NEXUSGUARD®

2025 DDoS Trends Report

Executive summary

Like most forms of cybersecurity, Protecting from Distributed Denial of Service (DDoS) attacks is a never-ending cat-and-mouse game. As this report shows, DDoS attacks come in many different shapes and sizes and attackers constantly shift their tactics.

In this annual report on DDoS trends, we have taken a different approach than previous iterations. In the following pages, you can find our top 10 takeaways. Full charts and data points are available in the index section.

When looking at DDoS trends, we can split these into two categories - broader 'macro' trends that we can track the progress of over longer periods and small 'micro trends' that focus on attack specifics and often vary wildly between reports.

For broad patterns, we must look at the size and volume of attacks. The former is perhaps the biggest takeaway from this report: the average attack size continues to increase, but this is mostly driven by a few very large attacks. These obscure a vast sea of small, short-burst attacks that still make up the bulk of attacks, suggesting that attackers are selectively saving their resources for larger and more impactful attacks.

Unsurprisingly, the most common attack categories and vectors have changed drastically from our previous report. These changes in method and vectors of attack (micro trends) are what make DDoS mitigation such a complex but fascinating field. There are volatile shifts in attacker behaviour, here today and gone tomorrow, showing great variance but few long-term patterns. They are still worth studying in the short term, however, as they can tell us gaps in mitigation that need to be plugged.

HTTPS Flood stood significantly above the rest, accounting for a fifth of all attacks. Amplification attacks on the other hand, which were until recently the most popular attack category, have fallen away massively. Another attack vector worth drawing attention to is DNS, which is theoretically easy to mitigate against but is becoming increasingly fruitful for attackers – something most organisations likely underestimate, and therefore leave undefended as a possible attack vector.

Companies looking to protect themselves from DDoS efforts need powerful, well-rounded mitigation strategies. With huge variances in attacks, end-to-end hybrid solutions offer the most complete protection from the many tools in an attacker's toolbox.

Donny Chong,
Product Director
at Nexusguard

Key observations

- **The total number of DDoS attacks shows little change, up 2% YoY**
- **85% of DDoS attacks are less than 1Gbps.** The average attack size, which grew 69% YoY, is largely driven by a small number of massive attacks, as seen by a 37% YoY increase in the maximum attack size.
- **HTTPS Flood is the top attack method,** making up 21% of all attacks
- **Amplification attacks (category) have decreased** by around 74% YoY

Key metrics

Total Attacks

vs 2023	+2%

Attack Size

	Maximum	Average
	962.2Gbps	1.35Gbps
vs 2023	+37.46%	+68.75

Attack Length (minutes)

