LINK11

EUROPEAN CYBER REPORT

2025 Mid Year

www.link11.com

Dear readers,

DDoS attacks are no longer a marginal phenomenon, but have become a central threat to companies, public institutions, and entire digital infrastructures. The figures and examples documented in the Link11 European Cyber Report illustrate the scale of the problem: attacks in the terabit range, packet rates in the hundreds of millions, and increasingly sophisticated Layer 7 strategies that are almost indistinguishable from regular traffic.

Our job as a security provider is not just to respond to these developments, but also to stay one step ahead of them. Modern attackers rely on precision, deception, and economic efficiency—we rely on automation, artificial intelligence, and experience. This is the only way we can ensure that digital business processes and critical services remain available, even as attacks continue to escalate.

The European Cyber Report is intended to provide guidance and increase awareness of the dynamics of a threat that can no longer be measured in numbers alone, but rather in its ability to undermine trust in and the stability of digital systems.

With Link11 at their side, companies can strengthen their digital resilience and protect critical systems in the long term.

I hope you find it an interesting read!

Best regards
Jens-Philipp Jung, CEO, Link11

Inhalt

Executive Summary

The threat posed by distributed denial-of-service (DDoS) attacks intensified dramatically in the first half of 2025. The Link11 network recorded 225% more attacks than in the same period last year. This represented not only a massive increase in quantity, but also a qualitative evolution in the methods used to carry out the attacks.

Key findings

Strong increase in large-volume „ISP killer attacks“

Backbone attacks increased by

143 %

and threatened the infrastructure of providers and data centers.

Attack duration at record levels

The longest documented attack lasted

over 8 days,

following the documented pattern of a coordinated long-term campaign with changing attack methods.

Explosive data volume

The cumulative attack volume rose from 110 TB to

438 TB

– enough for 7 years of Netflix streaming in 4K.

Record bandwidth and packet rates

Maximum values of

1,2 Tbit/s

and **207 million packets per second** can overload even high-performance systems.

> *“The dimensions are truly frightening. In the first half of 2025, 438 terabytes of DDoS traffic were moved. That‘s more than seven years of uninterrupted Netflix streaming in 4K. Numbers like these illustrate the threat better than any statistics.”*

Jens-Philipp Jung, CEO, Link11

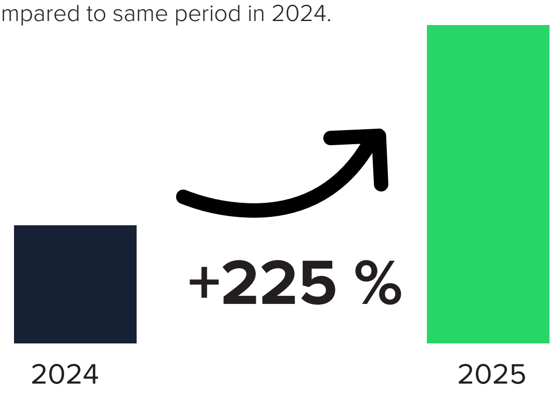
In addition to these technical dimensions, politically motivated attacks continued to increase. Groups such as NoName057(16) targeted critical infrastructure in Europe, often in connection with geopolitical events. The findings of the IBM X-Force 2025 Threat Intelligence Index[1] confirm this trend: in 2024, 70% of all attacks examined were directed at critical infrastructure. In addition to DDoS attacks, the exploitation of vulnerabilities remains a key risk, exacerbated by outdated technologies and slow patch cycles. This combination makes it easier for attackers to use known exploits and botnets from the dark web.

But the threat goes far beyond technical factors. According to PwC‘s Global Digital Trust Insights 2025[2], only 2% of companies have enterprise-wide cyber resilience, even though the average cost of a data breach is over $3.3 million. While two-thirds of technology leaders rank cybersecurity as a key risk, operational preparedness often remains inadequate.

Criminals are increasingly working together, using artificial intelligence and offering cyber attacks as part of „crime-as-a-service“ models. In its „Global Cybersecurity Outlook 2025“[3] , the World Economic Forum (WEF) highlights the increasing complexity and automation of such attack platforms as a key driver. The threat landscape is therefore more professional, networked, and dynamic than ever before. This requires companies and institutions to consistently expand their defense and resilience strategies.

Massive increase in DDoS attacks

The DDoS threat situation worsened significantly in 2024, and this trend continued in the first half of 2025. The number of attacks registered in the Link11 network increased 225% compared to same period in 2024.



The increase in DDoS attacks in the first half of 2025 is the result of several factors. Global tensions are leading to an increase in politically motivated attacks in connection with international conflicts or elections. The World Economic Forum's „Global Risks Report 2025“[4] classifies geopolitically motivated attacks, armed conflicts, and political instability as immediate threats. It also highlights that cyberattacks, which are often driven by geopolitical conflicts, are among the most significant short- and medium-term risks.

Technological advances, particularly in the field of AI, also play a major role. Botnets are being managed more efficiently and used in a modular way. AI is being used to improve attack techniques and better conceal attacks.

Attackers use machine learning and AI to identify and exploit vulnerabilities more quickly. In addition, compromised devices and botnets can be automated and controlled with precision. Similarly, the increasing number of unprotected and vulnerable IoT devices worldwide offers a huge reservoir for botnets. Although there have been successful international investigations that have shut down so-called „DDoS stressors,“ there are still plenty of „DDoS-as-a-Service“ platforms.

In addition, DDoS attack techniques themselves are becoming increasingly sophisticated. Overall, it is clear that the professionalization and commercialization of the cybercrime scene is continuing to grow. This development is reinforced by other factors that make DDoS a serious current threat to the national economies, administrations, and societies.

This increase was driven primarily by two opposing trends:

1

More large attacks with higher peak values (peak bandwidth)

2

An increase in smaller DDoS attacks compared to the same period last year.

Political hacktivism in Germany

The first half of 2025 was marked by a large number of politically motivated attacks on German targets. The pro-Russian group NoName057(16) in particular carried out repeated waves of attacks, some lasting several weeks. Other actors such as Mr. Hamza, Dark Storm, and Keymous, also became increasingly active.

The targets were often selected in direct connection with geopolitical events. As a result, critical sectors such as energy supply, industry, finance, municipal services, and government and public authority systems came under increased scrutiny. Despite individual measures against the attack infrastructure, such as the shutdown of DDoS stressor services[5], the momentum of the attacks has hardly slowed.

