LINK11

EUROPEAN CYBER REPORT

2026 Mid Year

www.link11.com

Dear Readers,

Cybersecurity is no longer a niche topic for the IT department; it is a matter of corporate leadership. The current “Allianz Risk Barometer” 2026 confirms this. For the fifth consecutive year, cyber incidents top the list of the world’s most significant business risks, holding a clear lead over second place since the survey began. Anyone who still treats cyber risk as a peripheral issue is overlooking just how much the threat landscape has changed in recent years.

A key driver of this shift is artificial intelligence. AI is changing the playing field for both attackers and defenders. According to the World Economic Forum’s “Global Cybersecurity Outlook 2026,” 94% of security leaders surveyed worldwide expect AI to be the most significant factor influencing cybersecurity this year.

AI lowers the barrier to entry for attackers, speeds up the development of new malware, and enables more precise control over attacks. At the same time, AI provides defenders with new ways to detect threats faster and respond automatically. Ultimately, which side comes out ahead depends on how quickly companies adopt this technology.

This report examines where this development currently stands and what lies behind it. It shows where the threat landscape has intensified specifically, what is driving these changes, and what conclusions companies can draw for their own resilience.

I hope you enjoy the read!

Regards
Jens-Philipp Jung, CEO, Link11



Contents

Executive Summary 04

Network DDoS Protection 06

Bots, Botnets, and the Practice of Modern WAAP Defense 12

Web Application & API Protection 14

Conclusion 19

Executive Summary

The threat landscape continues to intensify across industries. According to the latest Allianz Risk Barometer[1], cyber incidents are once again the most significant business risk worldwide. With 42% of the responses, this risk clearly surpasses the second-place risk, "Artificial Intelligence," which received 32% of the responses.

German companies are also under growing pressure to act. According to PwC's "Global Digital Trust Insights 2026"[2], 92% of German companies recognize the need to adapt their cybersecurity strategy within the next year, primarily due to mounting financial consequences. More than a third (37%) of German companies surveyed reported that the cost of their most severe data incident in the past three years exceeded one million US dollars, which is significantly higher than the global average of 27%.

Within this threat landscape, DDoS attacks stand out: in the first half of 2026, individual attacks on the Link11 network reached record levels in terms of bandwidth, packet rate, and data volume. This means that the force of attacks has developed dramatically. At the same time, the number of registered attacks decreased by 42%. This apparent contradiction can be explained by two parallel developments.

"Superbotnets" and compromised cloud resources are setting new records

The main culprits are the IoT botnets Aisuru and Kimwolf, which consist of millions of compromised routers, cameras, and Android TV boxes. These botnets are responsible for a series of records. In December 2025, the same botnet family set a new record with 31.4 Tbit/s and 200 million requests per second, marking the largest publicly known DDoS attack to date.[3]

A second source of attacks is increasingly emerging: hacked virtual servers at cloud and hosting providers. Unlike a private IoT camera with just a few Mbit/s of upload bandwidth, a compromised server in a data center has a connection in the Gbit/s range. Therefore, just a few thousand hacked cloud instances can easily eclipse the attack potential of an IoT botnet with millions of end devices.

This is a particularly efficient shortcut for attackers because it requires far fewer compromised systems than a classic IoT botnet. This is made possible by access to cloud resources that are either hijacked outright or rented using stolen payment details.

> *"A common route is via stolen payment data. Stolen credit card details can be used to rent cloud servers. The servers are then used for two to four weeks before the provider notices the fraud and blocks access."*



Jens-Philipp Jung, CEO

Law Enforcement Is Dampening Mass Attacks

The decline in the sheer number of attacks coincides with increased international law enforcement pressure. For example, in July 2025, Europol and Eurojust dismantled much of the server infrastructure of the pro-Russian group NoName057(16) as part of "Operation Eastwood."[4] This group had carried out repeated DDoS attacks on critical European infrastructure since the start of the war in the Ukraine. More than 100 servers were seized, and several arrest warrants were issued. There were also arrests in France and Spain.