	Maximum	Average
	42018m	140m
vs 2023	+73.15%	+3.73%

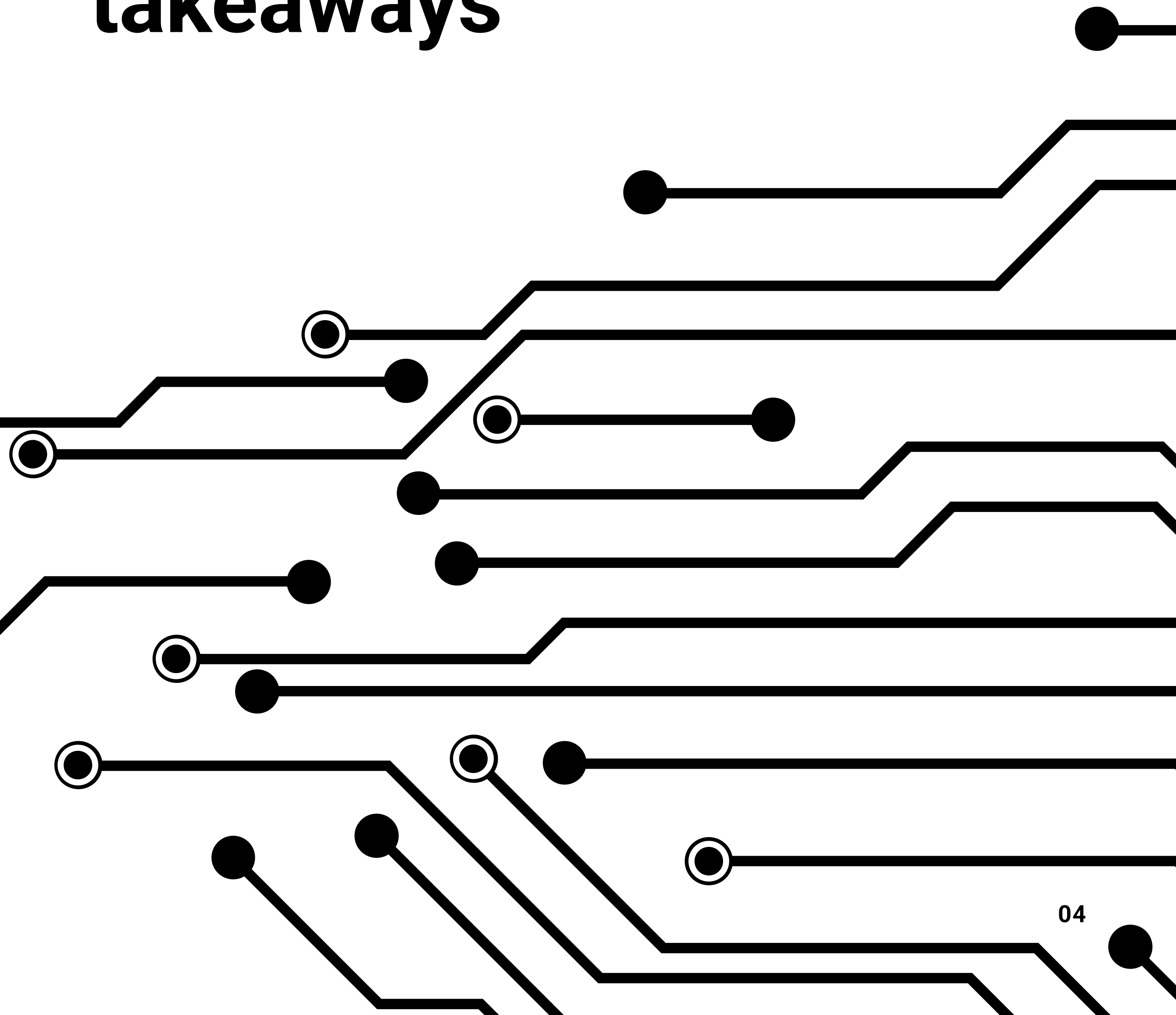
Top 3 attack types

	1	2	3
	HTTPS Flood (^1)	UDP Attack	UDP Fragmentation Attack
vs 2023	-24.78%	-5.77%	+27%

Attack Category

	Volumetric (Direct Flood)	Application Attack	Volumetric (Amplification)
	47.92%	24.96%	27.11%
vs 2023	+53.55%	-26.72%	-74.34%

Top 10 findings/ takeaways



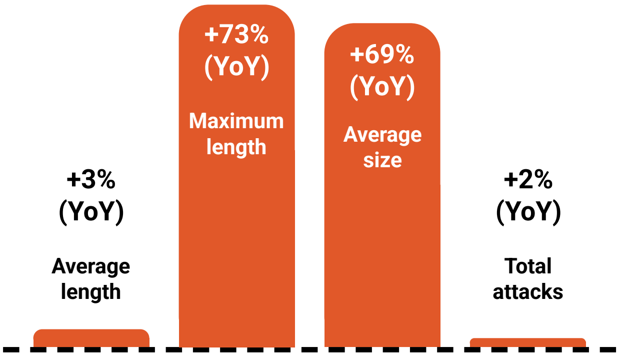
01 Big peaks of headline-worthy attack sizes mask an army of small DDoS attacks

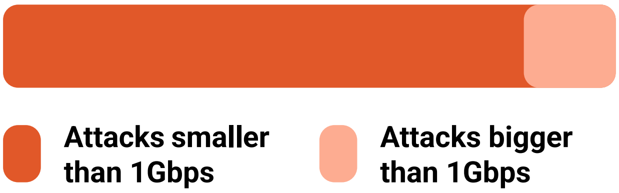
When looking at the statistical trends in DDoS attacks, the devil is often in the details. However, we will start our key takeaways by looking at the big picture.

On the surface, the total number and frequency of DDoS attacks remains largely unchanged in 2024, only up 2% YoY. But taking a closer look at the numbers reveals an ongoing trend in the current shape of DDoS attacks: a small number of extremely large attacks are inflating the average attack size, but the majority of DDoS incidents remain relatively small. This means attackers are adopting a two-pronged approach: launching frequent small-scale attacks while occasionally deploying massive, highly impactful ones. This is most likely a consequence of attackers trying to save their resources for more targeted attacks that wreak more havoc.

For some perspective, the average attack size has noticeably risen Year-on-Year – 69% increase compared to 2023 – but the more interesting observation is that 85% of attacks remain under 1Gbps in size. A small number of massive attacks are substantially inflating the average.

A similar observation can be made about the duration of attacks. While the longest attacks have become more extreme, with a 73% YoY increase in maximum duration, the majority of attacks remain short. In fact, 84% of attacks lasted under 90 minutes, and the average attack duration only rose slightly (105 minutes in 2024). This suggests that while ultra-long attacks are growing, most DDoS incidents continue to follow the short-burst pattern favoured by attackers. Balancing this out is the fact that attacks on the very long end are becoming more frequent, with 1 in 10 now lasting several hours.





