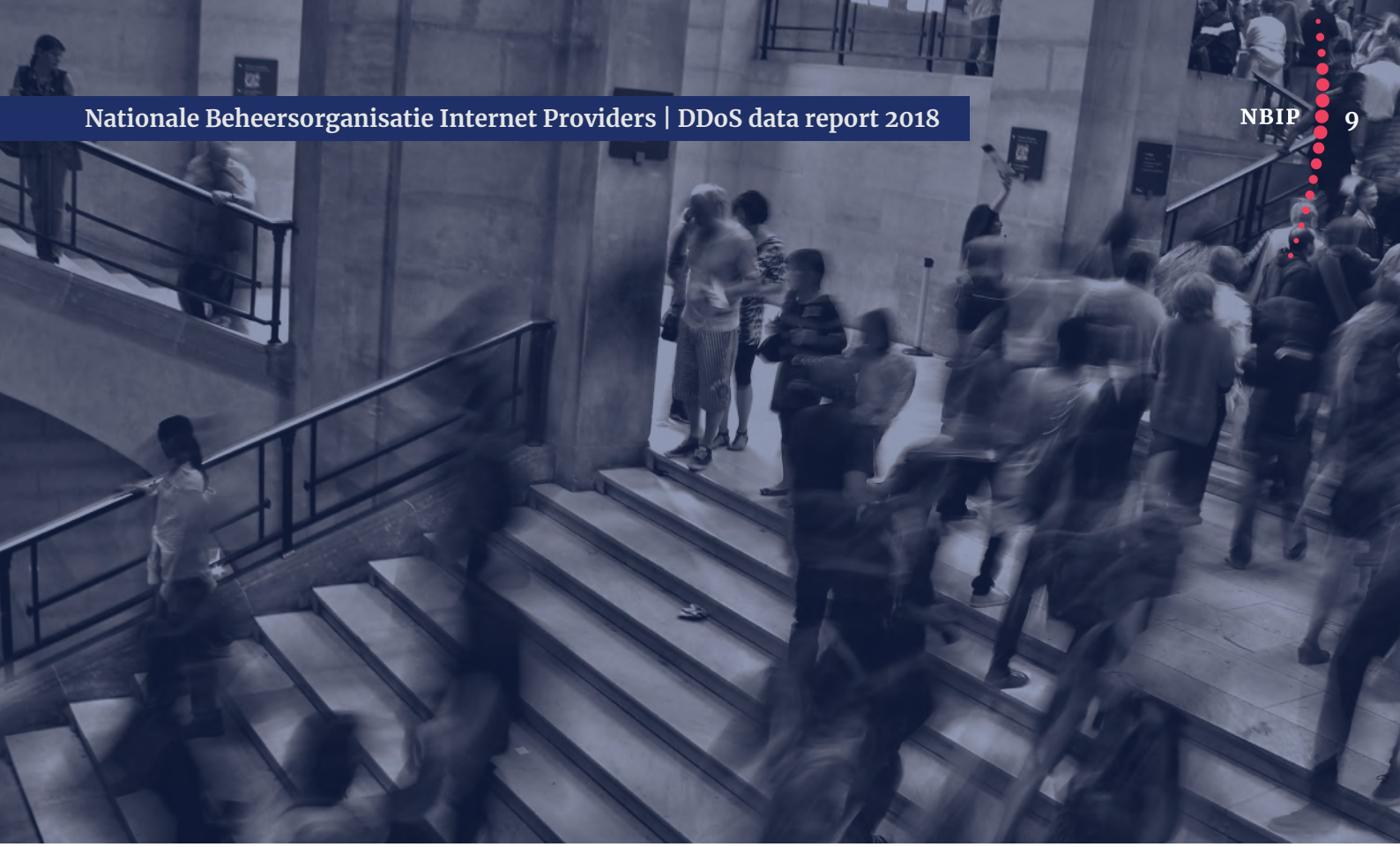
Methods of DDoS mitigation

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

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

First, the number, size and duration of DDoS attacks (2017/2018) were analysed. We then analysed the types of DDoS attacks that occurred in 2018 and in this report we will briefly discuss the results. An analysis of the measured numbers can be found in the conclusion.

4.1 Number of DDoS attacks

In 2018, NBIP again recorded more attacks in the Netherlands, namely 938 DDoS attacks, an increase of 13.6%. That is approximately 2.6 attacks per day.

In 2017 there were 826 DDoS attacks and in 2016 there were 680. The growth is flattening, where last year's growth (2016-2017) was 21.5 percent. The number of NaWas participants rose from 56 to 68 in 2018. The only positive aspect of these figures is that the NBIP's forecast in the first semester report 2018 about the total number of attacks was not achieved: namely 'over 1000'.

