EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR DoS ATTACKS

January 2022 to August 2023

November 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use etl@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

EDITORS

Eleni Tsekmezoglou, Ifigeneia Lella, Apostolos Malatras, European Union Agency for Cybersecurity
Sebastian Garcia, Veronica Valeros – Czech Technical University in Prague

ACKNOWLEDGEMENTS

The authors would like to thank the Members and Observers of the ENISA Ad Hoc Working Group on Cyber Threat Landscapes for their valuable feedback and comments.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-647-7 DOI:10.2824/859909 TP-02-23-131-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Denial-of-Service (DoS) attacks have been a constant security concern for organisations. However, in the last few years, DoS attacks have become easier, cheaper and more aggressive than ever before. The emergence of new armed conflicts around the world acted as fuel to new waves of DoS attacks where newly formed threat groups pick and choose various targets.

This report aims to bring new insights to the DoS threat landscape. Through a careful analysis of the motivations and impact of DoS attacks, this report aids organisations to understand this threat and how to better protect themselves if they are ever a target. The insights shared in this report are the result of a thorough mapping and analysis of DoS incidents discovered from January 2022 to August 2023. The findings of this study show that, although all sectors are affected by DoS attacks, the most targeted sectors are those associated with government services, which seem to be time and time again selected as a primary target of DoS attacks, mainly motivated by retaliation against their political actions and statements.

The main highlights of the report are the following.

- A novel **classification scheme** to categorise DoS attacks based on information about the attacks and the targets, allowing a more systematic analysis approach.
- An analysis of **DoS attacks' motivations and goals** as part of the proposed classification, making it possible to analyse not only the technical evolution of the attacks but also the changes in the roots of what triggers the attacks in the first place.
- An analysis of a total of **310 verified DoS incidents** – from January 2022 to August 2023. This is not the total number of incidents during that period, however.
- The most affected sector was the **public administration** sector, receiving **46 % of attacks**.
- It is estimated that **66 % of the attacks were motivated by political reasons or activist agendas**.
- Overall, **50 %** of the incidents were found to be **related to the Russian war of aggression against Ukraine**.
- The study shows that **56.8 % of the attacks caused total disruption** in the target.

This report also highlights the importance of cyber as a force multiplier or supporting vector in warfare, the changes that this brings to the landscape, and that it is vital that organisations prepare prevention and remediation strategies. Furthermore, this report raises awareness of the lack of maturity when it comes to reporting DoS attacks, which have not reached the same level as other types of cybersecurity threats.

1. INTRODUCTION

DoS attacks have been very common since the beginning of computer networks[1]. These attacks traditionally require a low set of skills and tools, while preserving the anonymity of attackers and have a very noticeable and mediatic impact. From small grudges between users to large international financial fraud, DoS attacks have been a permanent tool in an attacker's arsenal.

Since the beginning of 2022, DoS attacks have turned into a novel massive threat using new techniques and fuelled by warfare motivations. The number of organisations and countries attacked grew, as did the aggressiveness of the attacks, and resilience proved hard to sustain. This increase can be attributed to the growing influence of hacktivism among groups opposing various regimes and the ongoing geopolitical tensions worldwide, which have intensified this trend on a larger scale[2].

On top of that, DDoS-as-a-Service offered by cybercriminals have contributed to the upsurge in the number of observed attacks. Thanks to this service model, launching a RDoS attack is increasingly simple, while it is still difficult to spot its origin. Spreading malware or ransomware instead requires an important effort in terms of time and planning[3].

This report offers a large-scale analysis of publicly reported incidents focusing on the motivations of attackers, their goals and the socio-political characteristics of targets.

Despite being mediatic and well known by the general public, DoS attacks are hard to identify as actual attacks, measure and report. There are four main reasons as to why this is. First, organisations may be unsure whether they are under a DoS or even whether it was an intentional attack or a technical problem. Second, the size of the attacks can be hard to measure since the same computers that do the measurement can be the target of the attacks. Third, it is difficult to evaluate the financial impact of having slow services for some customers or some web pages not working. Fourth, there are no technical artefacts, code or binaries left behind to analyse deeper, and the few available indicators, such as IP addresses, are usually not trustworthy. Overall, the effect of these issues can be seen in the lack of official databases or lists of confirmed DoS attacks and their characteristics.

To understand the reality of DoS attacks, this study relies on the three main public sources of DoS reports: (i) news media, (ii) organisations measuring DoS attacks and (iii) the claims of attackers. News media reports on DoS mostly focus on the fact that the attack happened, but rarely on their technical aspect. Organisations measuring DoS attacks often focus on the experience of a single protection company or the size of the attacks as a whole and do not often report on specific customers affected or individual incidents. Finally, the attackers' claims make tracking and verifying DoS difficult since they often may claim attacks that did not work, or an organisation may not notice an unsuccessful DoS carried out against them. Overall, there are few large-scale official reports analysing DoS incidents together with their motivations and impact. This ENISA report provides a non-comprehensive but high-level overview of the DoS attacks.

The goal of this report is to provide organisations with awareness of the **motivations** and **consequences** of DoS attacks to help them understand and suggest defence recommendations. To accomplish this, the report explores the threat landscape of DoS attacks from **January 2022** to **August 2023**, identifying attackers and defenders, motivations, impact, classification and characteristics.

[1] US Federal Bureau of Investigation, 'The Morris worm – 30 years since first major attack on the internet', 2 November 2018, accessed 5 September 2023, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
[2] ENISA Threat Landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[3] Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020, https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf.

2. METHODOLOGY

This report focuses on analysing DoS incidents following a strict research method that is grounded on the ENISA Cybersecurity Threat Landscape methodology[4]. The research method consists of **five steps.**

First, a search of DoS incidents was conducted using open-source intelligence tools and techniques. The search included all regions and involved incidents reported by news and media organisations, security companies and specialised DoS protection companies; official statements by target organisations; and reports by the attackers themselves. The technical information was often found on websites and social media sites, and in industry reports and Telegram channels. Although most information is available in English, many incident reports in other languages were translated into English for analysis. Furthermore, the Internet Archive[5] service was used to access news reporting websites that were no longer available due to technical changes.

Second, all incidents were stored and indexed by date, followed by a manual verification to ensure they were within the scope of this report. The scope is discussed further in the following sections.

Third, for all incidents within the scope of the report, research was done to find additional third-party reports to confirm that the attack occurred, dismissing all the attacks that could not be verified.

Fourth, each attack was analysed in detail to extract information later used in the global analysis of incidents. If translation was necessary, automated translation engines were used. For each incident, the following features were extracted: target(s) name, target(s) industry, target(s) country and starting date of the incident. Additionally, the following information was extracted about the attackers: motivation, goal, method of attack and high-level technique of the attack. See Section 3.1 “Classifying attack information” for a list of attack motivations, goals, methods and techniques. Furthermore, the following information was extracted about the target of the attacks: service targeted, resource targeted, disruption level and disruption length. See Section 3.2 “Classifying target information” for a list of target services, resources, disruption level and length. Finally, additional notes were taken on attribution and the type of conflict the attack was related to for those cases where the information was available.

Fifth, incidents that were found to be different in terms of socio-political context, technical prowess and disruption effect were marked as prominent. See Section 4 “Prominent incidents” for a deep dive into these incidents.

The final list of incidents produced by the presented methodology was dissected, aggregated, summarised and analysed to extract insights and conclusions.

2.1 WHAT IS A DENIAL-OF-SERVICE ATTACK?

An important part of this study’s methodology is the definition of what a DoS is. DoS attacks are defined, for this report, as **availability attacks in which attackers partially or totally obstruct the legitimate use of a target’s service by depleting or exploiting the target’s assets over a period of time**.

The analysis is limited to attacks with measurable success as DoS, and attempts at DoS attacks are not considered. However, many attempts failed because of good protection mechanisms. Therefore, the most significant unsuccessful DoS attempts as identified by DoS protection companies are also considered.

[4] ENISA Cybersecurity Threat Landscape Methodology, accessed 18 September 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[5] Internet Archive website, accessed 5 September 2023, https://archive.org/.

2.2 DIFFICULTIES IDENTIFYING A DOS ATTACK

There is a wide range of difficulties when it comes to determining what a DoS attack is. These same difficulties are often shared by organisations at the time of identifying and reporting these types of attacks. Contrary to other threats, such as ransomware, where there is total certainty that an attack happened, certainty is often elusive when it comes to DoS attacks.

The most frequent difficulties can be summarised as follows.

- DoS monitoring systems or computers can be part of the target of the DoS, stopping the monitoring of traffic and making it very hard to see the DoS attack. These attacks are successful but leave few traces behind.
- DoS attacks can start slowly, making it hard to identify organic traffic growth from an incoming attack. This makes it difficult to know when the attack started.
- DoS attacks often happen in bursts without a clear start and end. Due to the lack of a technical definition of when an attack stops, it is hard to quantify if it was one attack or many. In these cases, this study considers one attack as one attempt to take down a service.
- With web services often sharing IP addresses, one attack can take down multiple sites. From a mediatic perspective, these can be seen as multiple attacks, although in reality there was only one. In these cases, this study considered further evidence to evaluate whether or not the aim was to affect multiple targets, and indexed them as such.
- DoS disruptions may live longer than the attack itself since the computers or systems may stop working completely, making the length of the attack very hard to estimate.

The detection, description and analysis of DoS attacks is quite complex, and different from other cybersecurity attacks. In other types of cybersecurity attacks, such as exploitation of services or even supply chain attacks, the attackers leave artefacts behind that the incident responders can find, analyse, share, confirm, verify and ultimately use for explanation, or even for attribution.

DoS attacks are different since most attacks are network based, meaning there are no software artefacts left behind, and the security analysts only have many packets from thousands of unrelated and unactionable source IP addresses to perform their analysis on. Unactionable IP addresses are often spoofed (i.e. faked) from cloud providers, home devices, the internet of things and other addresses that the attackers do not control. This complexity results in reporting that is incomplete, unrealistic and sometimes plain wrong.

Good-quality information i.e., high confidence data come from, paradoxically, reports and claims made by the attackers themselves. This information must be confirmed by third-party organisations or users who witnessed the attack taking place, or by statements from the target. Attackers usually share this information on the Telegram channels of those groups[6]. Attackers, in their need to show that the attack actually worked, usually share third-party sites to show that the target was down[7].