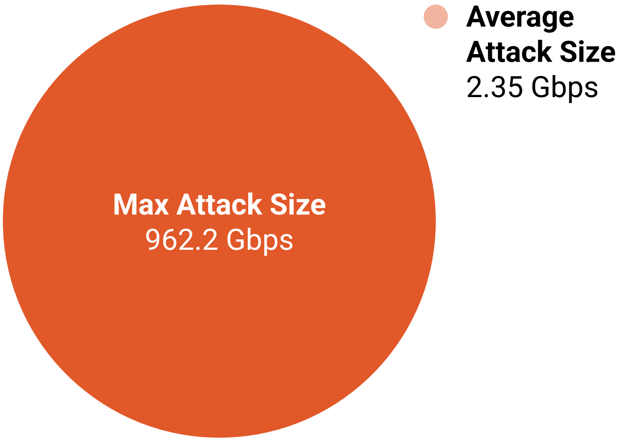
> ***"DDoS attacks have bucked the trend we normally expect to see in cybersecurity: more attacks happening more often. But this is no reason for businesses to be complacent about DDoS attacks. It doesn't take much effort or time to cause disruption. Attackers seem very aware of this, judging from our data, because they're focusing most of their attention on small and short attacks. Longer and bigger-scale attacks are being reserved for targeted campaigns in the places where they will hurt the most. We should never lose sight of the diverse tactics criminals employ. Yes, 'bigger' tends to draw more attention, but the risk is that smaller attacks go unnoticed and are not shut down as quickly."***
> **Donny Chong - Director, Nexusguard**

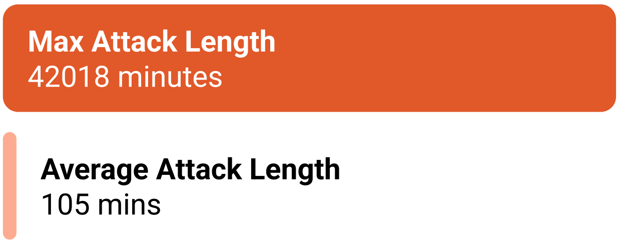
02 The Scary 1%

Most headlines and industry reports on DDoS focus on the increasing size of attacks. It's easy to see why - size matters in DDoS, and bigger attacks mean bigger problems. It is important, however, to remember that when doing this, we are only looking at the top 1% of attacks. These attacks are, admittedly, massive, but they are also rare. Still, they are a helpful example, or perhaps a warning, of what is now possible for DDoS attacks. .

The vast majority of attacks – typically around 1Gbps – are dwarfed in comparison to the largest attack we've seen so far this year (962.2Gbps). The same is true for the length of attacks. The distribution of attack sizes reveals that 85% of attacks are under 1Gbps and it's a similar story with attack length, 84% last under 90 minutes. Ultra-long attacks, while still a major drain on resources, should not be as concerning to an organisation with appropriate DDoS mitigation. Often these attacks are average size or even small in size, and the reason they run so long is they make little impact to the network and as such go undetected.

With attack size, however, the impact of the top 1% is severe, and the upper limit of what is possible is increasing. This is a trend that has continued from recent reports. The maximum attack size so far in 2024 was 962.2 Gbps - this naturally dwarfs the vast majority of attacks under 1Gbps. To put it in perspective, 962.2 Gbps is greater than the bandwidth of all but the largest enterprise networks, most non-hyper scaler CSPs and even some smaller ISPs.





> ***"With attack size, the gulf between the majority of attacks and the top 1% is so severe that it is hard to talk about them in the same conversation. One is a daily threat to businesses or ISPs which, while serious, can be mitigated. The other is closer to an act of god. It is hard to make predictions in DDoS, but the maximum size of attacks gradually increasing over time is one of the few you can confidently make. Computing resources only increase over time, and with more and more devices online every year, the size of botnets will only go up (see takeaway 7)."***
> **Donny Chong - Director, Nexusguard**

02 The Scary 1%

DDoS in the media

Outside of statistical reports, what most people see of DDoS 'in the wild' is through headlines. These naturally tend to be larger, something attacks, on high profile targets

Swiss websites hit by DDoS attacks during World Economic Forum in Davos

In January, Swiss websites, including those of the Federal Administration, were targeted by DDoS attacks from the politically motivated Russian hacker group NoName. Critical government resources, along with airports, railways, hotels, and restaurants, were impacted as NoName sought to disrupt infrastructure and protest perceived anti-Russian actions by European nations.

Top UK Universities Targeted by DDoS Attack

Shortly after, the hacktivist group Anonymous Sudan launched a DDoS attack on UK universities, disrupting student IT services at the University of Cambridge and Manchester. The group cited the UK's support of military action in Gaza and Yemen as the motive, attacking the high-speed data-sharing network used by multiple institutions.'

Cyber-Espionage Teams Target Asian Telecoms

In the first half of the year, Asian telecom operators were targeted by attackers who placed backdoors, stole credentials, and deployed custom malware to access valuable data and compromise other systems. These espionage-driven attacks aimed to leverage telecom networks for future cyber operations, demonstrating the strategic importance of telecom infrastructure.

03 Don’t underestimate the ‘little guys’

So, we’ve looked at the top 1% or ‘maximum’ attack sizes and while these often capture the imagination, it’s important not to let this warp our sense of scale.

While media headlines, and even many other industry reports, tell of “the largest attacks recorded to date”, the vast majority of organisations will not have to deal with attacks anywhere near this size.

However, that doesn’t mean they should underestimate the impact of the average ‘smaller’ attack. In fact, after looking at these ultra-massive attacks, it’s important to recalibrate our sense of scale - and challenge the notion of these attacks being ‘small’.

