LINK11

European Cyber Report

2025

Dear readers,

Cyberattacks are no longer an abstract risk - they dominate the risk agenda of companies worldwide. The Allianz Risk Barometer 2025 shows that digital transformation opens up opportunities, but also increases the range of opportunities for cybercriminals. DDoS attacks, data theft and industrial espionage are major challenges, and those who fail to continuously adapt their security strategy risk financial losses and long-term damage to their reputation and business operations.

The Bitkom study „Economic Protection 2024“ illustrates the urgency: 81% of German companies were affected by cyberattacks last year. The damage caused by cybercrime reached 178.6 billion euros and now accounts for two-thirds of all losses caused by crime.

The threat landscape is constantly changing, so organizations need to evolve their security infrastructure and adapt to new attack dynamics. In addition to the increased integration of AI into attack detection and prevention, the protection of web applications and APIs (WAAP) plays a key role. These components are now among the preferred targets of cybercriminals, as they often process sensitive data and support important business processes. As such, a holistic security strategy should include advanced WAAP solutions that can proactively prevent threats such as SQL injection, cross-site scripting, and API-specific attacks. Regularly updating security services and the continuous monitoring of network health are essential to respond to changing attack patterns. Supplemented by robust DDoS mitigation mechanisms, organizations can build a resilient security position.

In 2025, cybersecurity is no longer an afterthought, but rather a business-critical priority. Organizations must act now to strengthen their resilience and prepare for the next wave of attacks. Those who embrace cybersecurity as a strategic success factor will drive innovation and growth, and secure a competitive advantage.

Link11 can help you take your digital security to the next level and protect your critical assets.
I hope you enjoy reading this report!

Kind regards
Jens-Philipp Jung, CEO, Link11

Table of Contents

Executive Summary 04

Development of the total numbers in the Link11 network 06

Origin of the DDoS traffic 10

Development of attack duration 12

Development of attack bandwidths 15

Multi-vector attacks 18

Web Protection 20

Web Performance 24

Executive Summary

The year 2024 was marked by an unprecedented wave of Distributed Denial of Service (DDoS) attacks, which dominated the cybersecurity landscape with record numbers and increasing complexity. The proliferation of DDoS-as-a-Service and the use of AI intensified these attacks and presented new challenges to organizations. This increase represents not only an increase in the frequency of attacks, but also a change in tactics.

Key findings:

- **Record increase:** The number of DDoS attacks on the Link11 network increased by 137%.
- **From gigabits to terabits:** The largest attack measured in Link11 reached a new dimension in Europe at 1.4 Tbps.
- **New attack tactics:** Attackers are increasingly relying on fast, targeted attacks that use few resources but cause significant disruption.
- **Complexity and speed:** Attacks have become faster and shorter, with two-thirds of attacks peaking within 10 to 60 seconds.
- **Multi-vector attacks:** The combination of different attack points and protocols makes detection more difficult and requires more precise countermeasures.
- **Geopolitical tensions:** Conflict and political unrest are fueling the threat landscape, and less sophisticated actors are using powerful tools to launch complex attacks.
- **Traditional defenses are reaching their limits:** Older methods are often unable to keep up with the speed and complexity of new attacks.
- **AI is the key to defense:** Organizations are increasingly relying on AI-based systems to detect and neutralize attacks in real time.
- **Privacy and compliance:** Discussions about the EU-US data protection framework underscore the importance of European CDNs and geofencing technologies to protect sensitive data.

2024

How organizations can strengthen their defenses

As the threat landscape evolves, organizations must adapt their security infrastructures to meet the new attack dynamics. This means not only greater integration of AI into attack detection and prevention, but also comprehensive monitoring of network and server health. A holistic security strategy that includes network protection as well as web application and API protection is essential. So too is a greater focus on continuous adaptation to volatile attack patterns and the integration of advanced DDoS mitigation technology.

DDoS attacks in 2025 will be faster, more targeted, and more sophisticated than ever before. Organizations must continually modernize their security strategies, implement AI-based systems for rapid and accurate attack detection and mitigation, and prepare for increasingly subtle attack techniques. Only a holistic, adaptive security architecture can ensure that organizations are prepared for the increasingly sophisticated threats of the future.

Development of the total numbers in the Link11 network

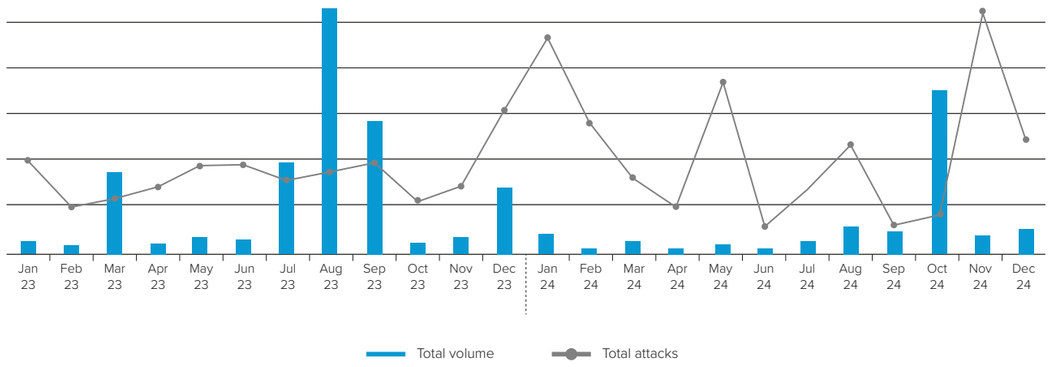
Attackers pick up the pace

The development of DDoS attacks in the Link11 network shows an alarming dynamic during 2024. After a significant increase of over 70% in attacks in 2023 compared to the previous year, this trend continued in an even more drastic form in 2024. The number of attacks increased by 137% compared to the previous year.

A strategic shift in attack types is noticeable: while large-scale attacks of more than 100 Gbps remain a serious problem, smaller and more frequent attacks have increased significantly. Classic brute force attacks based on pure bandwidth are less in the foreground; instead, attackers are increasingly relying on sophisticated, targeted attacks. While the number of attacks has steadily increased, the average amount of data per attack has decreased. This trend indicates that attackers are optimizing their methods to disrupt networks faster and more effectively, often with minimal resource usage but the maximum impact possible.

This is a major challenge for enterprises and institutions, as traditional DDoS defense measures are primarily designed to counter large-scale attacks. The increasing shift to smaller, more sophisticated attacks requires a new approach to network protection, particularly through adaptive detection systems and proactive defense mechanisms.

