



DDOS-REPORT

1st half year 2023

Table of Contents

Introduction and Summary	03
DDoS in the News	05
Development of total numbers in the Link11 network	07
Development of Onset	09
The development of attack duration	11
Evolution of attack bandwidths	13
Multi-vector attacks	15
Reflection Amplification Attacks	17
Outlook	19

Introduction and summary

More DDoS attacks: Smarter, more complex, and more intense.

At the beginning of the year, Sadie Creese, professor of cybersecurity at Oxford University, warned of the emerging „cyber storm“ at the World Economic Forum¹ in Davos. Although she couldn't have estimated how severe it would be in January 2023, looking back at the first six months of this year, she was right.

Ransomware, phishing, and distributed denial of service (DDoS) attacks are still among the biggest threats in the digital landscape, according to estimates by national and international authorities such as the German Federal Office for Information Security (BSI), the European Union Agency for Cyber Security (ENISA) and the Federal Bureau of Investigation (FBI). And the trend is upward.

This applies not only to the total number of cyber incidents registered worldwide but also to the complexity of individual attacks and the uncertainty on the part of companies and organizations. Increasingly, cybercriminals are combining different types of attacks. *Ransomware and DDoS attacks, for example, are a devastating combination.*

The so-called „triple extortion“ looks like this: The attackers threaten with a DDoS attack, followed by an overload attack, in the slipstream of which the perpetrators introduce the malware into the system unnoticed or extract data. Following the encryption by the infiltrated ransomware, they either threaten to publish the copied and analyzed data on the Darknet or publish the stolen data directly. The flourishing „cybercrime-as-a-service“ industry further reinforces this trend.

The consequences for companies can be enormous. Stolen or published customer data threatens the company's reputation, and customers lose trust. Such effects extend far beyond purely financial damage.

In addition to the growing „cybercrime-as-a-service“ industry, the rapid growth of smart IoT and cloud technologies is also

playing into criminals' hands. Botnets have become one of the biggest drivers of DDoS attacks. Globally, between 500,000 and 1,000,000 IoT hosts and cloud server instances are active every day. These generate more than 40% of all DDoS traffic². The perpetrators have access to a huge arsenal of botnets they know how to make the most of with increasingly intelligent attacks.

Link11 Security Operations Center (LSOC) also observed this increased activity in the first half of 2023: The number of attacks registered on the Link11 network increased by more than 70% in the first half of 2023. Especially from April to June, there were significantly more DDoS attacks than in Q2 2022.

The ongoing war between Russia and Ukraine has also triggered a further increase in politically motivated DDoS attacks by well-organized attackers. The pro-Russian hacker groups „REvil,“ „Killnet,“ and the new group „Anonymous Sudan,“ which has been operating since the beginning of the year, have even joined forces to form a hacker collective called the „Darknet Parliament,“ to further increase their clout.

The „hacktivists“ have attracted more than just media attention worldwide with their politically motivated DDoS attacks. Among the best-known victims are numerous German states and authorities³, the European Investment Bank⁴, and Microsoft⁵.

Even though no major outages have occurred so far, politically motivated DDoS attacks should not be underestimated. This is because, in contrast to the predominantly financially motivated attacks, ideological motives and, thus also, other objectives are in the foreground.

Critical infrastructures (CRITIS) are particularly at risk. Due to their outstanding importance for the economy and society, they are increasingly *in the crosshairs of cybercriminals*. A successful attack on critical infrastructure can have significant social, economic as well as political consequences.

Not only has the number of DDoS attacks increased significantly during the period under review, but the intensity of the attacks has also risen. High-volume attacks increased significantly in the first six months. Bandwidths measured by LSOC exceeded 200 Gbps every month. The average bandwidth peak was 454 Gbps, and the largest attack was stopped at 795 Gbps. In H1 2022, the largest attack was 574 Gbps in size.

While the intensity of attacks increased in the first half of the year compared to the same period last year, the average duration decreased compared to the first half of 2022. As soon as the intended results cannot be achieved, the DDoS attacks are stopped early.

It appears that attackers are increasingly using artificial intelligence to improve their methods and attack types. At the end of March 2023, Europol, the European Union's law enforcement agency, published its latest report on „ChatGPT,“ titled „The Impact of Large Language Models on Law Enforcement.“ In it, Europol warns of the potentially criminal misuse of artificial intelligence (AI)-based chatbots like ChatGPT.

In addition to the trend toward shorter attacks, DDoS attacks in the first half of 2023 reached critical volume after an average of just 60 seconds, compared with an average of 93 seconds in the same period of 2022.

In contrast, the picture is different for long-lasting attacks. The longest attack in the first half of 2023 was 1,444 minutes long, or 24 hours and 4 minutes. The longest DDoS attack in the first half of 2022 was only 981 minutes or just under 16.5 hours.

As far as multi-vector attacks are concerned, the biggest change is seen in HTTPS attacks. Their share has risen to 30%, indicating a significant increase in Layer 7 attacks. Defending against different attack vectors is a challenge for any protection solution, which can slow down time-to-mitigate (TTM).

Only DDoS solutions that are always up to date with the latest attack methods provide reliable protection. This is the only way they can keep pace with the ever-changing threat landscape. Even a single targeted attack vector can cause major damage if IT security is outdated.

DDoS in the News

January 2023

Hackers attack Danish central bank and financial services company



The websites of the Danish central bank and Bankdata, a company that develops IT solutions for the financial industry, have been hit by DDoS attacks.⁶

January 2023

Russian „hacktivists“ cripple German websites



In response to Berlin's decision to send tanks to Ukraine, Russian hacktivists took several German websites offline on January 25.⁷

January 2023

Russian cyber gang targets U.S. hospitals



In response to Biden's promise to deliver dozens of military tanks to Ukraine, Killnet has targeted at least 14 U.S. health-care facilities.⁸

February 2023

Several German airports hit by DDoS attacks



DDoS attacks hit the websites of seven German airports and were unavailable.⁹

February 2023

Danish hospitals targeted by DDoS attacks



Anonymous Sudan announced it had targeted nine hospitals in Denmark with DDoS attacks, crippling their websites for several hours.¹⁰

February 2023

Tor and I2P networks massively restricted



A wave of DDoS attacks has repeatedly attacked the network since at least July 2022, preventing users from loading pages or accessing services.¹¹

March 2023

Duesseldorf-based arms company Rheinmetall attacked by hackers











Duesseldorf-based arms manufacturer Rheinmetall was largely able to fend off a cyberattack on Tuesday.¹²

March 2023

Pro-Russian hacker group NoName057(16) attacks French parliamentary website



NoName057(16) crippled the French National Assembly website for several hours to send a message to French President Emmanuel Macron.¹³