4.2 Size of a DDoS attack

The size of a DDoS attack is measured in Gbps (gigabit per second).

month	< 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
Total	**294**	**437**	**71**	**24**	**0**	**826**

month	< 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
Total	**362**	**469**	**62**	**34**	**11**	**938**

What immediately strikes when studying both charts, is that the big attacks of more than 40 Gbps are back, after they were missing last year. In 2016 there were only 2 of them.

It is also remarkable that October was the month with the most DDoS attacks in 2017, whereas in 2018 it was the quietest month. One possible explanation is that a number of large botnets worldwide were taken down in 2018. But this cannot be said with certainty. July and August remain relatively quiet periods, probably because of the summer holidays.

The distribution of the size of attacks remained almost the same, although there is a slight shift to both ends:

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%

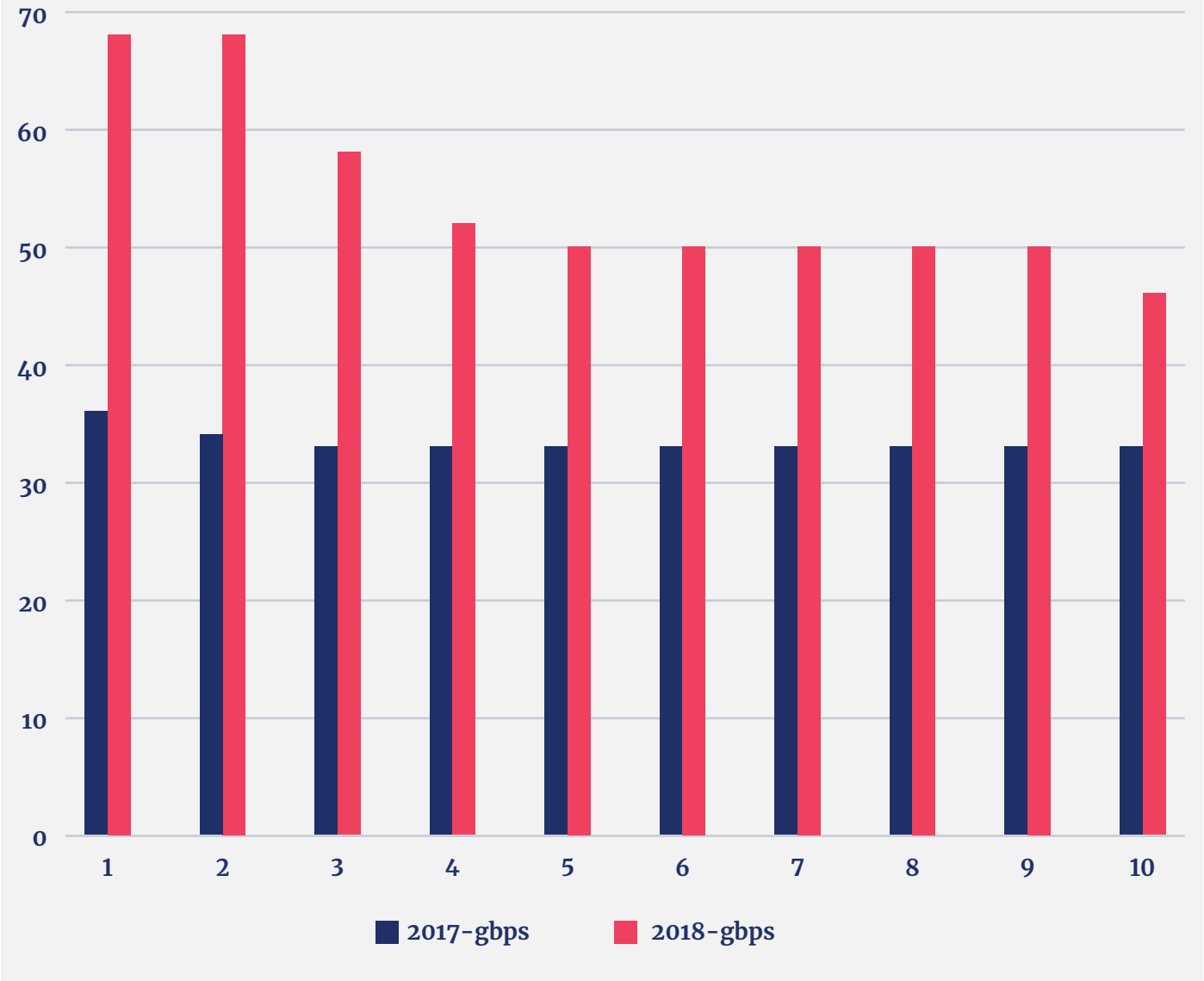
DDoS attacks in 2018 thus became both smaller and larger in Gbps. For the time being, there has been no real shift to both ends. The majority of attacks still do not exceed 10 Gbps.