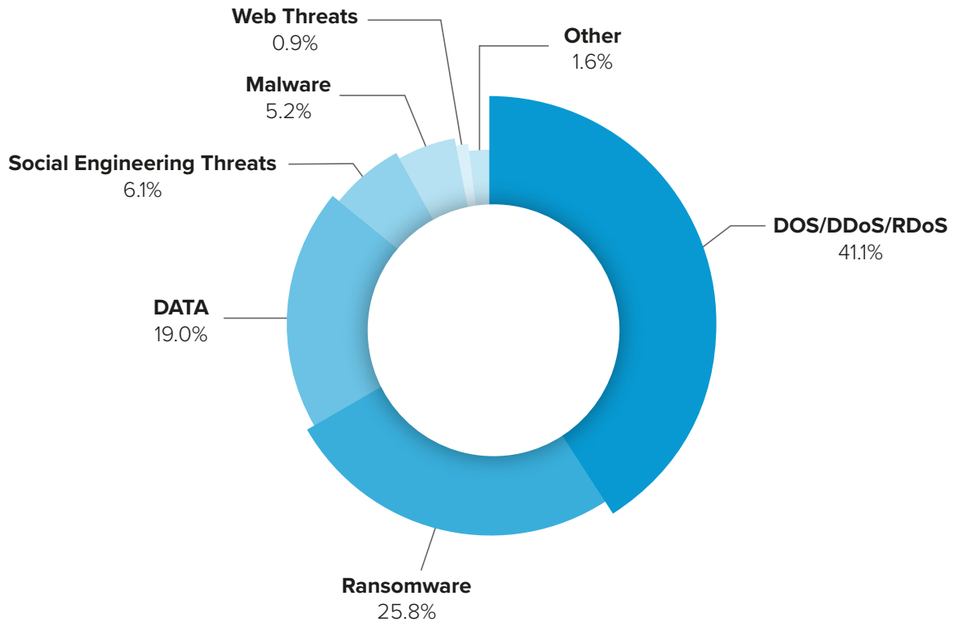
The graph below shows that the total volume has decreased.
At the same time, the number of attacks has increased.



Drivers of the increase in DDoS attacks 2024

The massive increase in DDoS attacks in 2024 is closely linked to geopolitical conflicts. According to the ENISA report, DDoS attacks are the most common cyberthreat in the EU - almost half of all attacks are aimed at shutting down systems. Government institutions, critical infrastructure, and economic institutions are particularly affected.

The pro-Russian group NoName057(16) remains the most active actor alongside groups such as Mr. Hamza. In addition to the war in Ukraine, the Middle East conflict and the formation of the Holy League have also led to an increase in politically motivated attacks. Attackers are using advanced tools, such as the DDoSia project, which allow less sophisticated actors to carry out effective attacks.



Quelle: ENISA Threat Landscape 2024

"The increasing complexity of DDoS attacks requires innovative solutions. AI-based systems are key to detecting and defending against faster and more sophisticated attacks."

Jag Bains, VP Solution Engineering, Link11

NoName057(16): More Capacity, More Sophisticated Attacks

NoName057(16) has significantly increased its attack capacity in 2024. Through targeted recruitment, its Telegram channel has grown to over 80,000 members. Its globally distributed server infrastructure and frequently changing IP addresses make countermeasures much more difficult. New attack techniques bypass traditional DDoS defenses, further increasing the threat.

Although their tools still require manual IP changes, this shows the high level of effort the group is putting in. The provision of attack tools such as „DDoSia“ has also facilitated the involvement of international actors, which has increased the political dimension of DDoS attacks in 2024.

Target profiles of the attacks

Critical infrastructure such as energy providers, banks and government agencies are affected, but increasingly also medium-sized companies. E-commerce platforms, telecommunications providers and cloud service providers are particularly at risk. Media organizations that report critically on geopolitical conflicts are also increasingly targeted.

Technology Evolution and Defense Strategies

With the increasing complexity of attacks, AI-based cyber defense is essential to keep pace with the speed of development. Simple bandwidth monitoring is no longer enough – intelligent systems must detect and block suspicious activity in real time. If defenses do not evolve, the threat to business and critical infrastructure will grow.

DDoS attacks are faster, shorter, and use multiple points of attack, challenging traditional monitoring methods. At the same time, attackers are systematically expanding botnets to launch targeted, high-volume attacks. Companies and institutions need to prepare for a long-term threat.

Political institutions are especially vulnerable during election years. In 2024, DDoS attacks were used to deliberately spread disinformation and disrupt democratic processes – a trend that is likely to increase as attackers become more professional.

The Holy League - An emerging threat

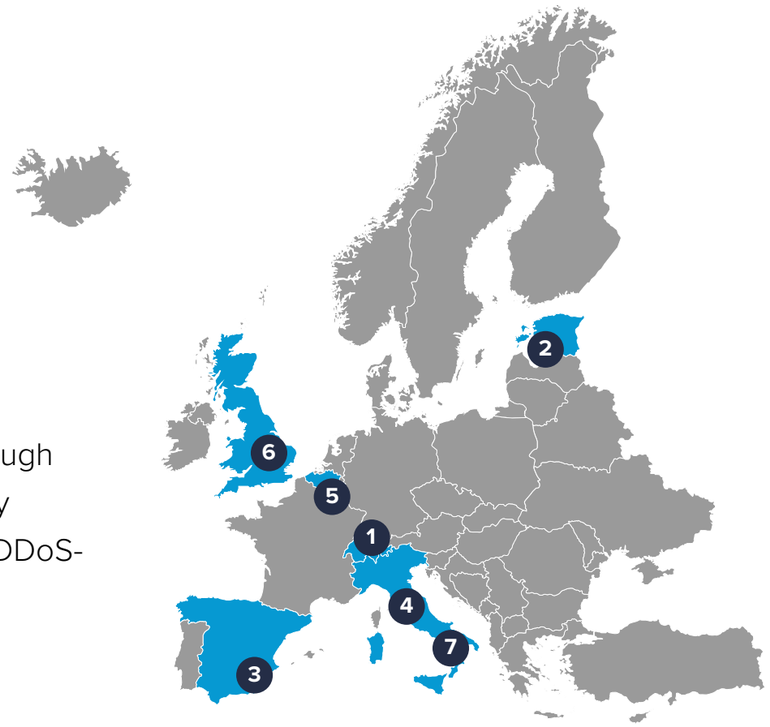
The Holy League is an alliance of pro-Russian and pro-Palestinian hacktivists formed in July 2024 that claims to be the largest coordinated cybercrime group targeting the West. The Holy League claims to now include over 70 active groups.

Its stated goal is to destabilize Western countries, particularly Europe, Ukraine, Israel, and NATO. Its attacks focus on DDoS attacks (such as those against the French government), data leaks, and system disruptions at government and corporate organizations.

The group uses a mix of religious rhetoric and political propaganda to attract followers. They urge other pro-Russian hacking groups to join their alliance. One of the campaigns targeted Spanish infrastructure after Spanish authorities arrested three pro-Russian hackers. In response, the Holy League called for a „vendetta“ against Spain.

Click here to through some of the many NoName057(16) DDoS-attacks in 2024.