In addition, there has been a clear increase in professionalism. The campaigns combined a wide variety of targets with regular shifts in focus. Furthermore, attacks against already known targets were repeated, indicating persistent attack lists and insufficient hardening on the part of the affected organizations.

The timing was often strategically chosen. The attackers often acted with calculated precision, launching their campaigns outside of core operating hours — precisely when security teams were least staffed, and response capacity was lowest. By striking at these vulnerable moments, they aimed to maximize their impact and delay the implementation of effective countermeasures. Success rates of 40 to 50 percent demonstrate that many systems are still inadequately protected against these tactics.

Political events and international decisions served as triggers, making it possible to predict the attack dynamics to a certain extent. The focus was on the energy, industry, finance, and municipal services sectors, as well as traditional government and public authority systems.

It also became clear that the attackers' capabilities have increased. Various DDoS protection providers are now documenting attacks with peak values in the terabit range. In addition, activity is increasingly spreading across multiple groups using different tactics and tools.

Along with a broader monitoring strategy, companies should therefore implement reliable and efficient DDoS mitigation, even in the terabit range. The repeated attacks on the same targets also underscore the need to quickly and consistently close security gaps after incidents.

High frequency and target diversity:
Several large-scale waves from January to May, with over 100 domains attacked per campaign in some cases. Combination of known and newly identified vulnerabilities.

Tactical adaptability:
Shifts in focus (e.g., from government agencies to public transportation or financial institutions) make defense planning difficult. Repeated attacks on targets that have previously been compromised demonstrate the use of persistent attack lists.

Geopolitical triggers:
Political events, including the Munich Security Conference in February and Germany's announcement of further Iris-T deliveries to Ukraine in April, triggered the attacks.

Increasing attack power:
Several providers reported peak values in the terabit range.

Fragmentation of the attacker landscape:
The dominance of NoName057(16) has waned. There were several groups with different tools and approaches, making defense more complex.

When internet service providers falter

In addition to particularly large-scale DDoS attacks in the terabit range, attacks on the infrastructure in the Link11 network have also increased. Such infrastructure or backbone attacks have an ambitious goal: they aim to overload the Internet uplink capacity of an entire Internet service provider (ISP) or data center. With a backbone connection of 100 Gbit/s, such an attack requires around 85 Gbit/s to almost saturate the link.

The data streams and the effects are correspondingly large: unlike targeted website attacks, entire customer networks or services can be affected at the same time. These are usually high-volume, distributed DDoS campaigns.

The number of these attacks has increased significantly compared to the first half of 2024. More than twice as many DDoS attacks (143%) reached a critical size to paralyze backbone connections ( ). This trend is critical because the damage is more widespread and significantly more costly for both providers and their customers.

Despite the general increase in DDoS attacks, the frequency of targeted website attacks has largely remained constant. Unlike attacks that paralyze an ISP's services, these attacks aim to take a single website or server offline.

Technically, a moderate data stream is often sufficient: an attack of around 850 Mbit/s can almost completely overload a server with a 1 Gbit/s connection. The utilization rate is then 85%, which leads to a massive slowdown or even a complete failure of the service.

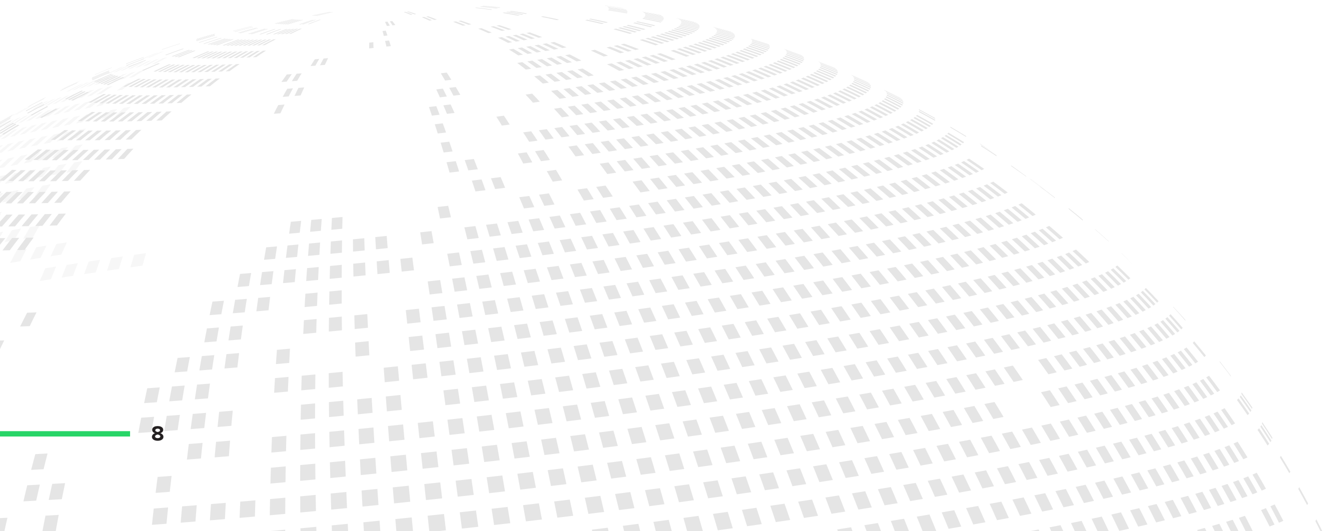
These attacks are characterized by relatively small data streams in contrast to backbone attacks. They are often used to target specific companies or online services and immediately render the affected service unavailable to users.

Another important category is „nuisance attacks. „ These are a form of DDoS attack whose goal is not to completely shut down a service, but rather to deliberately disrupt its performance and availability. Typically, these attacks occur in the low bandwidth range often below 1 Gbit/s and thus remain below many automatic defense thresholds.