Bad-quality information i.e., medium confidence data come from DoS protection providers that actually stopped the attacks. These reports are useful as high-level reports but are still considered bad because they cannot be used to assess targets or motivations. These providers protect thousands of customers in many countries, making it hard to understand who attacked whom, why, and where. Moreover, due to contractual reasons, they usually can not disclose the target's name. When the target does not confirm the report and the attacker does not claim responsibility, these reports are hard to verify.

Ugly-quality information i.e., low confidence data come from reports created by the targets. Without third-party confirmation, these are very hard to use since the target may exaggerate the attack or attribute the attack to a threat group without enough evidence. Examples of the unreliability of these reports are when targets of DoS attacks use the attack as an opportunity to boost their popularity ('we are important because we are attacked') or when they

[6] Noname057(16), (Telegram: @noname05716), 'Вступайте в наш DDoS-проект', accessed 5 September 2023, https://t.me/noname05716.
[7] Anonymous (Twitter: @YourAnonReal), 'Anonymous has taken down the website of the Chechen Republic', 26 February 2022, accessed 5 September 2023, https://twitter.com/YourAnonReal/status/1497662005754441728.

falsely claim a larger impact on their services to fuel legal actions or to claim without proof that an adversary is attacking to justify future actions.

To make the best use of all these different types of reporting, a thorough process of cross-checking and validation was used to guarantee that all the pieces of information around an incident were validated and used.

3. DOS CLASSIFICATION

There have been many taxonomies for DoS attacks[8], but all of them focus on their technical characteristics and defences. Broadly speaking, DoS attacks are often divided into three types: volumetric attacks (measured in bits per second), protocol attacks (measured in packets per second) and application layer attacks (measured in requests per second)[9]. In this report, a diverse approach is presented where the classification of DoS attacks is grounded on **motivation** and **goal**, as most DoS attacks are characterised by these parameters, generating disruptions of various lengths to a target.

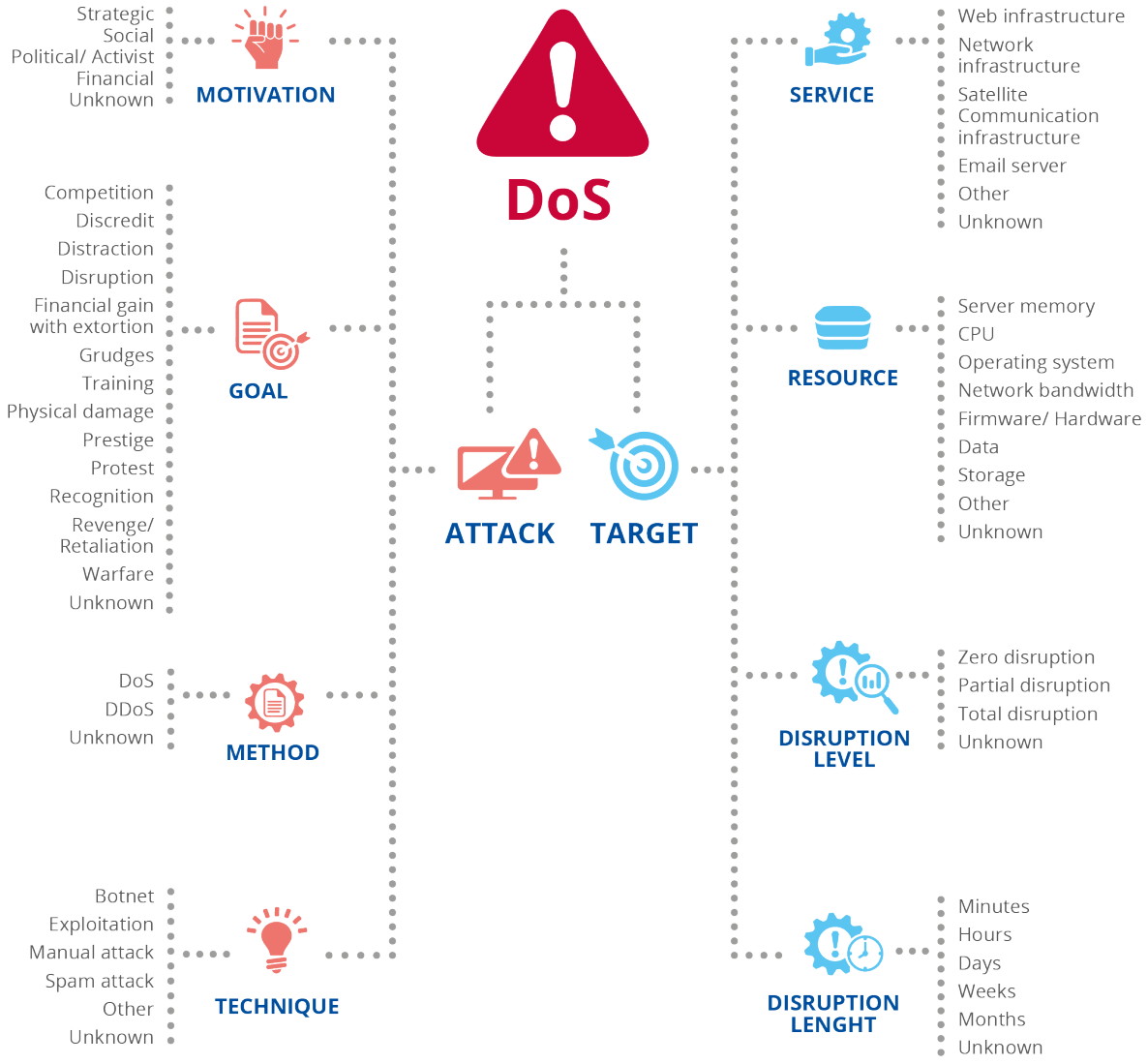
This report proposes a **new classification scheme** for Denial-of-Service attacks that focuses on key elements of the attack, capturing important characteristics about the attack and the target. Therefore, the classification criteria were selected to highlight common features of DoS attacks, that outline challenges and prescribe the design of countermeasures.

The benefits of introducing a DoS attacks' classification are multifold. First, it enables a first attempt to structure the knowledge in this field and supports the subsequent analysis. Second, the proposed classification is aimed to enhance strategic intelligence and is meant to promote better understanding of this type of threat and of the possible countermeasures. Finally, it is intended to bring coherence and standardisation to the area of DoS attacks. The proposed classification will likely foster cooperation, facilitate communication and offer a common language for discussing relevant solutions, while identifying areas for improvement.

The high-level view of the proposed classification scheme is presented in Figure 1. First, DoS attacks are classified into information about the attack and the target. Second, the attack information is further classified into four key elements: **motivation**, **goal**, **methods** and **techniques**. The target information is also classified into four key elements: **service**, **resource**, **disruption level** and **disruption length**. Third, each key element is further expanded with specific corresponding information. Each of these categories and elements is explained in detail in the following subsections.

[8] Mirkovic, J. and Reiher, P. (2004) "A taxonomy of DDoS attack and DDoS defence mechanisms' SIGCOMM, accessed 1 September 2023, https://dl.acm.org/doi/10.1145/997150.997156
[9] Imperva DDoS Attacks, accessed 29 November 2023, https://www.imperva.com/learn/ddos/ddos-attacks/

Figure 1: Classification scheme for Denial-of-Service attacks



3.1 CLASSIFYING ATTACK INFORMATION

Attack motivation. The motivation is what lies behind the decision to make a DoS attack, and is not the goal. Four core motivations were identified: *financial*, *political* or *activist*, *social* and *strategic*. DoS attacks can be financially motivated, whether to gain money (through extortion) or to make the target lose money through the disruption of their services. Motivations can also be political or activist in nature, where threat groups attempt to make a statement, exert pressure, conduct warfare or get revenge on a cause. Social motivations can also be a driver for DoS attacks rooted in grudges, personal recognition, revenge, etc. Motivations can also be strategic, where attacks are state sponsored or intended to gain a strategic competitive advantage in the corporate sector or a warfare situation.

Attack goal. The goal refers to what the attackers intended to achieve with the attack. For this study, in the context of DoS attacks, several goals have been identified: to *discredit*, to obtain *financial gain* with extortion, to *protest*, to gain *recognition*, to obtain *revenge* or *retaliation*, to gain *prestige*, to produce *distractions*, to cause *physical damage*, to engage in *warfare* and to cause *disruption*. This list is not exhaustive and could be expanded in the future. Note that

warfare is reserved for attacks between opposing sides during a declared conflict, as part of the conflict itself. This is contrary to revenge or retaliation attacks performed by supporters of a participant in the war towards third-party entities that are not officially part of the war (e.g., a group of hacktivists attacks a third-party country because it verbally opposed the war).

Attack method. The method refers to how the DoS attack is conducted at a high level. DoS attacks can be *distributed (DDoS)*, usually relying on large-scale botnets or proxies. DoS attacks can also be *non-distributed (DoS)*, often relying on manual attacks and exploiting vulnerabilities.

Attack technique/tools. To conduct the DoS attack, attackers use various high-level tools and techniques. This classification is not about the types of packets sent, but the high-level way in which the attack was conducted. The most common in this area are *botnets*, the *exploitation of vulnerabilities*, *manual attacks*, *spam attacks*, etc. Note that the classification scheme does not go into the technical description of the protocols used or the types of packets, but into the means by which the attack was conducted.

A summary of the discussed attack motivations, goals, methods and techniques is presented in Figure 2.

Figure 2: Classification of attack information in a DoS attack

3.2 CLASSIFYING TARGET INFORMATION

Target service. DoS attacks usually focus on a specific target service. Attackers commonly target *web infrastructure* such as websites and web application programming interfaces. Other services attacked include the *network infrastructure* in general, *email servers*, *satellite communication infrastructure*, others or *unknown*.