1 =

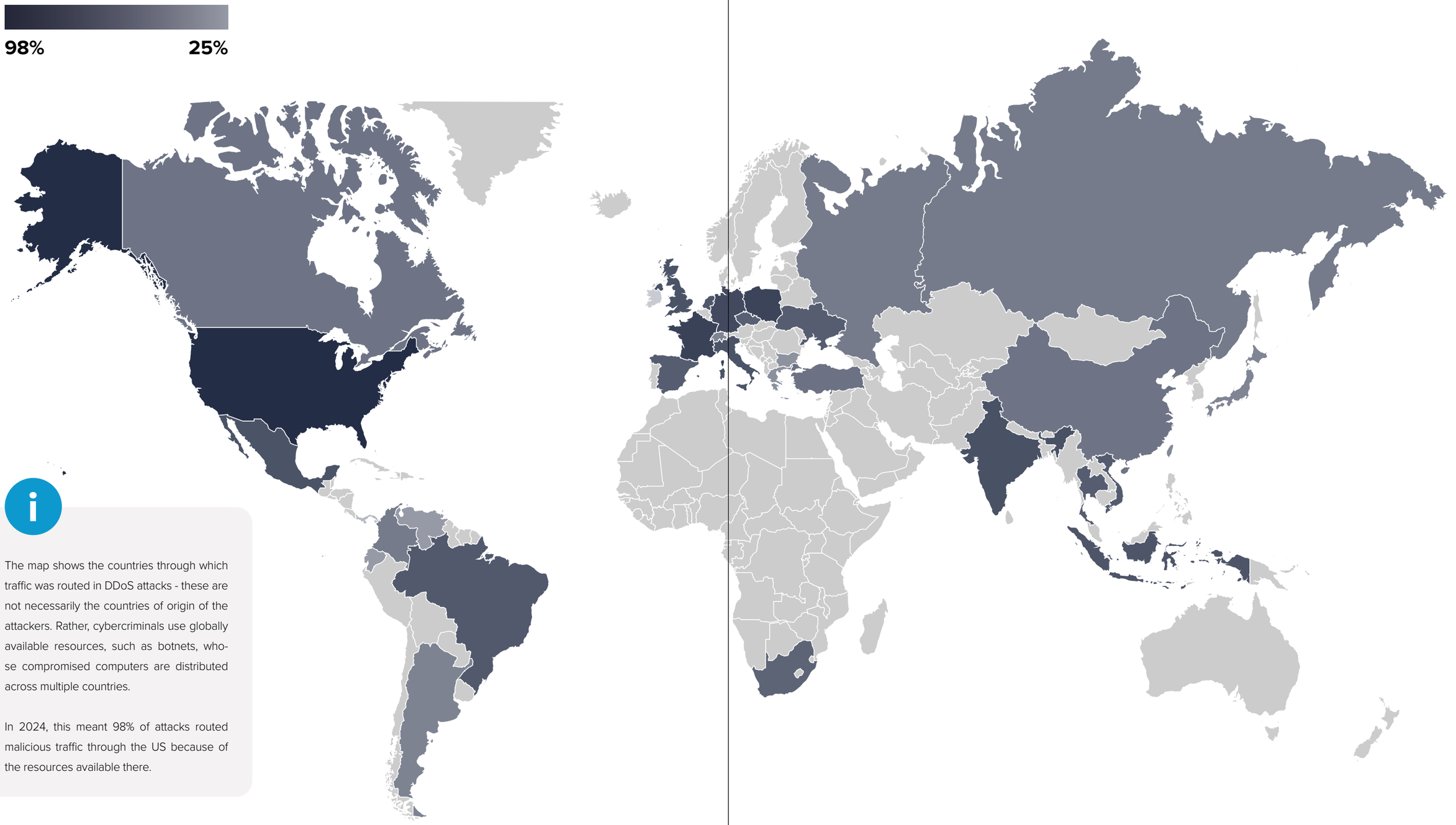


[illegible]

About [illegible], were taken [illegible] cyberattack[7].

Origin of the DDoS traffic

Global distribution of the attack infrastructure 2024



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 2024, this meant 98% of attacks routed malicious traffic through the US because of the resources available there.

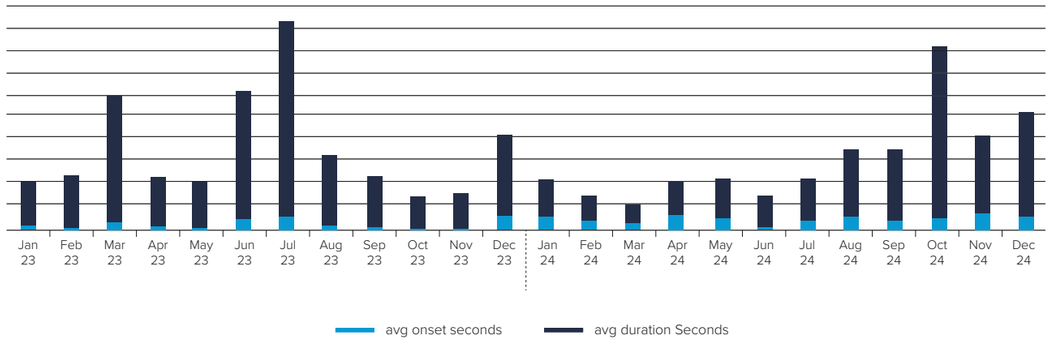
Development of attack duration

New tactics: shorter, faster DDoS attacks

Since the first half of 2022, the time it takes for DDoS attacks registered in the Link11 network to reach maximum traffic („onset“) has been analyzed. The key factor is how quickly an attack reaches a critical volume.

In 2024, DDoS attacks took an average of 29 seconds to exceed a critical threshold - longer than in 2023, when it was 14 seconds. At the same time, the number of attacks with short onset times increased significantly: two-thirds (65%) of attacks peaked within 10 to 60 seconds, compared to only 25% in 2023.

The graph shows that both the total attack duration (darkblue) and the time to peak (light blue) decreased significantly in the summer of 2024. DDoS attacks are therefore not only starting faster, but also lasting less time overall. Attackers are deliberately adapting their tactics to circumvent security measures with attacks that are as short as possible, but still effective.



“Defense windows are shrinking: two-thirds of all DDoS attacks in 2024 peaked within one minute.”

Sean Power, Solution Engineer, Link11

The duration and speed of DDoS attacks are changing:

Attacks start faster

Attack onset times are decreasing, with attacks reaching critical levels within seconds.

Shorter attack times

Attacks are shorter overall, but require a quick response.