The maximum size of a single DDoS attack in 2018 was 68 Gbps

The maximum size of a single DDoS attack in 2018 was 68 Gbps. In 2017, we saw a maximum size of 36 Gbps. The year before, in 2016, we saw a single 53 Gbps attack, but nothing more than 40 Gbps.

How different is that in 2018, where the top 10 consists of only larger attacks than the year before.

2017 - 2018 top 10 Gbps



Duration of a DDoS attack

Most of the attacks did not last longer than an hour, just like in 2017.
There were 29 DDoS attacks in 2018 that lasted longer than 4 hours, compared to 28 in 2017.

month	< 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
Total	**309**	**340**	**149**	**28**	**826**

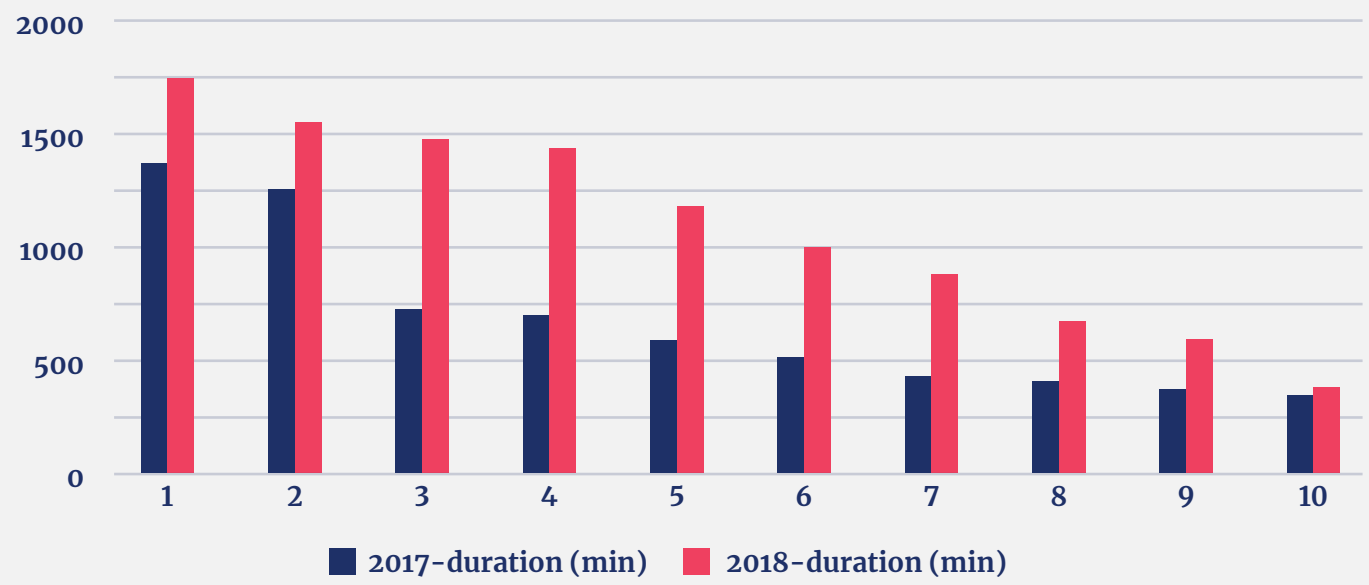
month	< 15 min	15-60 min	1-4 hours	> 4 hours	total
Jan-2018	40	37	20	2	99
Feb-2018	30	41	11	1	83
Mar-2018	44	47	20	2	113
Apr-2018	41	46	19	4	110
May-2018	20	39	9	2	70
Jun-2018	30	38	11	1	80
Jul-2018	15	26	11	4	56
Aug-2018	10	27	9	3	49
Sep-2018	19	44	15	1	79
Oct-2018	12	17	8	1	38
Nov-2018	32	43	17	4	96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

In terms of duration, there were no major differences in the distribution compared to the previous year. However, the number of very short attacks (less than 15 minutes) decreases, and the number of attacks just over fifteen minutes to an hour increase.

