The impact of DDoS attacks on Dutch enterprises.

Report by NBIP | SIDN

NBIP nationale beheersorganisatie internet providers

SIDN Jouw wereld. Ons domein.

Contents

1 Preface

Long ago, the name ‘DDoS attack’ was something for ICT staff to deal with. A number of incidents has changed this: a massive DDoS on Dutch Banking Services in 2013 and large scale attacks aimed at Dutch services in January 2018. The latter affected the entire country. Both caused a great deal of commotion, and the subject was widely discussed on Dutch TV programmes. There were rumours of a Russian counter-attack or someone who was structurally trying to shut down all internet services. However, it turned out to be an 18-year-old young man who ordered targeted DDoS attacks for the sheer fun of it.

The risks of such DDoS attacks are perpetuated by low costs for cyber criminals and the simplicity of carrying out DDoS attacks. However, what is the actual impact of DDoS attacks on the Dutch economy? NBIP has provided anti-DDoS services for its participants since 2015 through NaWas (Nationale Wasstraat/Dutch National Scrubbing Centre). Mitigating large or complex attacks is part of our everyday business. Due to its unique profile, NBIP knows the power of working together and sharing knowledge.

NBIP teamed up with SIDN to realise an ambitious plan aimed at answering relevant questions about DDoS attacks:

- How many companies were targeted by a DDoS attack in 2017?
- How large was the potential damage in relation to the turnover of these companies and the duration of the attacks?
- Which sectors were the most frequent target for DDoS attacks in 2017?
- How many of the of the companies operating in the .nl domain space are protected by NaWas?
- What percentage of the online economy do these companies represent?
- What is the direct and indirect (collateral) damage?

Acquiring this information is not easy. However, with this report, we aim to provide some initial relevant answers to these questions and a fresh perspective on this complex technical subject.

2 Introduction

A Distributed Denial of Service (DDoS) attack is an attack on a system from multiple sources aimed at making the system unreachable to its users or audience. Since its first appearance in 1988 , DDoS has further evolved and is now an almost continuous source of irritation for website owners, users and system administrators around the world.

Most literature on DDoS focuses on the technical aspects of the attack and the defensive measures available. Some defensive measures function without a conscious effort on the part of the system owner, who is often unaware that the attack has taken place unless it is successful.

Many system owners therefore tend to underestimate the risk of being affected by DDoS. Small business owners do not perceive DDoS to be a threat, as they consider themselves to be 'below the radar' for perpetrators. Also, a customer who tries to realise a transaction during a DDoS attack may or may not return, but will seldom contact the system owner to complain. The actual extent of damage to the owner is therefore obscured.

3 About NBIP

NBIP – founded by ISPs
NaWas is an initiative of the Dutch National Internet Providers Management Organisation (Dutch acronym NBIP). This non-profit foundation was established by Dutch ISPs to meet the lawful interception requirements stated in the Dutch Telecommunications Act. It now supplies services to over 100 ISPs and VoIP providers in and outside of the Netherlands. For further information about NBIP see www.nbip.nl

NaWas
NaWas (Nationale Wasstraat/ 'National Scrubbing Centre') is a full-service, on-demand protection against DDoS attacks provided by NBIP. NaWas was developed and built with state-of-the-art, anti-DDoS equipment and is centrally located in the Netherlands. In the event of an attack, the network traffic is routed through the NaWas scrubbing devices. NaWas recognises and cleans the traffic of any malicious packets. It then forwards the clean traffic on a separate VLAN to the client.

4 About SIDN

SIDN
SIDN registers and manages .nl domains. SIDN shares its knowledge and develops new services, and it supports initiatives aimed at making the internet better and safer. SIDN works to ensure sure that you can have confidence in your digital world. It delivers high-quality services linked to innovative, secure domains and digital identities.

SIDN Labs
SIDN Labs is SIDN's research and development team. It develops prototypes and tests new technologies and systems. The work of SIDN Labs helps to increase the security and stability of .nl domains, the Domain Name System and the infrastructure of the internet. SIDN Labs often works with other companies and research institutes, including the University of Twente, Delft University of Technology, TNO and NLnet Labs.

5 Data collection

NBIP has recorded all types of DDoS attacks that have occurred against NaWas participants. Types of DDoS attacks were procedurally documented within the operational team of NaWas. Data was then selected from this registration system for reporting purposes.

NaWas data
The data originated from attacks on NaWas participants. However, not every participant had to deal with a DDoS attack. Data from participants in the NaWas were analysed for this study. When this report was published, there were 67 participants, and most of them were 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 provide cloud and hosting services.

NaWas participants are not limited to ISPs, but also include large and medium-sized businesses.

DDoS and Domain Name data
Data from NBIP and SIDN were combined. This enabled us to analyse a large volume of DDoS attacks aimed at websites using a .nl domain name over a twelve-month period. Through NaWaS, NBIP protects 43% of all .nl domain names. The data therefore covers a significant proportion of websites in the Netherlands. Although the results are not a complete picture, they nevertheless provide valuable insights for professionals involved in fighting DDoS and are a stepping stone for further academic research.

› Chart 1: nl space, domains protected by NBIP and total number of DDoS attacks that occurred