For context, the average Google search uses about 3MB of bandwidth. So, the average DDoS attack generates roughly the same amount of traffic as around 56 simultaneous Google searches every second, or 135,000 emails sent every second, 34 songs downloaded on Spotify per second or 338 HD video streams at 4 Mbps.

While it may appear to be a ‘little’ attack, small or even medium-sized resources could be easily overwhelmed by such a surge, especially when on top of regular requests. Even large-scale applications, which are typically built to handle significant volumes of traffic, could be slowed down or put under strain. So ‘small’ attacks can still mean big problems - disrupted services, the need for emergency scaling, or even downtime. If that’s not enough, the ripple effects of this kind of traffic overload can extend far beyond just the immediate service, impacting connected systems or networks - they might appear ‘little’ but they pack a mighty punch.

56
Google Searches per second

338
Simultaneous HD video streams

Sending
135k emails every second

Downloading
34 songs from Spotify every second

04 The DDoS Stock Exchange

While our top three takeaways focused on broad ‘macro’ trends, showing the scale and shape of attacks, mitigating DDoS threats requires diving into details. This means looking at attack vectors.

Compared to the big-picture trends, patterns are much harder to predict here. Favoured attack vectors rise and fall and rise again. You can compare it to the stock market, attackers will bet on a certain attack while it pays dividends, but as soon as the market responds they will drop it in favour of something more lucrative.

This became evident in 2024 when we saw the continued rise of HTTPS Flood attacks and the fall of NTP Reflection.

The rise of HTTPS Flood is particularly interesting; it now accounts for a fifth of all DDoS attacks – a significant amount for a single attack vector. For comparison, DNS Reflection and UDP Fragmentation were the next dominant attacks, responsible for 13.99% and 13.38% respectively.

This illustrates the constantly shifting nature of DDoS attacks, attackers can pick from a dense toolbox of vectors and organisations need to be prepared for any, and all, of them.

We explore the implications of some of these attack vectors in the following sections, but the main takeaway here should be how quickly the scene can change.

Teams in charge of DDoS mitigation need to keep abreast of attack trends and ensure they can defend against the most common methods. However, they also need to be prepared for anything, as different methods can come out of the woodwork at a moment’s notice.

“Nowhere is the complexity and variance of DDoS attacks more evident than when analysing attack categories. Working in this space for nearly 15 years, I’ve seen methods rise and fall in popularity many times. Rather than newer, better methods replacing the old ones, it’s often more cyclical, attack types fall in and out of fashion. For example, attacks that were widely used last year are now nowhere to be seen. Does that mean it’s gone, and we must stop mitigating it? Absolutely not. As soon as a vector starts paying dividends for attackers, we will see it return.”
Donny Chong - Director, Nexusguard

04 The DDoS Stock Exchange

						Diff. by percentage	Diff by. actual value
	Attack Type	Type	Type	2024	2023	YoY	YoY
1	HTTPS Flood	TCP	APP	20.81%	16.19%	28.58%	24.78%
2	DNS Reflection Attack	UDP	AMP	13.99%	8.69%	61.08%	5.77%
3	UDP Fragmentation Attack	UDP	VOL	13.38%	6.16%	117.10%	27.00%
4	UDP Attack	UDP	VOL	10.06%	4.92%	104.31%	19.52%
5	NTP Reflection Attack	UDP	AMP	9.73%	38.90%	-74.99%	-85.37%
6	DNS Attack	UDP	VOL	9.65%	0.54%	1688.61%	946.32%
7	TCP ACK Attack	TCP	VOL	5.75%	3.06%	88.24%	10.12%
8	HTTP Flood	TCP	APP	4.15%	3.75%	10.91%	35.12%
9	TCP SYN Attack	TCP	VOL	3.51%	2.09%	68.20%	1.60%
10	IP Fragmentation Attack	Others	VOL	2.98%	0.46%	553.68%	282.40%
11	SSDP Reflection Attack	UDP	AMP	1.18%	0.75%	56.91%	-8.21%
12	TCP SYN-ACK Attack	TCP	VOL	0.98%	0.00%		

05 HTTPS Flood in the hot seat

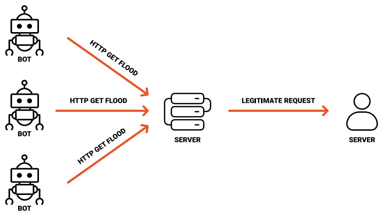
HTTPS Flood attacks stood out in 2024. While its relative share has decreased year-on-year, it's still the most common attack vector, making up about a fifth (21%) of all DDoS attacks. This suggests attackers are diversifying their attack methods, rather than relying solely on HTTPS Flood. The reason for this vector's popularity makes sense given its ability to consume server resources with encrypted traffic, making it harder to detect and mitigate.

An application layer attack, HTTPS Flood overwhelms the targeted server with a large amount of encrypted HTTP or HTTPS requests, flooding the server and causing it to slow down and potentially crash. HTTPS is dominating the DDoS landscape for several reasons. Firstly, regular HyperText Transfer Protocol (HTTP) has largely fallen out of use due to its lack of encryption. HTTP attacks were, naturally, quite popular but have obviously dropped alongside the protocol it looks to exploit. This volume has likely been picked up by HTTPS, as it uses similar methods and has similar aims.