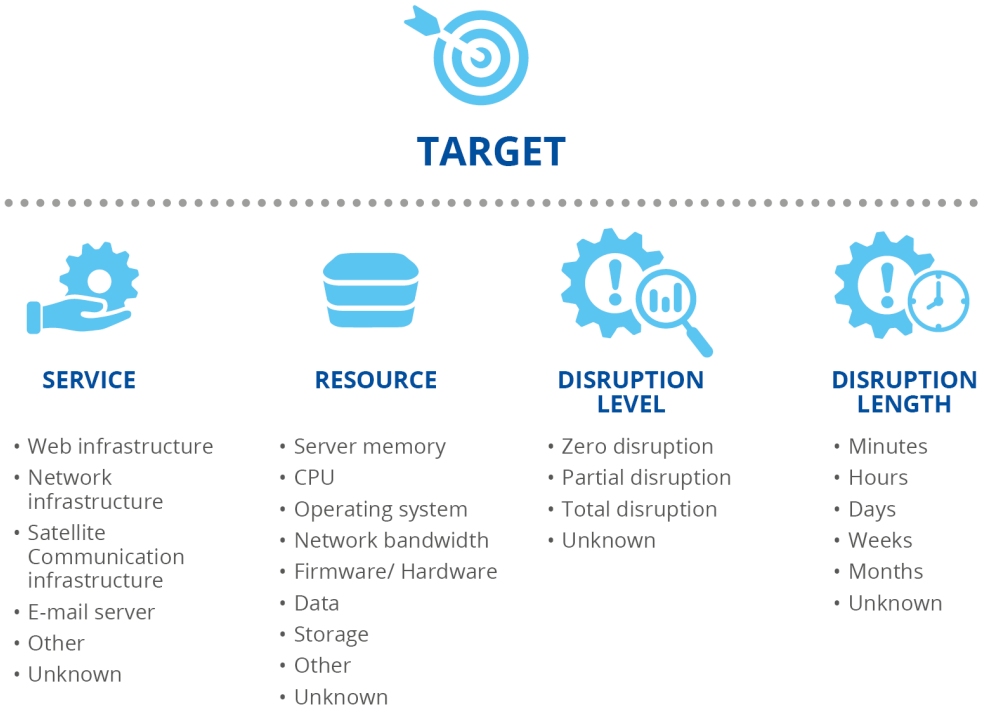
Target resource. DoS attacks aim to stop the availability of a service by depleting the resources of the target. These resources can be *network bandwidth*, *server memory*, *central processing units* (computational power), *data* (for deletion), *storage* capacity, *unknown*, etc.

Disruption level. DoS attacks' intensity and effectiveness vary significantly across incidents observed, and they are not always successful. To be able to make a comparison across incidents, the attack disruption was categorised into four levels: *zero disruption*, *partial disruption*, *total disruption* and *unknown*. Zero disruption is usually when the target experiences an attack, but due to the nature of the attack or the resilience of the target there is no noticeable impact on the target's availability or performance. Partial disruption is when the target experiences intermittent outages or performance degradation, but remains overall operational. Total disruption is when the target experiences severe disruption, with users unable to access or use the services.

Disruption length. The disruption length caused by the attack measures how long organisations experience disruptions caused by the DoS attack. This study defined six broad levels of disruption length: *minutes*, *hours*, *days*, *weeks*, *months* and *unknown*. This parameter was hard to find since almost no account reported it.

A summary of the discussed target services, resources, disruption level and disruption length is presented in Figure 3.

Figure 3: Classification of target information in a DoS attack



With this classification scheme as a tool, this report classifies and compares the various DoS attacks seen to understand the focus of the attacks, the motivations behind them and the quality of reporting.

4. PROMINENT INCIDENTS

For this report, the authors identified, verified and analysed 310 DoS incidents, shown in Section 5 “Global analysis of incidents”. A subset of those incidents is considered **prominent** and are presented in summary in this section, which follows the classification proposed in Section 3 “DoS Classification”. The period of 2022 to 2023 had numerous incidents that could be considered prominent due to their technical characteristics or disruption effects. Prominent incidents were selected due to their uniqueness in terms of socio-political context, technical prowess and disruption effect. The technical prowess is related to the volume or technical complexity of the attack; if an attack was massive, noticeable, or highly sophisticated, the incident was included in this report. The significance of the target refers to high-value targets or incidents that affect a large number of people.

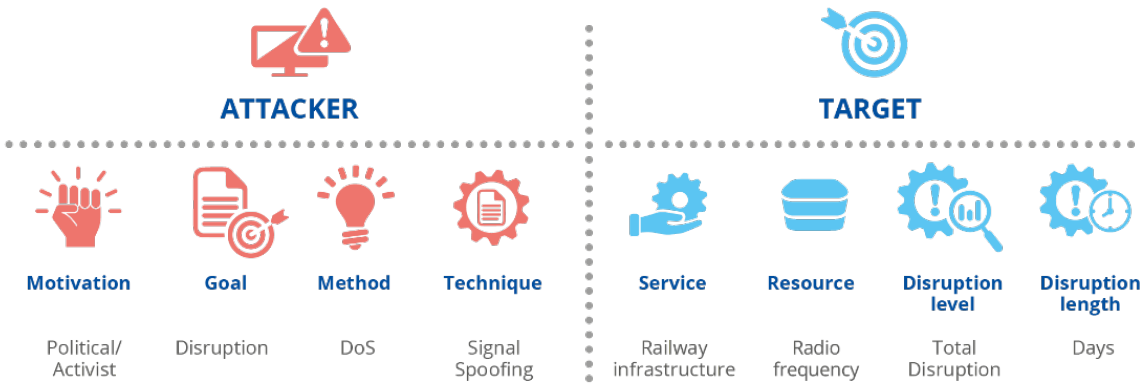
4.1 POLAND’S RAILWAY SYSTEM

On **25 August 2023**, the Polish railway system was disrupted by a DoS attack on the emergency-stop mechanisms of the trains. Attackers abused a vulnerability in the design of the system, specifically the lack of encryption in the radio signal used in the railway system to control these mechanisms. The attackers sent a stop signal that trains interpreted correctly, which led to the trains halting their operation. The attack disruption gained relevance as the Polish railway became strategic for the West’s support of Ukraine against the Russian invasion.

This attack is relevant because while most DoS attacks are focused on web infrastructure and the internet when it comes to active military conflicts, the attack surface changes, and organisations should consider all mediums as possible targets, including radio frequency signals, wireless systems and even physical devices [10][11]. The attack has attracted considerable attention due to indications that it might have been executed by sympathizers not originating from the nations engaged in the conflict. Ultimately, two Polish citizens were apprehended in connection with the incident.[12]

Applying the proposed classification, this attack can be classified as follows. Regarding the attack, the motivation could be assessed as **political/activist**, the goal was **disruption**, the method was **DoS** and the technique was **signal spoofing**. Regarding the target, the service was the **railway infrastructure**, the resource was **radio frequencies**, the **disruption level** was **total** and the **disruption length** was **days**. This classification is shown in Figure 4.

Figure 4: Poland’s railway system DoS attack analysis using the proposed classification



[10] Greenberg, A., ‘The cheap radio hack that disrupted Poland’s railway system’, WIRED website, 27 August 2023, accessed 28 August 2023, https://www.wired.com/story/poland-train-radio-stop-attack/
[11] i24NEWS, ‘Two suspects arrested following Poland railway hacking’, i24NEWS website, 27 August 2023, accessed 28 August 2023, https://www.i24news.tv/en/news/international/europe/1693168279-two-suspects-arrested-following-poland-railway-hacking.
[12] https://therecord.media/two-arrested-poland-railway-hack

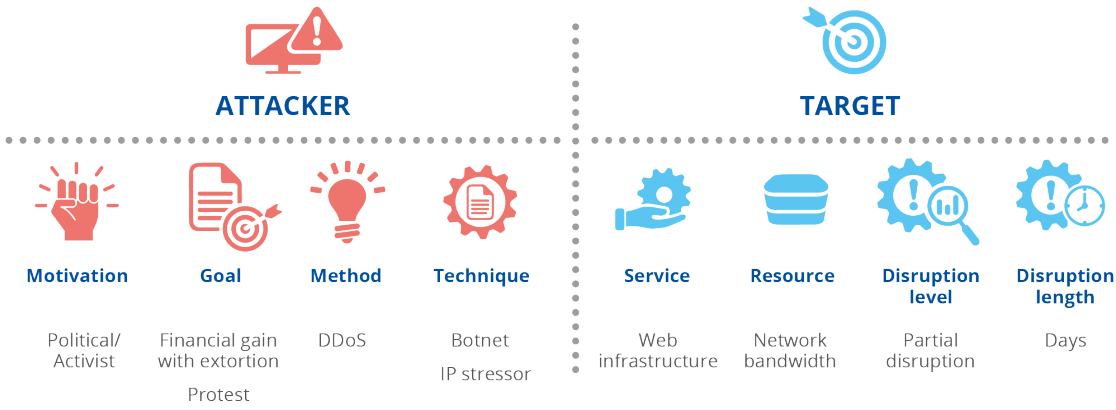
4.2 MICROSOFT AZURE

On **7 June 2023**, a threat group (Anonymous Sudan aka Storm-1359 claimed responsibility[13]) launched a DDoS attack against the Microsoft Azure application layer infrastructure, causing service degradation and minor disruptions[14]. The group said the attack was launched after news spread of a potential invasion of Sudan by the United States. The group used various DDoS tools and botnets to conduct the attack. The target suffered partial disruption for several days, after which the threat group attempted to extort money from Microsoft to stop the attacks.

The impact of this attack can be assessed as significant because of its strength in disrupting a portion of the Azure infrastructure. It is also an example that reminds us that extortion is still very much in the arsenal of tools of attackers looking to take advantage of any attack for financial gain. While in this case it was unclear whether or not the extortion was a serious extortion attempt, many organisations are facing this type of threat and are not as well prepared to dismiss the threat.

Applying the proposed classification, this attack can be classified as follows. Regarding the attack, the motivation was **political/activist**, the goal was a mixture of **protest** and **financial gain with extortion**, the method was **DDoS** and the technique was **botnets** and **IP stressors**. Regarding the target, the service attacked was **web infrastructure**, the resource was the **network bandwidth**, the **disruption level** was **partial** and the **disruption length** was **days** due to the intermittent nature of the attack. This classification is shown in Figure 5.