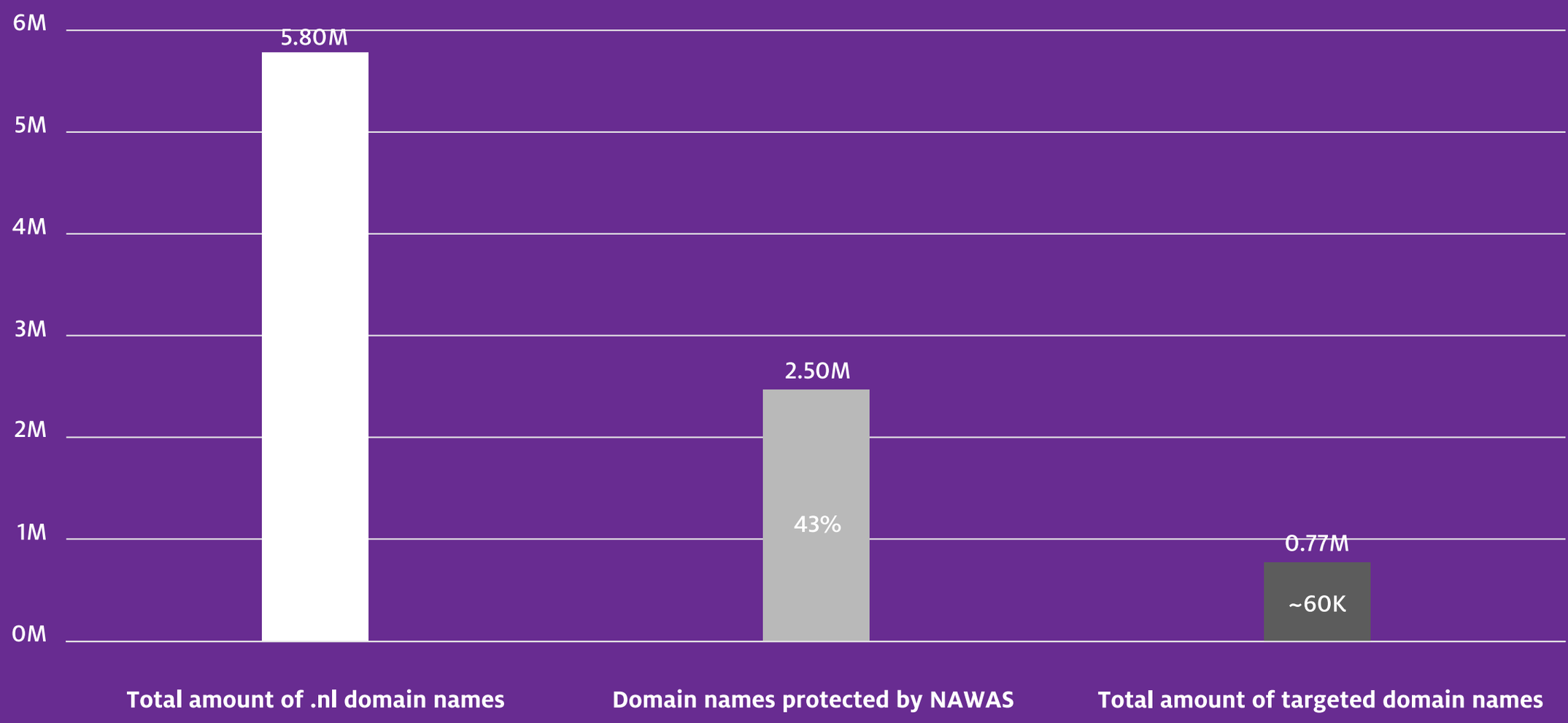

Chart 1: .nl space, domains protected by NBIP and total number of websites attacked

6 Methodology

The data provided by NBIP identifies 82,981 prefixes belonging to autonomous systems (AS) hit by 237 DDoS attacks between the 1 July 2017 and 30 June 2018. These autonomous systems can be linked to DNS records belonging to .nl domains available at SIDN, the registry for all .nl domains. The DNS data provides a crucial insight: it enables us to distinguish the actual targets from the indirect targets or collaterals (the term used throughout this report). We make this distinction by looking at the impact on DNS traffic. For each DDoS attack, we calculated the average amount of traffic three days prior to and three days after the DDoS attack occurred.

The domain name data enables SIDN to check the owner profile (company, private individual, chamber of commerce listing, etc.) and crawl the content of the accompanying website using a 'crawling spider' (What is the company selling? Is there an active web store? etc.). The website is where the actual company hit appears and where we can look into the potential damage caused by the attack.
> Table 1: Data sources used and their input

We use the term potential damage here because it is impossible to determine precisely how successful each of the DDoS attacks was and since NaWas protected the domains there is a high chance the attack was fended off. Our estimate of what the damage would have been is therefore based on missed revenue, as it is impossible to tell from the data what the additional costs per website or the costs of finding the perpetrator were. This calculation is based on revenue per year, online turnover, timeframe and duration of the DDoS attack.

We then enriched our dataset with external data (chamber of commerce, company information) to create a financial context for each domain. For each company, we looked at the annual turnover, net value and FTEs. If the annual turnover was not stated, we made an assumption about the annual turnover based on the net value and/or FTEs. In cases where a domain was hit by a DDoS attack, we assumed that the affected company would have suffered a day of revenue loss. This loss cannot be verified of course and so the outcome should be treated as an indicative effort to quantify the impact.

This report only covers websites with a .nl domain name and therefore not all autonomous systems in the Netherlands. It is essential to make that distinction as in some sectors the share of .nl is relatively low (gaming, gambling, adult content) and so these sectors are underrepresented in the data. The same holds for larger parties working with commercial suppliers such as Akamai. As these parties have not provided data, valid statements about the part of the internet covered exclusively by these parties cannot be made.

Before this report was published, we held several expert interviews to gain additional insights regarding our findings. These experts are not responsible for the content of this report but have helped us to enhance it.

NBIP data	DNS data	Domain name registration	Content crawling	Chamber of Commerce
IPs targeted and prefix sources. Time and date of the attack	Collateral or intended target Name servers Type of hosting	Owner data Date of registration Location of company	Use of website Web store Sector	Turnover FTEs Industry Age of company

Table 1: Data sources used and their input

7 Types of DDoS

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server. It is distinct from other Denial of Service (DoS) attacks, in that it uses a single Internet-connected device (one network connection) to flood a target with malicious traffic. There are three types of DDoS attack:

Volume-based attacks
A volume-based attack is where the attacker saturates the bandwidth of the attacked system (website) with traffic.

Protocol attacks
Protocol attacks consume server resources, e.g. firewalls and load balancers. These are also known as state exhaustion attacks.