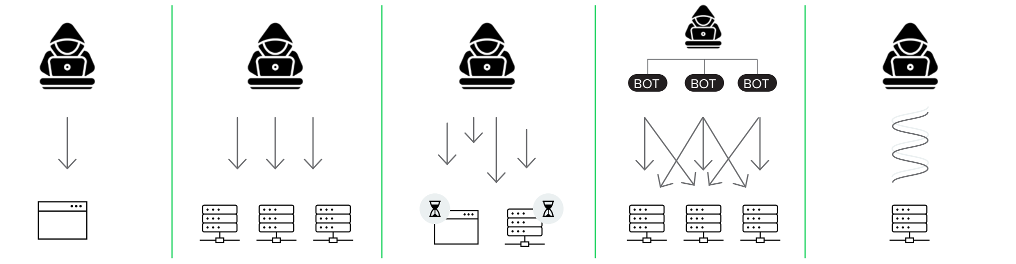
Nevertheless, they cause noticeable effects such as increased latency, packet loss, or unstable connections. Attackers use them for a variety of reasons: as a low-cost form of harassment to disrupt operations and cause downtime costs, as a distraction during other attacks, or to explore a target's defense mechanisms. The spread of such attacks is facilitated by easily accessible „DDoS-for-hire" services. This has led to a significant increase in these disruptive attacks in recent months.

These attacks do not fall into either the „website killer" or „ISP killer" categories. However, they have the potential to generate targeted costs and impair service performance. They illustrate that attackers are diversifying their methods to achieve different goals from immediately crippling individual services to causing subtle economic disruption.

In summary, while website killer attacks continue to pose a constant threat, the significant increase in ISP killer attacks is a serious trend. It places greater strain on providers' infrastructure and presents new challenges for security managers.



Vielfältige Angriffstypen: Vom Website-Killer zum Jo-Jo-Angriff



Criterion	Website killer	ISP-Killer	Nuisance Attack	Carpet-Bombing	Yo-Yo attack
Primary target	Single website or single server	Uplink capacity of an entire ISP or data center	Performance disruption without complete failure	Widespread disruption of entire subnets or IP ranges	Cloud infrastructure with auto-scaling function
Technical threshold	85% utilization, i.e. approx. 850 Mbit/s (with 1 Gbit/s connection)	85% utilization, i.e. approx. 85 Gbit/s (with 100 Gbit/s backbone)	From 50 Mbit/s to 1 Gbit/s, below defense thresholds	Depending on the target network, often medium to high total volumes	Even moderate load peaks are enough to trigger auto-scaling
Attack volume	Medium	Very high	Low	Medium to high (distributed)	Variable, often in waves with varying intensity
Typical effect	Target page not accessible	Large-scale failure of many services/ customers	Noticeable latency, packet loss, additional costs	Overloading of firewalls, routers, and upstream links	Instability due to constant scaling up and down, cost explosion
Characteristics	Targeted attack, relatively low data stream	High-volume, distributed campaigns	Frequent mini-attacks, often automated	Distributed traffic across many targets, more difficult to filter	Alternates between traffic bursts and quiet periods, takes advantage of cloud auto-scaling

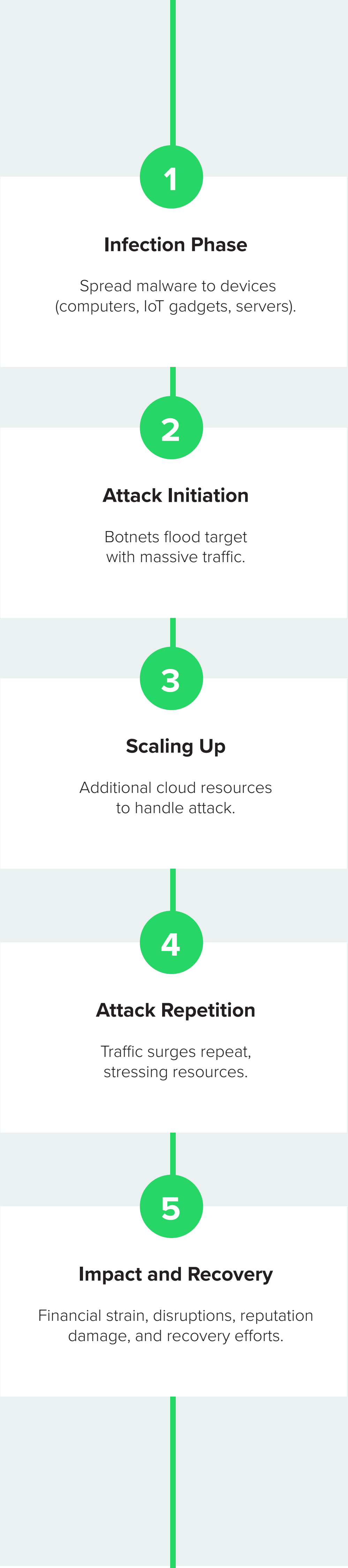
Yo-yo attacks[7] at Layer 7

Definition:
Yo-Yo DDoS attacks are a new form of Layer 7 attacks that specifically exploit the auto-scaling capabilities of cloud infrastructures. Unlike classic DDoS attacks, the aim is not simply to flood systems with traffic, but rather to destabilize them and make them costly to operate by repeatedly switching between peak loads and periods of inactivity.

How it works:
The attackers first generate a sudden spike in requests, forcing the cloud infrastructure to provide additional resources, such as computing power or bandwidth. Once these resources are active, the traffic is abruptly reduced so that capacities are scaled back again. Shortly after, the next wave of attacks begins, triggering a permanent cycle of scaling up and down. This is known as the “yo-yo effect.”

Impact:
For the companies affected, this means not only significantly higher cloud costs, but also noticeable performance losses and potential instability of the services provided. The repeated load changes cause latency and interruptions. In addition, there is unnecessary wear and tear on resources, which can jeopardize the availability of business-critical applications.

Prevention:
Targeted protective measures are required to ward off yo-yo attacks. These include rate limiting and throttling to absorb artificial load peaks, adaptive auto-scaling strategies with cooldown phases that prevent constant ramp-ups and ramp-downs, and AI-supported anomaly detection to identify unusual traffic patterns at an early stage. Intelligent load balancing methods and close cost monitoring can also help reduce risks.



1

Infection Phase

Spread malware to devices (computers, IoT gadgets, servers).

2

Attack Initiation

Botnets flood target with massive traffic.

3

Scaling Up

Additional cloud resources to handle attack.

4

Attack Repetition

Traffic surges repeat, stressing resources.

5

Impact and Recovery

Financial strain, disruptions, reputation damage, and recovery efforts.

More volume, more packets, longer duration – from lightning attacks to sustained fire

In addition to the sheer number of attacks, the attack patterns have also changed: While the first half of 2024 was still characterized by „turbo attacks,“ the first half of 2025 was dominated by longer-lasting campaigns with more complex vector changes and a more coordinated approach. The tripling of the number of attacks was accompanied by a significant increase in attack volume.