High attack frequency

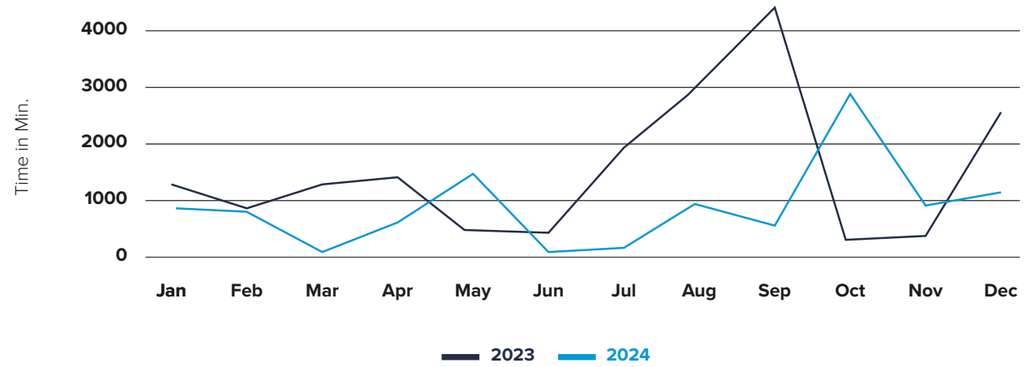
More attacks in short intervals overwhelm traditional defenses.

The increasing speed and brevity of attacks present new challenges for IT security solutions. Traditional, volume-based detection and defense is no longer sufficient in this scenario. A new generation of security solutions is needed that can detect and defend against faster and more complex attacks.

From longer to shorter attacks

The graph below illustrates the evolution of DDoS attack duration on the Link11 network: While 2023 was still dominated by particularly long-lasting attacks, 2024 shows a clear trend towards shorter but more frequent attacks, placing new demands on defense strategies.

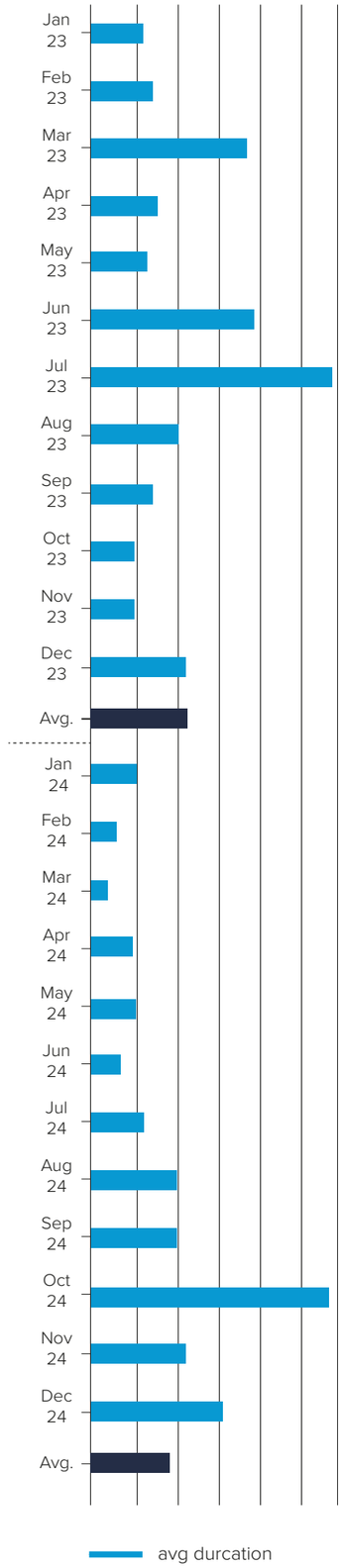
In 2023, the longest recorded DDoS attack lasted 4,489 minutes (74 hours and 49 minutes). By comparison, the longest attack in 2024 lasted 2,689 minutes (44 hours and 49 minutes) - a significant decrease of 40%. This reflects a general trend: instead of long-lasting attacks, cybercriminals are increasingly relying on shorter and tactically optimized attacks designed to specifically undermine existing defenses.



Another striking pattern: While the average attack duration increased in 2023 compared to 2022, there was a significant decrease in 2024. This indicates that attackers are adapting their methods - moving away from resource-intensive, long-term attacks and toward short, rapid disruptive maneuvers. This new strategy overwhelms traditional DDoS protection measures designed to counter large, long-lasting attacks.

The shortened attack duration requires a correspondingly fast response time. Of particular importance is the time to mitigate (TTM), i.e., the time it takes for a protection system to detect an attack and successfully a against it (see our study: „The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough“). Automated, AI-based defenses are becoming increasingly important to analyze attacks in real time and initiate countermeasures in seconds.

The numbers show that DDoS attacks are evolving - they are no longer just a bandwidth issue, but require an agile, intelligent and proactive security strategy. Those who rely solely on traditional defenses risk significant downtime and vulnerabilities in their IT infrastructure.



Development of attack bandwidths

From Gigabit to Terabit

The DDoS landscape has changed drastically over the past few years. While 2023 was marked by an increase in the frequency and intensity of DDoS attacks, 2024 marks a new peak. With the largest attack measured at 795 Gbps and an average total bandwidth of 3.0 Gbps, DDoS attacks in 2023 significantly exceeded the previous year's figures. Attackers dramatically increased not only the bandwidth, but also the packet rate.

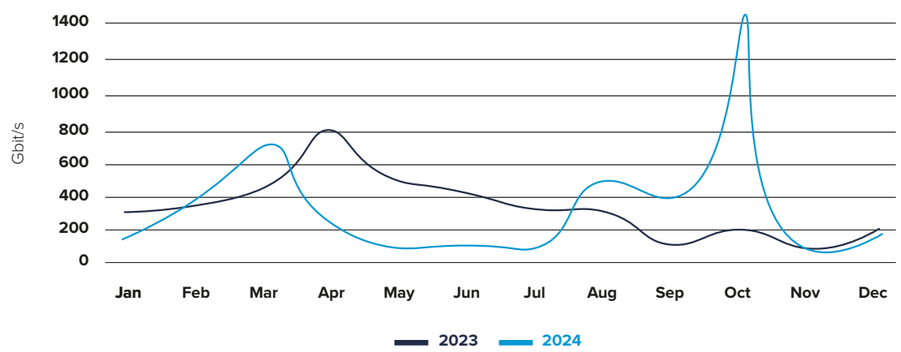
However, 2024 exceeded all expectations: A new dimension was reached with the largest attack measured in Europe at 1.4 Tbps. This more than twofold increase illustrates the rapid evolution of attack vectors. At the same time, however, a more differentiated picture of the threat situation is emerging.

In addition to massive, high-bandwidth attacks, attackers are increasingly using more sophisticated techniques to make their attacks harder to detect.