Application layer attacks
Application layer attacks target vulnerabilities in web servers or online applications with a flood of requests. The goal is to crash the web server. These are also known as layer 7 attacks.

8 Distribution of DDoS across Dutch enterprises

When analysing our data, we classified domains based on content. Looking at the intended target (Chart 2) we observed that most DDoS attacks were aimed at the education (schools, colleges) and entertainment (festivals, events) sectors.
> Chart 2: Intended target of DDoS attacks per sector

Education and No More DDoS
In education, the perpetrators we know of are often students looking to evade an exam. A seemingly innocent prank, but one that costs schools time and resources to find and suspend the perpetrator. The Dutch government has set up the multidisciplinary No More DDOS project specifically for this group. The project has a multidiscplinary setup involving among others the police and Twente University. It is based on five pillars: building a knowledge platform, sharing knowledge and information, improving digital research, alternative interventions and communication.

Intended and collateral targets excludes the websites hit as a result of collateral attacks. Chart 3 shows the combined number of intended and collateral DDoS attacks and the results are more spread out than in Chart 2. With adult sites having the highest chance of being hit. This spread is mainly the result of shared hosting. Therefore you do not necessarily have to be a high profile company to be a victim of a DDoS attack. Previous research done by SIDN revealed that 7% of businesses in the Netherlands had dealt with DDoS attacks and that 42% of companies with 250 or more employees have dealt with DDoS attacks. In general, DDoS attacks are perceived to be almost as threatening as phishing attacks.[1]
> Chart 3: Intended targets and collaterals of DDoS attacks per sector

[1] Source: Trends in Internet Use SIDN, 2016

"SURFnet develops, implements and maintains the national research and education network (NREN) of the Netherlands. As such we play a vital role in preventing DDoS attacks from harming the sector. We encourage our member] to actively look for the perpetrator and, in case it is a student, engage with them. Dealing with the perpetrators is an addition to taking defensive measures and necessary to minimize] the impact of DDoS."