The total attack volume in terabytes (TB) in the first months of 2025 was around **438 TB**, compared to 110 TB in the same period of 2024.

▶

4K-Streaming
438 TB is equivalent t**o more than 7 years of uninterrupted Netflix streaming** in 4K. Even if you stream day and night, you would watch thousands of series and movies during that time without experiencing a single buffer.

🎧

Audiobooks
Enough data for **more than 1,700 years of uninterrupted audiobook playback**. You could listen to the entire world's literature and still have enough storage left over for a few reference books.

♫

MP3 songs
This data volume **can hold around 93 million songs**. That's enough to **listen to music around the clock for over 500 years** without playing a single song twice.

📱

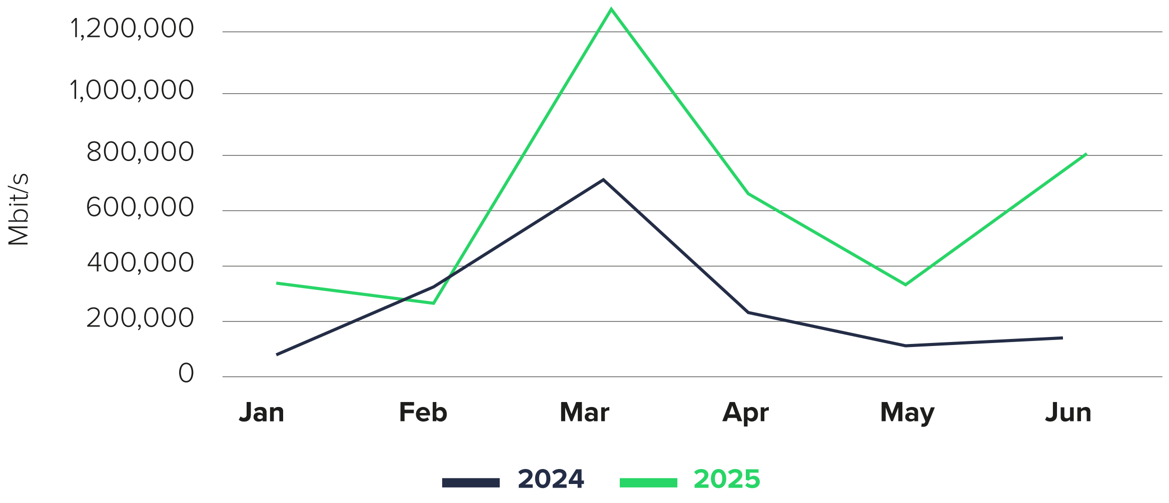
64 GB devices
That's equivalent to the storage capacity of **6,800 fully loaded smartphones with 64 GB each**. Imagine a whole warehouse full of such phones, each one filled to the brim with data.

> *“We no longer see just brute force in the form of bandwidth, but also in highly precise Layer 7 attacks. The use of 20,000 deceptively genuine requests per minute can be more dangerous than 200 million packets per second if they go unnoticed in legitimate traffic.”*
>
> **Jag Bains, VP Solution Engineering, Link11**

DDoS in XXL format

The size distribution of the attacks observed in the Link11 network paints a mixed picture: While peak bandwidth values have increased significantly and more large-volume attacks have been recorded, the average bandwidth has decreased overall. The large number of smaller attacks is pulling the average down. In the first half of 2025, the trend of both the number and peak loads rising continuously has further solidified. The largest DDoS attack between January and July 2025 reached a maximum bandwidth of over 1.2 Tbit/s. The largest attack in the first half of 2024 was „only“ half as large, at 694 Gbit/s.

Maximum bandwidth in Mbit/s

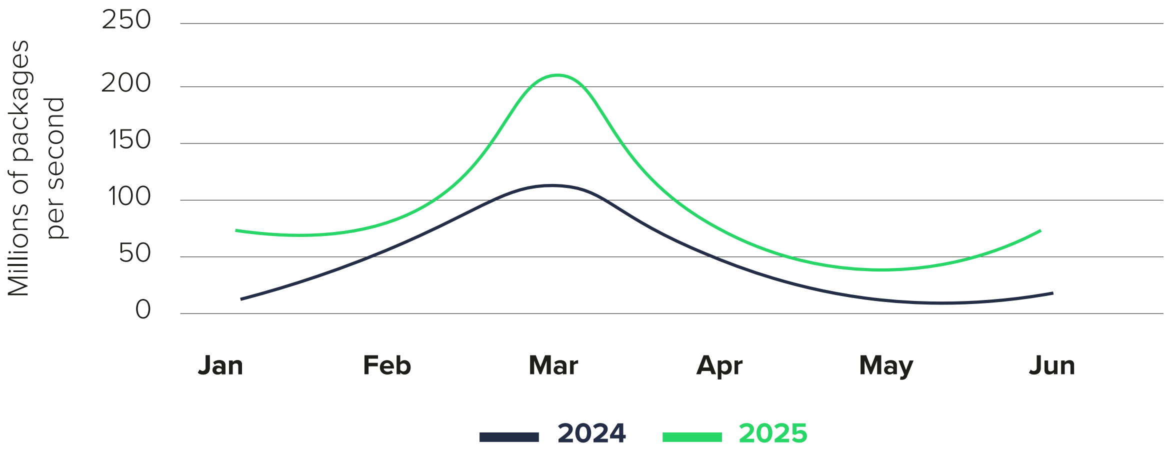


Parallel to the increase in maximum bandwidth, the maximum number of packets transmitted per second also rose in the first half of 2025. The highest value was 207,090,400 packets per second.

A DDoS attack volume of 207 million packets per second is very high and overwhelms even powerful enterprise servers or firewalls. Such values lead to massive network congestion, packet loss, and potential total service outages. They typically only occur in large-scale botnet attacks or ISP-level campaigns. To generate such values, attackers usually resort to large botnets that send many small packets simultaneously (e.g., SYN floods, UDP floods).

> *“207 million packets per second is not only a high overall value, but it can also paralyze firewalls, servers, and entire networks within seconds. In the event of an attack, speed is crucial.”*
>
> **Karsten Desler, CTO, Link11**

Maximum number of packets per second



Marathon instead of sprint

Unlike the turbo attacks we observed in the Link11 network in the first months of 2024, attackers in the first half of 2025 increasingly relied on longer and coordinated campaigns. These long-lasting attacks are more likely to overload defense systems and cause lasting damage.