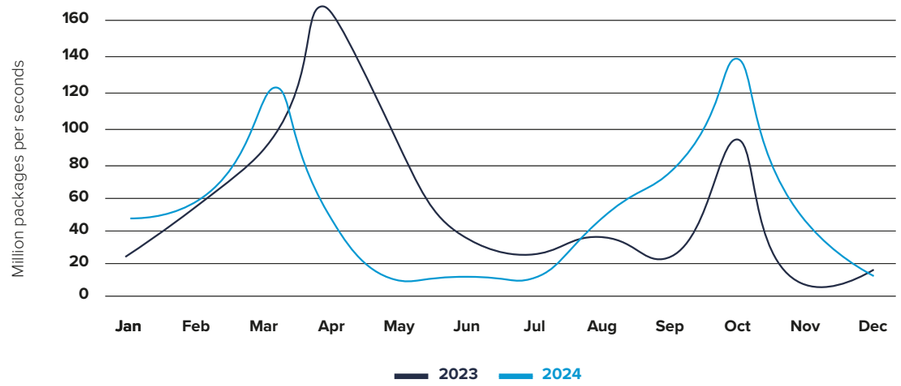
From quantity to quality: more subtle and targeted attacks

While the number of individual attacks is reaching new highs, we are also seeing a strategic shift. Attackers are becoming more subtle and targeted. They are using lower bandwidths and packet rates, making it harder for traditional monitoring systems to detect them. Instead of massive brute force attacks, attacks are often more stealthy and blend seamlessly into normal traffic. This trend shows that DDoS threats are not only increasing in intensity, but also in sophistication

Maximum Bandwidth



Maximum packet rates



Carpet Bombing

Carpet bombing is a particularly insidious form of DDoS attack that is increasingly challenging enterprises and critical infrastructure. Unlike traditional DDoS attacks, which deliberately overload individual servers or network nodes, carpet bombing uses a broad-based attack tactic: large volumes of malicious traffic simultaneously flood a large number of IP addresses within a network. This makes it difficult to identify the attack and means that even the most advanced defenses often fail to sound the alarm until the infrastructure is already overloaded.

Several incidents in Japan illustrate the alarming scale of the threat: between December 2023 and February 2024, a total of 158 attacks were recorded against 64 companies, including banks, airports, and telecommunications providers. Cybercriminals hijacked at least 300 IoT devices worldwide to control coordinated attacks from a hidden location. Most insidiously, many companies had implemented defenses against traditional DDoS attacks, but not against the widespread carpet bombing attacks. The result was widespread system failures that crippled key business processes.

Experts agree that traditional defenses are no longer sufficient to combat this escalating threat. A proactive security strategy is critical. Attacks are detected early and countermeasures are initiated before the system is crippled. This includes advanced detection systems, intelligent traffic filtering, and adaptive network protection that goes beyond reactive DDoS mitigation.

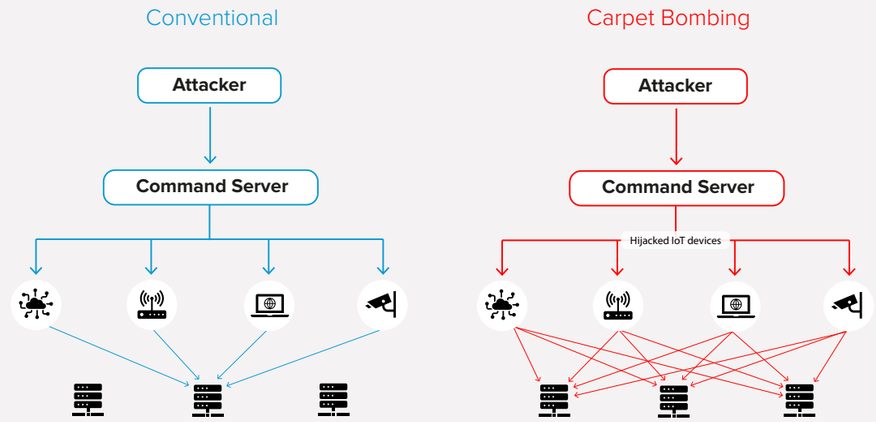
“Organizations must adapt their IT security strategies to defend against sophisticated DDoS attacks like carpet bombing. A layered defense with real-time monitoring and automated threat mitigation is critical.”

Rolf Gierhard, CRO, Link11

Carpet Bombing - Controlled Mass DDoS Attack

Unlike traditional DDoS attacks that target individual servers or network nodes, carpet bombing relies on a broadly distributed attack tactic: large volumes of malicious traffic simultaneously flood a large number of IP addresses within a network.

The botnet's focus is not on a single IP address, but is spread across 100 to several thousand IP addresses in order to cause widespread damage.



UDP Floods and TCP SYN Floods

UDP floods attack layers 3 and 4 because UDP does not require sender authentication and does not perform a handshake. This allows for fast data transfer, which is why UDP is often used in latency-critical applications such as streaming or gaming. Attackers generate massive packets to random UDP ports (packet storm), causing firewalls, routers, and switches to process and validate each packet. Since these systems can only handle a limited number of packets per second, they quickly become overwhelmed. Reflection techniques involving protocols such as DNS, NTP, SSDP, or Chargen can further enhance UDP attacks.

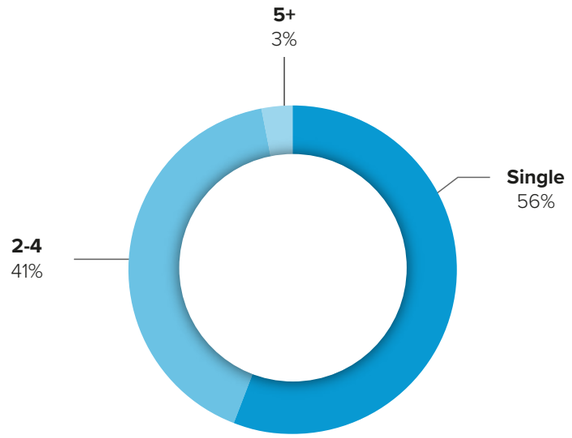
TCP SYN floods exploit weaknesses in the TCP three-way handshake. When establishing a connection, the client sends a SYN packet to the server, which responds with SYN/ACK and waits for an ACK. The server caches these half-open connections in the Transmission Control Blocks (TCB). If the acknowledgement is not received because the SYN requests come from fake or non-existent sender IP addresses, the TCB buffer overflows. The server will then be unable to accept new connections. Attackers keep the buffer artificially full by constantly sending SYN requests. Measures such as reducing the size of the buffer are ineffective against large-scale SYN flood attacks involving thousands of infected systems.

Multi-vector attacks

Precision over mass

The threat of multi-vector DDoS attacks has evolved in 2024. While 2023 saw a trend toward more targeted and resource-efficient attacks, cybercriminals refined their strategies in 2024.

Multi-vector attacks accounted for 52% of all attacks in 2023, while single-vector attacks accounted for 56% of all attacks in 2024. However, the proportion of complex multi-vector attacks remains high: up to 4 vectors were used in 41% of attacks, and more than 4 vectors were used in 3% of attacks. The highest number of vectors observed increased from 11 in 2023 to 12 in 2024.



DNS as the dominant vector

An analysis of the top five vectors shows a significant shift in weight: DNS attacks still account for the largest share of all vectors. This is followed by HTTPS-based attacks, while NTP has lost some of its importance as an attack vector. New to the top five are SNMP and batch attacks, which have not played a significant role in the past. These changes reflect the increasing sophistication and adaptability of attackers.