April 2023 Cyberattack on Canadian electricity provider		<p>A pro-Russian hacker group has claimed responsibility for a cyberattack on Quebec's state-owned electricity utility. As a result, Hydro-Québec's website, app, and info breakdown website for checking power outages went offline.¹⁴</p>
April 2023 European air traffic control: DDoS attack by pro-Russian hackers		<p>European air traffic control has been hit by a DDoS attack for which Pro-Russian hackers are blamed.¹⁵</p>
May 2023 Hacker group „Anonymous Sudan“ demands \$3 million from Scandinavian Airlines		<p>Anonymous Sudan has made a \$3 million ransom demand to Scandinavian Airlines (SAS) to stop DDoS attacks.¹⁶</p>
May 2023 DDoS attacks on Polish news agencies		<p>Several news agencies reported on Twitter that they were affected by DDoS attacks, including the Gazeta Wyborcza daily newspaper and the online news site.¹⁷</p>
May 2023 NoName057 has attacked several Icelandic websites		<p>There have been increased DDoS attacks on Icelandic infrastructure in the run-up to the Council of Europe summit.¹⁸</p>
June 2023 Microsoft Outlook out of service after hacker attacks		<p>Microsoft Outlook was down for thousands of American users on Monday. Anonymous Sudan declared a campaign against U.S. companies and infrastructure.¹⁹</p>
June 2023 Swiss government and federal railroads hit by cyberattacks		<p>A DDoS attack has hit several federal administration websites.²⁰</p>
June 2023 DDoS attack on the European Investment Bank		<p>Pro-Russian hacktivists have attacked European banking institutions, naming the European Investment Bank (EIB) as one of their victims.²¹</p>

Development of total numbers in the Link11 network

Number of DDoS attacks increased significantly

After a decline in DDoS attacks was recorded in the Link11 network for the first time last year, the number of attacks increased significantly again in the first half of 2023. From January to the end of June 2022, the number of DDoS attacks increased by more than 70% compared to the same period last year. The increase in the number overall is also associated with increased daily attacks. Especially in the second quarter, there were significantly more DDoS attacks than in Q2 2022.

The ongoing war between Russia and Ukraine has triggered a further increase in politically motivated DDoS attacks by well-organized attackers. Prominent players include the pro-Russian group Killnet, NoName057(16), and Anonymous Sudan. What they have in common is that *they use DDoS attacks as a preferred means of ideologically motivated cyberattacks*. As geopolitical tensions increase worldwide, the threat of such attacks is growing.

These DDoS attacks target critical infrastructure (CRITIS), public institutions, and political organizations. The pro-Russian hacker groups have already declared cyber war last year²². Their goal is to weaken the population's morale and cause maximum damage, as Microsoft pointed out in the report „Defending Ukraine: Early Lessons from the Cyber War.“²³

Germany, Denmark, Poland, and Switzerland have felt the effects of this statement this year. Barely a month has passed without cyberattacks on NATO countries and their critical infrastructure. As recently as July 2023, the new head of the BSI, Claudia Plattner, warned that the threat level was higher than ever.

In the first half of 2023, DDoS activities in the context of patriotic hacktivism reached a disturbing peak compared to the same period last year. The threat potential of politically motivated

cyberattacks continues to grow, threatening sectors such as energy, finance, and healthcare. These areas are particularly vulnerable to DDoS attacks, which not only cause millions of dollars in financial damage. Still, they can also lead to dangerous supply shortages and even endanger human lives.

It is also noticeable that several pro-Russian hacktivist groups such as Killnet, Anonymous Sudan, or NoName 057(16) are participating in the attacks. New actors like Anonymous Sudan are unpredictable, which could further escalate attacks.

Cybercriminals and state actors use DDoS attacks as an effective means to exert political pressure, sabotage critical systems, or make extortionate ransom demands. Currently, no organization is safe from politically motivated cyberattacks. Websites of Western countries are being targeted.

In the face of these multiple threats, protection against DDoS attacks is critical to maintaining the stability and security of our society. A coordinated and comprehensive defense strategy is needed to strengthen the resilience of our critical infrastructures and deter potential attackers. Read more in the Link11 whitepaper: [Critical infrastructures in the crosshairs](#).

”

„It is obvious that protection against cyber-attacks is an ever-increasing challenge to ensure security in our networked world. This makes it more important to have an effective IT security strategy that relies on automation and speed. In almost every situation in which a DDoS attack can be dangerous, we saw an increase in the first half of the year.“

Jens-Philipp Jung, CEO, Link11



i

Anonymous Sudan - who is behind it?

In January 2023, new attackers appeared on the global stage: Anonymous Sudan. Since then, the hacker group has carried out a series of DDoS attacks against countries, companies, and government institutions worldwide. They have particularly targeted critical infrastructure, including financial institutions, airlines, healthcare facilities, and government websites.

Countries affected in the first half of 2023 included Sweden, Denmark and the Netherlands, Australia, and Israel. The attack on Scandinavian Airlines' (SAS) website and mobile app led to widespread flight disruptions. At Microsoft, DDoS attacks by Anonymous Sudan also caused outages and disruptions to several products and services, such as Teams and Outlook.

There appear to be several links to pro-Russian hacker groups such as Killnet and other cyber criminals. As recently as June 2023, Anonymous Sudan announced it would join forces with Killnet and REvil to carry out a „massive attack“ on European and U.S. financial institutions²⁴. Ultimately, the European Investment Bank was attacked.

Despite the name, Anonymous Sudan has no connection to Sudan or the former Anonymous group active there. Many security

researchers²⁵ agree that Anonymous Sudan is state-sponsored by Russia²⁶. There is some circumstantial evidence to suggest that it is Russian actors posing as Sudanese individuals with Islamist motives. For example, the group originally posted only in Russian or English. As observers began to question the hackers' origins, they began communicating in Arabic. This camouflage allows them to target Western targets under the guise of hacktivism.

Anonymous Sudan uses various tactics in their DDoS attacks, including HTTP(S) flood attacks, cache bypass attempts, and Slow Loris techniques²⁷. Anonymous Sudan's attacks suggest a well-funded and sophisticated operation. The group uses paid proxy servers and cloud infrastructure, distinguishing it from traditional hacktivist groups. Countering their attacks requires robust DDoS mitigation strategies that can account for the use of paid proxy services and effectively combat application-layer attacks.

It remains to be seen how the situation will evolve and which targets Anonymous Sudan will target next. The international community and companies must be vigilant and take appropriate measures to protect their digital infrastructures from such cyberattacks.