Wim Biemolt, *Surfnet*

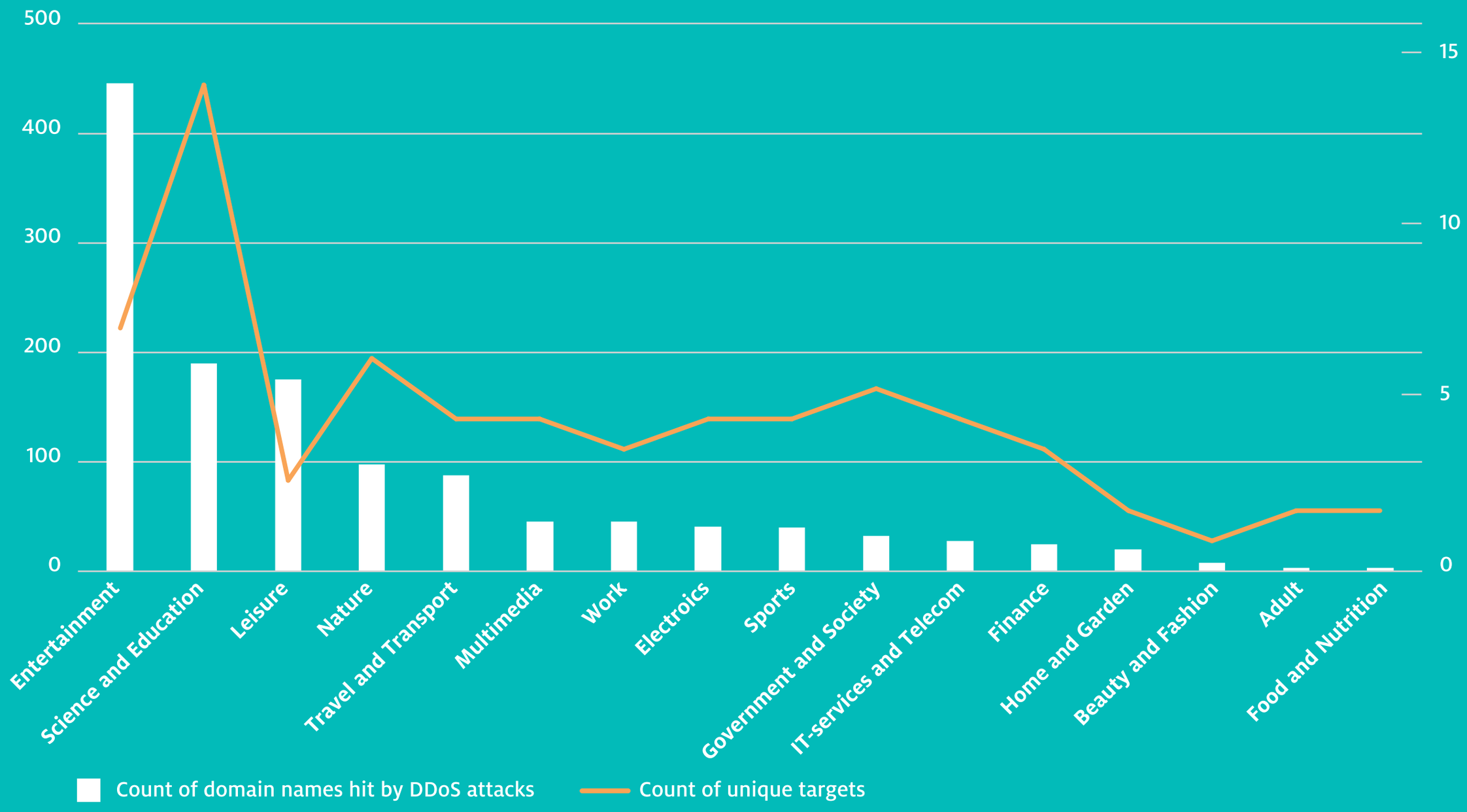

Chart 2: Intended target of DDoS attacks per sector

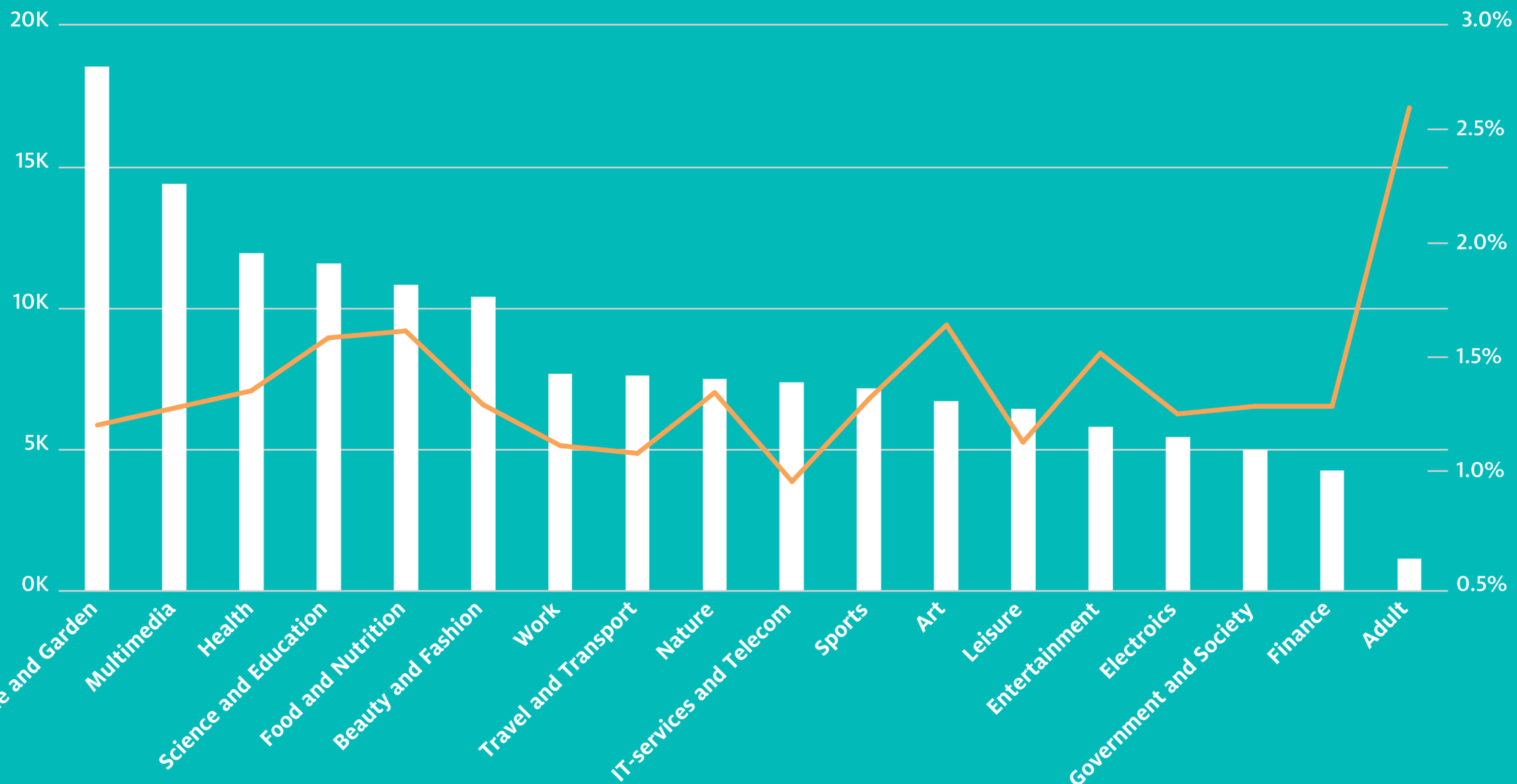

Chart 3: Intended targets and collaterals of DDoS attacks per sector

9 Impact on enterprises

The impact of DDoS on Dutch Enterprises is hard to determine. Most studies stay well clear of this question, as it is relatively complex and requires the combining of datasets. The experts we talked to while preparing this report distinguished the following factors that must be considered:

- Missed revenue;
- Cost of protective measures;
- Cost of finding perpetrators, forensic readiness;
- Reputation damage;
- Impact on society (e.g. the perpetrator in the justice system).

As stated earlier, we have used a relatively simple calculation based on potentially missed revenue. The result may not be accurate in absolute terms but provides valuable insights regarding patterns and differences between sectors, for example. As the data is biased towards SMEs, we will focus on these.

Total damage estimate

The damage estimate for all websites listed in the available data adds up to € 425,000,000 (see Chart 5). As our data covers 43% of the .nl domains and the estimate is based solely on missed revenue, we estimate the total potential damage to Dutch companies to be more than a thousand million euros. This figure covers 237 recorded attacks. Therefore the amount of damage per attack is approximately € 1,800,000.
Chart 4 shows the distribution of revenue for intended targets. The highest average revenue (almost 400 million euros) is sustained by companies classified as Travel and Transport (travel websites). Our data set also contained some highly valuable Finance as well as Government and Society targets, though many of those use commercial scrubbing services of which we do not posses the data.
Chart 4: Average annual revenue of intended targets DDoS

Based on the turnover of companies and the frequency of DDoS attacks, we estimated the financial impact per sector
Chart 5: Impact of DDoS per sector

Variation between sectors

The most valuable insight is the large variation in collateral damage and direct attacks between sectors. Some sectors tend to be targeted almost exclusively directly and others mostly as collateral. For example, websites in the Home and Garden category (garden centres and DIY stores) suffer more collateral damage than any other sector. For some sectors it is difficult to gauge the damage, as few revenue figures are known (e.g. adult content).