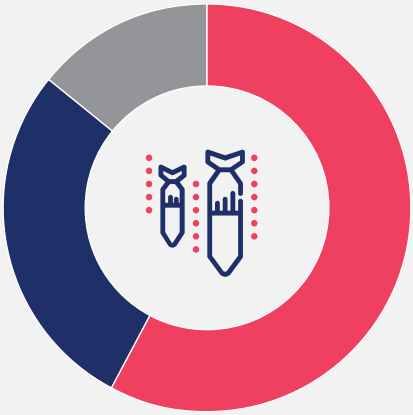
year	< 15 min	15-60 min	1-4 hours	> 4 hours
2017	37,4%	41,2%	18,3%	3,4%
2018	34,4%	45,9%	16,6%	3,1%

The maximum duration of a DDoS attack in 2018 was more than a day, as it lasted 29 hours. In 2017, the maximum duration was 23 hours. Multi-day attacks have not been detected since 2016.

2017 - 2018 top 10 duration (min)

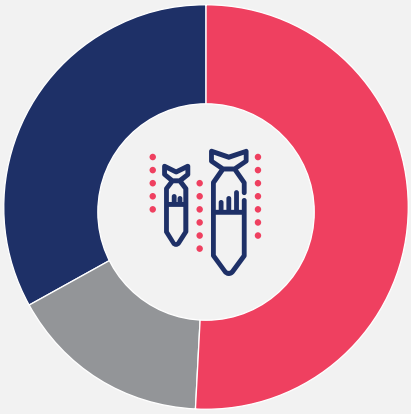


DDoS type main groups



28% TCP flood
58% UDP amplification
14% UDP flood

DDoS type main groups



23% TCP flood
51% UDP amplification
16% UDP flood

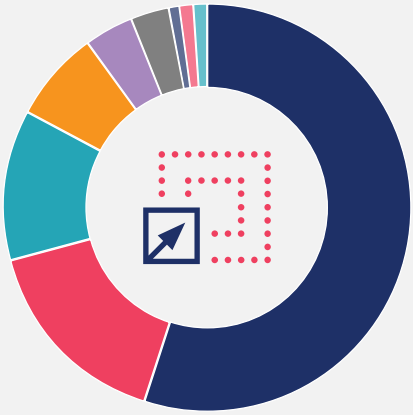
4.4 Types of DDoS attacks

In 2017, we observed 46 types of DDoS attacks. In 2018, this number increased to 56 types of attacks. We usually divide them in three main groups: UDP amplification, TCP flood and UDP flood.

Still more than half of the attacks are UDP amplifications, although that number dropped by 7 percentage points. The percentages of the rest of the attacks (TCP floods and UDP floods) therefore increased in 2018.

In 2018, still more than half of the attacks are UDP amplifications

UDP amplification DDoS-types 2017

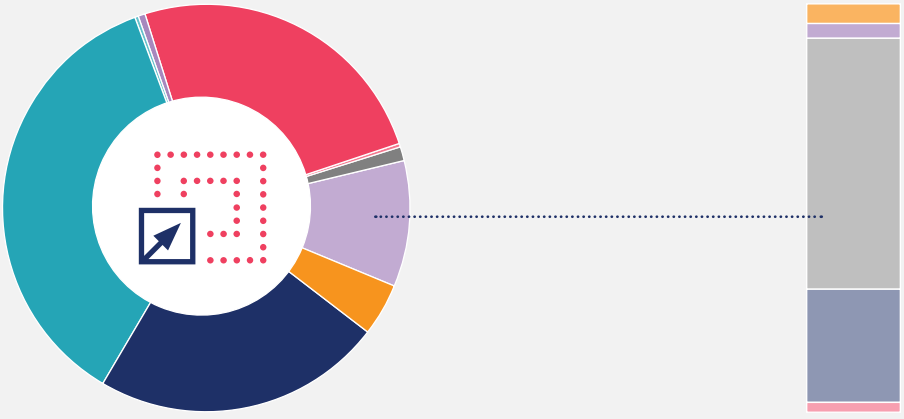


55%	DNS	3%	SSDP
16%	NTP	1%	RIPv1
12%	LDAP	1%	RPC port
7%	Chargen	1%	SNMP
4%	Netbios		

Within UDP amplification there is a wide variety of attacks, as can be seen in these graphs.

In 2017 there were 9 types of UDP amplification to be seen, in 2018 this number has risen to 11 types. Which wasn't a surprise, as the overall total of types have increased (from 46 to 56). Within UDP amplification, LDAP amplification is the most common DDoS attack with 36%.