Development of Onset

A New Era - Smart Turbo Attacks

DDoS attacks registered on the Link11 network since the first half of 2022 have been measured by how many seconds pass after transmitting the first bytes before 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 no time at all.

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

In the first half of 2023, DDoS attacks reach a critical level after an average of just 60 seconds. Compared to the average of 93 seconds in the same period from January to the end of June 2022, these „turbo attacks“ reach a critical volume much faster.

A look at the distribution of the time it takes for a DDoS attack to reach its peak shows the following results for the first half of 2023: In just under a quarter of attacks (24%), the critical payload was

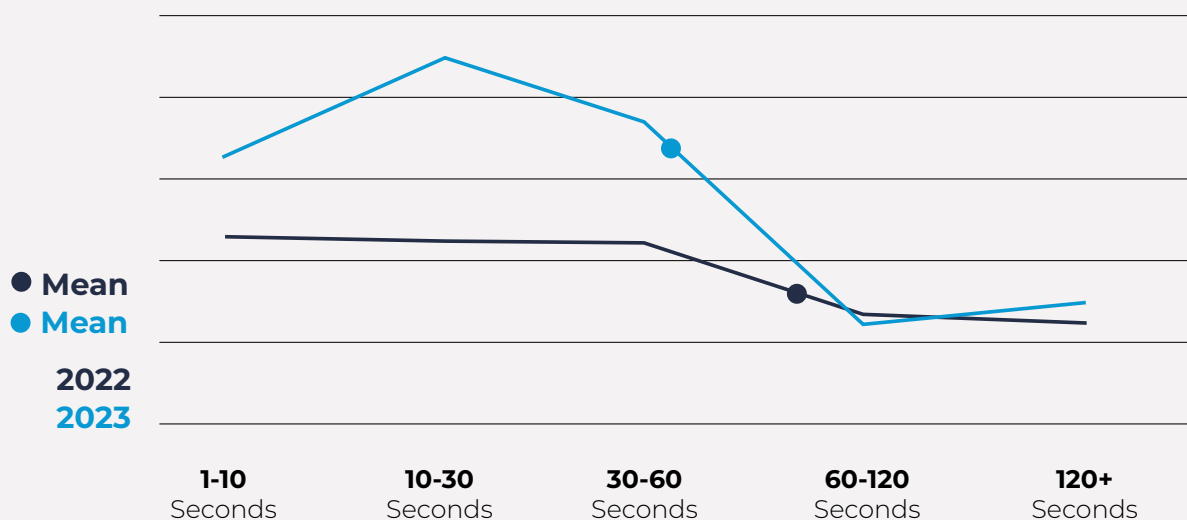
reached within the first ten seconds. In the first half of 2022, this percentage was also 24%.

In the first half of 2023, attacks that reached their maximum value in ten to 30 seconds accounted for about a third of all attacks registered in the network (32%). This compares to a quarter of attacks (24%) approaching their peak at the same time in the same period in 2022.

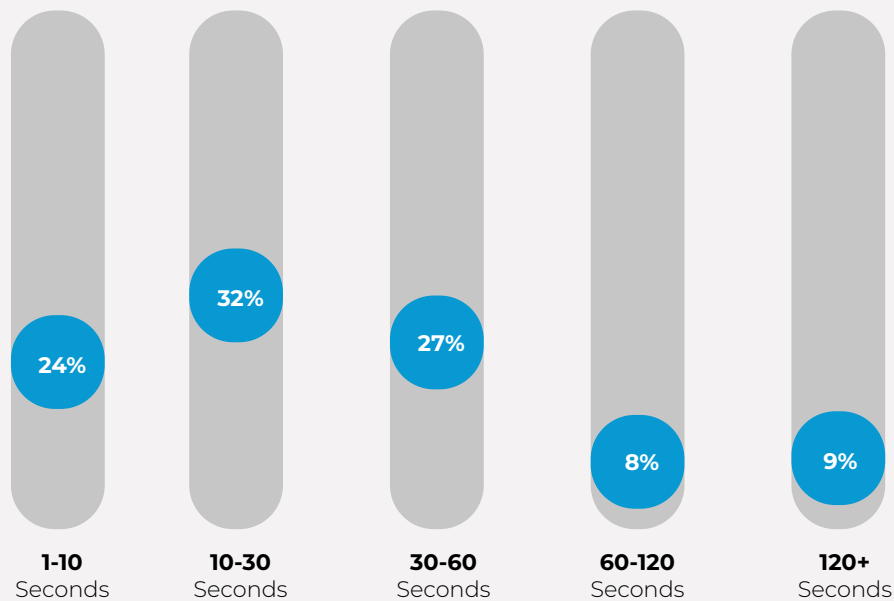
In just under a third (27%) of cases, it took between 30 and 60 seconds for DDoS attacks in the first half of 2023 to reach the critical maximum value. This figure was less than a quarter (24%) in the same period last year.

For attacks lasting more than one minute, the proportion was 8%, and only around one in ten attacks (9%) of the DDoS attacks recorded by LSOC took more than two minutes to reach the critical level. In the first half of 2022, 15% of attacks peaked in one to two minutes, and 13% of cases took more than two minutes.

Duration until peak of an attack | 1st half of 2023 vs. 1st half of 2022



Distribution of the duration until the peak of the attack



In the event of an attack, it is critical to avoid wasting valuable time manually assessing incidents or reactively switching traffic and routing changes. Additionally, unexpected routing issues or more complex attack methods can cause further delays in defenses that can cause significant damage.

To effectively protect the network, traffic should be analyzed in real-time using smart, fast, and secure methods to provide maximum visibility across all network traffic. With an effective IT security strategy, arguably, the most effective way to defend against DDoS attacks is through a mix of basic protection and intelligent and automated AI technology.