Figure 5: Microsoft Azure DoS attack analysis using the proposed classification



4.3 LARGE DDOS ATTACK IN AKAMAI CUSTOMER

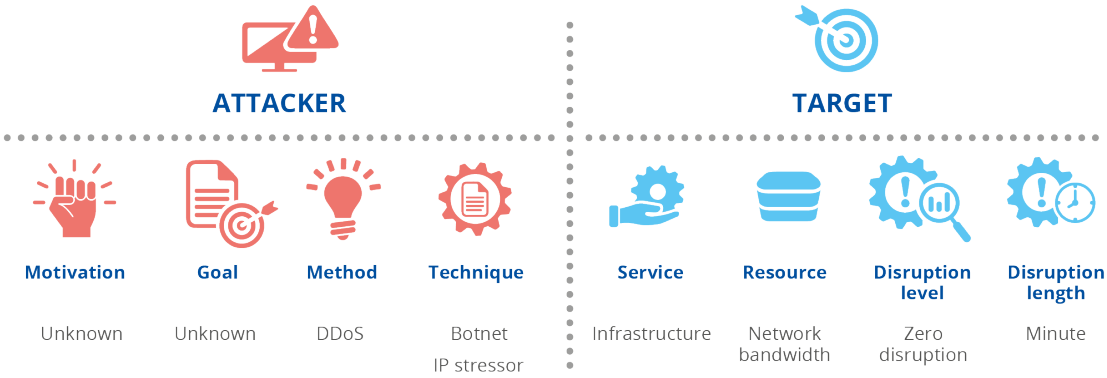
On **23 February 2023**, an unidentified Akamai customer was the target of the largest DDoS attack based on traffic detected on the Akamai platform[15]. The attack was identified as a DDoS attack, presumably generated by the use of botnets and IP stressors[16][17]. The attack was short-lived, lasting a few minutes, presumably not successfully disrupting the targeted service. The target, motivation and goal of the attack are unknown, and no technical details were shared to confirm the attack's origin or the potential threat group behind it.

[13] https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/
[14] 'Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks', Microsoft Security Blog website, 16 June 2023, accessed 29 August 2023, https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/
[15] Sparling, C., 'Akamai mitigates record DDoS attack in Asia-Pacific (900 Gbps)', Akamai website, 8 March 2023, accessed 28 August 2023, https://www.akamai.com/blog/security/record-breaking-ddos-in-apac.
[16] Toulas, B., 'Akamai mitigates record-breaking 900Gbps DDoS attack in Asia', BleepingComputer website, 9 March 2023, accessed 28 August 2023, https://www.bleepingcomputer.com/news/security/akamai-mitigates-record-breaking-900gbps-ddos-attack-in-asia/; Balaji, N., 'Record breaking DDoS attack – 158.2 million packets per second' GBHackers on Security website,11 March 2023, accessed 28 August 2023, https://gbhackers.com/record-breaking-ddos-attack-on-asia/.
[17] Balaji, N. (2023) 'Record Breaking DDoS Attack - 158.2 Million Packets Per Second' GBHackers on Security website, accessed 28 August 2023 https://gbhackers.com/record-breaking-ddos-attack-on-asia/[18] 'HHS alerts health sector to pro-Russian hacktivist threat', American Hospital Association website, 30 January 2023, accessed 18 October 2023, https://www.aha.org/news/headline/2023-01-30-hhs-alerts-health-sector-pro-russian-hacktivist-threat

This is a clear example of the aggressiveness of today's DDoS attacks and the importance of implementing preventive measures. This also exemplifies the impact of an anonymous DoS attack, as in this case there are several unknowns, such as who attacked, what the motivations and the intended goal were, who the target was (not released by Akamai) and whether or not it was related to any ongoing armed conflict.

Applying the proposed classification, this attack can be classified as follows. Regarding the attack, its motivation was **unknown**, the goal was **unknown**, the method was **DDoS** and the technique was **botnets** and **IP stressors**. Regarding the target, the service targeted was the **infrastructure** (unclear which part of the infrastructure was targeted), the resource targeted was the **network bandwidth**, the **disruption** level was **zero** (as reported but not confirmed) and the **length of the disruption** was **minutes**. This classification is shown in Figure 6.

Figure 6: Akamai customer DoS attack analysis using the proposed classification



4.4 ATTACK ON HOSPITALS IN THE UNITED STATES

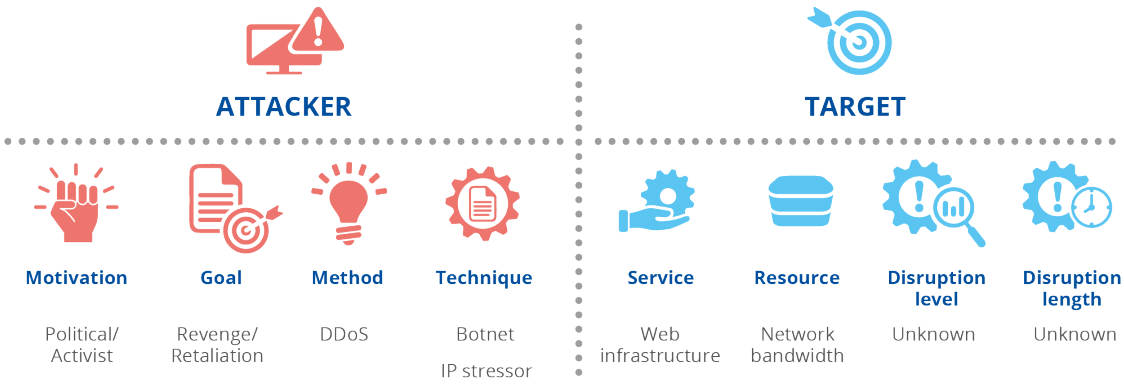
On **30 January 2023**, a Russia-affiliated group launched a DDoS attack against hospitals in the United States[18]. The attack was coordinated to target the web infrastructure of more than a dozen hospitals through a network-based DDoS. The group announced the attack and claimed on Telegram that targeting US institutions was retaliation for the United States' support for Ukraine following Russia's invasion.

This attack stands out due to its contentious targeting of civilian healthcare facilities, seen in the framework of retaliatory actions amid an ongoing Russian-Ukraine conflict. The real impact of the disruption caused by the attacks is unclear. However, this serves as a clear example of the risk that digital attacks pose in inflicting tangible, physical harm to healthcare systems. Furthermore, as physical damage and possible loss of life are a real risk stemming from these attacks, international laws may apply, such as the Geneva Convention, which has clear statements about protecting medical facilities and preventing indiscriminate attacks during wartime.

Applying the proposed classification, this attack can be classified as follows. Regarding the attack, its motivation was **political/activist**, given the relationship with the war. Its goal was **revenge/retaliation**, as was stated by the attacker when claiming responsibility. The method was **DDoS**, as was confirmed by the target, and the technique was **botnets** and **IP stressors**. Regarding the target, the service targeted was **web infrastructure** based on the reports, although other services may be included. The resource was **network bandwidth**, the **disruption** level was **unknown** and the **disruption length** was **unknown**. This classification is shown in Figure 7.

[18] 'HHS alerts health sector to pro-Russian hacktivist threat', American Hospital Association website, 30 January 2023, accessed 18 October 2023, https://www.aha.org/news/headline/2023-01-30-hhs-alerts-health-sector-pro-russian-hacktivist-threat

Figure 7: Analysis of DoS attacks on US hospitals using the proposed classification



4.5 KA-SAT NETWORK (VIASAT): DAY OF THE RUSSIAN INVASION OF UKRAINE

On the day of the Russian invasion of Ukraine[19][20], **24 February 2022**, attackers exploited a virtual-private-network (VPN) misconfiguration on KA-SAT (a worldwide satellite provider owned by Viasat), which provided remote access to the trusted management segment of the KA-SAT network[21]. This allowed attackers to control the satellite modems that provide internet access. The attack partially consisted of re-flashing the modems' firmware, rendering them unusable.

The attack caused disruptions primarily in Ukraine, and to neighbouring countries, including Czechia and Slovakia. Bringing the modems back online required reconfiguration, which meant the disruption lasted for more than 2 weeks.

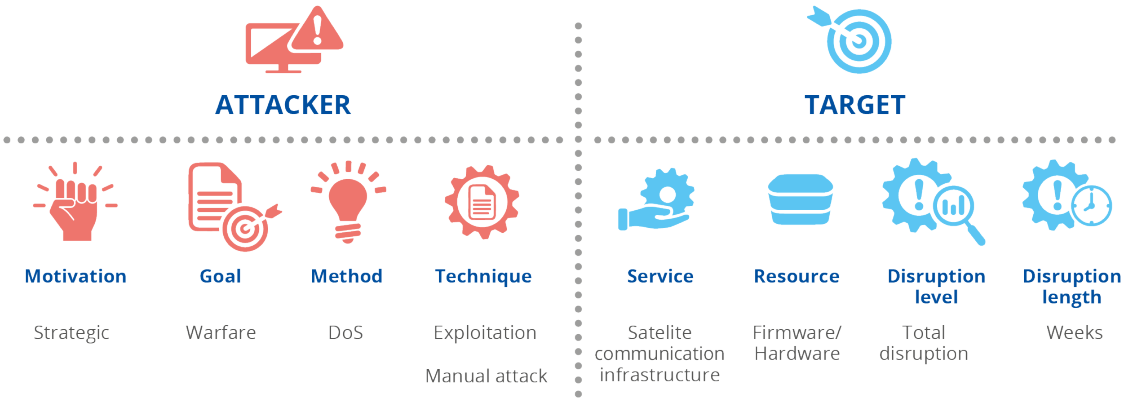
As collateral damage, more than 5 000 wind turbines in Germany were affected as they were using the KA-SAT network to send data for maintenance and updates. Other customers in Greece, France, Italy, Hungary and Poland were also affected[22][23][24].

