LINK 11

Reblaze

European Cyber Report

Threats and Trends in Network Security and Web Protection

Table of Contents

Editorial

Dear readers,

Following the acquisition of Reblaze Technologies, a renowned provider of cloud-native web application and API protection (WAAP), we want to take a truly collaborative approach to making the Internet a safer place. The threat landscapeis more acute than ever. Politically motivated hacker groups are targeting international critical infrastructures, bots are becoming increasingly sophisticated, and every critical security vulnerability is a potential gateway for cybercriminals.

The daily challenges for companies are increasing, making a proactive cybersecurity strategy and innovative defensive measures all the more important. The „European Cyber Report - Threats and Trends in Network Security and Web Protection“ now replaces the previous DDoS Report. This report not only highlights the increasing complexity of the threat landscape, but also shows how AI-based and automated security solutions can increase cyber resilience. In addition to the in-depth analysis of DDoS attacks registered in Link11‘s own network, we have integrated additional cutting-edge content from the areas of web protection and web performance.

Link11 is stepping up to help its customers protect their critical assets and brands. Instead of seeing cybersecurity as a pure cost factor, we want to shift perspective to how it enables innovation and growth with secure environments and ultimately transform abstract security concepts into competitive advantages. It is important to pay much more attention to known vulnerabilities and to take effective protective measures.

I wish you an exciting read!

Kind regards,
Jens-Philipp Jung, CEO, Link11 Group

Introduction and summary

The state of network security and web protection in 2023

At the beginning of the year, Sadie Creese, Professor of Cybersecurity at Oxford University, warned of an impending „cyberstorm“[1] during the World Economic Forum in Davos. Although she could not predict exactly how severe this storm would be in January 2023, her prediction has proven to be very accurate.

According to the latest Allianz Risk Barometer[2], cyberattacks are one of the biggest threats to companies worldwide. Almost all companies now rely on digital services and infrastructure. Technological progress has brought a huge number of achievements, but at the same time, comprehensive networking harbors major risks. Every network, website or interface that is connected to the Internet is a potential gateway for cybercriminals.

Cyber threats are now part of everyday life. Whereas they used to be purely an IT problem, they now have to be taken into account in every corporate strategy. The activities observed by the Link11 Security Operations Center (LSOC) in 2023 also make one thing very clear: the impact of cyber incidents requires a risk-based, holistic cybersecurity strategy to support business objectives and achieve corporate growth.

This year‘s Cybersecurity Report highlights relevant security findings in the areas of bot management and WAF, also known as WAAP (Web Application and API Protection), in addition to the development of DDoS attacks in the Link11 network. The report also outlines the interplay between speed and security for online presences with regard to the Content Delivery Network (CDN). The report is divided into the sections Network Security, Web Protection and Web Performance.

Network Security

In 2023, the Link11 network saw a drastic increase in DDoS attacks of more than 70% compared to the previous year, with politically motivated attacks contributing significantly. These attacks targeted well-known targets worldwide, such as German federal states and authorities[3], the European Investment Bank[4], and Microsoft[5]. Critical infrastructure is particularly at risk, as successful attacks can have serious social, economic, and political consequences.

“The need for a proactive approach and innovative defense strategies is becoming increasingly urgent in light of current developments. By implementing AI-based and automated security solutions, companies can effectively counter the growing threat. In addition to security aspects, the focus should always be on the user-friendliness of the solution used.”

Karsten Desler, CTO, Link11 Group

There are also worrying trends in the characteristics of attacks: “turbo attacks” reach their critical payload in less than 20 seconds, and the intensity of DDoS attacks is increasing. There are indications that attackers are increasingly using AI to refine their attack methods, as Europol warns in its report „The Impact of Large Language Models on Law Enforcement“[6]. In addition, increasingly smart multi-vector attacks with a focus on efficiency and resource conservation are being registered in the Link11 network. The duration of attacks has also increased. The longest attack in 2023 lasted almost 75 hours, compared to 28 hours and 15 minutes in 2022.

Web Protection

In addition to comprehensive DDoS protection, bot management has also become a critical necessity. Organizations are increasingly confronted with a variety of automated traffic types, from harmless to malicious bots. While some bots increase efficiency and automate operational processes, „bad bots“ pose a serious threat through the spread of spam and credential stuffing, for example. The ongoing development of generative AI and the increasing sophistication of attacks make effective protection essential, while many companies are still vulnerable to simple bot attacks.

Various techniques are used to distinguish human traffic from machine-generated traffic. In view of the rapid increase in bot attacks and their serious impact on companies, a differentiated approach is required that, in addition to technical solutions, also relies on increased security awareness among employees and continuous adaptation to new threats.

The increasing number of security vulnerabilities and the growing complexity of web applications have highlighted the importance of a reliable security solution such as the Web Application Firewall (WAF). With an alarming 15% increase in reported vulnerabilities in 2023, it is clear that traditional firewalls are often not enough to protect against increasingly sophisticated attacks. The WAF provides a solution by monitoring traffic at the application level, detecting suspicious activity and defending against potential attacks such as SQL injection, cross-site scripting, and remote code execution.
WAFs help ensure the security and integrity of web applications by detecting and blocking suspicious activity. However, to maximize their effectiveness, WAFs must be properly configured, regularly updated, and supported by clear security policies and regular audits.

Web Performance

Content Delivery Networks (CDNs) offer performance improvements for the delivery of web content through the global distribution of content. With a redundant network and seamless integration of security features, Link11‘s CDN ensures continuous availability of content and an additional layer of security for infrastructure. In addition, when selecting a provider, attention should be paid to its compliance and guarantee of European data protection regulations.

Network Security

DDoS in the news

January 2023

Hackers attack Danish central bank and financial service providers

The websites of the Danish central bank and Bankdata, a company that develops IT solutions for the financial sector, were hit by DDoS attacks.[7]

February 2023

Several German airports affected by DDoS attacks

The websites of seven German airports were hit by DDoS attacks and were unavailable.[8]

March 2023

Cyberattack on a Canadian electricity supplier

A pro-Russian hacker group has claimed responsibility for a cyberattack on the state-owned electricity supplier of Québec.[9]

April 2023

European air traffic control: DDoS attack by pro-Russian hackers

European air traffic control was hit by a DDoS attack blamed on pro-Russian hackers.[10]

May 2023

Hacker group „Anonymous Sudan“ demands 3 million dollars from Scandinavian Airlines

Anonymous Sudan made a ransom demand of 3 million dollars to Scandinavian Airlines (SAS) to stop the DDoS attacks.[11]

June 2023

Microsoft Outlook out of service after hacker attacks

Microsoft Outlook was unavailable for thousands of American users on Monday. Anonymous Sudan declared a campaign against US companies and infrastructure.[12]

July 2023

DDoS attack on Norwegian government websites

DDoS attacks on 12 of the Norwegian government's websites due to a software vulnerability at a technology service provider.[13]

August 2023

Several Italian bank websites paralyzed

Italy's cybersecurity authority detected hacker attacks on the websites of at least five banks, making access to some of their services temporarily impossible.[14]

September 2023

Wells Fargo online banking out of service

Anonymous Sudan paralyzed the US financial services institution Wells Fargo and disabled online banking.[15]

October 2023

Host of the EU summit in Spain targeted by DDoS cyberattacks

Several public and private websites were the target of a DDoS attack by pro-Russian hackers.[16]

November 2023

DDoS attack responsible for ChatGPT outage

OpenAI has confirmed that a DDoS attack is responsible for the outage of ChatGPT and its developer tools.[17]

Dezember 2023

DDoS attacks on several Belgian websites

Several websites of Belgian government agencies were down due to a DDoS attack.[18]

Development of the total figures in the Link11 network

Significant increase in the number of DDoS attacks

After a decline in DDoS attacks was recorded in the Link11 network for the first time in 2022, the number of attacks rose again significantly in 2023. The number of DDoS attacks increased by more than 70% compared to the same period last year. This is also associated with an increase in daily attacks.

In addition to the ongoing war between Russia and Ukraine, the conflict in Israel has triggered a further increase in politically motivated DDoS attacks by well-organized attackers. Prominent actors include the pro-Russian groups NoName057(16), Anonymous Sudan, and Killnet. What they all have in common is that they use DDoS attacks as their preferred method for ideologically motivated cyberattacks.

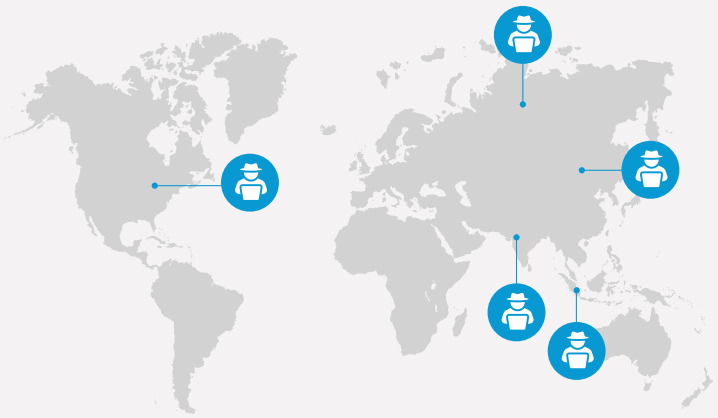
Geopolitical tensions are increasing worldwide, meaning that the threat of such attacks continues to grow, as does the number of related cyberattacks. Many of these DDoS attacks target critical infrastructure („CRITIS"), public institutions, and political organizations. Hardly a month has gone by without cyberattacks on NATO countries and their critical infrastructure. The new head of the BSI, Claudia Plattner, warned at the beginning of July 2023 that the threat situation has never been so serious.[19]

Throughout the year, DDoS activities in the context of patriotic hacktivism continued to increase compared to the previous year. With the launch of the „DDoSia project", a special DDoS toolkit, the possibilities for attackers are greater than ever, as is the number of attacks. The project, which was launched in 2022, has since been further developed by NoName057(16) and its supporters. Such a tool means that the threat potential for politically motivated cyberattacks is constantly growing and threatens sectors such as energy, finance, and healthcare.