The key difference with HTTPS is that the packets between the browser and server are encrypted. This means they are more resource-intensive (for the attack and the server), and mimic legitimate traffic, making it harder to spot and stop.

HTTPS' resource intensity is a large part of why it's such an effective attack vector, it means servers have fewer resources to handle large volumes of traffic and so are vulnerable to overloading. For attackers, the resource required to launch this attack may be a factor in the drop in attack volume, but the use of botnets or cloud resources can be used to distribute the load, making the attack feasible. So, with a large enough network of compromised devices, attackers can still generate the volume of traffic needed for a successful HTTPS flood.

WANTED



PUBLIC ENEMY NO. 1:
HTTPS FLOOD ATTACK

Alias: "Web Server Overwhelm"
Attack Method: Bombards a target web server with a high volume of HTTPS requests, using encrypted communication to consume more resources.
Target: Websites, web services, and cloud platforms.
Payload: HTTPS GET/POST requests designed to overload server processing capacity.
Effect: Causes slowdowns or total service outages for legitimate users by overloading the target's resources.
Threat Level: High – particularly resource-intensive and more difficult to mitigate due to encrypted traffic
Modus Operandi: Uses botnets to issue thousands of encrypted requests, forcing web servers to allocate processing power to decrypt and respond, consuming bandwidth and server resources

> ***"As HTTPS continues to dominate, it is more important than ever that organizations have multilayered applications protection. Like a physical filter has several layers, effective DDoS mitigation combines methods like Web Application Firewalls, Load Balancing and Real-Time Monitoring."***
> **Donny Chong - Director, Nexusguard**

06 Don’t sleep on DNS

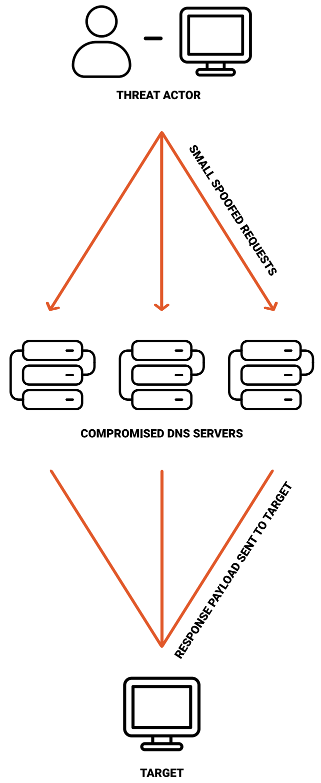
Another attack vector worth drawing attention to in this report is attacks targeting the arguably overlooked vector, Domain Name System (DNS). This started almost a year ago with DNS Reflection Attacks. One of the top attack vectors in the previous report, these use DNS as a tool to launch attacks on other targets .

In 2024 however, we are seeing a dramatic shift towards DNS Attacks - up 876% Year-on-Year. This surge may be due to a combination of factors: many organizations lack robust DNS-layer protection, and attackers are shifting toward less-defended infrastructure. Additionally, improved detection capabilities may have contributed to better visibility into DNS-layer attacks, further increasing the number of reported incidents.

As the name of the attack vector suggests, it specifically targets the DNS server itself. Sometimes described as the ‘internet phonebook’, DNS (Domain Name System), translates website domains as humans see them, (e.g. www.nexusguard.com) to machine-readable IP addresses (e.g. 192.0.2.44). This request—a DNS query—is triggered each time someone visits a website, and as such is a vector for DDoS attacks.

DNS-level attacks flood DNS servers with these queries, and because DNS is so critical for internet communication, this can quickly affect website availability or bring down service entirely. These attacks are fairly easy to execute, not requiring sophisticated techniques like spoofing or reflection. However, they are also fairly easy to detect and mitigate. This is exactly what makes this trend particularly concerning, and is perhaps why we are seeing these attacks on the rise - many businesses are unaware that DNS can be targeted for DDoS attacks, and as a result, many companies lack protection. With this in mind, it’s more important than ever that companies don’t sleep on DNS threats and ensure their online sites and servers include DNS-level DDoS mitigation.

DNS attacks are up 876% year-on-year



DNS Reflection Attack	UDP	AMP	13.99%	8.69%	61.08%	-5.77%
DNS Attack	UDP	VOL	9.65%	0.54%	1688.61%	946.32%

07 More devices, more problems

In this report, the top three attack methods (HTTPS Flood, DNS Reflection, UDP Fragmentation) all commonly use botnets to increase their power and make them more difficult to mitigate. While the concept of botnets—networks of infected computers or devices remotely controlled by attackers to overwhelm targets with traffic—is not new, the scale of this threat and the number of potential bots available for exploitation is rapidly expanding.

Currently, it is estimated that there are over 15 billion connected devices connected to the internet worldwide. Thanks to the growth of smart devices and the Internet of Things (IoT) this number has skyrocketed in recent years and will continue to do so. GSMA Intelligence forecasts IoT connections to reach more than 38 billion by 2030.