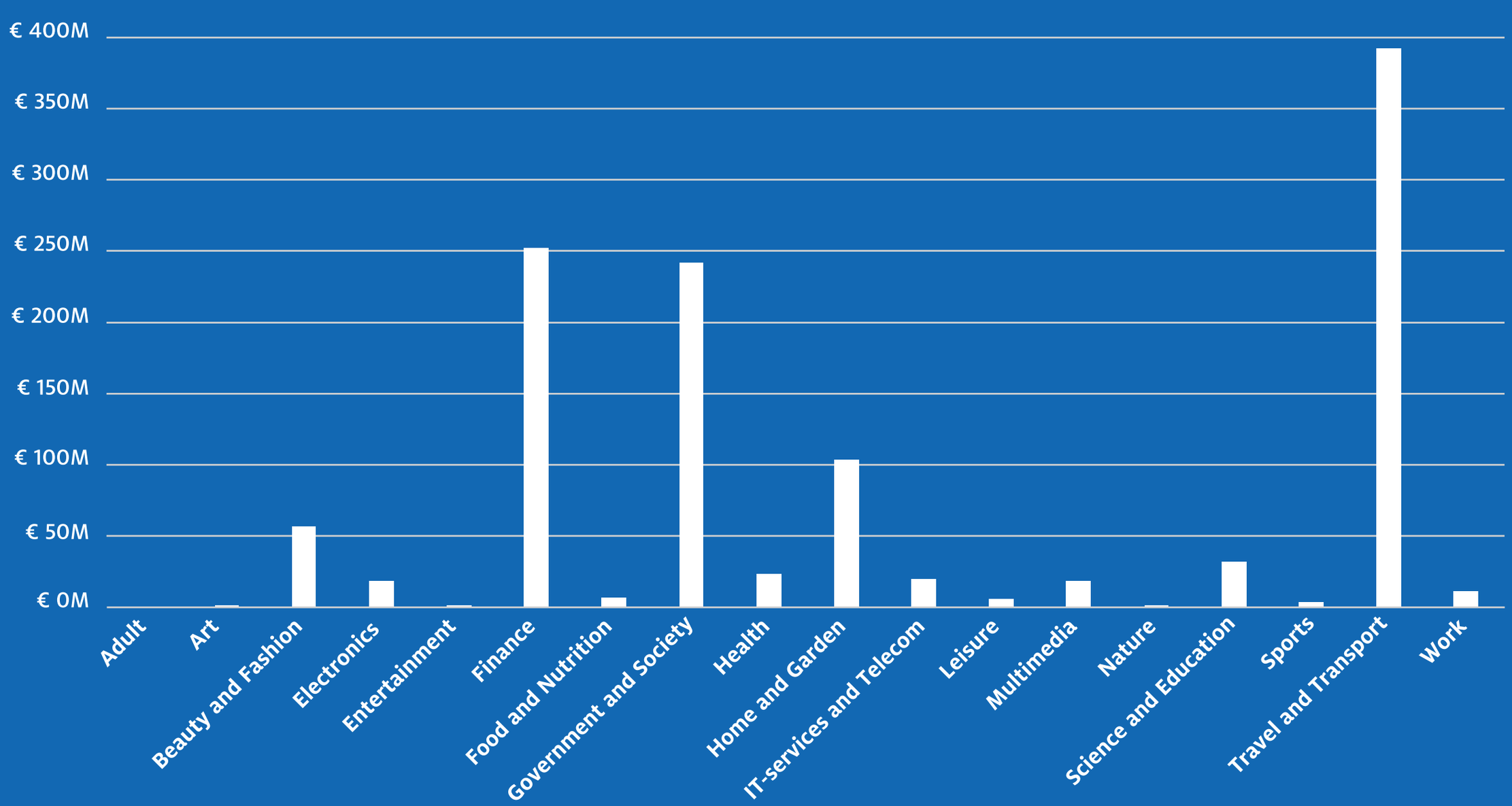

Chart 4: Average annual revenue of intended targets DDoS

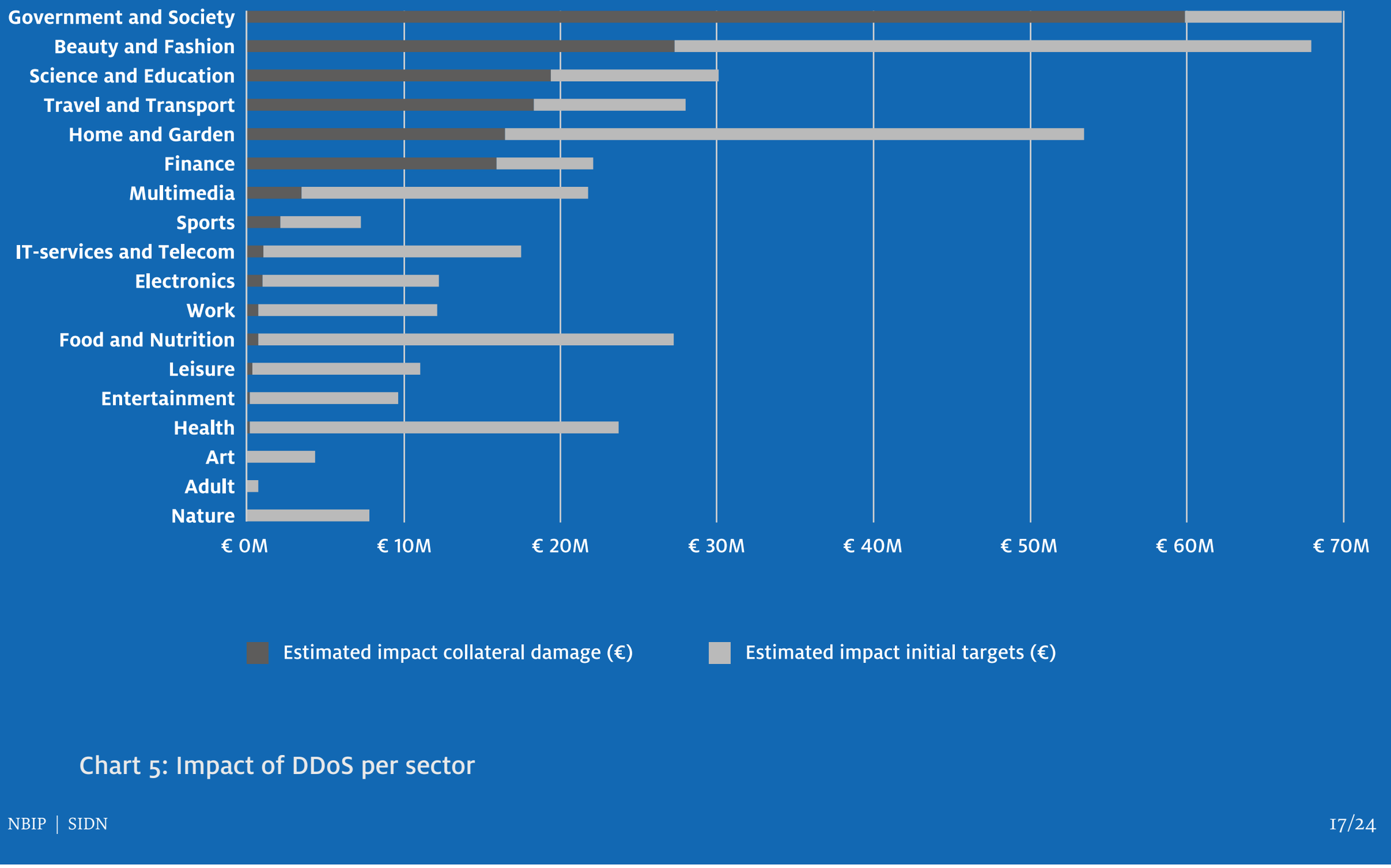

Chart 5: Impact of DDoS per sector

10 Online stores often indirect targets

DDoS is often associated with larger organisations and therefore overlooked as a potential risk by small businesses. Often, however, these businesses are targeted indirectly as collateral. When looking into small and medium-sized web stores (overrepresented in the data), it appears that 70% of all attacks are 'collateral'. For this group, the probability of suffering collateral DDoS damage is significantly higher than the probability of being the intended target.

Chart 6: Probability of collateral damage versus intended target (web stores)