These sectors are particularly susceptible to DDoS attacks, which not only cause millions in financial damage, but can also lead to dangerous supply bottlenecks and even endanger human lives. A look at the geographical distribution shows that the attacks affect organizations and critical infrastructure providers worldwide.

A particularly high volume of malicious data traffic originated from the USA, Russia, and China, closely followed by Indonesia and India. At the same time, several countries will always be involved in a DDoS attack. In addition to the above-mentioned nations, more malicious traffic was also observed in Germany, the UK, Thailand, and Italy.

Main Countries of origin of DDoS traffic



DDoS attacks are no longer just a minor nuisance, but a real threat to companies and institutions worldwide. They have become an effective tool to advance political agendas and compromise critical infrastructure. A proactive approach and innovative defense strategies are essential to effectively counter this threat and protect our society from serious consequences. Find out more in the Link11 whitepaper: *Critical infrastructures in the crosshairs.*

“The threat situation is more acute than ever. Given limited resources such as budgets and skilled staff, companies should rely on IT security solutions that are easy to implement and operate. AI-based and automated security solutions guarantee effective protection.“

Rolf Gierhard, CRO, Link11

NoName057(16) - Hacktivism 2.0 and the DDoS attack tool „DDoSia“

In the ongoing conflict between Russia and Ukraine, NoName057(16) has received particular attention as a pro-Russian hacktivist group. Operating since March 2022, the group launched politically motivated distributed denial-of-service (DDoS) attacks on European nations and their critical infrastructure. With a success rate of 40 percent, NoName057(16) executed more than 5,000 attacks[20], with government facilities and transportation and financial sectors among the main targets.

The group has grown from a seemingly insignificant entity to a well-organized collective with a strong online community. With more than 60,000 subscribers on its Telegram channel, the group is taking an innovative approach with the crowdsourcing botnet project „DDoSia“[21], the successor to the Bobik DDoS botnet[22].

NoName057(16) combines ideological motives with financial incentives for members and supporters. The „heroes“ are able to register on the Telegram bot with their ID number and a crypto wallet and benefit from crypto payments of 20,000 (200€) to 80,000 (800€) Rubles, depending on how large their own attacks were in relation to the number of all DDoS attacks for a given period[23]. Although the hacker group launches at least one DDoS attack a day based on global events or the current news cycle, its repertoire now also includes disinformation and intimidation campaigns. The professionally organized group even maintains its own support channel in English.

DDoSia is the toolkit specially developed by NoName057(16) for DDoS attacks. It consists of command & control servers and DDoSia clients that allow volunteers to make their computers and Internet connections available for attacks. The attacks are organized via Telegram. This is used to bundle targets and cause maximum damage.

Originally written in Python, the hackers switched to Go to improve efficiency. The communication between the DDoSia clients and the C2 servers is personalized and employs user hashes to identify the participants. The attack targets are received by the C2 servers and the tool generates corresponding requests. As is common in DDoS attacks, legitimate traffic is imitated to bypass automated detection systems. This technology makes the automatic detection and blocking of malicious requests much more difficult. In light of the constant development and growth of the DDoSia community, one thing is certain: the „DDoSia“ attack tool has arrived in the cyber world and will not disappear any time soon. Protection solutions that are integrated into a comprehensive security concept are therefore crucial to effectively protect against such attacks.

Development of the „onset“

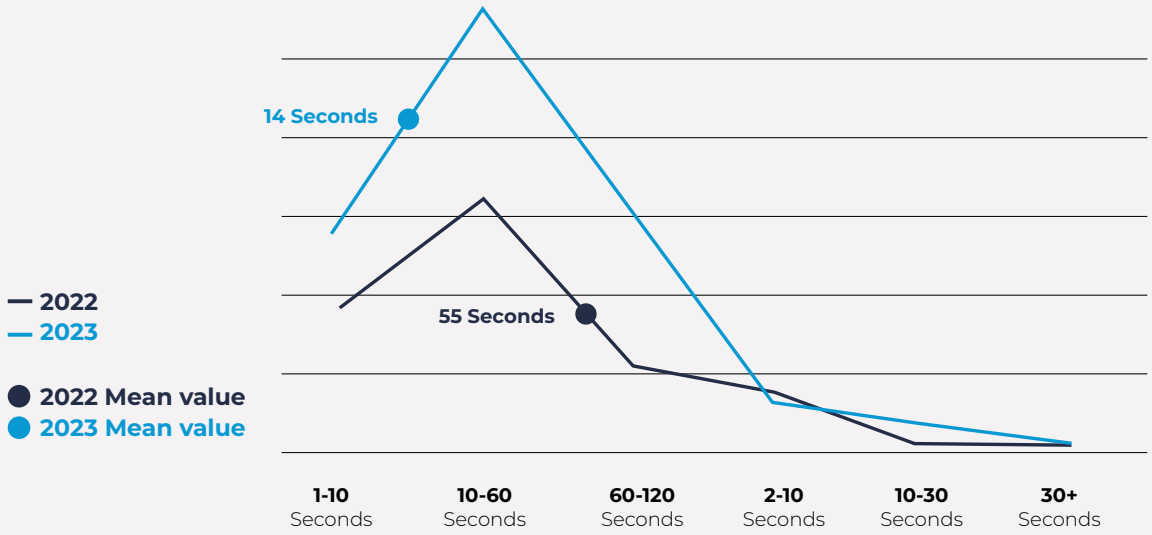
Smart turbo attacks on the rise

Since the first half of 2022, the DDoS attacks registered in the Link11 network have been used to determine how many seconds pass after the first bytes are transmitted until the traffic reaches its maximum value. These DDoS attacks are different: they do not announce themselves with a slow increase in the attack but reach their critical payload in the shortest possible time.

As a result, network systems can be paralyzed before their defensive measures take effect. The LSOC refers to this attack period as the „onset“. The focus here is on the time it takes for an attack to reach a particularly powerful volume.

In 2023, DDoS attacks reached a critical level after just 14 seconds on average. Compared to the average of 55 seconds in the same period in 2022, these „turbo attacks“ reached critical volume significantly faster.

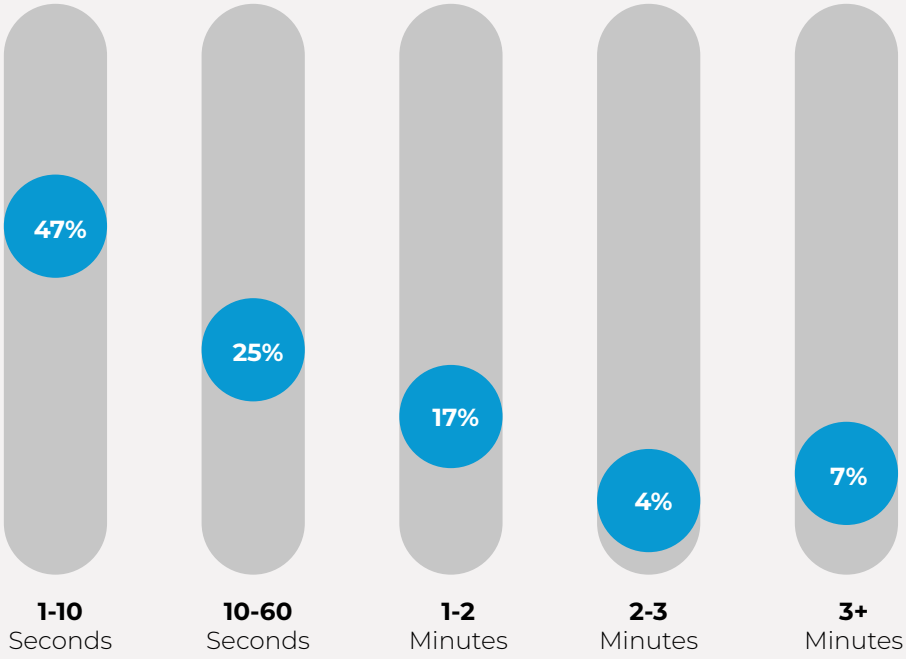
Duration until the peak of an attack I 2023 vs. 2022



“Normally, attacks have a ramp-up time before they reach their critical potential. Onset is an important factor in the evaluation of DDoS attacks because it measures how quickly an attack reaches its critical volume. The sooner the critical payload is reached, the more professional and coordinated the attack was.“

Sean Power, Solution Engineer, Link11

Distribution of the duration up to the peak of the attack



Looking at the distribution of the time it takes for a DDoS attack to reach its peak shows the following results for the period under review: In just under half of the attacks (47%), the critical payload was reached within the first ten seconds. In 2022, this proportion was a quarter (28%).

In 2023, attacks that reached their maximum value in 10 to 60 seconds accounted for a quarter of all attacks registered in the network (25%). In comparison, almost half of the attacks (47%) in 2022 peaked in the same period.

In just under a fifth of cases (17%), DDoS attacks in the first half of 2023 took between one and two minutes to reach their critical peak. This figure was 13% in the same period last year.

For every tenth attack (11%) of the DDoS attacks recorded by the LSOC, it took more than two minutes to reach the critical level. In the same period in 2022, 12% of attacks peaked in more than two minutes.