Automated defense through AI and adaptive defenses

2024 shows that attacks are more targeted, harder to detect, and use a variety of protocols and techniques to defeat defenses. Incremental attacks are particularly dangerous.

Classic DDoS attacks were characterized by high bandwidths or packet rates, but modern attacks often stay below detection thresholds. As such, traditional traffic monitoring systems are reaching their limits.

AI-powered systems are essential to analyze complex attack patterns and take timely countermeasures. Enterprises should rely on a combination of automated DDoS protection, comprehensive monitoring, and AI-based detection. Holistic security solutions also detect subtle anomalies in network behavior.

“Despite its long history, the DDoS threat landscape continues to evolve as attackers seek new ways to amplify and diversify their attacks.”

Karsten Desler, CTO, Link11

SNMP DDoS Attacks: A Dangerous Combination of Reflection and Amplification

The Simple Network Management Protocol (SNMP) is increasingly being exploited for DDoS attacks. Attackers use open SNMP instances to redirect large amounts of data to their target by sending spoofed requests. Particularly problematic is the combination of reflection, where devices unintentionally send data to the victim, and amplification, where response packets are many times larger than the original request. The result is attacks with massive amounts of data that overload networks and disrupt services.

Critical vulnerabilities

Insecure SNMP servers with default community strings, such as „public“	**Lack of network filtering, allowing IP spoofing**	**Botnets that coordinate and amplify attacks**

To protect against such attacks, organizations should consistently secure SNMP, disable unnecessary instances, and rely on SNMPv3 with authentication and encryption. In addition, ingress filters against IP spoofing and comprehensive monitoring of suspicious SNMP activity are essential. ISPs should also implement proactive filtering to block suspicious SNMP traffic at an early stage. Only a combination of secure configuration, traffic filtering, and proactive detection can effectively defend against SNMP DDoS attacks.

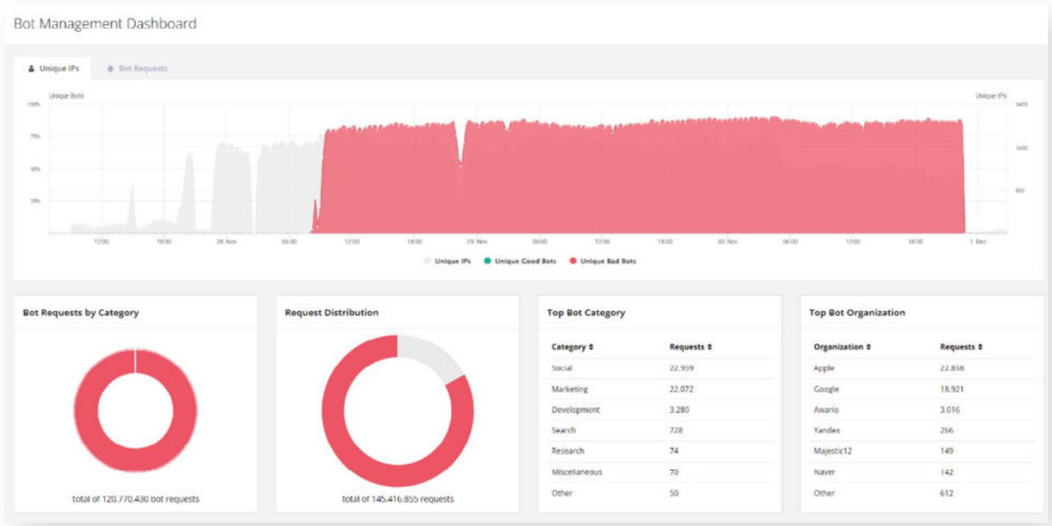
Web Protection

WAAP in an emergency: Analysis of a Multi-Vector DDoS Attack

A recently documented attack highlights the complexity and enormous effort that attackers invest in overloading systems. This attack combined both Layer 3/4 and Layer 7 DDoS techniques and set new standards, particularly in terms of the resources required and the attack vectors used.

The attack: complex interplay of DDoS techniques

The attack lasted four days and involved a sophisticated combination of attack methods. Of particular note was the simultaneous use of layer 3/4 and layer 7 attacks, a combination that is rarely seen in practice. Layer 3/4 attacks focus on the network layer and overload the infrastructure with massive data packets, while layer 7 attacks at the application layer specifically target web servers and APIs by consuming their resources and significantly increasing response times.



In this instance, the attackers reached the staggering number of 120 million requests, resulting in more than one million Web Application Firewall (WAF) logs - a number far beyond the usual volume. The nature of the attack and the tactics used indicate a highly organized group operating with

WAF Violations Top 5
2023 vs. 2024

In 2024, the number of protocol attacks increased significantly compared to 2023. These attacks exploit vulnerabilities in communication protocols to compromise web applications or servers. Attackers use various techniques to bypass security mechanisms, manipulate data, or gain unauthorized access. The most common protocol attacks include:

- **HTTP response splitting:** This involves manipulating a server's HTTP response so that it is split into multiple individual responses. The attacker can then inject additional headers or content that may be misinterpreted by intermediate systems (e.g., proxies or caches). This can lead to cache poisoning, cross-site scripting (XSS), or session-fixing attacks.

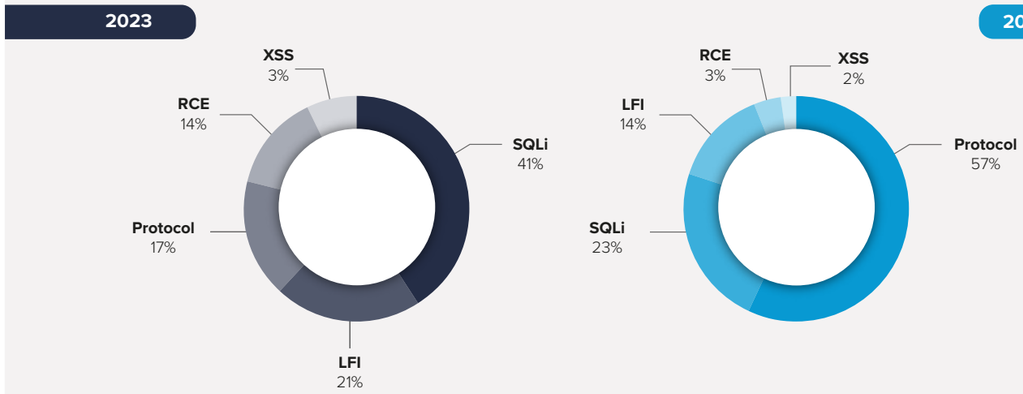
- **HTTP smuggling:** This attack exploits differences in the interpretation of HTTP requests by different server instances (e.g., load balancers, reverse proxies, and backend servers). By formulating requests that are processed differently by the systems, attackers can bypass security mechanisms, gain access to restricted areas, or inject unauthorized code. HTTP smuggling is often used to bypass firewalls or intrusion detection systems.