Another blow followed in March 2026 when authorities in the U.S., Canada, and Germany shut down the command-and-control servers of four major IoT botnets: Aisuru, Kimwolf, JackSkid, and Mossad. These botnets had collectively controlled over three million devices. According to the Department of Justice, botnet operators had infected over three million devices worldwide by March 2026, including hundreds of thousands in the US.[5]

Artificial Intelligence Lowers the Barrier to Entry for New Botnets

Nevertheless, AI is accelerating the intensification of the threat landscape at an enormous rate. For example, the developer of the IoT botnet "TuxBot v3 Evolution"[6] used a large language model (LLM) to generate large portions of the code, including the C2 communication, exploit engine, and encryption. This enabled the development of a multi-architecture framework for 17 processor architectures.

However, the AI origin left traces: unremoved security warnings, uncommented model reasoning chains, and a password-hashing function falsely declared as "Argon2id" that was much weaker. Consequently, the sample was only about 70% functional. However, the errors could be corrected with a few prompts, suggesting that a functioning version is likely already in circulation.

This case demonstrates how AI reduces the development effort and expertise required for new botnets. This aligns with the World Economic Forum's "Global Cybersecurity Outlook 2026,"[7] in which 94% of security leaders see AI as a key driver for both attackers and defenders in 2026.

Key Findings

1

New record levels in bandwidth and packet rates reached

Peak values of 2.3 Tbps and 322 million packets per second. These values clearly exceed the capacity of even powerful systems, as they nearly double the peak values of 1.2 Tbps and 207 million packets per second recorded in the first half of 2025.

2

Attack duration remains high

The longest documented attack in the first half of 2026 lasted around six days (in the first half of 2025, it lasted more than eight days).

3

Explosive data volume

The cumulative attack volume increased from 438 TB to 705 TB (a 61% increase) — enough for approximately twelve years of uninterrupted 4K Netflix streaming.

Network DDoS Protection

More Impact, Fewer Attacks

At first glance, the figure appears to be good news. In the first half of 2026, there were 42% fewer DDoS attacks on the Link11 network than in the same period the previous year.

-42%



Decline in DDoS Attacks on the Link11 Network

However, the data tells a different story: individual attacks reached record levels in terms of bandwidth, packet rate, and duration. Additionally, the distribution shifted from short, sharp attacks to long-running campaigns. Once targeted, customers were significantly more likely than the previous year to face further waves. Therefore, the threat has shifted — from breadth to depth — but not weakened.

The decline in the sheer number of attacks can be attributed to increased international law enforcement pressure. In July 2025, Europol and Eurojust, together with authorities from twelve countries, targeted the infrastructure of NoName057(16) as part of “Operation Eastwood.” This pro-Russian group was responsible for extensive DDoS attacks against Ukraine and its supporting states. According to the previous report, this group was responsible for most politically motivated attack waves in Germany in the prior six months.

However, the group has not disappeared entirely. At the turn of 2025/2026, a new, concentrated campaign by NoName057(16) was registered, with more than 2,600 attack entries. 88 % percent of these targeted German infrastructure, and the attacks took place between December 29, 2025, and January 4, 2026. The attacks primarily targeted cultural and political institutions, as well as government agencies. The group is adapting, apparently operating in smaller, more targeted waves than before.

Additionally, investigative authorities continued their campaign against DDoS stresser and booter services. The latest wave of “Operation PowerOFF” targeted DDoS ecosystems in 21 countries in April 2026. Earlier waves had already shut down dozens of booter and stresser websites.

NoName057(16) & DDoSia

NoName057(16) is a pro-Russian hacktivist group that has been active since March 2022, shortly after the war in Ukraine escalated. In response to the “IT Army of Ukraine,” the group developed a DDoS tool called “DDoSia” and positions itself ideologically as a defender of Russian interests against the West and NATO member states.