> **The characteristics of such „turbo attacks“ allow conclusions to be drawn that the attacks could have been organized by a botnet with a suitable capacity. Attacks only reach their critical peak in such a short time if sufficient data traffic volume is generated, as is the case with the „DDoSia“ botnet, for example. This is because, unlike conventional botnets, „DDoSia“ involves privately provided computing power.**

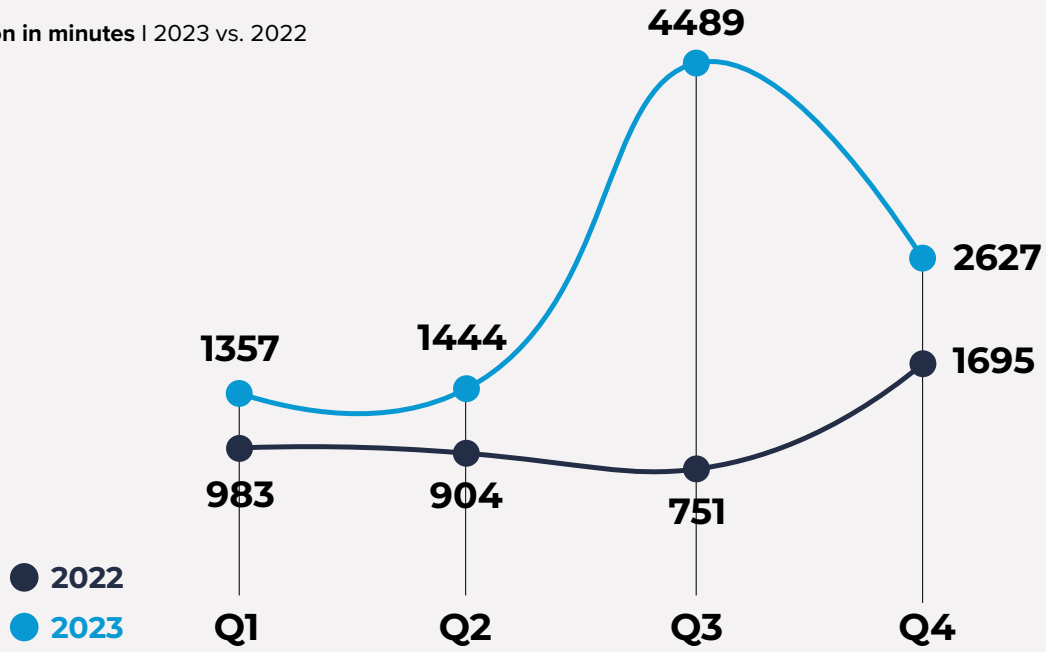
Development of attack duration

Attacks are getting longer

The duration of DDoS attacks registered in the Link11 network in 2023 has increased overall compared to the previous year. A look at the chart below clearly shows how the duration of DDoS attacks developed in 2023 compared to 2022.

Overall, the longest attacks differ significantly from one another. The year 2023 was characterized by longer attacks overall, whereas in 2022 there was a trend towards shorter DDoS attacks. The longest attack in 2023 was 4,489 minutes long, which corresponds to 74 hours and 49 minutes. The longest DDoS attack in 2022 was only 1,695 minutes, or 28 hours and 15 minutes.

Attack duration in minutes I 2023 vs. 2022



“Time is a crucial factor. In the event of an attack, every second counts - bypassed defense mechanisms, routing problems or manual assessments put additional pressure on IT departments. Real-time analysis of data traffic with cloud-based AI technology is the key to defending against DDoS attacks at lightning speed and preventing a system failure.“

Jag Bains, VP Solution Engineering, Link11

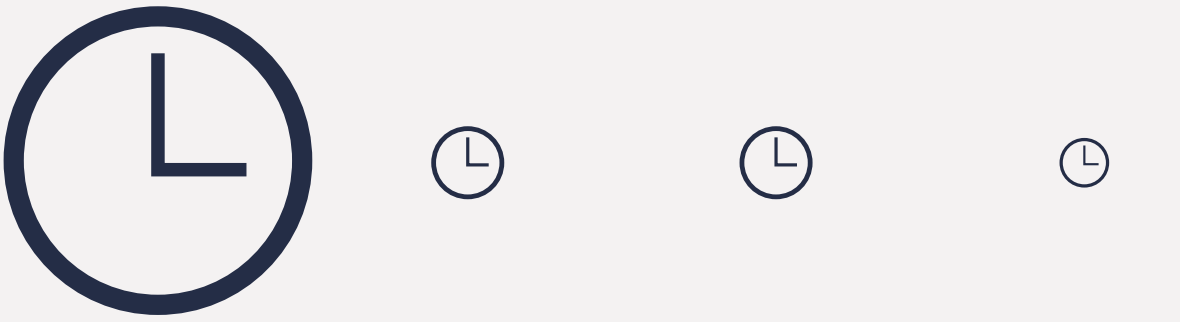
Further analysis shows that the length of the attacks varied between a few minutes and several hours. Most attacks (88%) lasted less than 5 minutes. 5% of all registered attacks lasted between 5 and 10 minutes, another 5% up to 60 minutes. 2 % of attacks lasted longer than 60 minutes. Compared to the previous year, the number of these long-lasting attacks has doubled.

The duration of a DDoS attack depends heavily on the attack technique used. Hackers often use lightning attacks on individual IP addresses to identify vulnerabilities in their target's IT infrastructure. On the other hand, small, fast DDoS attacks often serve as a cover for parallel hacker attacks on servers and networks. Using a DDoS smokescreen allows hackers to penetrate undetected through the back door.

In such cases, existing IT resources are mobilized quickly to minimize system failures and damage. Short attacks that are suddenly interrupted also indicate that the attackers were unable to reach their target. In the case of well-protected infrastructures, attackers withdraw to save resources. However, in the case of long-lasting attacks, their objective is to permanently disrupt and damage their targets.

However, duration alone is not an indicator of the strength of a DDoS attack. One attack may reach its peak without causing much damage. Another attack may already have critical effects, such as a complete outage, before the maximum attack potential is exhausted. Time-to-mitigate (TTM) is crucial, especially for fast-onset attacks. The Frost & Sullivan study, „The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough", shows how well Link11 and other providers perform in terms of this crucial factor.

Distribution of attack duration 2023



<5 min	5-10 min	10-60 min	60+ min
88%	5%	5%	2%

An effective IT security strategy requires real-time analysis of data traffic using smart, fast, and secure methods to ensure maximum transparency in the network. The combination of basic protection and intelligent, automated AI technology forms the backbone of defensive measures against DDoS attacks.

Development of the attack bandwidths

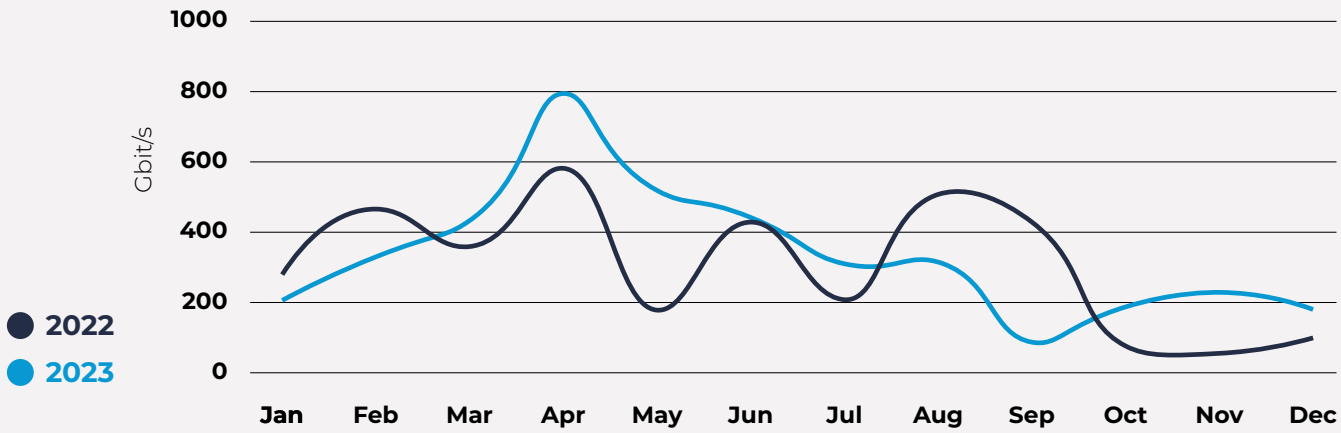
DDoS attacks: intense and complex

In 2023, we saw more high-volume attacks than in 2022. While the bandwidths measured by the LSOC exceeded the 100 Gbps mark every month in 2023, the graph below shows significant fluctuations over the course of 2022. In October and November 2022, the bandwidth peaks were even well below 100 Gbps.

The largest attack in 2023 was stopped at 795 Gbps, which represents a significant increase compared to 2022 (574 Gbps). In the first half of the year, the bandwidths of high-volume attacks fluctuated between 261 Gbps and the highest single peak of 795 Gbps measured. In the second half of the year, the intensity of the attacks decreased again. The largest DDoS attack in the third and fourth quarters of 2023 was stopped at just 303 Gbps.

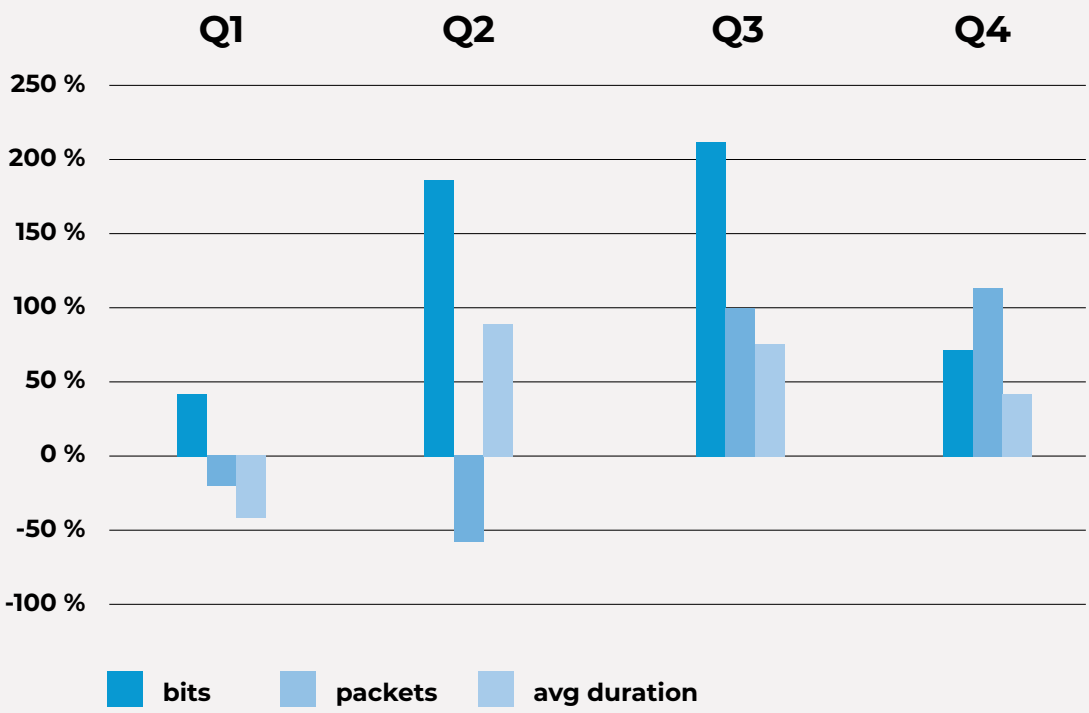
The average total bandwidth increased again from 2.6 Gbps in 2022 to 3.0 Gbps. The intensity is reflected not only in the higher average bandwidth, but also in the number of packets transmitted. At more than 168 million packets per second, the highest packet rate ever recorded in the Link11 network was observed during the period under review. The average packet rate in the period under review was 625,000 packets per second, so the average in 2022 was significantly higher. In the event of an attack, an average of 3.3 million packets per second were transmitted.