The longest documented attack in the first half of 2025 lasted 12,388 minutes, or 8 eight days and 14 hours. In the same period last year, the longest DDoS attack lasted only 1,523 minutes, or about 1 day and 1 hour.

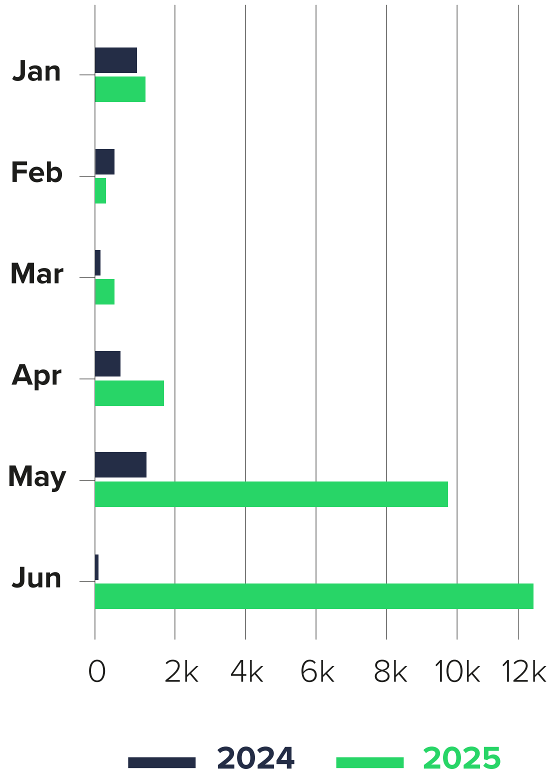
The chart illustrates the variation in attack duration during each month and the different levels. The biggest difference can be seen in the figures for June. While the longest attack was measured in June 2025, the maximum attack duration in June 2024 was only 73 minutes.

The increase in attack duration is also an indication of the attackers‘ varying tactics. Several factors contribute to this increas: more complex vector changes, the use of automated botnets and AI-supported tools, encrypted attack vectors, and timing to coincide with geopolitical events.

Politically motivated groups such as NoName057(16) also carried out more coordinated, long-lasting DDoS campaigns that targeted government agencies, the public sector, and financial and healthcare institutions.

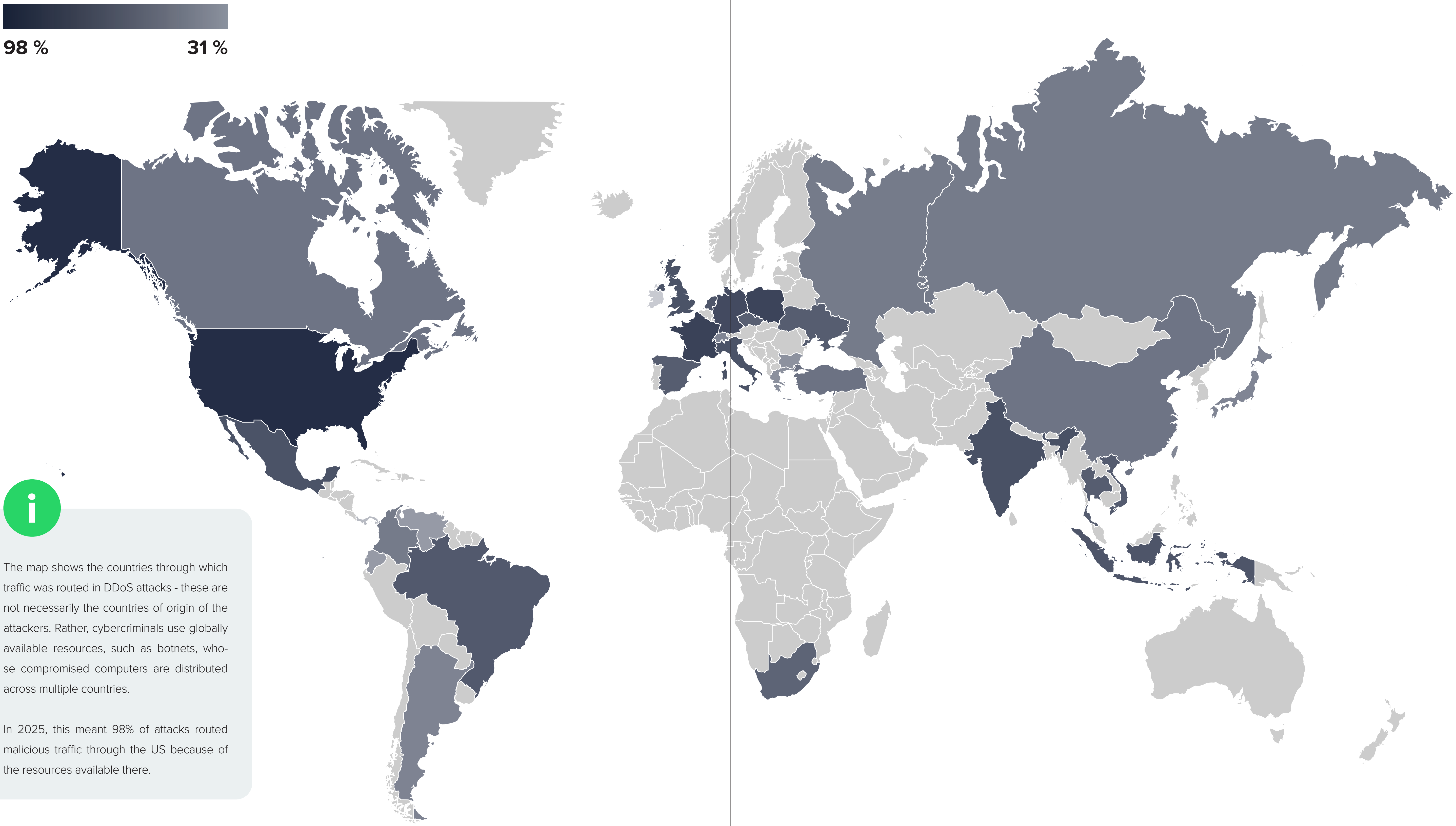
Overall, the figures show that security managers need to increase not only the scalability but also the endurance of their defense systems in order to effectively counter the increasing number, complexity, and duration of attacks.