Peak season

The potential damage for online stores is, of course, significantly higher when an attack occurs during the peak sales season. Cyber criminals are, for example, known to use the busy December month to launch fake online stores. When we look at the seasonal figures for DDoS attacks, a similar picture emerges, namely a huge peak in December (Chart 6). An interesting follow-up question here is: What is the intention of these attacks? Is it to deny competitors revenue? Or is blackmail, often seen in the financial sector, a motive?

Chart 7: Domain names hit by DDoS attacks: seasonal trends (excluding parking pages, placeholders)

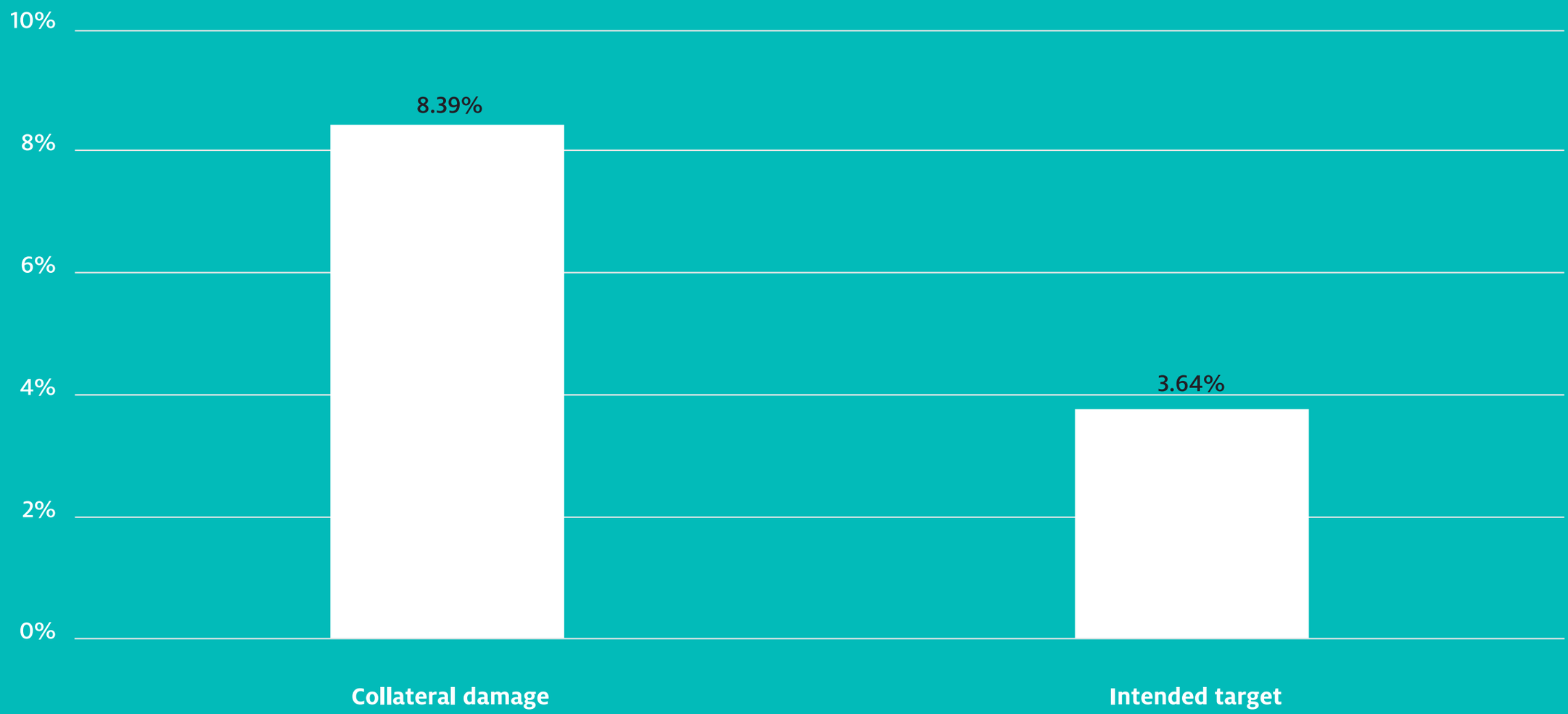

Chart 6: Probability of collateral damage versus intended target (web stores)