Bandwidth peak per month | 2023 vs. 2022



An increased intensity of attacks could already be observed in 2022. This trend continued in 2023 with a further increase in average bandwidths. At the same time, a look at the correlation between the duration and intensity of DDoS attacks reveals a further change, particularly from the second quarter of 2023: the more intensive attacks last longer.

Change in duration and intensity of attacks in 2023



Website vs. ISP-Killers

A further look at the DDoS attacks registered in the Link11 network shows that the size distribution of attacks has changed. Compared to the previous year, attacks larger either 850 Mbit/s, 8.5 Gbps or 85 Gbps have increased. But what does this mean for companies?

Many companies now have 10 Gbit/s uplink capacity. If attacks reach 85% of the total capacity of this upstream line, it can be overloaded and, in the worst case, completely paralyzed. All attacks greater than 8.5 Gbit/s are capable of this. The same applies to the less frequent 100 Gbit/s uplink capacities of large Internet service providers (ISPs). A DDoS attack of more than 85 Gbit/s has the potential to completely overload an ISP or its upstream line.

At the same time, an increase in smaller attacks has also been observed. The number of attacks larger than 850 Mbit/s has increased. This suggests that the intelligence of DDoS attacks is increasing. These smarter attacks do not reach a critical level for either a 10 Gbit/s or a 100 Gbit/s upstream line. Instead, attacks of this size can already paralyze websites.

A robust IT security strategy requires continuous real-time analysis of data traffic to ensure maximum transparency in the network. A promising defense against DDoS attacks consists of basic protection and a combination of intelligent and automated AI technology. In view of the growing complexity and intensity of attacks, it is crucial to rely on precision and speed in detection and defense. The time windows for an effective response to such attacks are often very short. This makes it even more important to continuously review and optimize the defensive measures implemented.

Change in size distribution of DDoS attacks | 2023 vs. 2022

Multi-vector attacks

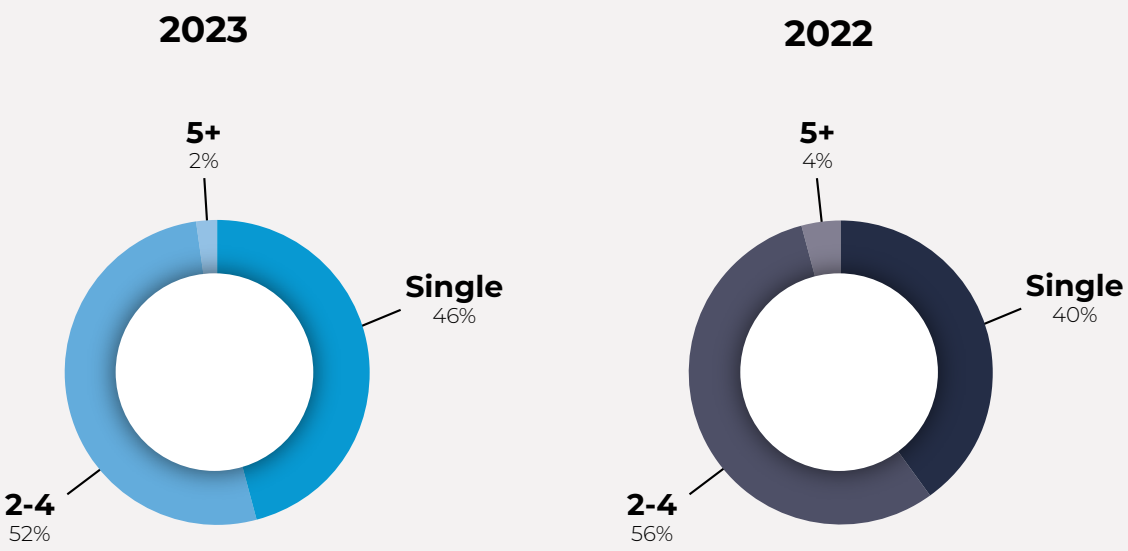
Multi-vector attacks: smarter and more efficient

Multi-vector attacks are characterized by their complexity. In contrast to conventional attacks, in which only one attack vector is used, multi-vector attacks simultaneously target several weak points in the areas of transport, application, and protocol. This combination makes it considerably more difficult to detect and defend against the attacks, as the defense systems are confronted with several attack vectors.

These attacks are particularly dangerous as they increase the probability of success for the attackers. The use of different vectors increases the probability that at least one will be successful and break through the defenses. When IT security lags behind the threat landscape, a single vector used in a targeted and concentrated manner is enough to cause major damage.

In 2023, the proportion of multi-vector attacks decreased slightly compared to the previous year. The proportion of multi-vector attacks was 52% in 2023, while we measured 56% multi-dimensional attacks in 2022.

Number of single and multi-vector attacks I 2023 vs. 2022



Companies should rely on a comprehensive IT security strategy with regard to multi-vector attacks. This includes specialized DDoS protection solutions that can work effectively against different attack vectors at all filter layers. Such a system can detect and defend against attacks in real time to minimize the risk of prolonged downtime. It is also important to regularly update the security infrastructure.

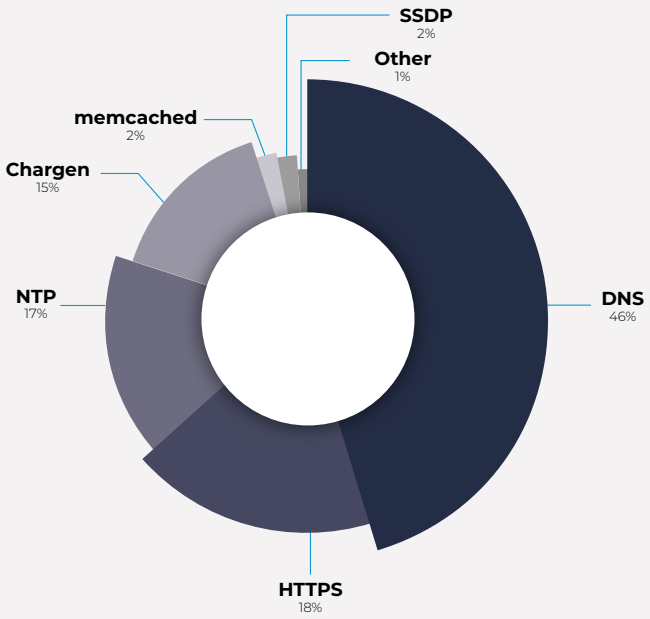
The highest number of simultaneously deployed vectors observed in the Link11 network was 11. In 2022, the number of simultaneously deployed vectors was 18. These were the largest multi-vector attacks observed in our network so far.

Instead of attacking indiscriminately with many different vectors, the vectors that promise the most success are used in a targeted manner. The number of vectors therefore moves more and more towards the „middle“, i.e., mainly using between two and four vectors. This suggests that DDoS attacks are becoming smarter and more resource friendly.

By exploiting the identified vulnerabilities at the same time, attackers can make their attacks more complex and cause more targeted damage. It is therefore essential for companies to optimize their DDoS defense strategies and deploy robust security solutions that are capable of detecting, analyzing and effectively neutralizing multi-vector attacks.

In almost half (46%) of multi-vector attacks, DNS was used as a vector, while in just under a fifth (18%) the attackers used HTTPS or NTP (17%).

Attack vectors 2023



“The threat landscape is constantly changing. Even if the use of fewer vectors looks like a respite, the danger has not gone away - the efficiency of DDoS attacks is increasing. They are becoming smarter and more diverse.“

Jens-Philipp Jung, CEO, Link11 Group

Reflection amplification attacks

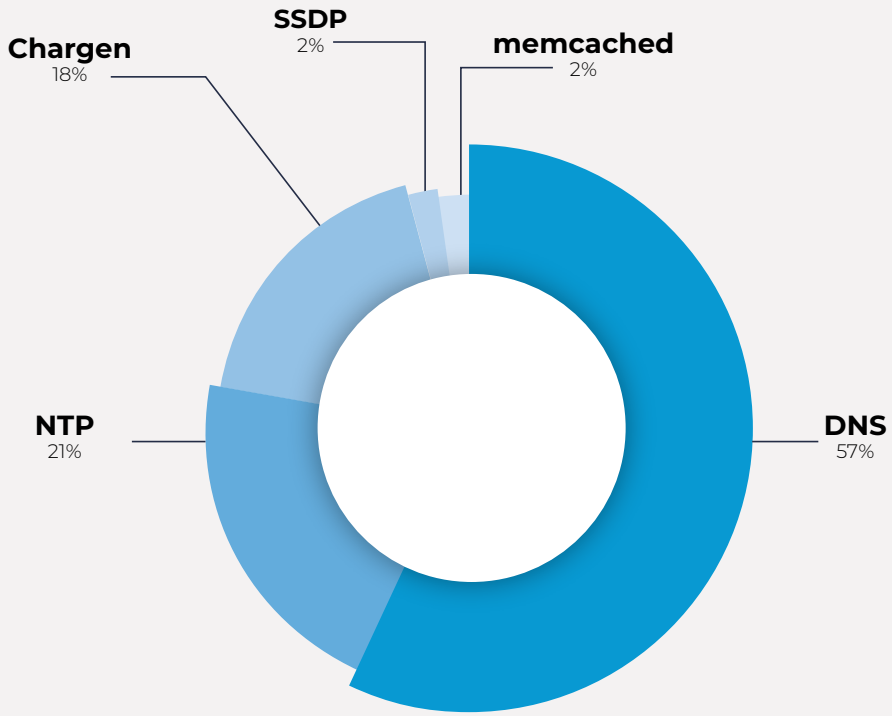
Attacks are based on fundamental internet systems

Reflection amplification attacks are malicious multi-vector attacks that exploit misconfigured servers and services on the Internet. In a reflection attack, the attacker disguises the IP address of the target (also known as spoofing) and sends information requests via services such as DNS or NTP. There are many such Internet services where verification of the sender is not supported or required.