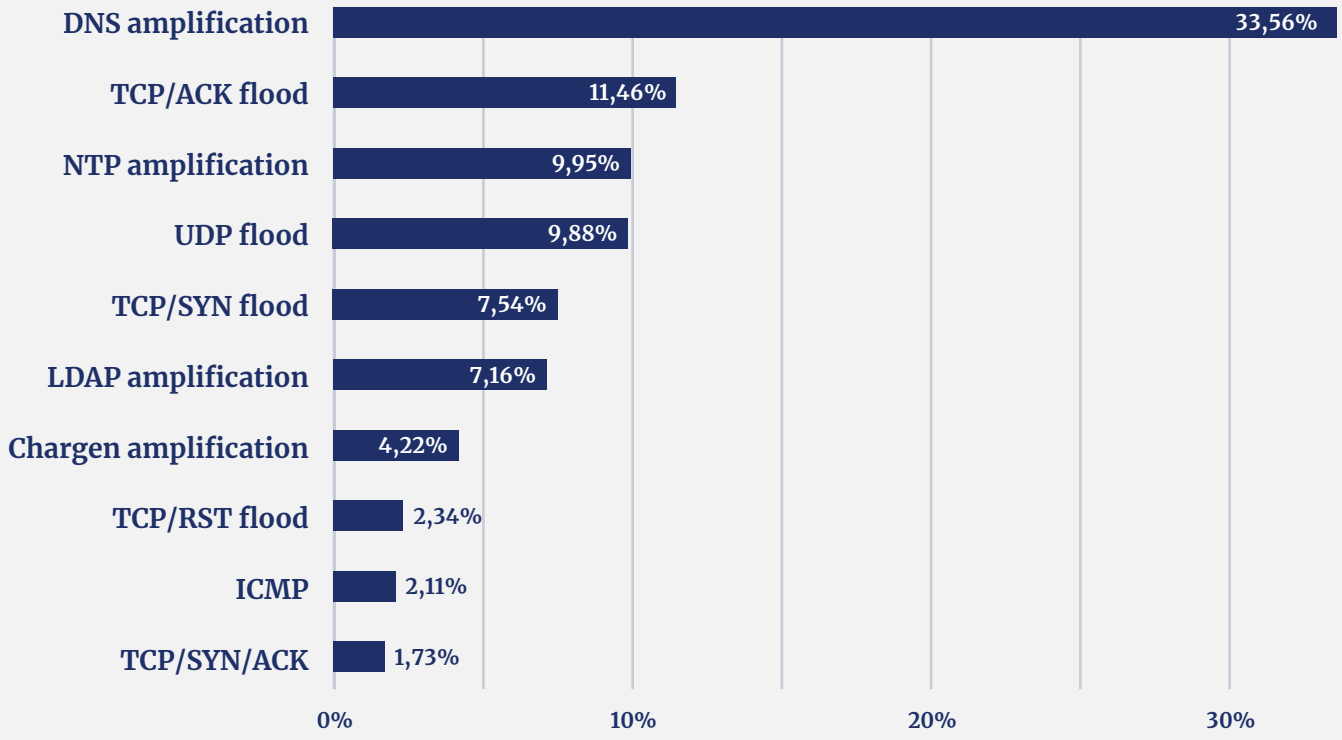
UDP amplification DDoS-types 2018



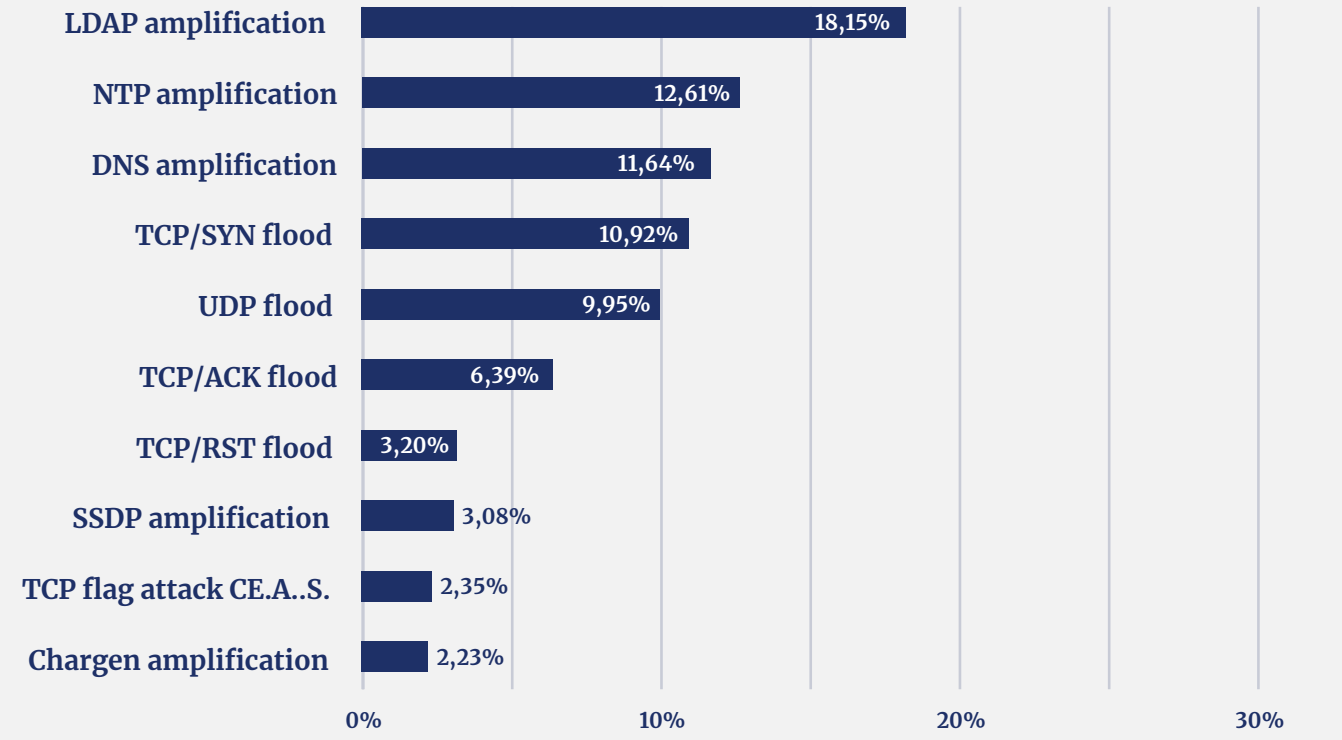
36%	LDAP	1%	RPC port	0,5%	UDP memcached
25%	NTP	0,5%	Netbios	0,4%	UDP flood
23%	DNS	0,4%	MS SQL monitor	6%	SSDP
10%	Other	0,1%	RIPv1	3%	SNMP
4%	Chargen			0,1%	Sentinel

This also means that LDAP amplification dethroned DNS amplification:

DDoS-type top 10 2017



DDoS-type top 10 2018



DNS amplification in 2017 was the most used DDoS attack with a 33% share. In 2017, LDAP amplification was still in 6th place.

Multivector attacks, where multiple types of attacks are packed together, are still present. Usually this is a 'simple', heavy attack type combined with a small, advanced type of attack. NBIP does not expect this form of DDoS attack to disappear quickly - on the contrary, there is even a trend (see section 4.6).

4.5 Notable DDoS attacks

In addition to the common types of attacks, we also saw some interesting and notable DDoS attacks in 2018.

STUN servers

It was notable that at one of the participants of the NaWas a remarkable number of different IPs contacted a STUN server, which happened at irregular times. This traffic was not filtered by our systems but nevertheless made us curious.

After some research by the participant it appeared that the STUN server was used by a cryptocoin to validate public IP addresses. Cryptocoins usually use a number of websites to do this (showmyip.com for example). Due to privacy and decentralisation, open STUN servers are used for this purpose. These requests are legitimate.

Geoblocking

In one very small attack with a very low bps (bits per second), the standard anti-DDoS measures could not be used properly. This was because the distinction between DDoS and legitimate traffic was too small. At that time, effective filtering was applied based on geographical IP blocking or geoblocking. This way of mitigating is efficient, but not subtle, as we discussed in chapter 2. With geoblocking the traffic is stopped based on the (IP) location from which it is sent.

So sometimes it is necessary for a scrubbing centre to use this method of mitigation.

4.6 New types of DDoS attacks

In 2018, almost 40 DDoS attack types were added. In most cases, however, this concerns an existing attack that attacks another specific port. If we filter these attacks, there was an increase of 10 new types of DDoS attacks.

> In 2018, almost 40 new DDoS attack types were added

The most striking newcomers compared to 2017:

MS SQL monitor amplification; abuse of a Microsoft SQL server environment - an old form of DDoS attack, especially popular around 2015. Many SQL servers were internet-facing, which made them vulnerable to botnets, among other things. The fact that this attack is resurfacing indicates that companies still do not have their basic security in order - because MS SQL is an old technique. It is a common practice in DDoS attacks: legacy that is no longer updated or patched is vulnerable, and it is therefore scanned to see if there is anything to be gained. This is known as 'knocking on the door'.