”

„Onset is a measure of how quickly an attack reaches its critical volume. Initiating DDoS attacks across thousands of systems requires good coordination and organization. As a result, attacks typically have a ramp-up time before they reach their full potential. The faster the critical payload is reached, the more professional and coordinated the attack was. For potential attack targets, the onset is an indication of how much time they have to mobilize their defenses.“

Jag Bains, Vice President of Solution Engineering at Link11

The development of attack duration

Attack efficiency due to intelligent DDoS attacks

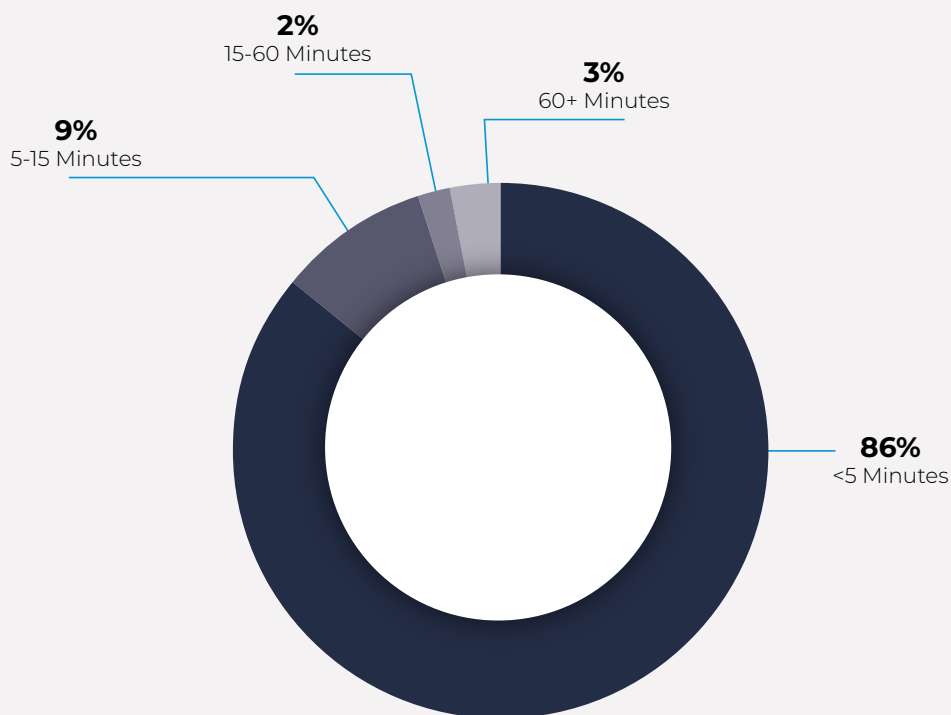
The duration of DDoS attacks registered in the Link11 network in the first half of 2023 shows different developments compared to the same period of the previous year. The trend toward shorter attacks was already evident in the prior-year period. The average attack time has decreased further compared to the first half of 2022. This can be attributed to many attacks being aborted in the first two minutes.

It stands to reason that attackers use increasingly smart attack methods and abort an attack early on if the intended results are not achieved. Moreover, if the attacks bounce off well-protected infrastructures, the attackers usually retreat to conserve their resources and deploy them elsewhere if necessary. But when they are concerned with permanently affecting targets and successfully causing damage, they resort to long-lasting attacks.

When it comes to long-lasting DDoS attacks, it is evident that the longest attacks in each case differ significantly. The longest attack in the first half of 2023 was 1,444 minutes long, corresponding to 24 hours and 4 minutes. The longest DDoS attack in the first half of 2022 was only 981 minutes or just under 16.5 hours.

Further analysis shows that the length of attacks varied from a few minutes to several hours. Most attacks (86%) lasted less than 5 minutes. One-tenth of all registered attacks (9%) were between 5 and 15 minutes long, and only two percent were between 15 and 60 minutes long. Only around 3% of attacks were longer than 60 minutes.

Attack duration 1st half of 2023



The distribution of attack duration shows how versatile the attack landscape is—the tactics attackers choose to vary depending on the attack technique and objective. On the one hand, they rely on „lightning attacks,“ which scan individual IP addresses of their target's IT infrastructure for vulnerabilities at very high speed.

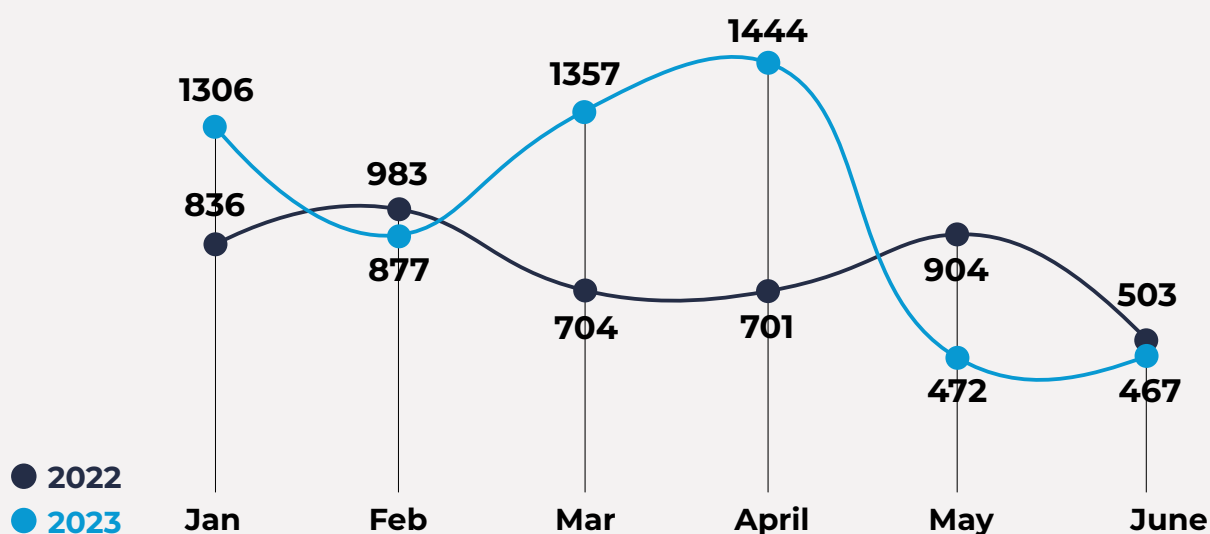
On the other hand, they use small but high-frequency DDoS attacks as camouflage while targeting servers and networks in parallel. Hidden in this background noise, cybercriminals can enter the system unnoticed through the backdoor.

Another option for a shorter duration can be smarter attacks. Most attacks that can rotate vectors within the attack have some detec-

tion capability. That is, they can determine if one or more vectors are successful. Consequently, the attack is aborted when it can no longer reach the target with any available vectors.

To successfully defend against a DDoS attack, existing IT resources must be mobilized in the shortest possible time. Responding quickly to the attack minimizes system downtime and further damage. With unpredictable attacks, attackers cause chaos and overwhelm many security systems. Effective defense, therefore, requires maximum precision and speed to protect the IT infrastructure efficiently.

Attack duration in minutes | 1st half of 2023 vs. 1st half of 2022



Evolution of attack bandwidths

Intensity of attacks on the rise

In the first half of 2023, high-volume attacks increased significantly. In the past six months, the average bandwidth peak was 454 Gbps, while in the first half of 2022, the bandwidth peak averaged 325 Gbps. Bandwidths measured by LSOC exceeded 200 Gbps every month. The intensity of DDoS attacks continued to increase during the period under review compared to the same period in the previous year. The largest attack was stopped at 795 Gbps.