- **HTTP Header Injection:** Manipulated headers are inserted into HTTP requests or responses to change the behavior of the server or downstream systems. This can be used to bypass security measures or exploit vulnerabilities in web applications. Possible consequences include cross-site scripting (XSS), open redirects, or even remote code execution (RCE).

- **HTTP Parameter Pollution (HPP):** In this attack technique, attackers insert multiple identical or manipulated parameters into an HTTP request to influence server-side processing. This can cause applications to use incorrect values, bypass security checks, or exhibit unexpected behavior. HPP can be used for attacks such as privilege escalation, SQL injection, or denial of service (DoS).

In addition to these specific attack techniques, there are also other protocol attacks that target vulnerabilities in transport or application layer protocols. These include TLS downgrade attacks, in which attackers attempt to downgrade encryption to an insecure version, or DNS spoofing, in which fake DNS responses are used to redirect users to malicious websites.

In the face of the growing threat of protocol attacks, it is crucial to implement modern security mechanisms such as web application firewalls (WAFs), strict header validation, and secure server configurations to detect and defend against potential attacks at an early stage.



Attackers with high resources

A distinctive feature of the attack was its origin. Sources came from international companies whose infrastructure is not normally associated with DDoS attacks. In addition, a large number of IP addresses were blocked simultaneously, indicating that the attackers are able to scale their resources quickly and purposefully.

Another striking aspect was the use of up to 2,000 unique IP addresses, a massive increase from the usual hundreds of IP addresses. The fact that the attackers used an increasing number of outdated user agents towards the end of the attack, such as Windows XP and browser versions from the last five years, also suggests the use of automated botnets controlled by compromised systems worldwide.

Cost and Motivation of the Attack

There is a significant cost associated with an attack of this magnitude. It is unlikely that such an attack was carried out for free. The 145 million requests generated by the attackers in four days would cost several thousand dollars in a normal hosting infrastructure. This leads to the conclusion that this was a highly organized operation.

The possible motivation behind this attack could be politically motivated hacktivism or an attack on behalf of political actors. Another plausible background could be the use of DDoS-as-a-Service - a practice that is becoming increasingly important in the field of DDoS attacks. However, the high level of complexity and effort involved in the attack argues against the simple idea of a script kiddie or a single actor.

Unusual attack patterns

One particularly interesting detail was the behavior of the attackers: it seemed as if they had tested all their methods to see which were effective against the target systems‘ defenses. The attackers tried every tool and tactic in their arsenal, from layer 3 to layer 4 to layer 7 attacks. This was an attack where the entire spectrum was tested to further optimize future attacks.

There was also an „on-off scenario“ during the attack, where the attacks periodically paused and then resumed with full force. This indicates that the attackers experimented with the protection mechanisms of the target systems and tested how they reacted to different attack patterns. Such a change in techniques was observed at the beginning of the attack.

The Role of Bot Management and Web Application Firewall (WAF)

In response to the attack, measures such as bot management and web application firewalls (WAF) were deployed and played an important role in defending against the attacks. WAF systems, which were initially in a learning phase, were eventually able to identify and block the majority of the attacks. This underscores the importance of organizations regularly adapting and optimizing their security solutions to keep pace with the ever-evolving threat of DDoS attacks.

In addition, a continuous protection mode was enabled in this case to ensure that attack protection was not prematurely disabled, further increasing the effectiveness of the defense.

“Attacks like this show that effective protection is only possible through a holistic approach that combines bot management, WAF, and continuous monitoring.”

Ziv Greenberg, VP Product, Link11

An increasingly complex threat

This case is a prime example of how DDoS attacks are becoming more complex and prolonged. Attackers are not only using traditional methods, but are combining different attack techniques and constantly testing new strategies to defeat existing defenses.

For IT professionals and organizations that need to protect web applications and APIs, a holistic protection strategy that combines bot management, WAF, and layer 3 and layer 7 defenses is critical. This approach is the key to being prepared for the increasingly sophisticated DDoS attacks of the future.

The above case illustrates the need to focus not only on the technology, but also on the motivation and resource potential of the attackers. Targeted and continuous monitoring and rapid adaptation of protection mechanisms are essential to successfully counter the threat of sophisticated DDoS attacks.

In today's threat landscape, DDoS attacks are not only numerous, but also increasingly complex. Of particular note in this attack was the simultaneous use of layer 3/4 and layer 7 attacks - a combination that is rare in DDoS attacks, but increasingly used as a strategy to bypass defenses.

Layer 3/4 attacks target the network layer and overload the infrastructure with massive amounts of data and manipulated packet streams. These attacks are designed to overwhelm server capacity and network bandwidth. In contrast, layer 7 attacks target the application layer, where it specifically attacks web applications and APIs to overload resources such as CPU and memory. They are much more targeted and require less bandwidth but can cause enormous damage by exploiting the specific vulnerabilities of web applications.

The combination of these two types of attacks poses a significant challenge to modern web application and API (WAAP) protection. While layer 3/4 attacks overload the infrastructure in the early stages of the attack, layer 7 attacks specifically target the applications themselves, requiring a differentiated defense strategy.

In this case, the attackers tested both layers of attack in parallel to determine which defenses, such as web application firewalls (WAFs) and bot management systems, were most effective at bypassing them. This strategic approach demonstrates the importance of a holistic WAAP strategy that includes both the network and application layers.

Web Performance

EU-US Data Privacy Framework Falters - An Opportunity for European CDNs and Geofencing

Recent developments regarding the transatlantic data agreement, officially known as the EU-US Data Privacy Framework (DPF), have significant implications for the exchange of personal data between the EU and the US. Since Donald Trump took office on January 20, 2025, there have been serious concerns about the future of the agreement.

Key issues include the weakening of the Privacy and Civil Liberties Oversight Board (PCLOB), the review of all national security decisions made by the previous administration, and the threat of legal uncertainty for European companies using US cloud services. If the DPF fails, thousands of companies could find themselves in a legal grey area and be forced to find alternative solutions.

In this context, European content delivery networks (CDNs) and geofencing technologies are becoming increasingly important. These mechanisms allow the targeted control of data flows within secure legal jurisdictions, helping companies to ensure compliance with the General Data Protection Regulation (GDPR). Geofencing can prevent personal data from entering countries with inadequate data protection, while European CDNs offer a GDPR-compliant alternative to US providers.

Geoblocking: Effective access control to thwart threats

Geoblocking allows organizations to selectively control access to their IT infrastructure by blocking traffic from specific countries or regions. This is particularly useful for defending against cyberattacks such as DDoS, which often originate from specific geographic regions. For example, a sudden increase in malicious traffic from a particular country can be effectively mitigated by specifically blocking that country of origin.

In practice, geoblocking is best implemented at the edge, with the CDN acting as the first line of defense. Modern providers integrate DDoS mitigation directly into their network to neutralize attacks at an early stage.

Geoblocking also plays a central role in controlling access to digital content. Streaming services and media libraries use geoblocking to ensure that content is only accessible in certain countries. Without geoblocking, a user in a blocked country could still access cached content, which can lead to legal and licensing issues.