Applying the proposed classification, this attack can be classified as follows. Regarding the attack, its motivation was **strategic**, given that it was pre-planned with clear coordination with kinetic attacks to support and maximise the overall impact of the war. It was also not published by a group (no media attention), but was discovered, verified and reported by the targets. Its goal was support to **warfare** since it was conducted by one party in a declared war. The method was **DoS** and not DDoS since there was no evidence of multiple simultaneous coordinated and automatic attacks. Instead, it was based on VPN access, configuration problems and the wiping of firmware (even though it may have happened simultaneously). The technique was **exploitation** and **manual attack**, given the reports. Regarding the target, the service was the **satellite communication infrastructure** and the resource was **firmware and hardware** (notice that the VPN was a medium but not a target). The **disruption** level was **total** (concerning the

[19] Pearson, J., Satter, R., Bing, C. et al., 'Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say', Reuters website, 12 March 2022, accessed 20 July 2023, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
[20] Lyngaas, S., 'Ukraine detains "hacker" accused of aiding Russian troops amid broader struggle to secure communications', CNN website, 15 March 2022, accessed 20 July 2023, https://www.cnn.com/2022/03/15/europe/ukraine-detains-hacker/index.html.
[21] Viasat, 'KA-SAT Network cyber-attack overview', Viasat website, 30 March 2022, accessed 18 July 2023, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.
[22] Gatlan, S., 'Viasat shares details on KA-SAT satellite service cyberattack', BleepingComputer website, 30 March 2022, accessed 20 July 2023, https://www.bleepingcomputer.com/news/security/viasat-shares-details-on-ka-sat-satellite-service-cyberattack/
[23] Der Spiegel, 'Satellitennetzwerk offenbar gezielt in Osteuropa gehackt', Spiegel Netzwelt website, 5 March 2022, accessed 20 July 2023, https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa-gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024
[24] Sheahan, M., Steitz, C. and Rinke, A., 'Satellite outage knocks out thousands of Enercon's wind turbines', Reuters website, 28 February 2022, accessed 20 July 2023, https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

services targeted and not the whole satellite infrastructure) and the **disruption length** was **weeks**, given that the effects and recovery time were that long. This classification is summarised in Figure 8.

Figure 8: KA-SAT network (Viasat) DoS attack analysis using the proposed classification



5. GLOBAL ANALYSIS OF INCIDENTS

This section presents the results of analysing a large number of worldwide DoS incidents that took place from **January 2022 to August 2023**. This analysis aims to aid in the understanding of the current DoS threat landscape and its key characteristics. The **310 incidents** analysed were selected based on the methodology already discussed and the scope of this report, which is described in the following paragraph.

5.1 SCOPE OF INCLUDED INCIDENTS

This report analyses worldwide incidents caused by DoS attacks. The criteria for including incidents are limited. Incidents must meet the following criteria to be included in the analysis. First, incidents should have taken place between January 2022 and August 2023. Second, incidents should have been verified as DoS attacks by at least one third-party source.

A special note should be made about whether the attack caused disruption or not. If an attack was mitigated, therefore unsuccessful, but was still large enough or attacked an important target, it was considered for analysis. This criterion is subjective since many small attacks are not noticed or not reported.

Regarding the granularity of the attacks, it is usually the case that one reported attack is composed of many smaller attacks happening one after the other. Hence, it is unclear when one attack ends and the next starts. The number of attacks is taken as it was reported.

5.2 NUMBER OF INCIDENTS AND SAMPLING

It is difficult to assess the total number of DoS attacks. This study relies on third-party reports and open-source intelligence verification, as there is no public access to network monitoring platforms that can be used to witness and track these attacks. In the case of DoS (Denial of Service) attacks, the level of reporting and analysis has not yet achieved the maturity found in other types of cyberattacks, making it challenging to thoroughly understand the specifics of what occurred.

Adding to the difficulty of measuring DoS attacks in reality, entities with a high degree of visibility offering DDoS protection often report that thousands of DDoS attacks get blocked every day[25][26]. These attacks are mostly not reported outside quarterly metrics documents and do not provide specific details on the nature of the attacks or the definition of what an attack is from their business perspective.

This study's sampling method for selecting incidents is biased and leaves out many incidents that were hard to track or did not make it into the news. Thus, the outcomes of this report should be considered as guidelines and not as an accurate portrayal of the overall number of attacks. Additionally, the classification methodology was tailored to assist in the analysis solely to this study.

5.3 TARGETED SECTORS

In general, no industry is immune to DoS attacks. Yet, in the timeframe covered by this report, 46 % of registered attacks targeted the public administration sector. Other sectors also experienced a notable share of attacks, including the transport sector (aviation, railway, maritime, road) with 11 % of the attacks, the media/entertainment sector with

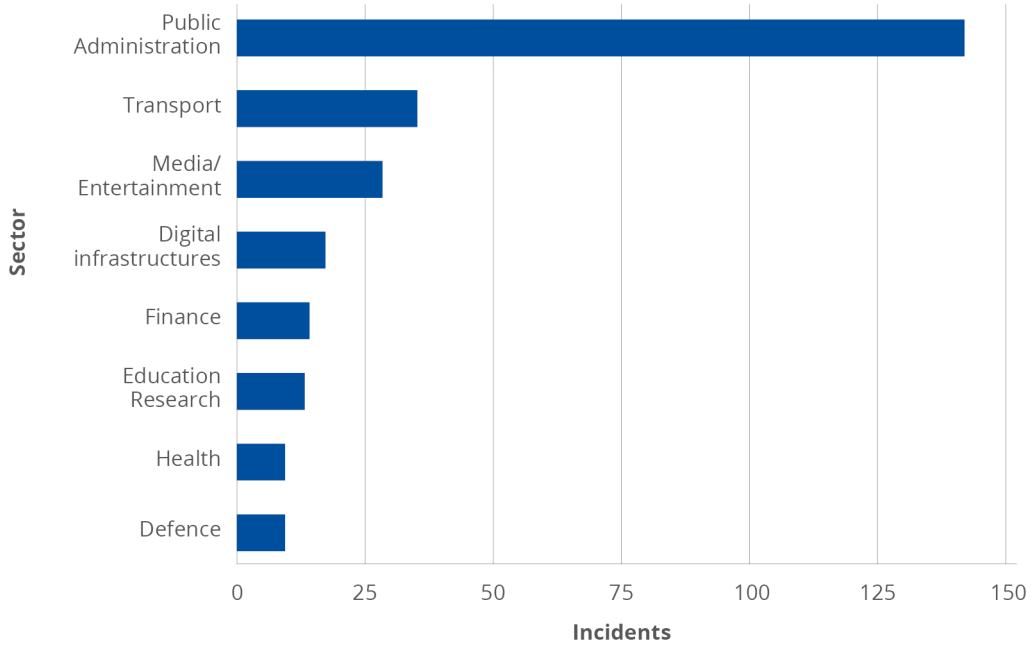
[25] Azure Network Security Team, '2022 in review: DDoS attack trends and insights', Microsoft Security Blog website, 21 February 2023, accessed 29 August 2023, https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights
[26] Yoachimik, O. and Pacheco, J., 'DDoS threat report for 2023 Q2', The Cloudflare Blog website, 18 July 2023, accessed 29 August 2023, http://blog.cloudflare.com/ddos-threat-report-2023-q2/[27] 'Italy stops wide-ranging Russian attack on websites of parliament, military, health agency', 12 May 2022, accessed 7 September 2023, https://therecord.media/italy-killnet-hacking-military-parliament-national-health-institute

9 % of attacks and the digital infrastructures sector with 5 % of the attacks. The eight most affected sectors by number of observed incidents are shown in Figure 9.

Attacks targeting the public administration sector are significantly more frequent in number compared to others. This surge is largely a consequence of retaliatory actions linked to ongoing conflicts. Countries expressing support have often become targets of threat groups. As a result, these incidents have prompted numerous warnings and advisories to government institutions.

The online media/entertainment sector should also be highlighted, as it is also one of the first targets of any military conflict. Silencing the voices of the opposition and stopping the population from learning other versions of the official stories is a well-known technique to maintain control. It is unclear how effective these tactics are, but it is possible that the goal of these attacks on this sector goes beyond disruption into seeking to provoke fear, uncertainty and doubt.

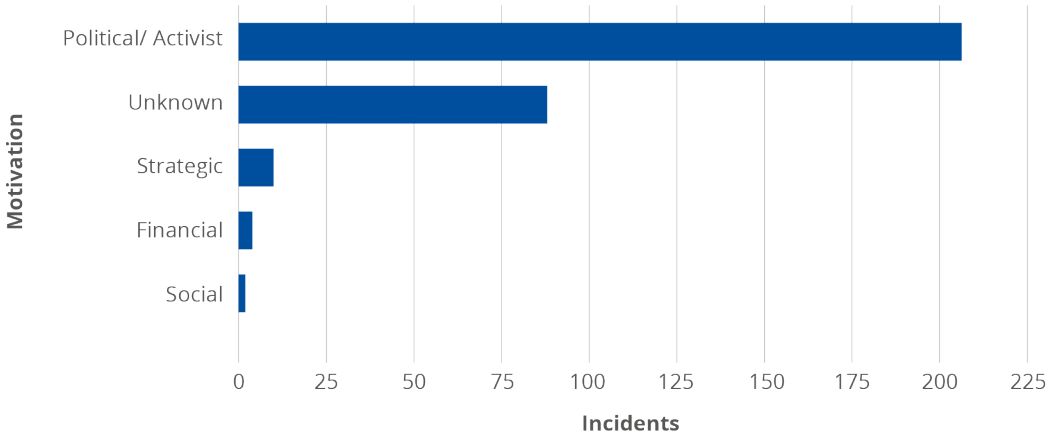
Figure 9: Top 10 sectors by number of incidents between January 2022 and August 2023



5.4 INSIGHTS ON DOS MOTIVATIONS & GOALS

This study's analysis shows that the most prevalent driving factor in DoS attacks is political or activist motivations, accounting for 66 % of the observed incidents. Strategic, financial and social motivations were only observed in 5 % of the cases. In the remaining 28 % of the cases, the incident's motivation was unknown. Although, in specific cases, the motivation behind an attack is hard to understand, the bulk of these unknowns are due to other factors, such as poor-quality reporting or the fact that the targets themselves are too small or deemed not interesting enough for media outlets to report on. The full breakdown of motivations by the number of incidents is shown in Figure 10.