ESP flood is an attack in which the UDP Encapsulating Security Payload protocol is a protocol for providing authentication of data and payload network packets in IPv4 and IPv6 networks.

5. Trends

We also spotted some trends outside the analysed data.

Smaller DDoS attacks and memcached

Despite some large DDoS attacks (> 40 Gbps), the trend is that attacks are mostly shifting towards smaller attacks (also in pps, packets per second). We saw smaller quantities of packets that were just enough for a web server to fail.

The attack which had to be solved with geoblocking, as discussed in section 4.5, is a form of such a very small attack. This is a memcached-attack, a trend that we already saw emerging last year, but which is now becoming more common.

It was also striking that a few relatively small attacks, which should normally be handled by a web server (farm), still disrupted the web server.

Multivector

Multivector attacks continue to increase in number. The maximum number of simultaneous type DDoS (multi-vector) attacks in 2017 was the same as in 2018: the record is still 13 types. In 2018, 358 of 938 (38%) were multi-vector attacks. In 2017, this was 262 out of 826 (31%).

DDoS attacks worldwide

Kaspersky Lab research into DDoS attacks in 2018 shows that the number of attacks worldwide has dropped by 13% - while in the Netherlands we have seen an increase of 13%.

> Worldwide the number of DDoS attacks have decreased; but they have increased in The Netherlands

Kaspersky Lab states that this is mainly due to longer DDoS attacks. We have not been able to observe this significantly in the Netherlands. A cautious explanation for this worldwide trend in 2018, in our opinion, is that a considerable number of botnets was taken down.

Despite the fact that DDoS attacks were treated more seriously by companies and cyber criminals or bored youngsters were punished more severely by authorities, the number in the Netherlands has not dropped. The growth was less, however, and especially in the second half of 2018 this growth did not continue. This fits the picture that early 2018 there was a lot of attention, then other young people tried it out because of the attention, and then it wasn't that fun when the punishments came. In our first semester 2018 report, we stated for good reason that we would see over a thousand DDoS attacks in 2018. Fortunately, that number has not been reached.

6. Conclusion

Based on the research results, the NBIP draws four conclusions, which we will bring together in one overall conclusion about the state of DDoS attacks in the Netherlands.

Large attacks (> 40Gbps) are back, but most attacks are significantly smaller. It's no suprise large attacks are back: the number of attacks increased, in every size and duration. The tendency is still that attacks are just big enough to be disruptive. The percentage of attacks below 1 Gbps increased the fastest.

The duration of the longest attack has increased slightly. In 2017 there was no attack over 24 hours, in 2018 there were four DDoS attacks that lasted longer than 24 hours. There is no immediate explanation for this, other than that these longer attacks proved to be effective at the beginning of the year. A number of organisations did not have their systems in order, which meant that they could be "switched off" for a longer period of time.

A new type of DDoS attack is the most popular among cyber criminals: LDAP amplification. In 2017, DNS amplification was the most popular - and this may have led to action by companies. "Open" DNS servers, which are abused for an attack, are now better protected. For a number of years now, various parties such as NBIP and SIDN have paid a lot of attention to securing the DNS infrastructure. So most likely, the "open" LDAP server has emerged as the new easy target.

Last year, we stated that DNS will remain in the lead for a while, because it is the easiest DDoS attack to carry out. Now that old LDAP servers seem to be the biggest target, we hope that the same attention will be paid to securing LDAP servers as to DNS servers.

> Continuously changing DDoS attacks show us that this threat has matured

In addition, the number and percentage of multivector attacks is rising again. The trend of complex attacks continues and that makes defending them more difficult, despite all the attention for DDoS attacks.

DDoS: a mature threat

The technology of DDoS attacks is constantly changing. They are getting smaller and smaller, just big enough to be disruptive, and are often put together rather professionally. The rise of multivector attacks continues the trend of complex attacks. Together, this still makes fighting DDoS attacks very difficult. Continuously changing DDoS attacks show us that this threat has matured. A mature threat that, ironically enough, often does not come from adults. Fortunately, the response to a DDoS attack is becoming more and more stringent. A sign that DDoS attacks are finally taken seriously.

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

CharGEN amplification

CharGEN is a very old protocol which can be exploited to execute amplified attacks. In such

an attack, small packets carrying a spoofed IP are sent to a server, through internet enabled devices running CharGEN. Most internet-enabled printers and copiers have this protocol enabled by default. The server then faces a UDP flood. The server will eventually exhaust its resources and go offline or reboot.