Duration of the longest DDoS attack per month in minutes



Origin of the DDoS traffic

Global distribution of the attack infrastructure 2025



The map shows the countries through which traffic was routed in DDoS attacks - these are not necessarily the countries of origin of the attackers. Rather, cybercriminals use globally available resources, such as botnets, whose compromised computers are distributed across multiple countries.

In 2025, this meant 98% of attacks routed malicious traffic through the US because of the resources available there.

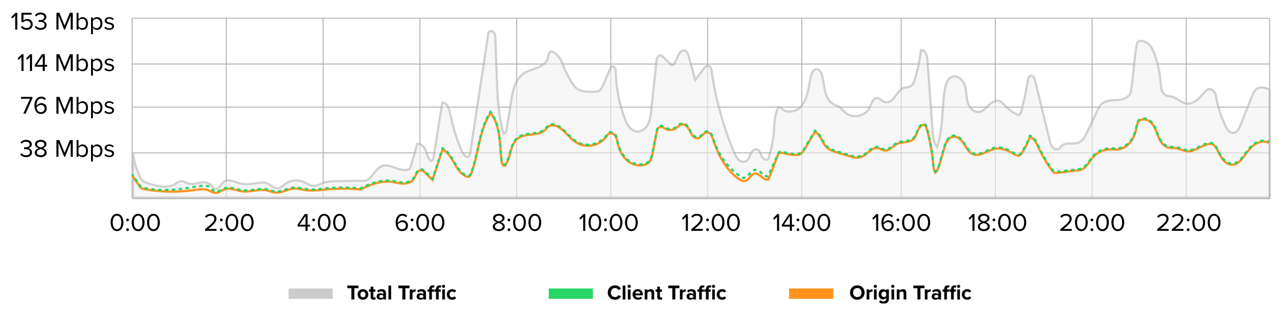
Web **Protection**

The web DDoS attacks in the first half of 2025 on the Link11 network were characterized by high intensity and a clear focus on web applications and APIs. They targeted critical web services and interfaces, especially those of e-commerce, gaming, finance, and media companies. APIs are increasingly the main target because they control business processes and sensitive data. As a result, digitized business models are under threat like never before—protection concepts must urgently take into account the new dimensions and attack tactics.

Precision instead of brute force

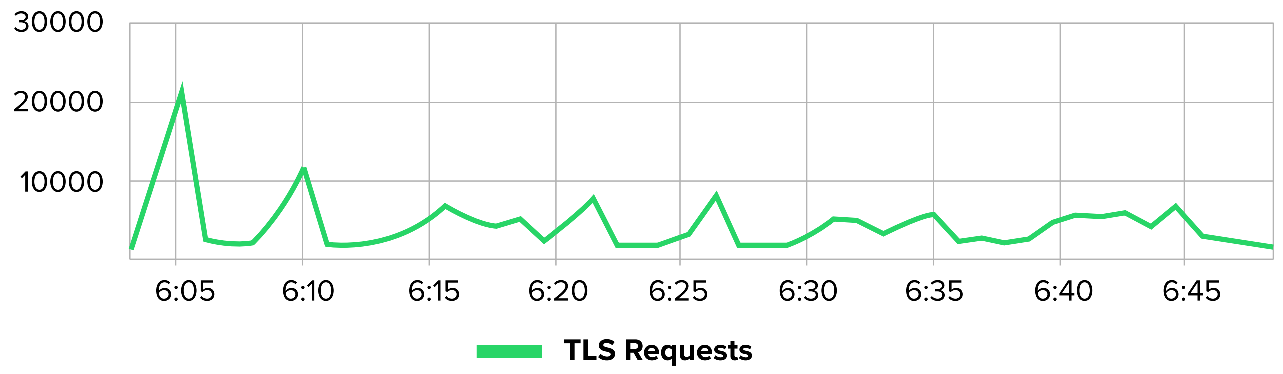
At the end of April 2025, geopolitical tensions in Germany led to a series of targeted cyberattacks, including by the pro-Russian hacker group NoName057(16). Within a few days, websites of state banks, industrial companies, and city administrations such as berlin.de and stuttgart.de were unavailable for hours or sometimes even days. While many attacks relied on high data volumes, one Layer 7 DDoS attack observed in the Link11 network stood out for its sophistication: it did not generate massive traffic, but instead targeted the application layer with precision. To do this, it used legitimate HTTP requests that consumed backend resources.

Maximum bandwidth



To conceal their attacks, the attackers deliberately used the infrastructure of well-known hosting providers that also served VPNs and CDNs. Through geo-IP spoofing and the use of edge-based nodes, some of the requests appeared to come from Germany, even though they were distributed globally. With around 20,000 requests per minute, the attack was not critical for large systems, but it was able to effectively disrupt sensitive areas. Modern protection solutions detected and blocked it primarily due to inconsistencies in HTTP headers, missing cookies, JavaScript challenges, and incomplete human interaction patterns.