The increase in attack volume is particularly due to the proliferation of IoT devices and cybercriminals' access to more unsecured computing power and capacity in hosting and public clouds. Between 500,000 and 1,000,000 globally distributed IoT hosts or cloud server instances are active every day. This generates more than 40% of all DDoS traffic²⁸.

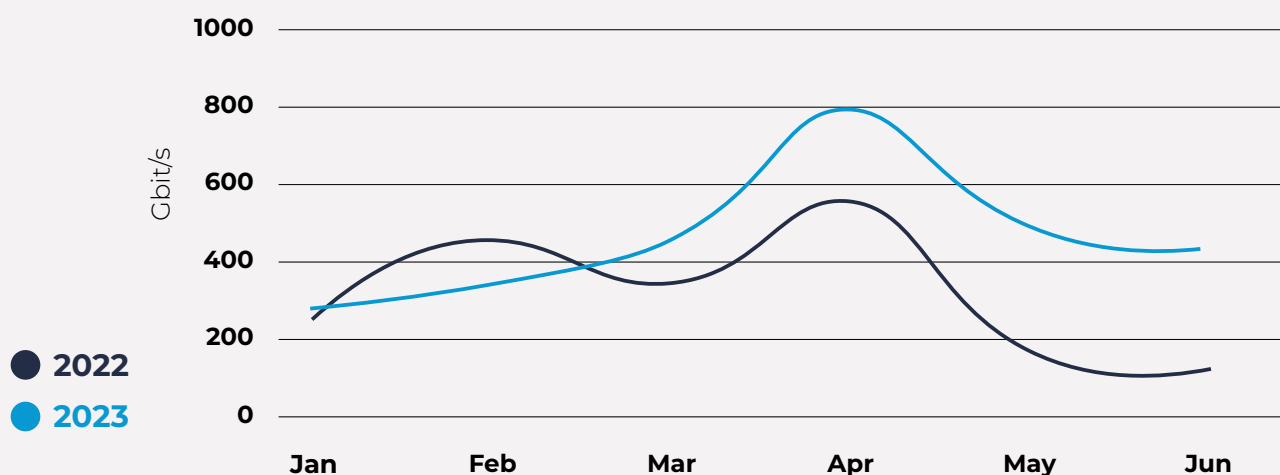
As recently as February 2023, security researchers discovered a new variant of the Mirai malware.²⁹ The malware, named „V3G4,“

particularly targets Linux-based servers and IoT devices. The malware developers are said to sell DDoS services to cybercriminals so that websites and online services can be attacked via this botnet.

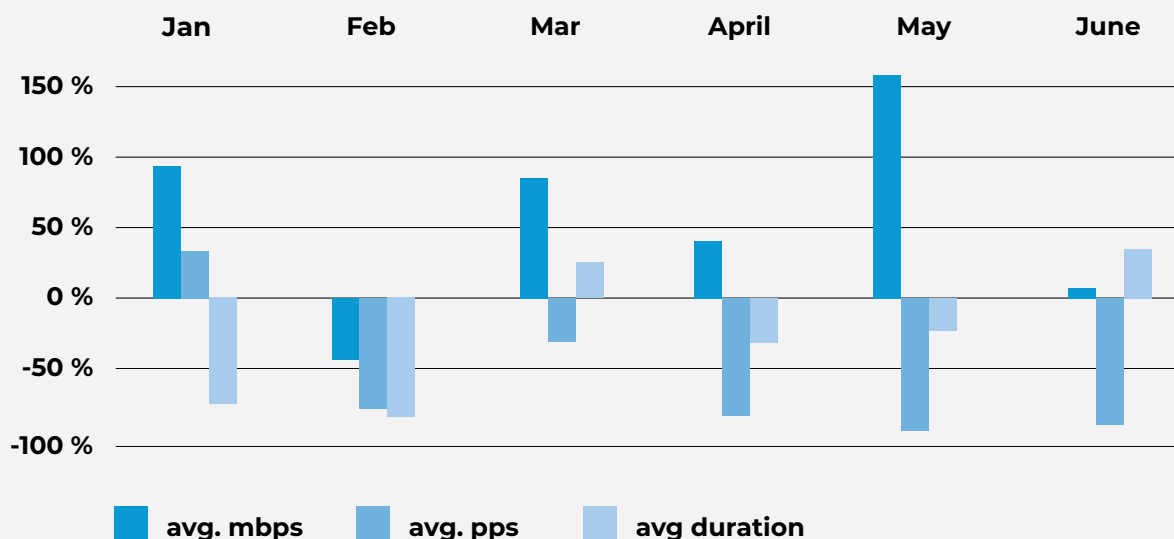
In the first half of the year, with more than 168 million packets per second, the largest packet rate recorded so far was observed in the Link11 network. The average packet rate in the period under review was 413,000 packets per second, and the average number in the first half of 2022 was significantly higher. An average of 1.4 million packets per second were transmitted in the attack case.

If we look at the correlation between the duration and intensity of DDoS attacks, the following can currently be seen: the LSOC detected longer and shorter attacks of all intensities. The average duration has decreased overall, but at the same time, the total volume of attacks has increased significantly.

Bandwidth peak per month | 1st half of 2023 vs. 1st half of 2022



Change in duration and intensity of attacks 1st half 2023



Many attacks are designed to have a dangerous payload without being detected by traditional protection measures. A „Layer 7 slow post-attack,“ for example, can completely consume a Web server’s resources by sending in many requests at 1 byte per minute each, the sum of which is far below typical attack thresholds.

SLOW POST ATTACKS

A finite number of destination ports can be used on a server, and the slow post-attack seeks to occupy all available ports with minimal bandwidth. The slow post-attack opens many connections to a web server, and each starts submitting a POST request (POST is an HTTP method like GET) but decreases the transmission rate to the bare minimum to keep the port in use. Effectively consuming all the available ports so there are none free to listen to legitimate requests.

Similarly, „carpet bombing“ attacks distribute their bandwidth to every IP in a network block. As a result, no single IP has a suspicious amount of traffic. Instead of targeting a single IP address, attackers spread the attack across several IPs within the same network with hundreds or thousands of addresses, which is nearly impossible for inadequately protected hosting and cloud pro-

viders to mitigate. Often, protection solutions do not detect this traffic as an anomaly. Instead, detecting these attacks requires smarter detection methods than traditional thresholding.

As DDoS attacks become more concentrated, targeted, and sophisticated, precision and speed in detection and mitigation become more critical. Protection solutions reach their limits, especially for fast-occurring and intense attacks with high bandwidth and packet rates. On-premises solutions can defend against simple and uncoordinated attacks, but on-premises devices can be overwhelmed by more complex and particularly intense attacks.