The attackers send small amounts of data to intermediary servers that serve as amplification. These servers are selected so that their responses are many times larger than the original request, thereby increasing the amount of traffic sent. The abused servers then mirror the requests and forward them in their amplified form to the actual target of the attack. Reflection amplification attacks are particularly dangerous as they not only increase the amount of malicious traffic but also disguise the origin of the attack traffic. In 2023, the LSOC recorded a flood of amplification techniques. Many of these attack techniques, such as DNS Reflection Amplification and NTP Reflection Amplification, have been standard equipment for DDoS attackers since 2013. These techniques are characterized by immense amplification; for example, a 100-fold amplification for DNS attacks and up to 200-fold amplification for NTP attacks.

Although attackers are constantly discovering new vulnerabilities, such as inadequately protected Internet services and open services, known and proven vectors were used for almost all attacks

Reflection amplification vectors 2023



during the period under review. The Internet service most frequently exploited for attacks and misused as an amplifier in 2023 was DNS (57%), followed by NTP (21%), and batches (18%). Memcached and SSDP were only used as attack vectors in 2% of attacks each.

DNS and NTP are two fundamental Internet systems that every user needs. DDoS attacks on these two systems are cheap and promising. DNS stands for Domain Name System, a protocol that links domain names with IP addresses. In a DNS amplification attack, the attacker sends manipulated queries to open DNS resolvers, which then generate large responses and overwhelm the target system. The mismatch between the small request and the large response is exploited to increase traffic. The target system is flooded with a massive data stream and access to the server and its infrastructure is blocked. Fake source IP addresses allow the attackers to remain anonymous, and the attacks are comparatively inexpensive to carry out.

”

“There are still many misconfigured servers and services on the Internet that attackers use for reflection amplification attacks. These attacks are not only cheap, but also particularly dangerous, as they disguise the origin of the attack and overload the target systems. It is therefore essential that companies take sensible and effective measures to protect themselves against such DDoS attacks.“

Karsten Desler, CTO, Link11 Group

Web Protection

Bot management: controlling the invisible

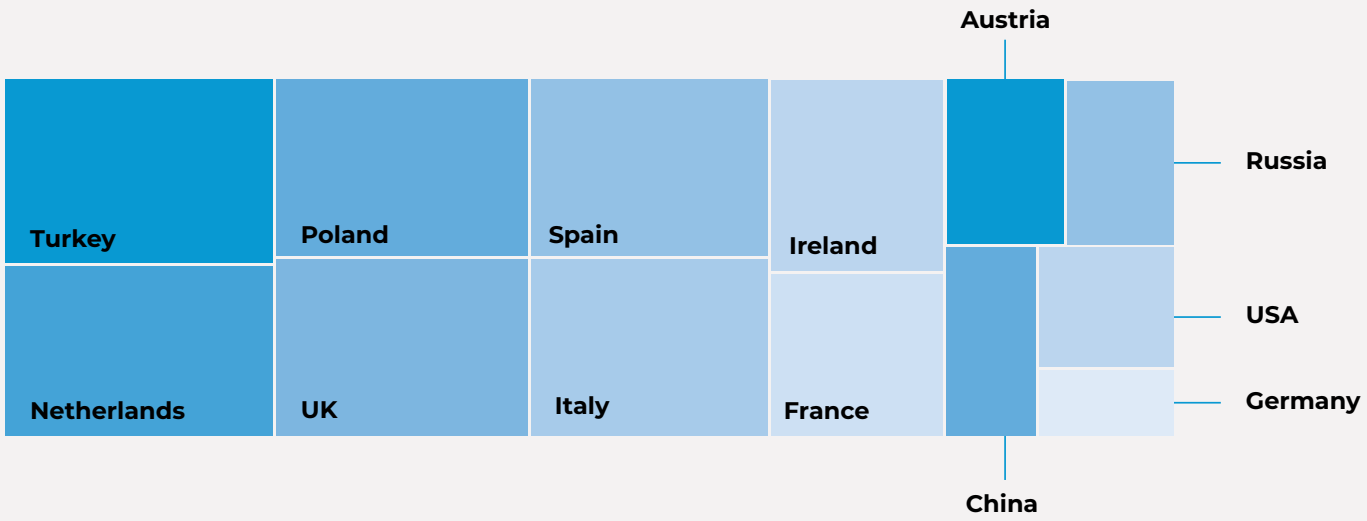
There are good bots, bad bots, and botnets. Although we need some bots for the proper function of major Internet services, the negative impact of the invisible army spreading across the Internet, in many cases, can cause great damage. There are bots that are increasingly being used for automated processes to increase efficiency. These include SEO analysis, link previews, social media interactions, and data scraping for market analysis. These bots play a crucial role in automating tasks and improving various operational processes.

At the same time, bots are also used for fraudulent activities such as spam or credential stuffing. These bad bots are a serious threat to the security of companies, as they can have a damaging impact on websites and online resources. This makes it even more important to protect against these dangers.

In addition, there are also botnets. These are networks of compromised computers or devices that are remotely controlled by attackers without the owners' knowledge. These networks can be used for a variety of malicious purposes, from sending spam to large-scale DDoS attacks. Importantly, they can grow to enormous proportions and remain undetected for a long time. This can not only overload networks but also steal sensitive data and disrupt online services.

According to analysts at Forrester[24], anyone with an Internet connection is now able to launch a bot attack, which are also becoming increasingly sophisticated. Generative AI is helping attackers to improve their bot armies, increasing the need for advanced and effective protection for businesses. Nevertheless, according to the latest U.S. Bot Security Report[25], two out of three U.S. websites surveyed are unprotected against simple bot attacks.

Countries of origin of bad bots



Companies face significant damage each year from bad bot attacks on their digital assets. According to Juniper Research[26], online fraud by bots is expected to increase by 131 percent by 2027. The rapid development of generative AI technologies could even accelerate this further. Companies in all sectors are affected by this trend, as automated attacks pose an increasing threat.

A variety of techniques are now available to recognize human traffic from machine and bot traffic:

- Behavioral analysis: This technique aims to identify patterns in user activity, as humans and bots tend to behave differently. For example, while a human might move their mouse or scroll, a bot would not.
- CAPTCHA: Users must solve tasks that are easy for humans but difficult for bots. This includes recognizing distorted text or images.
- IP reputation: Incoming data traffic is compared with known malicious IP addresses and blocked accordingly.
- Artificial intelligence: Machine learning is used to analyze patterns in data traffic, such as traffic logs, to detect abnormal behavior.

Lisa Froehlich, Company Spokeswoman, in dialog with Eyal Hayardeny, President, Link11 Group

What are the biggest challenges for companies when it comes to bot management?

It is especially difficult to differentiate between good and bad bots. Not all automated data traffic is bad or damaging per se, but at the same time an effective solution is needed to identify malicious bots and mitigate them in a second step. Users should not be affected in any way, but the fact that the volume of bot traffic can overwhelm traditional security measures means new measures are needed to maintain the user experience.

That is indeed a tricky business. Could you explain some of the most common types of bot attacks that companies face?

Organizations may face a variety of bot attacks, each posing different risks. DDoS attacks can lead to extended downtime, scraping and credential stuffing can steal data or take over user accounts completely - the threats are varied and constantly evolving. In the e-commerce sector, hoarding of stock or click fraud in digital advertising can also occur.

There are many different bot attacks; are there any sectors that are particularly affected?

Definitely. The threat scenarios vary from industry to industry. They also reflect the different motivations of cybercriminals. E-commerce websites are at greater risk of stock hoarding, while financial institutions are struggling with the misuse of online forms. Healthcare companies are more concerned with the extraction of patient data, while digital media companies must defend themselves against click fraud.

What are the main motives for bot attacks?

The motives for bot attacks are diverse, ranging from financial motivation to competitive advantage. Threat actors try to sell stolen data, undercut competitors, or disrupt business processes. State-sponsored attackers can also engage in spying and sabotage. These different motives are key to anticipating the potential threats and effectively mitigating bot attacks.

What strategies should companies use to minimize the risks posed by bot attacks?

The unique risk profile of each industry is critical for deploying the appropriate defense strategy. A multi-layered approach is required. In addition to state-of-the-art technologies to detect the malicious bots, the implementation of robust authentication measures such as multi-factor authentication is necessary to reduce the risks. Companies should also regularly update their security protocols to effectively counter new threats and collaborate with security experts. In addition, security awareness should be continuously encouraged among employees.

Sneaker bots: when shoes become prey

In the world of „limited edition“ sneakers, it is often a race against time. Thousands of users wait impatiently on a landing page or in a virtual waiting room to get their hands on one of the highly desired unique pieces. For many, this venture ends in disappointment - without their dream sneaker. This is because other users run a lucrative business: they buy up most of these shoes to resell them on alternative markets. To do this, they rely on „sneaker bots“ that automate the purchase of multiple items.

The business model behind these bots is as simple as it is profitable: the operators have licenses that are offered in limited numbers and generate profits of several thousand dollars per license. The bot operators, in turn, rely on the fact that they can resell the purchased shoes in alternative markets to realize their profits.

The operators of these bots use sophisticated techniques to disguise their identity and circumvent security mechanisms. By using private proxies, their IP addresses remain blocked, while other online services even offer phone numbers for SMS and alternative delivery options to avoid using a single delivery address.