Figure 10: Attacker motivations by number of incidents between January 2022 and August 2023



In terms of the end goal behind the attacks, the research in this study shows that nearly 43 % of the incidents observed were intended as retaliation or revenge against a target. In this category, the bulk of attacks were found to be by pro-Russia hacktivist groups, who launch attacks against all countries or organisations that oppose Russia's invasion of Ukraine or are providing support to Ukraine. In the same context, warfare-related goals were behind 9.4 % of the incidents studied.

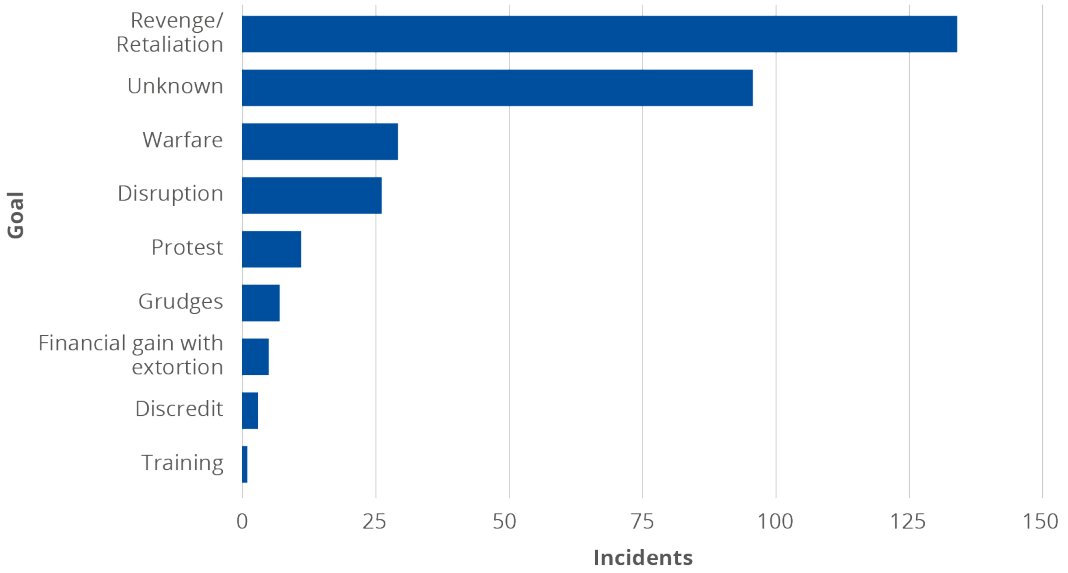
DoS attacks were also conducted to cause disruption in 8.4 % of the incidents. DoS attacks continue to be a tool for protesting against and discrediting a target, although these goals were observed on a much smaller scale during the period studied, with 3.5 % and 1 % of attacks respectively. Similar in scale, DoS attacks with a goal of financial gain with extortion were observed in 1.6 % of the cases.

A new end goal of DoS attacks was identified during this study, which is Denial-of-Service attacks conducted as a means of training attackers in the art of DoS. Hacktivist groups and other attackers were observed to launch attacks against smaller targets as educational experiences that would pave the way for their crews to launch attacks against larger and more important targets. An example of such activity is the Killnet hacking group that admitted attacks against the Italian public sector with the purpose of training and skills improvement[27].

The full breakdown of observed goals by number of incidents is shown in Figure 11.

[27] 'Italy stops wide-ranging Russian attack on websites of parliament, military, health agency', 12 May 2022, accessed 7 September 2023, https://therecord.media/italy-killnet-hacking-military-parliament-national-health-institute

Figure 11: Attacker goals by number of incidents between January 2022 and August 2023



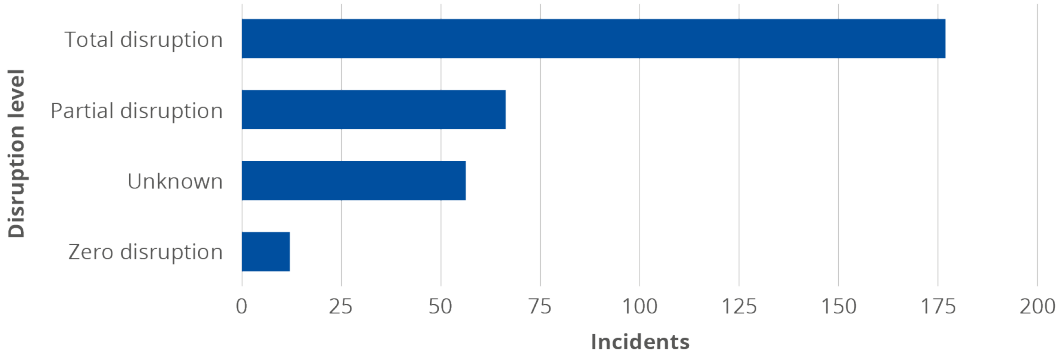
5.5 INSIGHTS ON DOS TARGET DISRUPTION

The definition of a DoS attack is an attack intended to make a resource unavailable. However, the real effects of a DoS attack are hard to measure. This report attempts to measure both the disruption level and disruption length. The measurements were obtained from qualitative statements in the reports of the attacks and later categorised according to the proposed classification.

Overall, 56.8 % of the attacks caused total disruption in the target, with users experiencing severe outages during the duration of the attack. Partial disruption was observed in 21.3 % of the incidents, which were said to undergo intermittent outages or severe service degradation. Only in 3.9 % of the cases did the attacks cause what was labelled as zero disruption, in which the attack itself was ineffective or the DoS protection of the target that was in place meant that there was no noticeable impact on the target.

In 18.1 % of the incidents, the level of disruption was not reported, making it unclear whether the attack was unsuccessful, the target was not affected due to their own DoS protection or something else affected the attack. The full breakdown of the target disruption level by the number of incidents is shown in Figure 12, while the target disruption length by the number of incidents is shown in Figure 13.

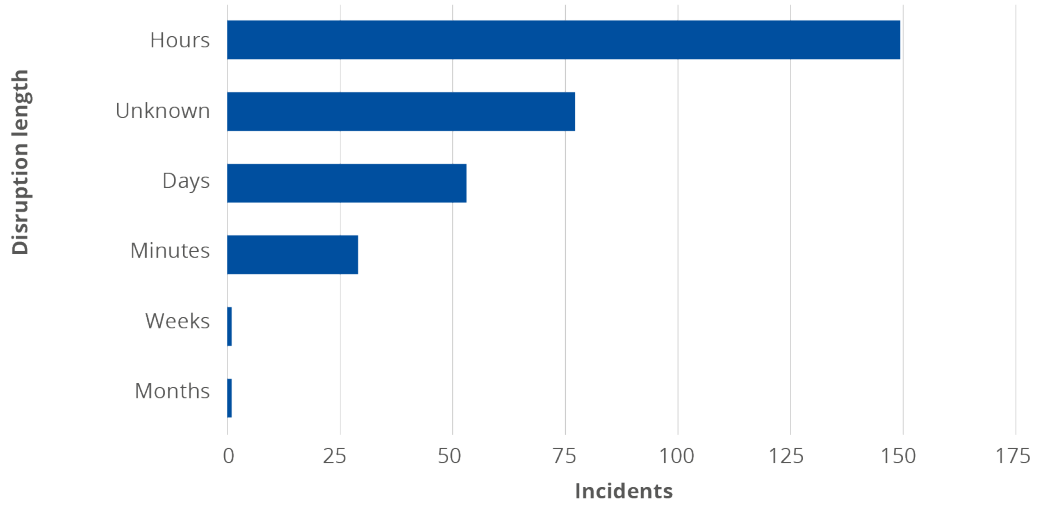
Figure 12: Target disruption level by number of incidents between January 2022 and August 2023



In terms of disruption length, nearly half of the incidents, 48.1 %, the targets declared that they experienced a disruption of hours before measures were taken to counteract the attacks. Disruptions lasting for days accounted for 17.1 % of the incidents, while those lasting for minutes made up 9.4 %. Remarkably, a very small fraction of incidents, just 0.6 %, reported disruptions extending for weeks or months.

In 24.8 % of the incidents, there was no information available on the duration of the incident. This highlights yet another aspect of DoS attacks, which, contrary to other types of cyberthreats, are rarely followed up on by the press.

Figure 13: Target disruption length by number of incidents between January 2022 and August 2023



5.6 ATTRIBUTION & CONFLICTS

One key aspect of DoS attacks is the inherent need for notoriety and attention. Threat groups often announce their attacks publicly, giving defenders the opportunity to cross-check the information with these actors' known tactics, techniques and procedures, helping not only identify but also increase their attribution confidence. Nevertheless, attribution is still hard, and this study identified that in 59 % of the cases, incidents were not clearly attributed to any threat group.

In the analysed incidents that were attributed, it was observed that 30 % of the incidents were caused by pro-Russia hacking groups KillNet and NoName057(16). On a much smaller scale, Anonymous Sudan was responsible for 3.2 % of the attacks, followed by a long tail of threat groups attributed to a few dozen other incidents.