Volumetric and Application layer attacks often use botnets as they allow the attacker to generate massive amounts of traffic or requests from a distributed set of compromised machines, making the attack larger and more difficult to mitigate. As the number of connected devices globally continues to rise, so will the threat from these kinds of attacks.

Growth of connected devices on Earth - 2024

Growth of connected devices on Earth - 2030

H1's DDoS red herring

At the start of the year, we saw a big piece of DDoS #fakenews grip the tech world. A false report stole the headlines, claiming that 3 million smart toothbrushes were being used in a DDoS attack. While this story (unsurprisingly) turned out to be false, theoretically it is entirely possible. Practically any 'smart device' from a toothbrush to a dishwasher can be weaponised in a botnet. So while you don't need to fear your toothbrushes (not yet anyway), the next DDoS attack utilising household appliances could well be a reality.

08 The rising threat of TCP SYN-ACK

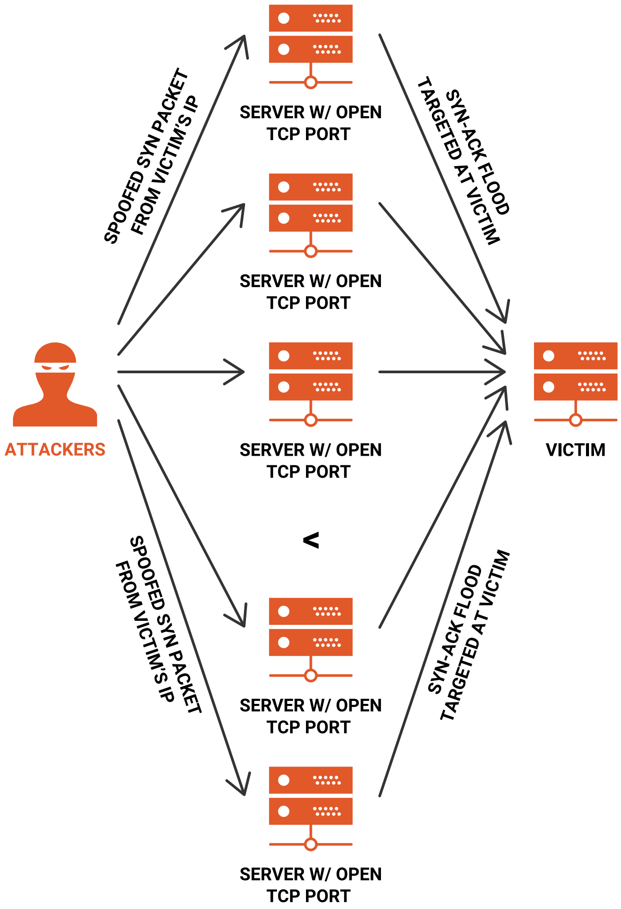
As a building block of the internet, Transmission Control Protocol (TCP), ensures reliable communication between devices. Naturally, this means that DDoS attacks exploiting this process are fairly common.

TCP uses a three-part 'handshake' process to establish a stable connection between client and server - SYN, SYN-ACK, and ACK. Unfortunately, all three steps of this handshake can be exploited by DDoS attacks, and all three of these methods are on the rise.

While ACKand SYN-based attacks rank as the 7th, 9th, and 12th most common types of DDoS attacks, it's the SYN-ACK attack, despite being only the 12th most frequent, that draws the eye. Despite accounting for just over 1% of DDoS attacks in 2024, it is rising fast, appearing in our top 12 for the first time.

So, while SYN and ACK-based attacks are by no means new, attacks targeting SYN-ACK, the middle step of the handshake process have been relatively uncommon - until now. SYN-ACK spoofs requests forcing servers to waste resources matching responses to requests that don't exist.

This technique is particularly dangerous because it's harder to distinguish from normal traffic, making defences more challenging. The increasing availability of botnets could also make these attacks more frequent and harder to counter. As these types of attacks continue to grow, organizations must enhance their network defences and adopt advanced DDoS protection strategies to keep up with evolving threats.


SPOOFED SYN PACKET FROM VICTIM'S IP
SERVER W/ OPEN TCP PORT
SYN-ACK FLOOD TARGETED AT VICTIM
SERVER W/ OPEN TCP PORT
ATTACKERS
SERVER W/ OPEN TCP PORT
VICTIM
<
SPOOFED SYN PACKET FROM VICTIM'S IP
SERVER W/ OPEN TCP PORT
SYN-ACK FLOOD TARGETED AT VICTIM
SERVER W/ OPEN TCP PORT

09 De-amplification

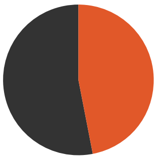
Often with statistical DDoS reports, looking at the popularity of the three broad attack categories (Direct flood, Amplification and Application) doesn’t tell us a great deal. We tend to see a fairly even split, with one leading the pack. In this report, we’ve seen a much starker shift.

In recent years, amplification attacks (volumetric attacks which exploit vulnerable services to turn small requests into large attacks) have been the most popular attack category. These attacks were likely popular because they required fewer resources from attackers, giving them great ‘bang for their buck’.