Requests per minute

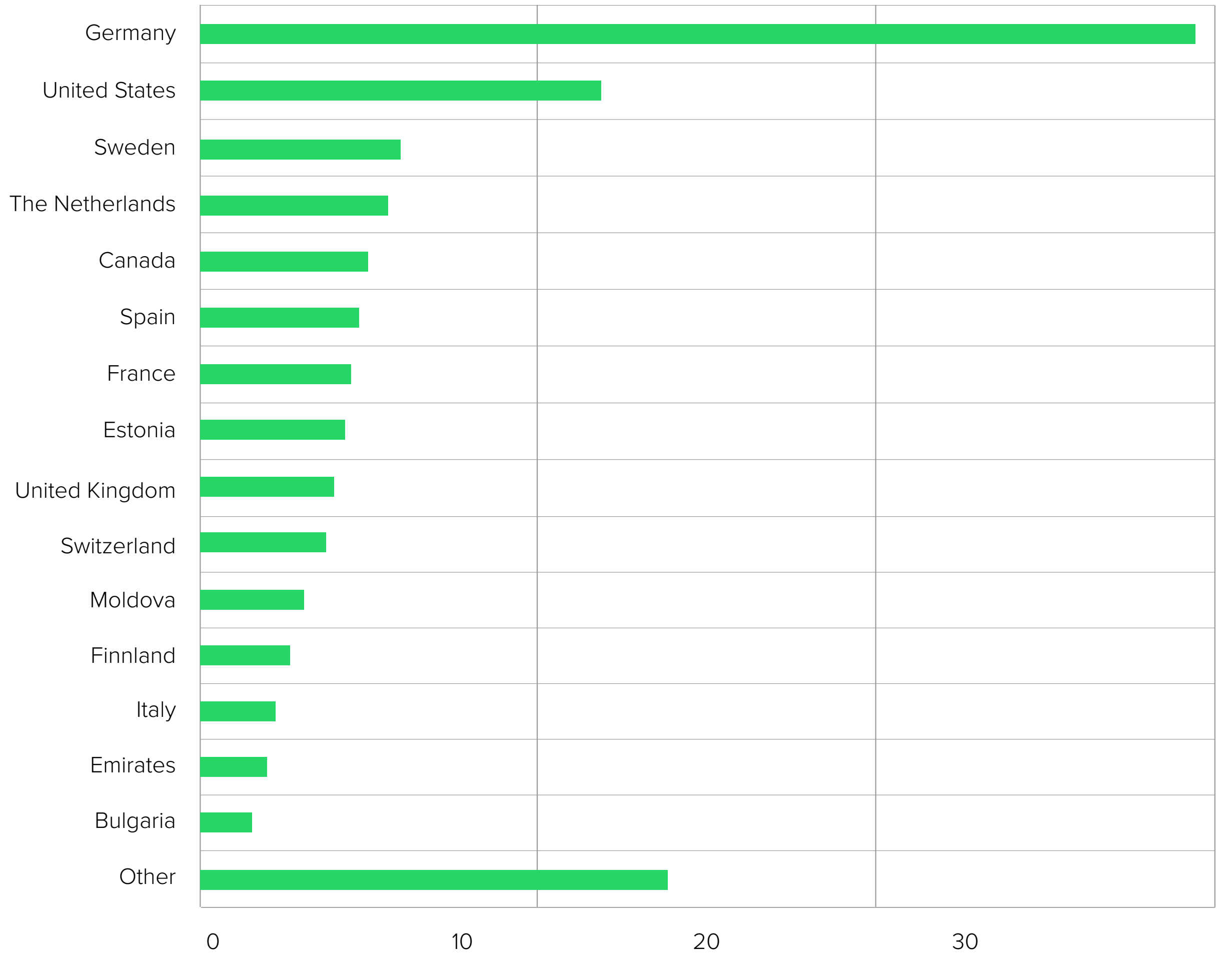


The economic efficiency was particularly striking: low entry costs for VPNs, test servers, or microjobs made it possible to carry out targeted disruptions with minimal effort. The attack made it clear that Layer 7 DDoS attacks rely not on brute force, but on precision, camouflage, and organization.

For companies, this means that traditional volumetric protection measures alone are not enough intelligent, automated web protection solutions are essential to ward off such subtle but potentially powerful attacks.

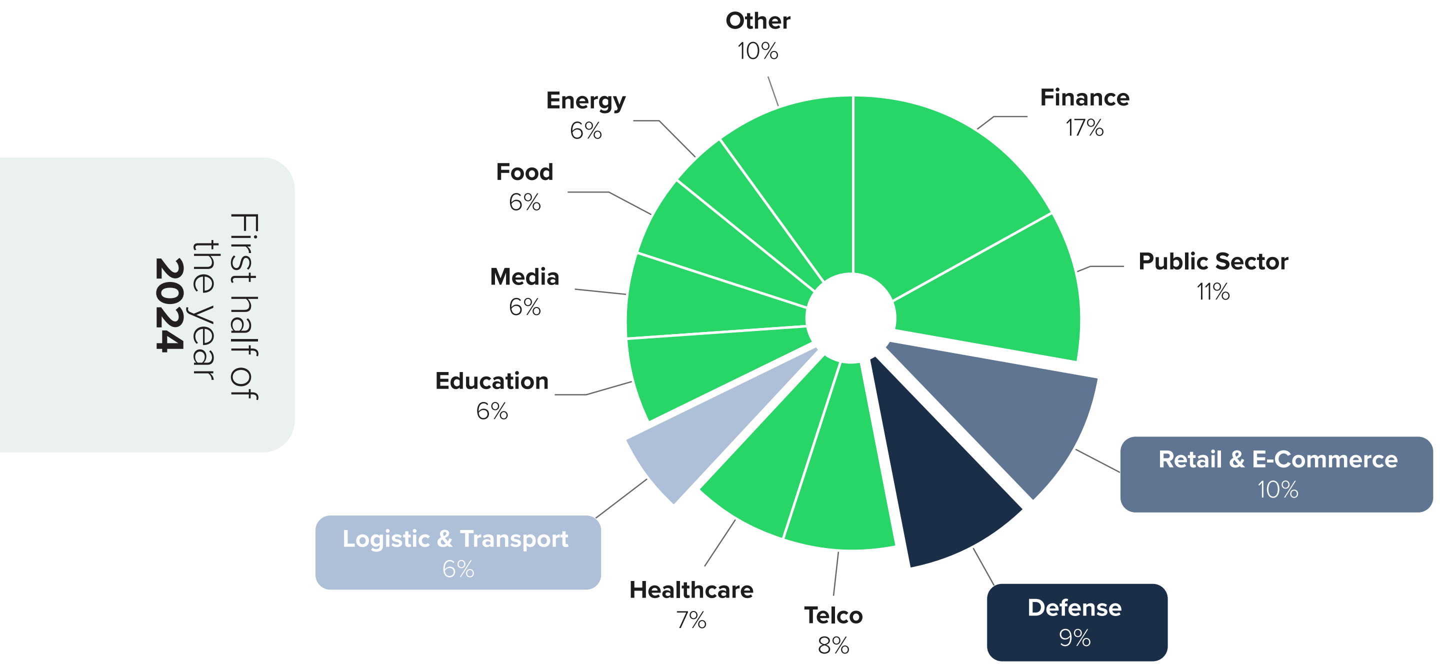
> *“The attackers cleverly disguise themselves using VPNs, CDNs, and geo-IP obfuscation. This suddenly makes it look as if the requests are coming from the neighborhood, while the system is simultaneously being bombarded from Vietnam, Russia, or the US.”*
>
> **Sean Power, Solution Engineer, Link11**