Geofencing: privacy, compliance, and targeted control

Geofencing extends the capabilities of geoblocking by not only regulating access, but also controlling where data is processed or stored. This is particularly important for GDPR compliance, as personal data cannot be transferred to third countries in an uncontrolled manner.

A specific example of the importance of privacy-compliant data processing is the use of security services, such as Captchas. Providers such as Google often store and process user data in the US, which raises privacy risks. While geofencing is not directly related to captchas, it can still allow companies to specifically control access to alternative GDPR-compliant captcha services within the EU and ensure that user data is processed in regions that comply with data protection regulations.

Technically, geofencing is enabled by specialized CDN technologies that route traffic and direct user requests to servers in specific geographic regions. This ensures that European users, for example, only interact with servers within the EU. Along with ensuring compliance with privacy regulations, it can also optimize network performance.

Geofencing and Flexible CDN Control

Many international CDN providers rely on technologies such as Anycast, which links one IP address to multiple server locations to maximize performance and redundancy. However, this can make it difficult to precisely control traffic.

European providers such as Link11 offer more granular control and use specially optimized mechanisms. This means that traffic can be kept within Europe or certain regions can be excluded, providing a flexible solution for companies with high data protection requirements.

Other providers use alternative technologies that may be less flexible in strictly tailoring traffic to meet privacy and compliance requirements.

Capacity vs. Compliance: The Role of Specialized European CDNs

An argument often used by global CDN providers is their huge infrastructure with a large number of points of presence (PoPs). However, it is not only the absolute number of servers that matters, but also their strategic placement in the relevant markets. For European companies, a regional infrastructure optimized for their specific needs can often be more advantageous than a globally distributed network.

Link11 operates numerous CDN nodes around the world, with a special focus on a high performance and dense infrastructure in Europe. This targeted selection of locations ensures optimal performance in key markets and offers companies a reliable alternative to globally distributed networks that may be less well developed in strategically important regions.

Balancing security, compliance, and performance

Geoblocking and geofencing are key to balancing IT security, regulatory compliance, and performance. While global CDN providers often strive for maximum performance, European providers are increasingly focused on data protection compliance and targeted traffic control.

Companies that need to comply with GDPR should consider whether a European CDN provider such as Link11 is a better alternative. Choosing the right IT security strategy depends both on technical feasibility and regulatory and business requirements. Geoblocking and geofencing are essential tools for a holistic IT security strategy.

DNS Security: The Often-Underestimated Achilles‘ Heel of IT Infrastructures

The lesson from Mastercard: A DNS bug with far-reaching consequences

In January 2025, a critical DNS misconfiguration at Mastercard made headlines. For five years, a simple but consequential typo in the company‘s DNS configuration had gone unnoticed. One of the five DNS addresses Mastercard used was misspelled and pointed to an unregistered domain. A security researcher secured this for as little as $300 and found that it was already processing millions of DNS requests. Had cybercriminals exploited this vulnerability, they could have done anything from redirecting Internet traffic to stealing credentials.

The incident is a stark reminder that even seemingly trivial components such as the Domain Name System (DNS) are critical to IT security. The DNS is the “phone book of the Internet“ that resolves domain names into IP addresses. A single bug or vulnerability can be enough to compromise all of an organization‘s traffic.

Why DNS Security Matters

Although the DNS is one of the most critical components of the Internet, it was originally developed without any built-in security mechanisms. Today, DNS-based attacks are a lucrative target for cybercriminals because many organizations pay too little attention to this area. The threat scenarios are diverse:

- **DNS spoofing and cache poisoning:** Attackers manipulate DNS responses and redirect users to fake websites to steal their information.
- **DDoS attacks on DNS servers:** DNS servers are overloaded and crippled by massive requests, rendering Internet services unavailable.
- **DNS hijacking:** Cybercriminals take control of DNS settings to redirect traffic or intercept email communications.
- **Data exfiltration through DNS tunneling:** Malware uses DNS queries to exfiltrate data from networks undetected.

Strategies to Improve DNS Security

In the face of these threats, a robust DNS security strategy is essential. A secure DNS infrastructure includes a variety of measures to prevent attacks and ensure high availability.

Key measures for improving DNS security

- **Global anycast infrastructure:** Servers located around the world provide fast and reliable DNS resolution.
- **Protection against DoS/DDoS attacks:** Advanced DNS filtering and monitoring mechanisms help detect and mitigate suspicious activity.
- **DNSSEC Implementation:** Use of DNS Security Extensions (DNSSEC) ensures that DNS responses are authenticated and cannot be tampered with.
- **Easy management and automation:** Modern management platforms and APIs enable secure and efficient configuration.
- **Redundancy and Resilience:** Multiple server locations ensure that DNS services continue to function reliably even in the event of outages.

DNS security is a necessity, not a luxury

The Mastercard incident shows that even billion-dollar companies can neglect basic security issues such as DNS integrity. Proper protection of this critical infrastructure is essential to prevent cyberattacks and protect business processes. Link11 Secure DNS is a robust and scalable solution that provides organizations with the protection and performance they need to secure their digital presence.

Nothing works on the Internet without DNS - and without secure DNS, everything is at risk.

“The DNS is the weak spot of the Internet. Just one wrong setting can put a company‘s whole data traffic at risk.”

Lukas Frank, Product Manager, Link11

2024

The year 2024 was marked by an unprecedented wave of DDoS attacks, which dominated the cybersecurity landscape with record numbers and increasing complexity. The proliferation of DDoS-as-a-service and the use of AI intensified these attacks and presented new challenges to organizations. At the same time, the ongoing skills shortage has led to increased automation of security-critical processes. Another area of focus is securing APIs, which are increasingly being targeted by cybercriminals.

2025

By 2025, attackers will have become even more professional, relying more heavily on AI-powered and automated attack techniques. Record-breaking volumetric attacks will continue to make headlines, while low and slow attacks – low-profile but highly effective attacks that bypass traditional defenses – will become more common. Organizations must constantly evolve their IT security strategies to keep pace with these threats. The key is AI-powered security systems, observability, and holistic cyber resilience to protect against increasingly sophisticated attacks.

Your contact person

Michael Scheffler
Vice President Sales

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

Sources

[1] https://www.seco.admin.ch/seco/en/home/seco/nsb-news.msg-id-99736.html

[2] https://news.err.ee/1609278921/ria-estonia-s-state-institutions-hit-by-largest-cyberattack-to-date

[3] https://thecyberexpress.com/tram-barcelona-cyberattack-noname/

[4] https://www.spf.org/iina/en/articles/osawa_04.html

[5] https://www.brusselstimes.com/belgium/1258228/pro-russia-cyberattack-targets-several-belgian-government-websites

[6] https://www.infosecurity-magazine.com/news/uk-council-sites-recover-russian/

[7] https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/

Head office

Link11
Lindleystr. 12
60314 Frankfurt