This means that time is of the essence when dealing with DDoS attacks. Modern on-premises systems often use hybrid cloud solutions that can redirect traffic once it reaches a critical level. Under laboratory conditions, this redirection occurs within 10 to 90 seconds, but laboratory conditions are usually not a given under the actual bombardment of a DDoS attack.

What matters is how much time elapses before the initial response to the attack and the start of mitigation, known as time-to-mitigate (TTM), and how long it takes to restore to the original state, known as mean-time-to-repair (MTTR). For how Link11 and other competitors are positioned on this critical factor, see Frost & Sullivan’s study, [„The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough.“](#)

”

„Time is critical in the event of an attack - every second counts with manual assessments, routing issues, and outwitted defenses. A fast TTM is essential for an effective defense strategy. A hybrid system can be used here - but only if it is regularly checked and always up to date.“

Jag Bains, Vice President of Solution Engineering at Link11



Multi-vector attacks

Multi-vector attacks with rotating attack vectors increased

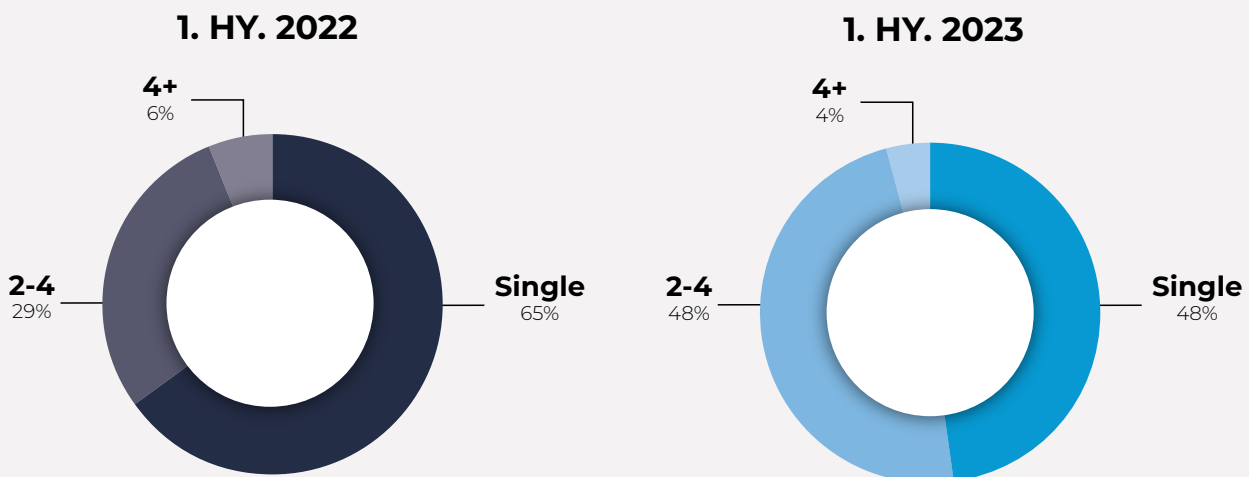
Multi-vector attacks are a particularly dangerous type of DDoS attack. Unlike traditional attacks that use only one attack vector, multi-vector attacks simultaneously target multiple transport, application, and protocol vulnerabilities. A larger number of vectors makes it more difficult for defense systems to detect and defend against attacks.

The combination of multiple techniques increases the likelihood of success for attackers, as many protection solutions are not up to date. Attackers launch their attacks with multiple vectors in the

hope that at least one of the vectors will get through. The more vectors are used, the greater the probability that one or more attacks will break through the protective measures.

Currently, more and more DDoS attacks are using different attack vectors within a very short time. These can successfully cripple the IT system or an online service due to misidentification or a gap in security measures. It is, therefore, important to use DDoS protection solutions that work effectively against multi-vector attacks at all filtering levels.

Number of single- and multi-vector attacks | 1st half 2023 vs. 1st half 2022

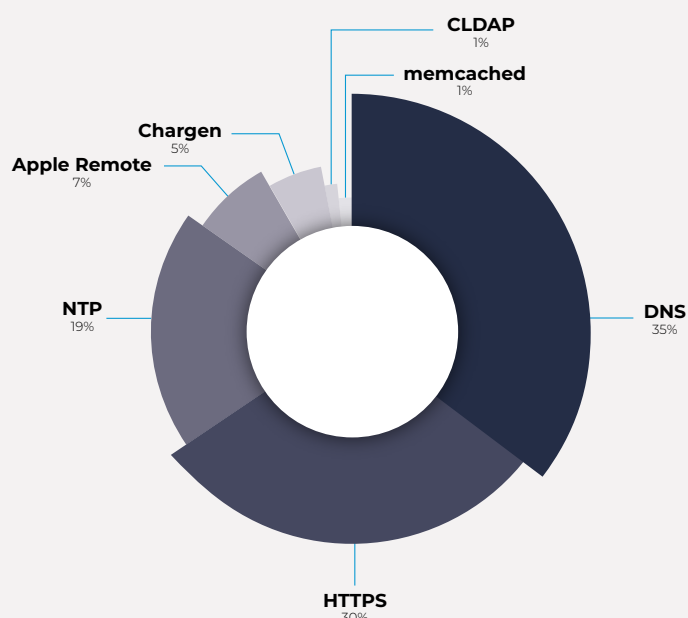


In the first six months of 2023, the proportion of multi-vector attacks increased year-on-year. While multi-vector attacks accounted for 52% of attacks in the first six months of 2023, only about one-third of attacks (35%) in the first half of 2022 were multi-dimensional. Instead of such multi-dimensional attacks involving multiple attacks running simultaneously, attackers preferred more resource-efficient attacks in the same period last year.

After the largest multi-vector attack observed in Link11's network to date last year (18 vectors), the number of simultaneously deployed vectors in the current period under review was only 11. However, the attacks are characterized by becoming more complex. This means the attackers rotate the attack vectors in the shortest possible time to inflict the greatest possible damage.

The biggest change in terms of attack volume is seen in HTTPS attacks (30%). This reveals a significant increase in Layer 7 attacks. In more than a third (35%) of the multi-vector attacks, DNS was used as the vector, and in around a quarter (19%), the attackers used NTP.

Attack vectors 1st half of 2023



Identifying each vector becomes more difficult with each new attack vector added in a complex multi-vector attack. One could say that in malicious traffic, a lot of additional „noise“ is added with each vector. This noise makes it more difficult to identify the multi-vector attacks. This is because it is much easier to understand a message when 1,000 people say the same thing than when they make 1,000 different statements.