By using such sophisticated mechanisms and APIs, sneaker bots abuse the backend of e-shops to mimic human users, bypass security mechanisms, and ultimately enable this type of fraud.

The legal situation is diffuse in most countries: using an alternative API to purchase items directly instead of through the actual interface is a legal gray area. If the purchased items are paid for, it is difficult to prosecute.

Automated data traffic

Automated data traffic on a website means a consumption of computing resources. Depending on who is requesting the data, this can be both positive and negative: Bots and software from partners and known organizations can be a benefit, while unknown bots are a grey area. In the Link11 network, around 65% of the observed traffic is of automated origin.

Some legitimate models use automated traffic: Indexes and services that use crawlers or services that offer test traffic. On the other hand, there are also illegitimate models based on automated traffic on the Internet. These include fraud methods such as credential stuffing, which is used to validate records of stolen accounts, or account takeover techniques. In addition, there are illegal markets and sniping bots that purchase, for example, limited edition shoes or cryptocurrencies at low prices.

The problem of credential stuffing and fraud is widespread and easy to carry out. Within minutes, data and services that enable fraud can be found on the dark web. To counteract this, it is crucial to differentiate between good and bad bots on our websites. Built-in resilience layers to validate customers not only add value to data storage, but also improve our security position. Preventing customer account intrusions or unwanted takeovers also reduces the likelihood of legal disputes.

Account Takeover: The risk of stolen credentials

The evolution of bot technologies is alarming. Bots used to be simple tools for phishing emails, but today they are highly sophisticated and can mimic human behavior, making them more difficult to detect. Between 2021 and 2022, the proportion of sophisticated bad bots doubled and now dominates global traffic.

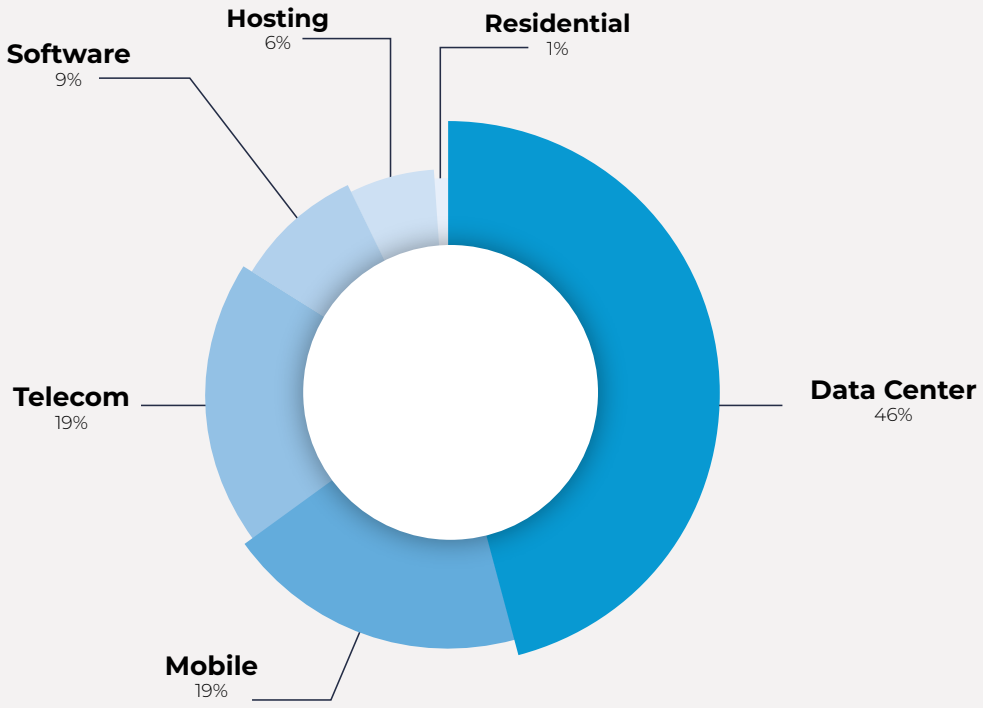
The following graphic shows the origin of the bad bots registered in the Link11 network. Most bots find their way via data centers, with an equal number of bots coming via traditional and mobile telecommunication channels. Software and hosting providers also play a role. These were the expected results, but why do so many bad bots come via mobile data traffic?

There are two explanations:

1. Mobile applications are now one of the main targets for bad bots: every mobile application comes with its own programming interface, or API for short. These are particularly vulnerable. Cybercriminals can attack these APIs in various ways, including reverse engineering or special automation software. This makes it even more important to protect smartphone app APIs.
2. The number of malicious bots originating from cell phones has recently increased[27]. The Android malware known as Badbox and Peachpit has infected thousands of devices. It is installed on devices before it is sent and spreads via low-cost set-top boxes and similar Android devices. It aims to implement fraudulent schemes and infect devices through ad fraud and the installation of malicious code.

In the future, cybercriminals will focus more on attacking API endpoints and mobile applications with sophisticated automation. One such attack is the so-called Account Takeover (ATO). In ATO attacks, hackers attempt to gain access to legitimate online accounts. The number of account takeovers increased by 155%[28] between 2021 and 2022, and successful ATOs can have potentially devastating consequences. Identities are stolen via this route, which the attackers can use to infiltrate the targeted systems. This can lead to data theft, fraud, or other criminal activities.

Sources Bad Bots



Gaining access to fraudulent data and services is scarily easy: a five-minute search on the dark web is all it takes to find dumps or purchase services that even come up with price lists. As a result, some accounts can be directly abused to commit fraud or prepare targeted attacks on organizations. The account takeover is not necessarily carried out by a bot, but often by humans who use the information gathered to take over selected accounts and carry out fraudulent activities.

In the context of criminal activity, „dumps“ refer to data extracted from stolen credit or debit cards. This data usually contains information such as cardholder name, card number, expiration date, and possibly even the security codes. Fraudsters can use this information to carry out fraudulent transactions or take over accounts. Finding and trading dumps is therefore a common practice in the field of cyber fraud.

To protect an organization, a strategy to maintain the confidentiality, integrity and authenticity of information is essential. The following defenses are the three most important when it comes to preventing account takeover attacks:

Multi-factor authentication: Strengthening the security of user accounts

Multi-factor authentication (MFA) is a crucial tool for increasing the security of user accounts. Requiring multiple proofs of user identity significantly reduces the effectiveness of stolen credentials. The combination of different authentication factors provides a robust line of defense against ATO attacks. By using different MFA mechanisms, organizations can further increase the security of their systems.

Phishing prevention: Multi-layered defense

Phishing is a widespread and dangerous form of social engineering designed to trick people into revealing sensitive information. Effective phishing prevention involves several defense measures. These include increasing security awareness and filtering phishing messages. By implementing a robust anti-phishing strategy, organizations can significantly reduce the risk of ATO attacks.

Rate limiting: Technology to prevent ATO

Rate limiting is an important part of the ATO defense strategy. A robust Web Application and API Protection (WAAP) solution monitors the rate at which clients send requests to the protected backend environment. If a particular data source sends too many requests within a defined period, it can be excluded from further access for a specified time. Monitoring and limiting the request rate restricts access by potential attackers. This reduces the effectiveness of ATO attacks.

“It‘s alarmingly simple. With just a few minutes of research on the dark web, fraudsters can easily find data, such as stolen account details or access services, that helps them in their criminal activities. It is therefore important to monitor requests from bots and other automated systems to detect and prevent potential attacks at an early stage. A comprehensive strategy to safeguard the confidentiality, integrity and authenticity of information is essential to minimize the risk of account takeover attacks.“

Mattia Rambelli, Solution Engineer, Link11

Reviewing customer requests on a website and understanding whether the requests are coming from botnets can help prevent incidents. In addition, it is important to monitor requests from bots and other automated systems to detect and prevent potential attacks at an early stage. Ultimately, however, a differentiated approach to the challenges of automated data traffic is crucial to ensure both the security and efficiency of digital platforms.

There are therefore several features to consider when selecting bot management:

AI and machine learning: Modern tools should utilize AI and machine learning to detect new threats and continuously evolve alongside them.

Integration with existing systems: A good tool integrates seamlessly with your IT infrastructure and security tools to avoid security gaps.

Ease of deployment and maintenance: Installation should be simple, and the tool should provide comprehensive protection without requiring constant maintenance.

Flexibility and customizability: It should be possible to adapt the tool to your specific requirements and create custom rules.

Data protection compatibility: Make sure the tool is compatible with applicable data protection frameworks and flexible enough to handle future compliance changes.

Real-time monitoring: The tool should be able to monitor each request in real time to immediately detect and respond to potential threats.

Scalability: It should be scalable with an increase in traffic without impacting the customer experience.

“Bot management is a complex challenge for companies in an increasingly digitalized world. Through a combination of technical security precautions, traffic monitoring and employee education, companies can protect their systems from the impact of malicious bots while reaping the benefits of automated processes.“

Ziv Grinberg, VP Product Management, Link11 Group

WAF: Reliable shield for security on the web

In 2023, there was another alarming increase in reported security vulnerabilities. According to network equipment manufacturer Cisco, the CVE database recorded an increase of almost 29,000 entries in 2023, corresponding to a 15% increase compared to the previous year[29]. Every critical security vulnerability in the form of unpatched software is a potential gateway for cybercriminals. Web applications represent a major security risk. Cybercriminals are using increasingly sophisticated methods to exploit vulnerabilities in such applications and access or manipulate confidential data.

Using a conventional firewall is often not enough to effectively protect web applications. Although they can monitor data traffic and block unauthorized access, they are not able to detect and ward off attacks on the application logic itself. This is where the Web Application Firewall (WAF) comes into play. Around 180,000 weakened WAF events are registered in the Link11 network every day.