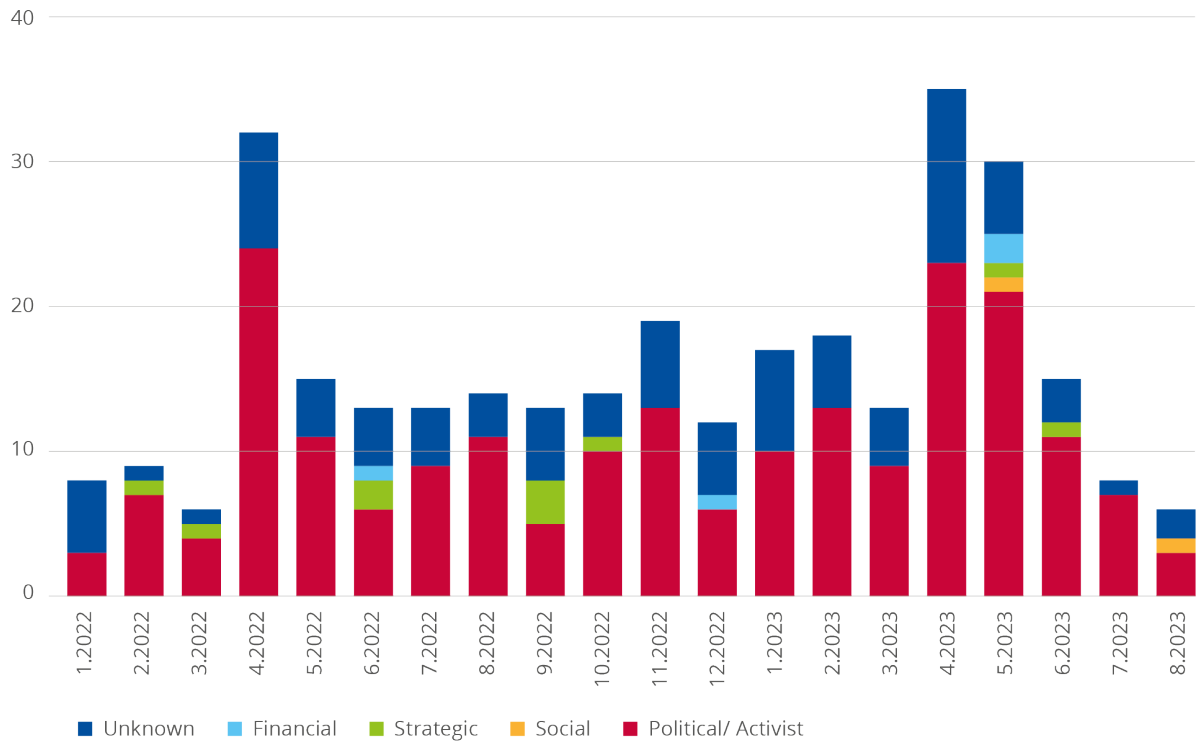
The high number of incidents attributed to pro-Russia threat groups should not come as a surprise, given the current state of affairs. Overall, 50 % of the incidents were found to be related to the Russian war of aggression against Ukraine. Other conflicts also resulted in DoS attacks, such as conflicts in the Middle East (ISR/PSE), tension between Sudan and other countries, Koran burnings in Western countries, and many others. However, in 37 % of the incidents, there was no reporting on the conflicts associated with the attacks.

5.7 TIMELINES

The timeline of DoS attacks represents the type and number of attacks produced during the scope of this study. Remember that the number of attacks is not definitive since there are many unconfirmed attacks. Therefore, this timeline should be taken as a representation of the 310 most publicised DoS attacks between January 2022 and August 2023.

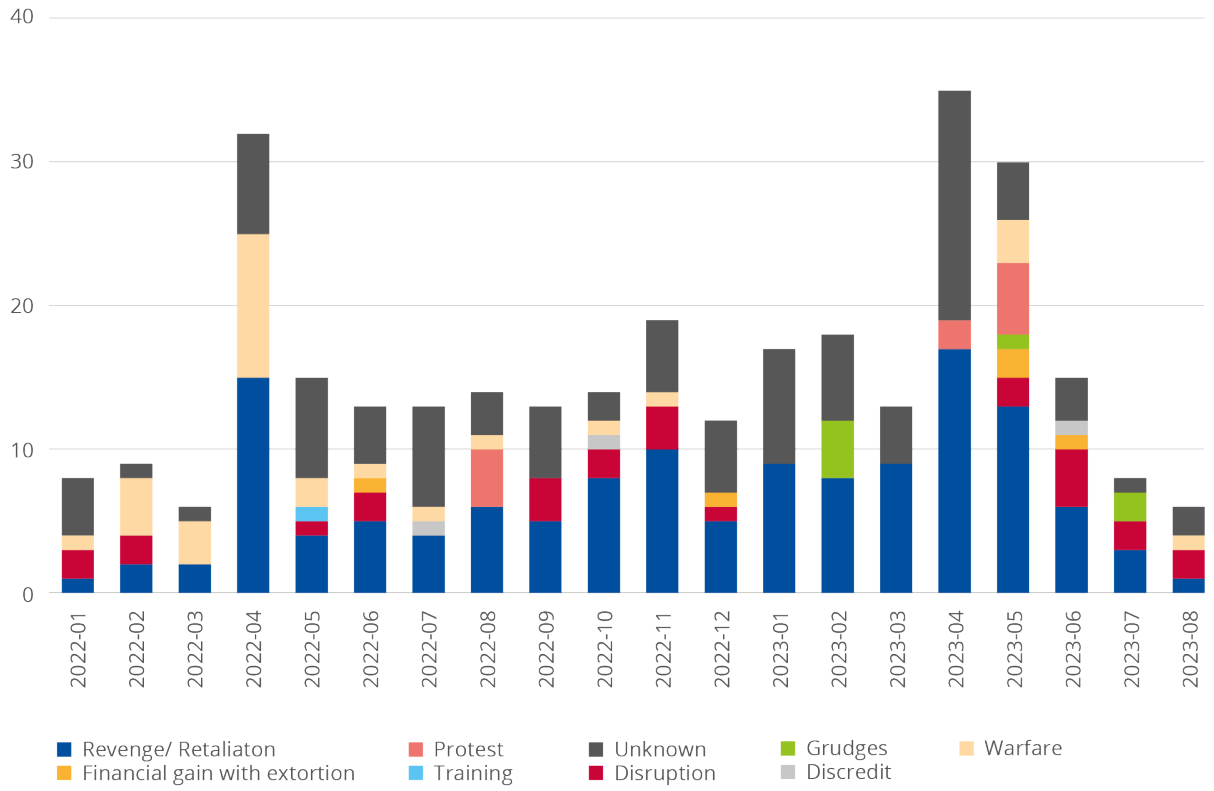
The first timeline illustrates the number of monthly incidents, focusing on the **motivations** for conducting DoS attacks, as shown in Figure 14. The figure shows that the most common motivation for DoS was political/activist, with the second most common being unknown. The **political/activist** motivation is more prevalent because the majority of these attacks are meant to attract media attention and want to show the power of the attacker, even for financial goals. Therefore, they are more publicised. The second most common is **unknown** because many DoS attacks are incorrectly reported or there is no way to verify the motivation of the attackers.

Figure 14: Timeline of motivations for conducting DoS attacks



The second timeline illustrates the number of monthly incidents, focusing on the **goal** of the attackers, as shown in Figure 15. It can be seen that the majority of attacks are carried out for **revenge/retaliation**, closely followed by **unknown** goals and then **warfare**. The goal of revenge/retaliation is more easily found due to the need to seek media attention as part of the attack. Notice that even though media attention is needed, it is not the primary goal. Warfare is the third most common goal, probably because of the intensive reporting of attacks during the Russian war of aggression against Ukraine so as to expose on-going operations.

Figure 15: Timeline of goals for conducting DoS attacks



The peak of political/activist-motivated attacks observed in April 2022 mostly had a goal of revenge/retaliation. This was an early peak in relation to hacktivist attacks, which decreased a little after April 2022 until April 2023, when there was another peaked observed. After April 2023, the number of revenge/retaliation attacks seems to have decreased slowly, but the reasons are unknown. The April 2022 events can also be correlated with the start of operations by Killnet (February 2022) and Noname057(16) (March 2022).

6. MEASURING THE IMPACT OF DOS ATTACKS

The real impact of a DoS attack depends on a myriad of factors, and is not easy to quantify. DoS attacks are conducted with a specific motivation and goal, and their impact on the target is closely related to this motivation and goal.

The impact of a DoS attack can be analysed based on the effects produced by the attack. The most common effects of a DoS attack are **downtime** and **publicity**. Downtime refers to the actual real unavailability of the target service as a result of the DoS attack. The more severe the downtime, the more impactful the attack is. Publicity relates to the extent of media attention an attack garner. The greater the media coverage of the attack, the larger its potential impact on reputation.

DoS attacks with the goal of disruption, gaining prestige, gaining recognition or warfare can be considered impactful only if they produce a real downtime. Without causing disruption, a DoS attack with these goals has no impact, even if it has publicity. By causing disruption, a DoS attack with these goals is impactful and can help the attacking group gain traction, notoriety and followers.

DoS attacks with the goal of protesting[28], discrediting, revenge/retaliation[29] or satisfying grudges are more impactful if there is downtime, but they **can be impactful without downtime**. However, these attacks can be impactful only if they generate sufficient publicity. Without publicity, a DoS attack that aims to discredit a target would have no impact, even if the disruption was total. The same can be said for DoS attacks that are launched to protest for a certain cause. These DoS attacks **need** the media attention to be impactful. The downtime plays a role in these attacks, but to a lesser extent.

A seldom-discussed by-product of DoS attacks is **fear, uncertainty and doubt (FUD)**, which refers to the psychological effects of the attack on the general public. It is in the nature of DoS attacks to generate FUD, as the attacks are unpredictable and the impact on the target is often unknown. Impactful DoS attacks generate FUD as a by-product. The combined level of publicity and downtime will impact the level of FUD generated by the attack.

[28] https://www.bbc.com/news/technology-52879000
[29] https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

7. COMPLEXITY OF "ATTRIBUTION"

Attribution of any type of cyber threat is very complex by default. When it comes to Denial-of-Service (DoS) attacks, defenders face additional difficulties. First, most DoS attacks are distributed Denial-of-Service (DDoS) attacks, which originate from thousands of sources from all over the world. Second, in most of these attacks, the source IP addresses are spoofed, leaving defenders without a trail to follow to investigate the source of the attacks. During this study, three forms were identified.

The most common form of attribution is through the attackers themselves when they publicly claim responsibility for the attack. The most prolific threat groups behind DoS attacks have their own medium for publicising them, announcing when and whom they will attack. This information can then be correlated to what really happened and help attribute the attack with a fair degree of confidence. It is not a failproof method, as attackers may claim credit for attacks by other threat groups.

A second form of attribution is through the target organisation when they publicly identify a specific attacker as the source of the attack. The attribution claims are usually born from past experiences, suspicions or known animosities between a threat group and the organisation. This attribution usually has low confidence as, in most cases, there is not enough public information available to corroborate the claims. This method should not be trusted since false attribution can be easily done and can muddy the waters for serious research.