It is the same with vectors: Add more and more vectors, and it becomes harder to identify each attack from the mass. In addition, more of these attacks reach their target either because they were misidentified or the protection solution does not provide defenses for that one vector. The more attacks there are, the more complicated it is to defend against them. Conversely, this means that they are more successful.



”

„A specialized DDoS protection solution that ensures continuous monitoring and can detect and defend against attacks in real-time protects against the dangers of multi-vector attacks. This also reduces the risk of prolonged downtime and potential consequential damage.“

Jag Bains, Vice President of Solution Engineering at Link11

Reflection Amplification Attacks

Oldie but Goldie - Memcached and Chargen Popular Amplifiers

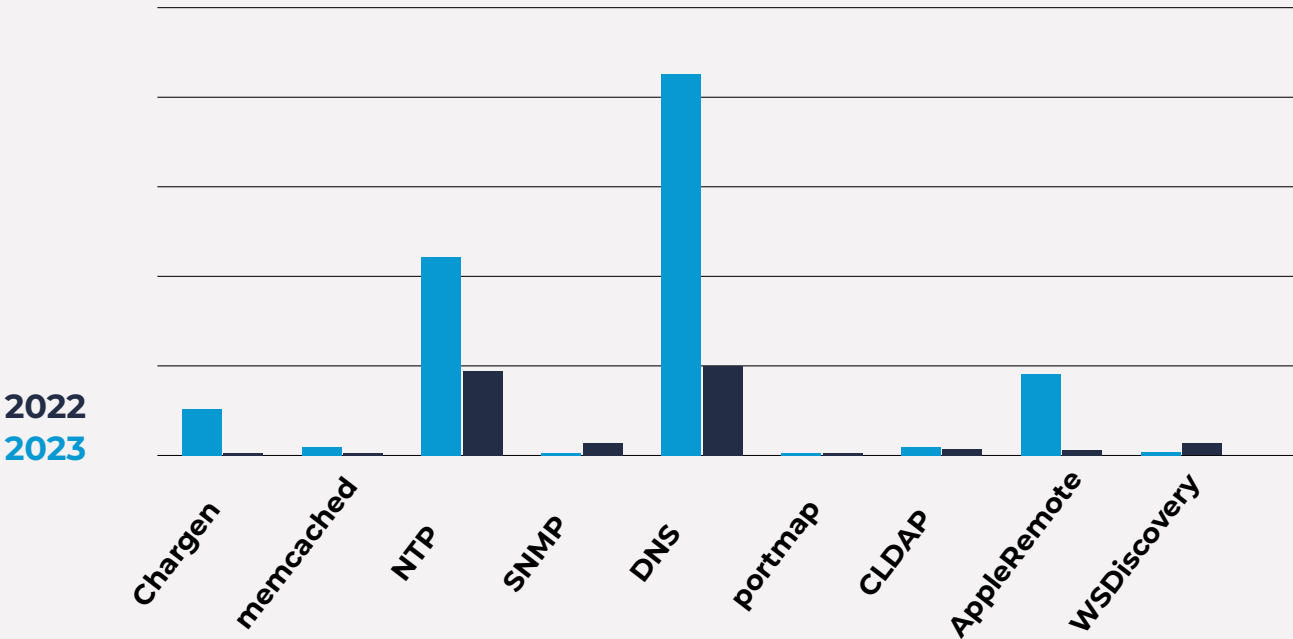
Reflection amplification attacks are a class of multi-vector attacks that similarly exploit various misconfigured open servers and services on the Internet. Instead of attacking the target directly, the attackers abuse services such as DNS or NTP. For many such Internet services, sender verification is not supported or not required. By forging the sender (also known as spoofing), the attacker makes these services send unsolicited responses to the real attack target (reflection).

Small amounts of data are first sent to intermediate servers that serve as amplifiers to increase the attack's clout. As a rule, attackers select services whose responses are many times larger than the original request. This greatly increases the amount of traffic sent. The abused servers repeatedly mirror the requests and forward them, amplified (amplified), to the actual attack target.

From January to the end of June 2023, LSOC has registered more than a dozen amplification techniques. Many attack techniques, such as DNS and NTP, have been standard equipment for DDoS attackers since 2013. These techniques feature immense amplification, for example, 100x amplification for DNS attacks and up to 200x amplification for NTP attacks.

Although attackers are discovering new vulnerabilities, such as inadequately protected Internet and open services, most attacks during the period under review used already known and proven vectors. DNS was the Internet service most frequently exploited for attacks and abused as an amplifier in the first half of 2023. NTP, Apple Remote, Chargen, and Memcached followed it.

Reflection amplification vectors | 1st half 2023 vs. 1st half 2022



Memcached continues to be the largest amplifier that has regained popularity during the period under review. With the help of Memcached, attackers can generate a 750-kilobyte response with a 15-byte request. This equates to a gain factor of over 50,000. Memcached is a database caching system that stores and quickly retrieves arbitrarily small amounts of data.

The attackers first create a data payload in an available Memcached server. Then they send an HTTP GET request to the Memcached server. In doing so, they impersonate the victim (spoofing). In the next step, the server responds to the request and sends a large amount of data to the IP address of the real victim. With the usually very large amount of data, the server in the data center of the affected company is overloaded and no longer accessible for legitimate users.

Besides Memcached, another very old reflection amplification attack has gained popularity: The batch protocol, also known as

Character Generator Protocol. Defined since 1983, the network service has been exploited for increased DDoS attacks for several years, as it is still used by default on Internet-enabled printers or copiers. The batch protocol can be accessed via both the TCP and UDP protocols.

The most common form of these attacks uses Chargen as an amplifier for UDP-based attacks with IP spoofing. The process is simple: the attacker mobilizes its botnet to send tens of thousands of batch requests to publicly accessible systems offering the service. The requests use the UDP protocol, and the bots use the IP address of the actual destination as the sender IP. As a result, the batch service responses are sent directly to the attack target instead of the attacker. The target tries to process the queries. However, the enormous amount of data overwhelms the target, bringing the servers to their knees.

Well-functioning DDoS protection solutions are essential for businesses as the attacks become more sophisticated. To stay on top of the latest threats, businesses must regularly update their protection measures. Effective protection enables them to respond quickly, detect, and mitigate attacks within the shortest possible time.



”

„Attackers are using both old familiar and new vulnerabilities to launch DDoS attacks. Although the potential for abuse has been known for so long, the vulnerabilities are often inadequately patched. Meanwhile, no UDP service is safe from abuse, as attackers are constantly looking for new ports and protocols to overload IT infrastructures.“

Jag Bains, Vice President of Solution Engineering at Link11

Artificial intelligence - chance for cybersecurity, leverage for cybercrime

At the end of March 2023, Europol, the European Union's law enforcement agency, published its latest report on ChatGPT, entitled „The Impact of Large Language Models on Law Enforcement.“³⁰ In it, Europol warns of the potentially criminal misuse of artificial intelligence-based text robots such as ChatGPT.