Origin of DDoS traffic

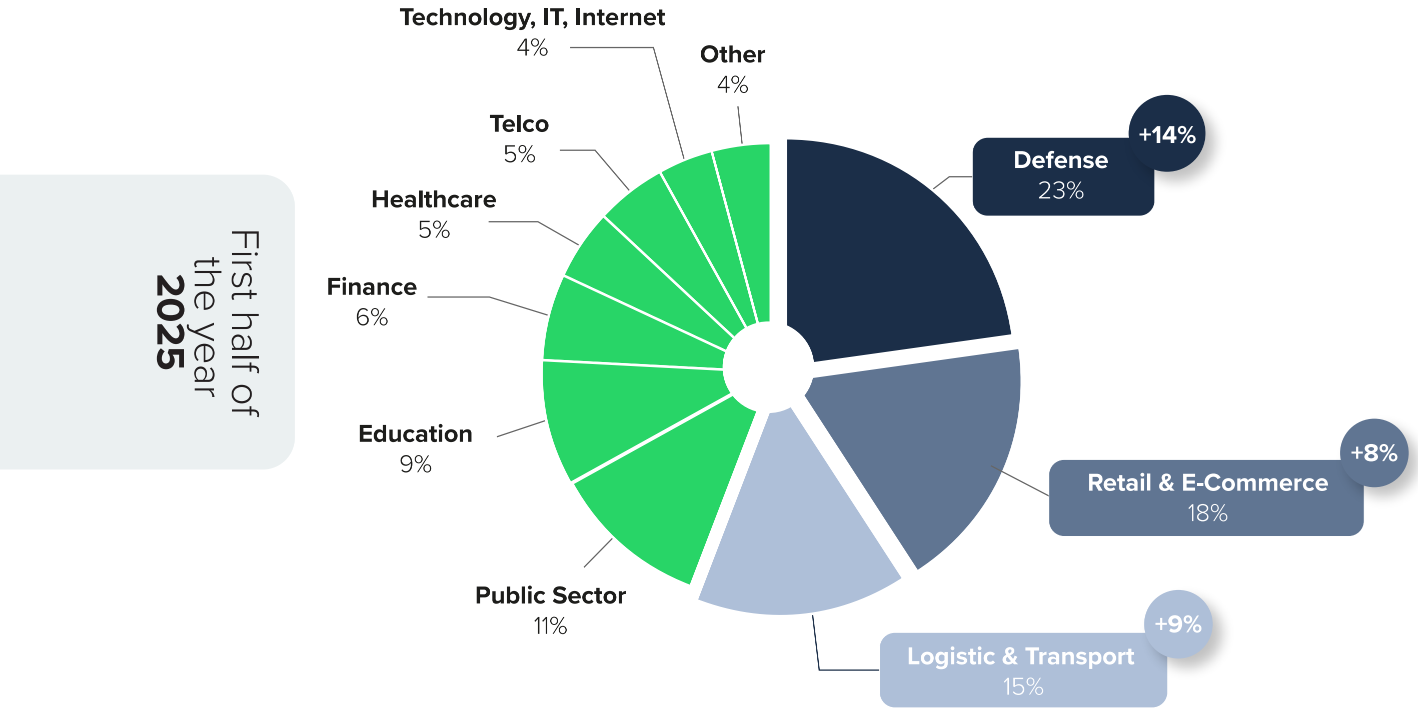


New targets in sight

Analysis of observed cyberattacks in the area of web application and API protection (WAAP) reveals some shifts within the affected sectors between the first half of 2024 and the first half of 2025: Finance, public sector, and retail, and e-commerce occupy the top spots. They are closely followed by the defense sector, the telecommunications industry, and healthcare.



In the first half of 2025, the targets of attacks shifted, with attacks on the defense sector, retail and e-commerce, and logistics and transportation increasing in particular. Attackers look for sectors that have the potential to significantly impact logistics, digital services, and critical information exchange. This could also be due to current geopolitical events or economic developments.



Conclusion

Analysis of the attacks in the first half of 2025 clearly shows that the threat landscape in the area of DDoS attacks has continued to intensify and diversify. While the number and intensity of attacks have increased, a shift in the types of attacks can also be observed. In addition to classic „website killers" and high-volume „ISP killers," sophisticated Layer 7 attacks are becoming more common. These attacks do not rely on raw data volumes, but on precision and obfuscation. This makes it clear that cybercriminals are adapting their tactics and exploiting vulnerabilities in different layers of the network in a targeted manner.

Geopolitical tensions, particularly in the context of the war in Ukraine, were the main trigger for many waves of attacks. Pro-Russian groups such as „NoName057(16)" exploited political debates such as the discussion about Taurus deliveries to attract attention with spectacular attacks on government institutions, banks, and industrial companies. In addition to these geopolitically motivated attacks, economically motivated „nuisance attacks" and highly automated botnet operations are also part of the current arsenal. This is an indication of the increasing professionalization and division of labor in the threat landscape.

The enormous bandwidth and packet rate of some attacks are just as striking. These range from terabit traffic to over 200 million packets per second. Such dimensions illustrate the potential scale of the impact on companies, institutions, and entire critical infrastructure. At the same time, more precise Layer 7 attacks show that, in addition to size, camouflage and deception also pose a risk.

Companies must be prepared for highly complex attacks of this kind. Contingency plans, real-time monitoring, and AI-supported defense systems are crucial for detecting suspicious traffic early on and blocking it automatically. Only rapid response mechanisms and continuous adaptation of security strategies can limit the consequences of such massive attacks.

Successful DDoS protection therefore requires more than just bandwidth management: Only by deploying intelligent, automated protection solutions combined with contingency plans and continuous monitoring can organizations counter the increasingly hybrid threats.

Your contact person

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

Sources

1 X-Force 2025 Threat Intelligence Index | IBM

2 https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html

3 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/

4 Global Risks Report 2025 | World Economic Forum

5 BKA - Meldungen - Operation „Power OFF“: weltweiter Schlag gegen Cybercrime-Infrastruktur und

BKA - Meldungen - Strafverfolgungsbehörden schalten die zwei weltweit größten Cybercrime-Foren mit rund zehn Millionen registrierten Nutzern ab

6 Emerging Threat: Yo-Yo DDoS Attacks Targeting Cloud Environments | Blogs - Cyberware Hub

https://www.flaticon.com/de/kostenloses-icon/hacker_6463383?related_id=6463392&origin=search

LINK11

Head office

Link11
Lindleystr. 12
60314 Frankfurt