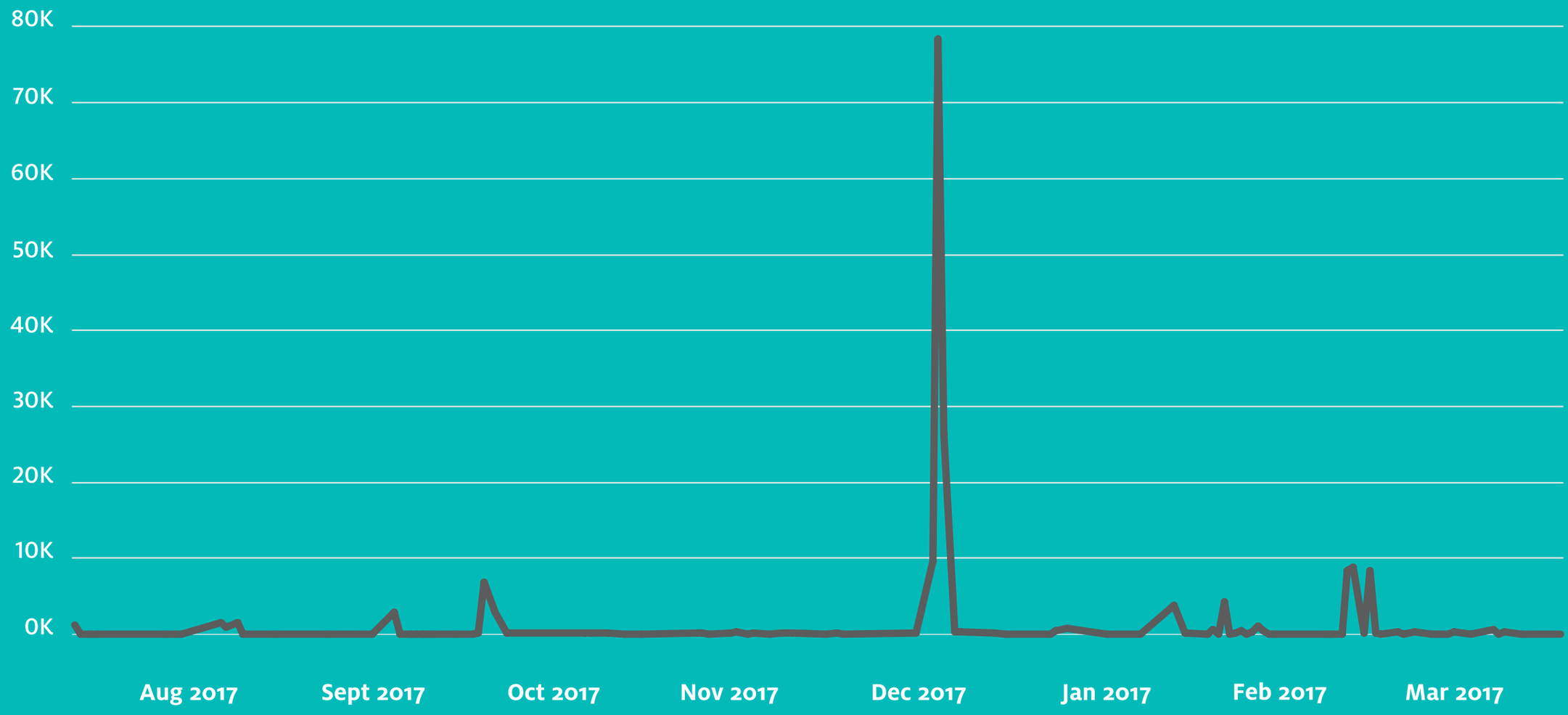

Chart 7: Domain names hit by DDoS attacks: seasonal trends (excluding parking pages, placeholders)

11 DDoS & hosting type

A next logical question is whether certain hosting types are more vulnerable to attacks. In this report, we distinguish between shared hosting and other types (VPS, dedicated). Distinguishing these other types is not possible based on the available data. Shared hosting can be distinguished by looking at the number of sites per IP. If an IP address has more than ten unique domain names (excluding redirects) hosted we count this specific IP address as shared hosting. The category includes dedicated hosting and VPS. More data from top organisations with dedicated hosting would be a welcome addition to our dataset.

Shared hosting vulnerable

From the available data, we can conclude that shared websites are far more likely to be hit. This is hardly surprising, since DDoS attacks target IP addresses and shared hosting lets multiple sites use the same IP. We found IP addresses hosting as many as 240,000 websites at the same time.

So even though the number of unique DDoS attacks is split evenly between the different forms of hosting, the chances of being hit on a shared hosting platform are far higher. Hosting providers should therefore inform their clients that shared hosting, although cost-effective, may not be the best choice from a risk and security perspective.

Chart 8 illustrates that the chance of being hit by a DDoS attack on shared hosting is approximately 35 times higher than VPS/dedicated hosting.
Chart 8: Chances of being hit by a DDoS attack per hosting type

"The majority of companies nowadays have online activities that require cloud infra or hosting. Quite often, price is the leading criterium for selecting such services. But now that DDoS attacks are increasingly common, and the law requires personal data to be protected, security and the ability to mitigate attacks should have a much higher priority."