DNS amplification

The attacker sends a DNS look-up request using the spoofed IP address of the target to vulnerable DNS servers. Most commonly, these are DNS servers that support open recursive relay. The original request is often relayed through a botnet for a larger base of attack and further concealment. The DNS request is sent using the EDNS0 extension to the DNS protocol allowing for large DNS messages. It may also use the DNS security extension (DNSSEC) cryptographic feature to add to the size of the message.

LDAP amplification

With LDAP amplification, a specific weakness (the CLDAP protocol) of older, still in use LDAP servers is abused. Originally to see what services are available on an internal network server, some servers have the UDP port 389 open.

MS SQL monitor amplification

This concerns abuse of a Microsoft SQL server environment - an old form of DDoS attack, especially popular around 2015.

Many SQL servers were internet-facing, which made them vulnerable to botnets, among other things. The fact that this attack is back again indicates that companies still do not have basic security in order. It is a common practice in DDoS attacks: legacy that is no longer updated or patched is vulnerable, and it is therefore scanned to see if there is anything to be gained. This is known as 'knocking on the door'.

Netbios amplification

NetBIOS is a protocol used in computer software to allow applications to talk to each other via LAN networks. The main victims of Netbios amplification were targets in the gaming and Web hosting sector.

NTP amplification

NTP amplification is a type of DDoS attack in which the attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.

Network Time Protocol (NTP) is one of the oldest network protocols, and is

used by Internet-connected machines to synchronize their clocks. In addition to clock synchronization, older versions of NTP support a monitoring service that enables administrators to query a given NTP server for a traffic count. This command, called "monlist," sends the requester a list of the last 600 hosts that connected to the queried server. Since the return address has been spoofed, the target of the attack therefore receives an enormous amount of data to process.

RIPv1 amplification

The Routing Information Protocol (RIP), helps small networks share network route information. It's been around since 1988, but has been deprecated since 1996.

To leverage the behavior of RIPv1 for DDoS reflection, a malicious actor can craft the same request query type as above, which is normally broadcast, and spoof the IP address source to match the intended attack target. The destination would match an IP from a list of known RIPv1 routers on the internet. Based on recent attacks, attackers prefer routers which seem to have a suspiciously large amount 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 map RPC service numbers to network port numbers. When RPC clients want to make a call to the Internet, Portmapper tells them which TCP or UDP port to use.

When Portmapper is queried, the size of the response can be up to an amplification of 20, but varies depending on the RPC services present on the host. Malicious actors can use Portmapper requests for DDoS attacks because the service runs on TCP or UDP port 111.

SNMP amplification

A SNMP (Simple Network Management Protocol) amplification attack works like a CharGEN attack, but instead connected devices that run SNMP are abused. The big difference: with SNMP the amplification is many times larger.

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, allowing spoofing and amplification.

(UDP) memcached

Last year, the NBIP saw memcached attacks appear. These are very small DDoS attacks that also last very short and abuse the memcached protocol. Normally port UDP/11211 should not be open to the internet, but if it is, then the attacks can be greatly amplified.

Floods

ESP flood

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

GRE flood

In a GRE flood, a large number of packets of the Generic Routing Encapsulation protocol are sent to a server. Normally, a firewall has to capture these, but the amount of GRE packets is so high that the server cannot handle them. 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 yet still very popular Denial of Service (DoS) attacks. The most common attack involves sending numerous SYN packets to the victim. The attack in many cases will spoof the SRC IP meaning that the reply (SYN+ACK packet) will not come back to it.

The intention of this attack is overwhelm the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size.

As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet.

Unlike other TCP or application level attacks the attacker does not have to use a real IP; this is perhaps the biggest strength of the attack.

UDP flood

UDP flood is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.

The receiving host checks for applications associated with these datagrams and - finding none - sends back a “Destination Unreachable” packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients.

ICMP flood

Internet Control Message Protocol (ICMP) is a connectionless protocol. An ICMP Flood attack - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing “ping” packets) - can overwhelm a target server that attempts to process every incoming ICMP request.

DNS request flood

One of the most well-known DDoS attacks,

this version of UDP attack is specifically aimed at DNS servers to attack web servers, among others. It is also one of the toughest DDoS attacks to detect and prevent. To execute, an attacker sends a large amount of spoofed DNS request packets that look no different from real requests from a very large set of source IP. This makes it impossible for the target server to differentiate between legitimate DNS requests and DNS requests that appear to be legitimate. In trying to serve all the requests, the server exhausts its resources. The attack consumes all available bandwidth in the network until it is completely drained out.

NBIP nationale beheersorganisatie internet providers

For more information:
www.nbip.nl