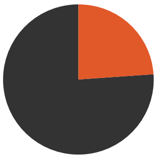
However, in 2024 this has changed dramatically - with amplification attacks making up just over a quarter of all attacks in 2024. This is a significant decrease, down by 74.34% when compared to 2023, where it was the most popular category. In its place, Direct Flood dominated in 2024, making up nearly half of all attacks, a 53% increase on last year.

But why have amplification attacks fallen away? The significant drop may be attributed to improved filtering and mitigation strategies that make traditional amplification vectors harder to exploit. At the same time, attackers appear to be shifting toward direct botnet-based attacks, which are harder to detect.

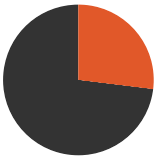
The increase in UDP Fragmentation attacks suggests that rather than abandoning volumetric DDoS, attackers are favoring alternative high-bandwidth techniques that evade modern defenses.



Volumetric (Direct Flood): 47.92%
Volumetric direct flood attacks use large amounts of malicious traffic to flood a server or network to consume as much bandwidth as possible and overwhelm the target’s network capacity.



Application attack: 24.96%
Application attacks target the ‘top layer’ of a server or system where common internet requests occur. They overwhelm it with illegitimate requests or traffic to slow down the target and even crash it completely, making it unavailable to legitimate users and requests.



Volumetric (Amplification): 27.11%
Volumetric amplification attacks use amplification to overwhelm a target with traffic by sending legitimate requests to a server from a spoofed IP address. This causes the server to respond to the request, using the spoofed IP address which is actually the intended target of the attack.

> **“Attack categories are chief amongst the ‘micro trends’ which are constantly shifting and changing. The significant drop in amplification attacks is noteworthy, however, as this has been the most popular attack category in recent reports. Attackers seem to be mixing up their tactics to more varied and potent attack types such as protocol (TCP Syn Floods) and application layer attacks (HTTP Floods).”**
> **Donny Chong - Director, Nexusguard**

10 End-to-end protection is the only way

If you are reading this report for insight on how best to protect your organization or network from DDoS threats, you could be forgiven for feeling overwhelmed by the various threats and increasing resources at attackers' disposal.

But the good news is, that the answer to all of this is fairly simple. End-to-end hybrid protection offers the most comprehensive defense against modern DDoS threats, as it balances cloud scalability with on-premise responsiveness. With attacks getting larger, networks need powerful mitigation tools to protect themselves. At the same time, attacks like HTTPS flood can be harder to detect, so being able to spot malicious traffic is both more difficult and more important than ever to stop these attacks. However, organizations should tailor their DDoS strategy to their specific risk profile, operational needs, and infrastructure constraints.

With all of this alongside huge variances in attacks, only end-to-end hybrid solutions offer complete protection from the many tools in an attacker's toolbox.

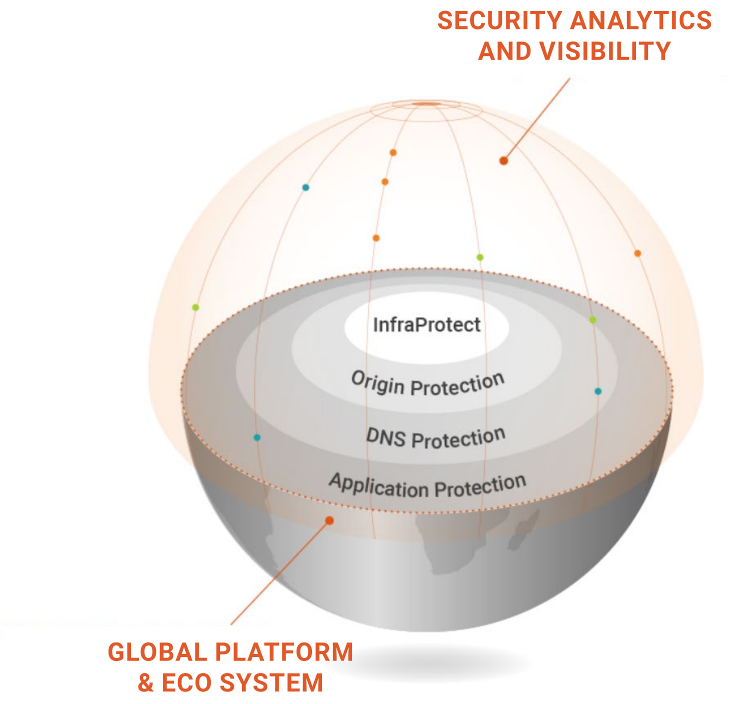
The unpredictable nature of DDoS attacks makes it clear that outdated or single-point solutions are no longer enough. To effectively combat these threats, businesses must adopt end-to-end protection, ensuring a comprehensive defence strategy capable of adapting to an ever-evolving threat landscape. Organizations must implement robust DDoS mitigation services that can handle both large-scale attacks and more sophisticated, stealthy threats

Nexusguard can help businesses meet these challenges, whilst also providing solutions to common blockers for implementing extensive DDoS mitigation such as skills gaps, cost and scalability.