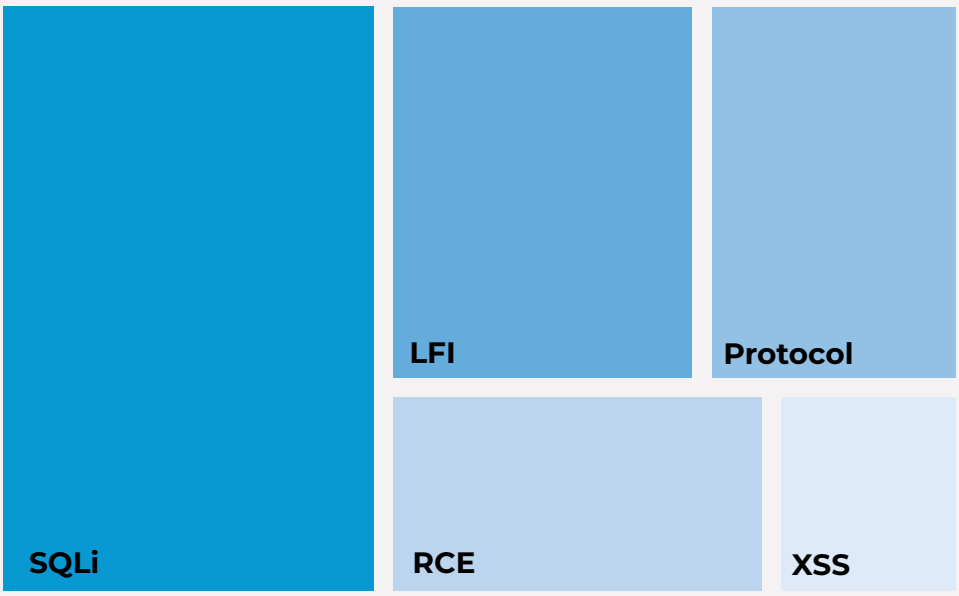
A WAF is designed to check data traffic at the application level and detect suspicious activity before it reaches the web application. For example, it can identify unusual user input that could indicate possible attacks such as SQL injection or cross-site scripting. By analyzing traffic at the HTTP packet level, a WAF can block potentially malicious requests or alert the user.

The use of a WAF is particularly important in areas such as payment transactions, where companies are obligated to adhere to strict security standards. Credit card companies and other payment service providers, for example, require web shop operators to use a WAF to ensure the confidentiality and integrity of their customers‘ payment data.

In addition, active monitoring and regular checks of web applications provide important protection mechanisms against potential threats. By identifying and fixing security vulnerabilities, companies can minimize the risk of data loss, business interruption, and reputational damage.

The top 5 web application attacks recorded on the Link11 network include the following:

Top 5 attacks on web applications



SQL injection (SQLi) is a security vulnerability in which attackers inject malicious SQL code into web applications to manipulate the underlying database. This is possible, for example, if user input is not sufficiently validated. By injecting manipulated SQL commands into input fields or URL parameters, attackers can trigger the execution of unwanted SQL queries. In this way, attackers can modify database queries, access confidential information, or compromise the entire database. By injecting additional SQL commands, data can also be extracted, modified, or deleted, posing significant security risks for the affected application and its users.

The Local File Inclusion (LFI) attack is a web vulnerability that allows an attacker to access files on the server that are not normally intended for public access. These can be password files or source code, for example. An attacker can exploit this vulnerability by manipulating the URL of the website to gain access to such files, allowing the attacker to view or download sensitive information. This can result in serious security issues such as cross-site scripting (XSS) and remote code execution. To prevent such attacks, developers must ensure that the website is programmed correctly, and that no user input can be applied directly to file paths.

Cross-site scripting (XSS) is a type of attack in which attackers inject malicious code into a seemingly trustworthy website. This is possible via web forms as well as URLs and can cause various types of damage. This ranges from compromising the attacked website to stealing user data, such as passwords. There are three types of XSS attacks: reflected, persistent, and DOM-based attacks. With reflected XSS, the attacker sends the code to the server, which then returns it to the victim. With persistent XSS, the code is stored on the server and displayed to all visitors to the site. With DOM-based XSS, the code is executed directly in the victim‘s browser.

Remote Code Execution (RCE) refers to the ability to remotely execute malicious code on a computer or device over a network such as the Internet. This type of attack often results from security vulnerabilities in operating systems, applications, or insecurely designed input screens. Cybercriminals use RCE to gain unauthorized access to systems, infiltrate malware, steal sensitive data or even gain complete control over the affected systems. No physical access to the device is necessary as the attacks are carried out via the Internet.

Protocol attacks include various techniques that are designed to exploit vulnerabilities in communication protocols to compromise web applications or servers. These include:

- **HTTP response splitting:** In this attack, HTTP responses are manipulated so that they are split into several parts. It allows attackers to inject additional content or headers that may be interpreted differently by the server or intermediate instances.
- **HTTP smuggling:** HTTP smuggling attacks exploit differences in the way frontend and backend servers handle and interpret HTTP requests. This allows attackers to bypass security mechanisms and perform potentially malicious actions.
- **HTTP header injection:** Attackers insert unauthorized HTTP headers into requests or responses to manipulate server behavior or exploit vulnerabilities in web applications. This can lead to various security problems such as cross-site scripting (XSS) or remote code execution (RCE).
- **HTTP Parameter Pollution (HPP):** In HPP attacks, attackers manipulate parameters in HTTP requests to confuse or bypass server-side processing logic. This can lead to unexpected behavior such as privilege escalation, information leaks, or denial of service attacks.

“Web application firewalls are crucial in the fight against web application attacks. They provide proactive protection and minimize risks by detecting anomalies and blocking suspicious activity. This ensures the long-term security and integrity of web applications.“

Ziv Grinberg, VP Product Management, Link11 Group

In addition to blocking malicious requests, web application firewalls (WAF) can do much more:

1. **Protect against zero-day attacks:** WAFs use signatures and behavioral analysis to detect web traffic anomalies and block suspicious activity, even without specific signature patterns for known attacks. This defends against zero-day attacks that exploit new vulnerabilities for which patches are not yet available.
2. **Filtering of user input:** WAFs can inspect and validate user input to identify and block potentially malicious code. This can help prevent SQL and command injection attacks by blocking malicious commands or script fragments.
3. **Protection against script attacks:** Some WAFs provide features to detect and block malicious scripts embedded in web pages, such as cross-site scripting (XSS). By filtering script content, WAFs can help prevent the execution of malicious code in users‘ browsers.
4. **Content and file filtering:** WAFs can check the content of incoming files, including uploaded files, to detect and block potentially malicious files. This can prevent attacks in which attackers upload and execute malicious files in order to achieve remote code execution, for example.
5. **Protection against bot attacks:** WAFs can also help ward off bot attacks. They detect anomalies in web traffic, such as automated login attempts, and can identify and block denial of service attacks.

By analyzing traffic at the application level, a WAF enables granular control over access to the web application. This means that companies can set individual security policies to block or allow certain types of requests or user behavior depending on the specific requirements of their application and business.
For a WAF to complement the company‘s own security measures and protect it as effectively as possible, there are a few important points to consider:

1. **Configuration and updating:** To detect new threats and attack patterns, the WAF must be properly configured and regularly updated.
2. **Whitelisting and blacklisting:** Based on IP addresses, URL paths, user agents and other parameters, unwanted traffic can be filtered, and potentially harmful requests blocked.
3. **Input validation:** User input should be checked and validated. This allows potentially harmful input to be detected and blocked at an early stage.
4. **Web Application Security Policies:** By defining clear security policies, applications can be adapted to specific threat models.
5. **Logging and monitoring:** Logging suspicious activities helps to detect anomalies or unusual patterns. Regular monitoring allows potential attacks to be detected at an early stage.
6. **Regular checks and audits:** Regular audits of the WAF configuration can ensure that it meets current best practices and security standards.

Web Performance

CDN: Speed and security for any online presence

Website users expect speed and security. It is precisely in this context that a Content Delivery Network (CDN) can play a decisive role for companies. A CDN helps to shorten website loading times and reduce server load while also increasing security. It works by storing content such as images, videos, and scripts on servers in different geographical regions and then redelivering them based on the user‘s location.

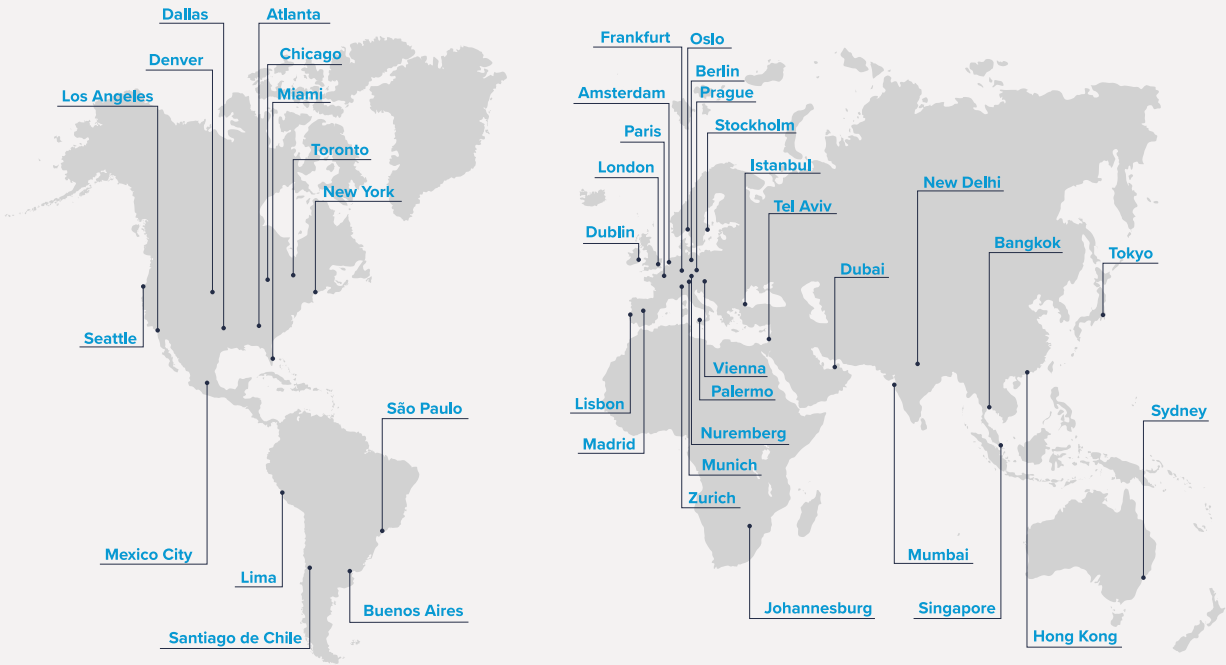
For a company’s online presence, this means that a CDN can reduce latency through shorter loading times and provide a better user experience. In addition, data transmission costs can be reduced through an optimized transmission path. Furthermore, a CDN can reduce the server load of the origin, as more content is delivered from the CDN servers. This means further savings in hardware costs.