Michiel Steltman, *CEO DINL*

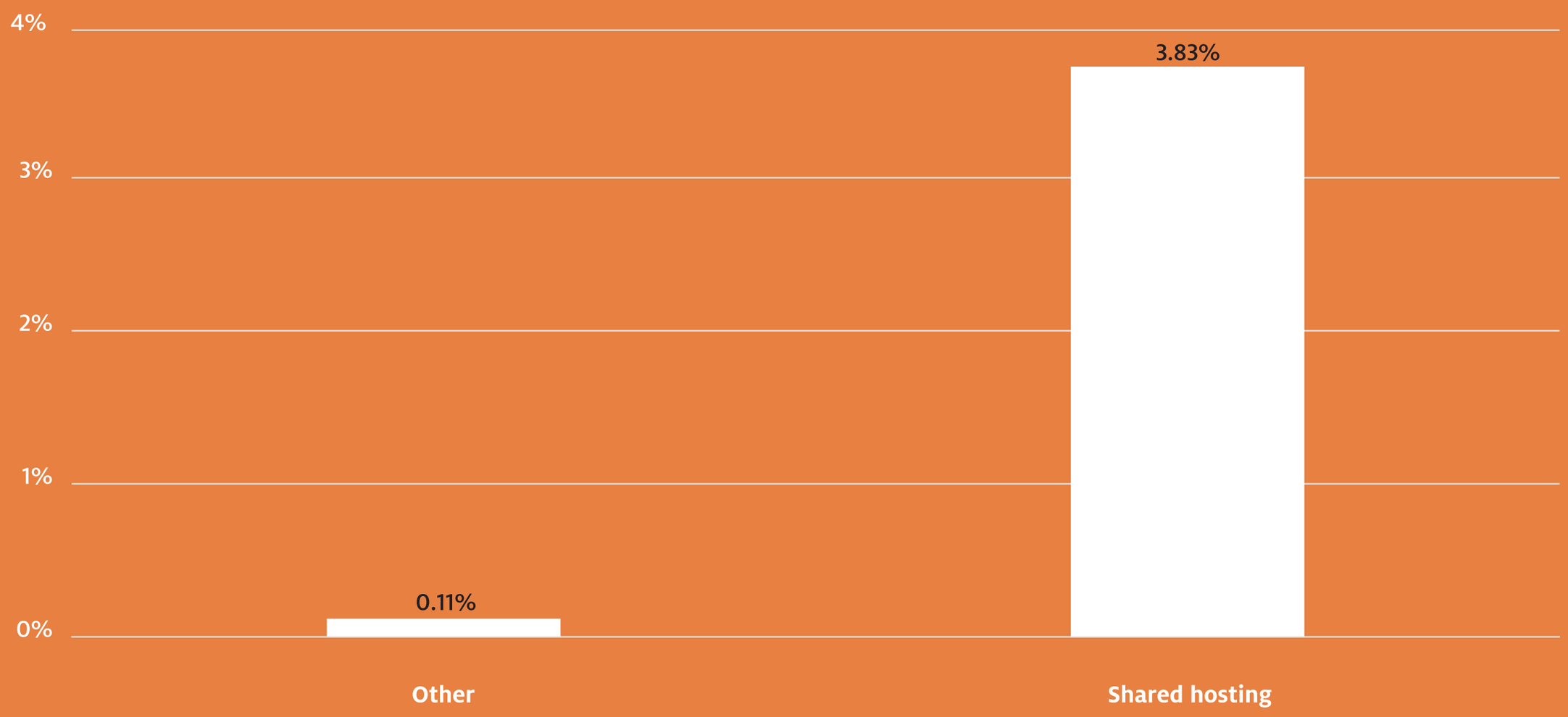

Chart 8: Chances of being hit by a DDoS attack per hosting type (Source: Statistics Netherlands)

12 Recommendations

Awareness
There are still many online businesses for whom hosting is a simple sum: capacity required versus price paid. Yet as our study shows, the cheapest option may not always be the best, as shared hosting significantly increases the chance of being hit by a DDoS attack. Hosting companies should consider their clients' interests in this respect and make them aware of this risk. We recommend offering an anti-DDoS solution as part of an integrated package. From a client perspective, a proactive attitude is also desirable. Ask your provider what measures they have taken in the field of anti-DDoS protection and check whether these are sufficient.

Perpetrators: patterns & motives
Our data focus on the target side and therefore have a blind spot with respect to the perpetrators. Nevertheless, several experts we spoke to recognise that differences between sectors, for example, may be explained by differences in perpetrators' motives. Finding perpetrators needs to remain a high priority, as our potential damage impact shows that DDoS is a phenomenon where much damage can be done with little effort.

Additional data analysis
As stated earlier: we consider this report to be a starting point for further research. NBIP and SIDN will continue to explore the available data and gain useful insights. We also invite third parties possessing similar data to join us or to conduct benchmark studies that will enable us to make better substantiated statements. Using our method, it would be relatively simple to conduct a benchmark study in other countries.

Follow-up research
We hope that this data will inspire others to initiate research of their own. Combining domain name and DNS data with data on reported incidents is a valuable way of gaining the insights needed to enhance our defences against DDoS attacks.

Together, smarter and stronger
This report once again shows the value of cooperation and knowledge sharing in the battle to make and keep the digital infrastructure of the Netherlands a safe place to do business. Only through radical transparent cooperation will we be able to create a sustainable solution against DDoS attacks. NBIP and SIDN support every broad-based initiative that enables parties to share knowledge and therefore to become stronger and smarter together.

Credits

Contributors

SIDN
Nick Boerman
Michiel Henneke

SIDN Labs
Dr Giovane Moura

NBIP
Gerald Schaapman
Octavia de Weerdt

SIDN & NBIP would like to thank the following experts for providing us with valuable feedback during the research and the writing of this report:

Dr Jair Santanna, *Lecturer, University of Twente*

Teun Vink, *Security Officer, BIT BV*

Michiel Steltman, *CEO, DINL*

Wim Biemolt, *Network Engineer, SURFnet*

Remco Ruiter, *Liaison Officer Dutch Payments Association*

If you have any questions about the NaWas or NBIP, please e-mail bureau@nbip.nl

SIDN
P.O. Box 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
The Netherlands
T +31 (0)26 352 55 00
www.sidn.nl

NBIP
P.O. Box 628
6710 BP Ede
The Netherlands
T +31 (0)318 48 93 50
www.nbip.nl