- **Hybrid DDoS Mitigation:** Nexusguard offers hybrid solutions combining on-premise and cloud-based protection, providing comprehensive coverage against diverse attack types.
- **Bastion Servers and Services:** Nexusguard's "cloud-in-a-box" Bastion servers integrate proprietary technologies with global cloud scrubbing capabilities, offering a seamless hybrid experience. Deployed on-premises, these servers enable rapid local mitigation for critical traffic.
- **Transformational Alliance Partner (TAP) Programme:** Tailored for Communications Service Providers (CSPs), Nexusguard's TAP programme delivers customised, cost-effective DDoS protection, empowering CSPs with the technology, processes, and expertise to build and profit from DDoS mitigation services.
- **Nexusguard Academy:** Nexusguard offers practical training courses that equip teams with actionable skills in DDoS mitigation, ensuring businesses have the expertise to

By offering these comprehensive solutions and services, Nexusguard enables businesses to implement robust, multi-layered DDoS protection strategies capable of adapting to the evolving threat landscape.

10 End-to-end protection is the only way



Methodology

As a global leader in Distributed Denial of Service (DDoS) attack mitigation, Nexusguard observes and collects real-time data on threats facing enterprise and service-provider networks worldwide. Threat intelligence is gathered via attack data, research, publicly available information, Honeypots, ISPs, and logs recording traffic between attackers and their targets. The analysis conducted by our research team identifies vulnerabilities and measures attack trends worldwide to provide a comprehensive view of DDoS threats.

Attacks and hacking activities have a major impact on cybersecurity. Because of the comprehensive, global nature of our data sets and observations, Nexusguard is able to evaluate DDoS events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on our global research network. These threats, among others, are summarized in the Annual Statistical Report.

Index

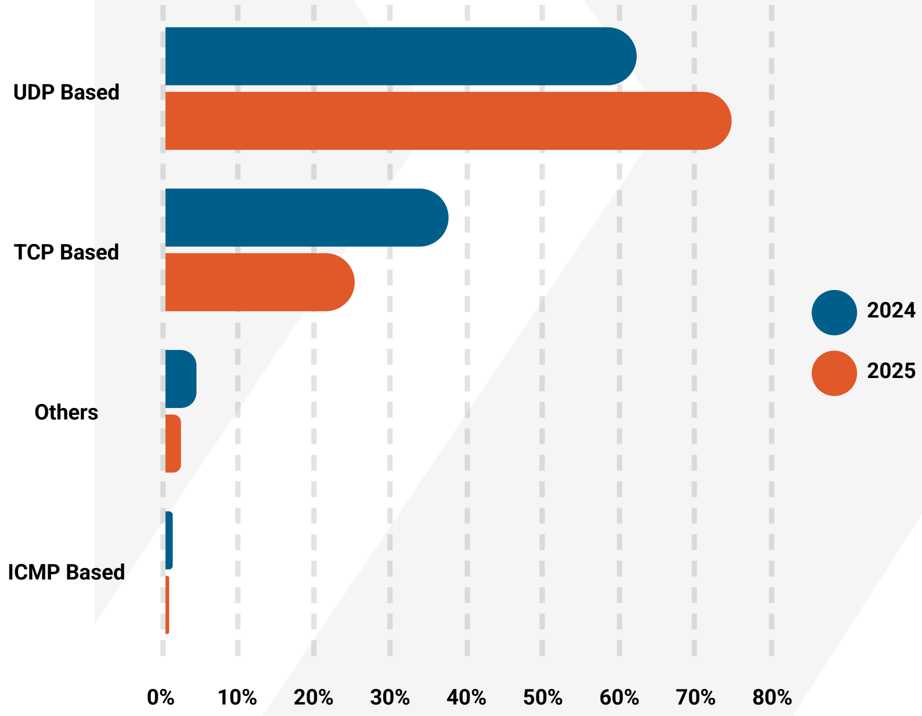
Attack Length

Duration (Minutes)	2024	2023 (YoY)	YoY Change
Maximum	42018.52	24267.33	73.15%
Average	105.41	101.68	3.73%

Duration (Minutes)	Percentage 2024	Percentage 2023
<90	83.64%	81.15%
90-240	7.04%	8.81%
240-420	2.76%	4.46%
420-720	2.15%	1.93%
720-1200	2.95%	2.74%
1200+	1.46%	0.91%

Attack Protocol

	2024	2023 (YoY)	Diff by percentage
	Percentage		
UDP Based	60.33%	73.50%	-17.92%
TCP Based	35.87%	25.46%	40.86%
Others	3.22%	0.58%	452.37%
ICMP Based	0.58%	0.46%	27.71%



Attack Vector	Count
1	281,976
2	46,269
3	22,644
4	1,563
5+	687

Total count - 353,139

About Nexusguard

Founded in 2008, Nexusguard is a leading distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance.

Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communications service providers to deliver DDoS protection solutions as a service.

Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime. Visit **www.nexusguard.com** for more information.

Contact:

https://www.nexusguard.com/contact-us