However, Link11 not only offers improved performance through its CDN, but also integrates security features that protect companies from threats such as DDoS attacks. The use of layer 3 and layer 4 filter clusters protects CDN nodes from such attacks. The so-called Site Shield function, on the other hand, protects the customer‘s origin from direct attacks. This seamless integration of CDN and security layer ensures continuous availability of the CDN nodes and provides additional protection for the relevant infrastructure.

Compliance and data protection regulations can be crucial aspects of using a CDN. As a European company, Link11 already meets the strict requirements of the GDPR. In addition, the geo-blocking feature allows precise control over which users from which geographical regions can access certain content, making it easier to comply with specific data protection regulations. By combining geo-fencing and geo-blocking, customers can define exactly which CDN nodes should be used for content delivery, ensuring that content is only distributed in selected regions.

Link11 currently offers three different options for processing traffic via the CDN in combination with the WAAP Security Proxy. These range from full page caching and WAAP protection for maximum security to static caching and partial WAAP protection for a balanced combination of performance and security. The choice of configuration depends on the individual requirements and priorities of the company.

Worldwide Link11 network



Lisa Froehlich, Company Spokeswoman, in dialog with Lukas Frank, Product Manager, Link11 Group

Many companies are subject to strict compliance regulations or data protection laws. For this reason, many users do not want to store sensitive data on servers outside the EU. Customers may therefore be interested in selecting CDN nodes accordingly. Does your own choice of CDN nodes entail security or speed losses? If so, what are they?

Choosing your own CDN nodes can have an impact on both the speed and performance of your website. If there are fewer nodes that are accessed from certain regions, this can result in performance losses. Users from more distant regions must access nodes in other regions, which leads to longer loading times. In general, however, even in this scenario, performance should be better with CDN than without. The choice of nodes primarily has an impact on performance and less on security.

Does the use of a CDN automatically reduce the probability of website downtime in the event of a DDoS attack because overloads are avoided?

That is correct. If a CDN is used, the probability of a website outage automatically decreases during a DDoS attack. The CDN can cushion overloads. Some DDoS attacks can be partially mitigated on the CDN nodes, especially using layer 3/4 protection measures. In addition, the website content is already cached. This means that users can continue to access this cached content even if the origin server does not respond due to the attack.

How does load balancing work in a CDN?

Load balancing in a CDN works independently of load balancing, although the two concepts can be combined. Load balancing in a CDN aims to reduce traffic from the origin server infrastructure. By distributing requests to the various CDN nodes and caching content on these nodes, the load on the origin server is significantly reduced.

Are there any GDPR compliance issues by transferring the IP to a replica server? Where is it hosted?

Transferring IP addresses to a replica server in a CDN can theoretically pose problems in terms of GDPR compliance, as IP addresses can be considered personal data. However, in many cases the IP addresses are processed in aggregated or obfuscated form and the data is hosted in Europe to comply with data protection requirements.

To what extent can CDNs be used for dynamic website content, and for which sites or applications is a CDN not suitable?

CDNs are ideal for accelerating and efficiently delivering static website content. CDNs are less suitable for highly dynamic website content, as the caching of content can be problematic. Dynamic content is generated for the respective user and other users could then receive „incorrect“ content. On the one hand, this can be harmless if it is only a matter of an incorrect time zone. On the other hand, it can also be dangerous if, for example, login pages are cached.

Websites with dynamic content can also benefit from a CDN if HTTP headers such as cache control are handled properly.

When does it make sense to migrate from a client-based CDN to a cloud computing model? What are the challenges and benefits involved?

Migrating to a serverless computing model can make sense if a website or application contains a lot of dynamic content and requires improved performance and scalability. The challenges of migration include the complexity of configuration and management as well as a different cost structure.

A Content Delivery Network (CDN) offers numerous advantages for the delivery of web content, but also comes with specific security risks. The most important risks include:

1. **DDoS attacks:** Some CDNs are vulnerable to Distributed Denial-of-Service (DDoS) attacks, where many requests are sent to the CDN simultaneously to overload resources and disrupt services.
2. **Caching of malicious content:** If an attacker manages to inject malicious content into the CDN, it can be distributed over the network. As a result, users may accidentally access dangerous content and be compromised.
3. **SSL/TLS vulnerabilities:** CDNs may have security vulnerabilities in SSL/TLS communication, especially if encryption is not properly implemented or outdated protocols are used.
4. **Data leaks:** Configuration errors or lack of protection of sensitive data can lead to data leaks where confidential information can be intercepted or compromised.
5. **Failure of the CDN provider:** If the CDN provider is affected by a failure or security incident, this can lead to significant disruption for all customers using its services.

In addition, the CDN itself can be misused as part of an attack. In a so-called range amplification attack (range amp for short), specially crafted requests are used to undermine the basic function. Instead of improving performance and reducing the load on web servers, the CDN is turned into an attack amplifier.

The HTTP standard allows HTTP range requests, which allow a client (usually a browser) to request a specific part (byte range) of a file. The intended use is to pause/resume downloads or recover aborted requests.

The implementation of range requests in CDN networks works as expected from the visitor‘s perspective. However, if the CDN does not have the requested resource in its cache, there are various possible actions: Either it will request the entire resource so that it is available for the next visitor from the cache, or it will request the specific range and not bother to cache part of the resource.

Such a range-amp attack is most effective when applied to CDNs that retrieve the entire resource. If the attacker creates precisely tailored requests, the CDN‘s function can be abused and turned into an attack amplifier. These include:

An effective Range amp attack:

1. Targets a large resource available on the CDN.
2. Convinces the CDN that it needs to retrieve a new copy from the vicitm‘s web server.
3. Requests only a small byte range.

If such requests come repeatedly from distributed sources, the CDN will see very little traffic from outside. There are only a few small requests, with correspondingly small responses from many different IP addresses. Instead, there is a significant increase in data traffic at the victim of the attack, i.e., its direct client, which responds to the requests with large files.

The target of the attack is an unusually high number of requests for a large resource by the CDN, which uses up all available resources. There is usually a trusting relationship between the website and its CDN. This means that all traffic to/from the CDN is whitelisted or automatically allowed. This leaves the victim of the attack virtually defenseless. If the CDN is not on such a whitelist, the sudden increase in traffic can lead to the victim accidentally blocking traffic from the CDN temporarily, making large parts of the website unavailable.

Implementing a Content Delivery Network (CDN) offers numerous performance benefits such as improved load time, lower latency, and reduced data transfer costs. CDNs can also increase security and fulfill compliance requirements. To make the most of this, it is advisable to use a reliable CDN provider that offers comprehensive security solutions and ensures compliance with data protection regulations.

Looking forward, the integration of generative AI will play a crucial role in cybersecurity. As AI-driven attack and defense mechanisms become increasingly complex, there is a risk that the gap between the best- and worst-equipped organizations will widen. Organizations worldwide should be aware of these challenges and adapt their security strategies accordingly. By taking a holistic approach that considers both technological innovation and the human dimension of cybersecurity to build a futureproof ecosystem. This will enable organizations to strengthen their cyber resilience and protect themselves effectively against the security threats they may face.

Sources

1 https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/

2 https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2024-press.html

3 https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/

4 https://cybernews.com/news/european-investment-bank-cyberattack-russia/

5 https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/

6 https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement

7 https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/

8 https://www.reuters.com/technology/websites-several-german-airports-down-focus-news-outlet-2023-02-16/

9 https://www.cbc.ca/news/canada/montreal/hydro-quebec-website-cyberattack-1.6808947

10 https://edition.cnn.com/2023/04/21/business/eurocontrol-russia-hackers/index.html

11 https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas

12 https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/

13 DdoS attack on 12 Norway government websites - Cybersecurity Insiders (cybersecurity-insiders.com)

14 Russian hackers crash Italian bank websites, cyber agency says | Reuters

15 Wells Fargo banking services halted by Anonymous Sudan DDoS - Cyber Daily

16 Host of EU summit Spain target of DDoS cyberattacks | Reuters

17 ChatGPT Down As Anonymous Sudan Hackers Claim Responsibility (forbes.com)

18 Several websites of Belgian institutions disrupted yesterday by DDoS attack | Centre for Cyber security Belgium

19 BSI-Chefin: „Die Bedrohungslage ist so groß wie nie“ – Wirtschaft – SZ.de (sueddeutsche.de)

20 Inside the World of NoName057(16): Unmasking the Notorious DDoS Hackers | FalconFeeds

21 https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

22 https://decoded.avast.io/martinchlumecky/bobik/

23 https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/fachberichte/Bericht-Analyse-DDoS-NCSC-DE.pdf.download.pdf/Bericht-Analyse-DDoS-NCSC-DE.pdf

24 https://securityboulevard.com/2024/01/datadome-recognized-in-forrester-landscape-Bot Management-q1-2024-report/

25 https://datadome.co/resources/us-bot-security-report/

26 https://www.juniperresearch.com/research/fintech-payments/fraud-identity/online-payment-fraud-research-report/

27 https://www.zdnet.com/article/newly-discovered-android-malware-has-infected-thousands-of-devices/

28 https://www.security-insider.de/bad-bots-ki-roboter-uebernehmen-internet-a-8620c7f12b55dd1db2e15e55b29a0c66/

29 https://www.heise.de/news/Sicherheitsluecken-Statistik-2023-gab-es-15-Prozent-mehr-CVEs-als-im-Vorjahr-9591523.html

Headquarters

Link11 Group
Lindleystr. 12
60314 Frankfurt
Germany