ChatGPT is a chatbot developed by OpenAI based on the Generative Pre-trained Transformer-series or GPT large language models. *The „Large Language Model“ ChatGPT* can write text, generate music, and generate code. Since its launch in November 2022, the technology has attracted a lot of attention due to its impressive capabilities.

As Europol also points out, this technology can therefore be used for fraud, misinformation, and cybercrime. Authentic-sounding texts can fool people - the criminal variant WormGPT is already capable of generating deceptively genuine phishing emails³¹. Also, the FBI emphasized the growing threat of cyberattacks fuelled by artificial intelligence (AI) programs.³²

Even though attackers are increasingly using artificial intelligence to improve their methods and attack types. ChatGPT has unlocked a new level. Because while generative AI can make life much easier for many of us, it unfortunately also makes the job of cybercriminals easier. With the help of ChatGPT, even inexperienced attackers can launch more sophisticated attacks, such as phishing campaigns, or write malware and hide it in an Excel spreadsheet.

For the World Economic Forum³³, the following attack techniques are among the biggest risks:

- Developing better malware
- Personalized phishing emails
- Generating deep fakes
- Bypassing passwords and captchas
- Deceiving AI-based security systems

The race between attackers and defenders is heating up. Artificial intelligence may not yet completely replace malicious hackers, but at the same time, it speeds up their work³⁴. AI is especially good at pattern recognition and correlating large amounts of data.

At the same time, defenders can use AI to identify threats faster and protect organizations better and more effectively than ever before. Intelligent and robust DDoS protection solutions like Link11's AI-powered, cloud-based solution can help defenders stay ahead in this race.

Link11 DDoS protection has a proven advantage over modern attacks thanks to the machine learning it employs. The Link11 system can learn from thousands of attacks each year. As the number of offensive AI-based attack systems grows, this training data will multiply accordingly. This makes the protection solution not only smarter and faster but also demonstrably more secure.

EU-US data protection framework principles - Does this hold legal certainty?

On July 10, 2023, Ursula von der Leyen, President of the European Commission, announced the entry into force of the [Trans-Atlantic Data Privacy Framework \(TADPF\)](#), also known as „Privacy Shield 2.0,“ aiming to ensure secure data transfers between the EU and the USA. The new agreement addresses concerns the European Court of Justice (ECJ) raised, invalidating the previous „Privacy Shield“ agreement in 2020.

The TADPF limits surveillance possibilities by providing a redress procedure for EU citizens. An independent data protection tribunal will handle complaints and impose remedies. US intelligence agencies are required to implement oversight measures to comply with the new privacy and civil liberties standards.

The EU Commission's recent adequacy decision in July has relieved many companies relying on data transfers to U.S. entities certified under the EU-US Data Privacy Framework. The decision provides a reliable legal basis, easing data transfers to these certified companies without additional requirements.

However, doubts loom over the long-term sustainability of this legal certainty. The new regulation has sparked significant opposition within relevant circles, with prominent data protectionist Max Schrems, chairing the non-profit organization nyob, already hinting at possible challenges at the ECJ, marking a potential Schrems-III.

The U.S. administration claims to have made unprecedented commitments to strengthen privacy and civil liberties protections under the EU-US Data Privacy Framework. Yet, the crucial challenge lies in convincing the ECJ that the requirements outlined in the Schrems II decision regarding U.S. surveillance and spying activities have now been effectively implemented.

We would be pleased to advise you on all matters relating to a legally compliant cybersecurity strategy.

- ¹ <https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/>
- ² <https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/>
- 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.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/>
- ⁷ <https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/>
- ⁸ <https://cybernews.com/cyber-war/russian-killnet-targets-us-hospitals/>
- ⁹ <https://www.reuters.com/technology/websites-several-german-airports-down-focus-news-outlet-2023-02-16//>
- ¹⁰ <https://www.scmagazine.com/news/threats/danish-hospitals-latest-target-of-ddos-attacks-on-nato-backed-countries>
- ¹¹ <https://www.bleepingcomputer.com/news/security/tor-and-i2p-networks-hit-by-wave-of-ongoing-ddos-attacks/>
- ¹² <https://www.privacyaffairs.com/rheinmetall-ddos-attack/>
- ¹³ <https://cybernews.com/news/kremlin-hackers-strike-french-parliament/>
- ¹⁴ <https://www.cbc.ca/news/canada/montreal/hydro-quebec-website-cyberattack-1.6808947>
- ¹⁵ <https://edition.cnn.com/2023/04/21/business/eurocontrol-russia-hackers/index.html>
- ¹⁶ <https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas>
- ¹⁷ <https://cybernews.com/cyber-war/russian-hackers-hit-polish-news-sites-ddos-attack/>
- ¹⁸ <https://www.euractiv.com/section/politics/news/heightened-cyber-attacks-threat-before-council-of-europe-summit-in-reykjavik/>
- ¹⁹ <https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/>
- ²⁰ <https://www.swissinfo.ch/eng/politics/swiss-government-and-federal-railways-hit-by-cyberattacks/48583086>
- ²¹ <https://cybernews.com/news/european-investment-bank-cyberattack-russia/>
- ²² <https://www.emcrc.co.uk/post/killnet-declare-war-on-the-uk-and-nine-other-nations>
- ²³ <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>
- ²⁴ <https://www.darkreading.com/risk/killnet-threatens-imminent-swift-world-banking-attacks>
- ²⁵ <https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf>
- ²⁶ <https://www.bloomberg.com/news/articles/2023-06-28/anonymous-sudan-does-group-behind-microsoft-cyberattack-have-ties-to-russia>
- ²⁷ <https://cybernews.com/editorial/anonymous-sudan-explained/>
- ²⁸ <https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/>
- ²⁹ <https://unit42.paloaltonetworks.com/mirai-variant-v3g4/>
- ³⁰ <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement>
- ³¹ <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/>
- ³² <https://www.fbi.gov/news/speeches/director-wray-s-remarks-to-the-atlanta-commerce-and-press-clubs>
- ³³ <https://www.weforum.org/agenda/2023/01/davos23-generativeai-technology-artificial-intelligence/>
- ³⁴ <https://www.bugcrowd.com/blog/inside-the-mind-of-a-hacker-2023-edition/>



Contact

Link11 GmbH
Lindleystr. 12
60314 Frankfurt