A third form of attribution is through a deep analysis of the distribution of source IP addresses to identify where most attacks originate. This type of analysis is based on the hypothesis that first, not all the source IPs are spoofed; second, not all the participants are really distributed around the world; and third, some core infrastructure for the attack is used repeatedly to provide some consistency in the attack. 'Distributed' refers to the type of organisational attack where a coordinating group asks volunteers to participate, for free or for money, in their DoS attack by using a botnet-style tool. There are not many of these reports, but in the ones published, the attribution has a strong technical basis[30].

Ultimately, the precise attribution of a cyberattack may not significantly alter the approach of defenders. For those tasked with safeguarding systems, understanding who is behind an attack is less critical than knowing how to effectively counter it. Their focus remains primarily on implementing the necessary defensive measures, regardless of the attacker's identity.

[30] S2 Research Team, 'A blog with NoName – Further insight into the hacktivist operation targeting NATO and affiliated nations', Team Cymru website, 27 January 2023, accessed 7 September 2023, https://www.team-cymru.com/post/a-blog-with-noname.

8. DOS DURING ARMED CONFLICTS

The existence of large armed conflicts, such as the Russian war of aggression against Ukraine or the Israeli–Palestinian conflict, is the most prominent instigator for renewed waves of DoS attacks[31]. Most of these attacks are carried out against military targets, involve a tactical or strategic component and are classified as warfare or disruption.

DoS can also be used by unrecognised supporters of those at war, as a tool for retaliation or revenge against supporters of their enemy. These attacks usually seek media attention and, therefore, are targeted at websites and publicly recognised on the internet. Additionally, DoS attacks like these ones usually have as a by-product the gaining of supporters for their cause by showing their power.

During armed conflicts, DoS attacks may have the support of more experienced and resourceful attackers. This allows better tools to be created, larger network infrastructures to be maintained and, in consequence, larger and more stable attacks to be performed. Several reports describe the increase in DoS attacks after the start of the Russian war of aggression against Ukraine and the new techniques used[32][33]. Among the new variations identified are DoS simultaneous attacks from different cloud providers, a large increase in attacks using Tor and the confirmation that the NoName057(16) group primarily uses two very specific and country-related autonomous system number (ASN) networks to attack: MIRHosting and Stark Industries[34].

According to a traffic provider, of the total internet traffic to .ua domains in the first month of the war, 'DDoS attack traffic accounted for over 80 % of all traffic by early March 2022'[35], with this number dropping in the following months: '12.6 % of network-layer traffic was DDoS activity in Q1 2022'[36]. This means that it is hard to assess how many individual attacks happened and against whom[37].

The fog of war also covers the goals and details of the DoS attacks. For example, a possible unsuspected goal of a DoS attack may be to block the citizens of the attacking country from accessing the target sites. However, this tactic does not involve obstructing access by taking down the target site, but by forcing the attacked site to **block** the IP addresses of the attacking country, including their legitimate citizens. This is a commonly discussed problem among news sites and DoS protection providers, which may refuse to block the IP addresses of the country conducting the DoS to avoid blocking its citizens' access to the news.

[31] CERT-EU, 1 Year Ukraine – Russia's war on Ukraine: One year of cyber operations, 2023, https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.
[32] Craig, 'How to survive getting DDoSed by Anonymous, Cyberberkut, Killnet and noname057(16) since 2012', media.ccc.de website, 2023, accessed 2 August 2023, https://media.ccc.de/v/camp2023-57023-how_to_survive_getting_ddosed_by_anonymous_cyberberkut_killnet_and_noname057_16_since_2012
[33] Costin, A., Khandker, S., Hämäläinen, T. et al., 'Cybersecurity of COSPAS-SARSAT and EPIRB: Threat and attacker models, exploits, future research', arXiv website, 16 February 2023, accesses 28 August 2023, https://doi.org/10.48550/arXiv.2302.08361
[34] S2 Research Team, 'A blog with NoName – Further insight into the hacktivist operation targeting NATO and affiliated nations', Team Cymru website, 27 January 2023, accessed 7 September 2023, https://www.team-cymru.com/post/a-blog-with-noname.
[35] Tomé, J., Belson, D. and Berdan, K., 'One year of war in Ukraine: Internet trends, attacks, and resilience', The Cloudflare Blog website, 18 October 2023, accessed 26 August 2023, http://blog.cloudflare.com/one-year-of-war-in-ukraine/.
[36] Ibid.
[37] Ibid.

9. RECOMMENDATIONS FOR PREVENTION AND REMEDIATION

DoS attacks are a prevalent global problem, and this study shows that no organisation is exempt from being a potential target of these attacks. The nature of the threat makes it clear that there are no easy ways to predict how organisations become a target. DoS can be rooted in various factors, from personal grudges to warfare. The recommendations in this report are grouped into **prevention** and **remediation**. Prevention is still the most important way to avoid a DoS attack, but remediation is necessary as a last resort and contingency plan.

9.1 PREVENTION

Like other cybersecurity attacks, the best protection against a DoS attack starts with good prevention. Prevention means having good threat modelling, assessing the risk of being the target of a DoS attack, assessing the possible threats and assessing vulnerabilities or weak links in the organisation and infrastructure. The first step in a threat model should be to identify the position of the organisation in the threat landscape and its value as a target. Critical infrastructure, governmental agencies and media are usually the most important areas to keep safe.

A good threat model should also consider the increasing power of DoS attacks shown in this report. If the organisation is at risk of being related to a military conflict, and if the organisation is related to critical infrastructure, this study recommends actively working to prevent DoS attacks[38].

Among the most standard protections against DoS attacks are the use of **content delivery networks (CDN)**, **upstream internet service provider protection**, **cloud service providers' DoS protections** and **on-premises solutions**[39]. Different solutions meet different needs and different levels of acceptance of downtime. It is important to note that the new layer-7 attacks may overcome most protections, given that they will reach the website's back end easily. Therefore, it may be necessary to design an on-premises solution tailored to a layer-7 attack, even if other protections are in place. However, this report strongly recommends having automatic solutions and not only manual activations.

Another concern that a threat model should evaluate is the privacy of the data and the legality of having cloud-based DoS protection organisation take care of the service to be protected. In most cases, such as protecting a website, cloud-based DoS protection needs to open the web encryption and access the content of the private information to provide its protection service, and therefore all communication to and from the website would be shared with the DoS protection organisation. This should be evaluated in the balance of power of protection, privacy and legality (especially considering the rules set out in the general data protection regulation).

9.2 REMEDIATION

Remediation is concerned with actions to decrease the impact of the attack, including the technical impact and the mediatic impact. Organisations should understand that it is not possible to fully mitigate the risk of a DoS attack ([40]). Therefore, designing a remediation plan is vital.

[38] US Cybersecurity & Infrastructure Security Agency, Capacity Enhancement Guide: Volumetric DDoS against web services technical guidance, 2023, https://www.cisa.gov/sites/default/files/2023-09/TLP%20CLEAR%20-DDOS%20Mitigations%20Guidance_508c.pdf.
[39] US Cybersecurity & Infrastructure Security Agency, Understanding and Responding to Distributed Denial-of-Service Attacks, 2022, https://cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf.
[40] US Office of Information Security, 'HC3: Analyst note – Pro-Russian hacktivist group "KillNet" threat to HPH sector', 2023, https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf.

Remediation should include confirming the attack, verifying whether protection measures were activated, contacting the third-party DoS protection organisation (if any), contacting other partners that should know about the downtime and considering whether to make an official media statement.

The media statement should consider the responsibility and legal obligations to customers and clients, the need to explain why the service is not working and the impact of confirming to the attacker that the attack was successful. Since most DoS attacks are mediatic in nature, answering in the media can also be counterproductive.

The last step of the recommendations is to report the attack to the authorities. Despite DoS attacks being hard to confirm and not leaving many artefacts behind to analyse, a conscious report of an attack to the proper organisation is paramount for building the knowledge that can later support actions regarding DoS attacks. Without good reporting there cannot be an organised understanding of the problem.

10. CONCLUSIONS

Unlike other cybersecurity attacks, detecting and analysing DoS attacks poses a considerable challenge, distinct from other cybersecurity threats, where attackers often leave traceable artifacts.

This report presents a study and analysis of DoS incidents identified between January 2022 and August 2023. The analysis is grounded on a proposed classification scheme for DoS attacks.

Although DoS attacks are one of the earliest appearing cyberthreats, they are still evolving. As the cost of launching DoS attacks gets lower, the tools get easier to operate and the available bandwidth increases, organisations face unique challenges to protect themselves from these attacks. While the DoS field is growing, new types of DoS attacks will likely appear, that will highlight additional features for classification. The proposed classification is by no means exhaustive or all-encompassing in this regard.

The change in DoS attacks is, however, not only technical or merely related to the amount of bandwidth available. The current DoS threat landscape is severely influenced by the current armed conflicts, especially the Russian war of aggression against Ukraine. This report highlights the importance of analysing and studying the motivations and goals behind this type of attack, showing how there has been a change in the motivations as the new waves of DoS attacks are more motivated by revenge, retaliation and warfare.

This study also shows that public/government infrastructure is a particularly preferred target of threat groups, and DoS attacks are often successful and impactful in causing downtime and attracting the necessary media attention. However, this study shows that no sector is exempt from DoS attacks. Even small organisations can be targets of DoS attacks as threat groups train others on how to conduct successful attacks.

This study also highlights the current lack of maturity surrounding the reporting of DoS attacks. Contrary to other cybersecurity threats, where organisations are more compelled to report that a data breach has occurred or that a supply chain attack took place, organisations are not sufficiently reporting on DoS attacks. New and better mechanisms to identify the attacks and report them should be put in place to allow governments and supporting entities to measure, quantify and better provide assistance in these cases.

Although DoS protection companies report that thousands of attacks are prevented every hour, there is a general lack of good reporting of DoS incidents by online media and cybersecurity companies. The classification scheme proposed in this report aims to help with better and more unified reporting and documenting of DoS incidents that would allow more in-depth future research in the area.

Threat modelling is the right approach for organisations to measure the potential risk of DoS attacks, the impact of such an attack and the best strategies for prevention and remediation based on the organisations' technology and resources.

978-92-9204-647-7

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-647-7
DOI: 10.2824/859909