DDoSia is distinctive in that it operates as a “voluntary botnet”: participants knowingly install the software and actively take part in the attacks. The group motivates its affiliates through a gamified system of points, leaderboards, and cryptocurrency rewards distributed via well-organized Telegram channels with more than 20,000 followers.

DDoSia runs on Windows, Linux, and Android, and it has undergone continuous development since 2022, evolving from a basic proof-of-concept version to the current modular architecture (V5). This advanced version includes Cloudflare bypasses, encrypted C2 communication, and anti-analysis techniques.

Attacks follow a clear geopolitical pattern; the group usually responds within 24–72 hours to events such as NATO accessions, sanctions decisions, or arms deliveries to Ukraine. There is no evidence of official state control, though Russia tolerates the activity without criminal consequences.

Key Facts

Attack vectors

Predominantly TCP flood (53%) and HTTP(S) flood (38%), supplemented by UDP flood and Slowloris.

Main targets

Government agencies, media outlets, the financial sector, and critical infrastructure

Top Target Countries

Ukraine, Lithuania, Poland, Estonia, the Czech Republic, and Germany

Alliances

Cooperation with KillNet, CARR, UserSec, and Z-Alliance, among others.

Law enforcement

“Operation Eastwood” (Europol/Eurojust, July 2025) led to C2 seizures.

Given the ongoing geopolitical tensions, continued and increasingly sophisticated activity is to be expected.

Between Record and Reality

The cumulative attack volume on the Link11 network increased from 438 terabytes (TB) in the first half of 2025 to approximately **705 TB** in the first half of 2026. This represents a 61% increase.

4K-Streaming

705 TB is equivalent to about **11 years of continuous Netflix streaming in 4K** resolution.

Audiobooks

Enough data for **more than 2,700 years** of uninterrupted audiobook playback.

MP3-Songs

This amount of data can hold about **150 million songs**.

64-GB devices

That's equivalent to the storage capacity of **11,000 fully loaded smartphones**, each with 64 GB of storage.

"Attacks are shorter, but the total volume that we had to mitigate is higher than ever. Attackers are steering their botnets with greater precision and control, generating more traffic in less time."



Karsten Desler, CTO

The Biggest Attacks Compared

The largest DDoS attack recorded on the Link11 network to date reached a peak bandwidth of 2.3 Tbps in the first half of 2026. In the first half of 2025, the peak value was still 1.2 Tbps. Thus, the current record is about 85% higher than that of the same period last year.

The maximum packet rate also increased significantly, rising from 207,090,400 packets per second in the first half of 2025 to 322,055,800 packets per second in the first half of 2026, representing a 56% increase. An attack volume of this magnitude can overwhelm even powerful enterprise servers or firewalls within seconds. This can lead to massive network overload, packet loss, and potential total service outages.

Bandwidth: Why Perspective Matters

The average bandwidth per attack also increased significantly, though this increase varied greatly depending on the averaging method used. A single extreme outlier, such as the 2.3 Tbps attack, can distort a simple average to the point of being meaningless. Therefore, we examine three metrics in parallel.

Key metrics examined:

	2025		2026	%
Maximum value	**1,2** Tbit/s	→	**2,3** Tbit/s	+85%
Simple Average	**4,6** Gbit/s	→	**10,6** Gbit/s	+131%
Average of the middle range	**1,4** Gbit/s	→	**2,3** Gbit/s	+66%

The mid-range average excludes the extremely small attacks at the lower end and the extreme outliers at the upper end. This makes it a more realistic reflection of a "typical" attack than the simple average.

Specifically, we eliminate the extreme values at the top and bottom, then calculate the average from the middle 85% of attacks. This prevents a single record attack from distorting the result. The figure shows how large a "typical" attack is, not the size of the most spectacular individual case.

The picture is mixed but revealing. At the top of the distribution, the threat has intensified dramatically. In the "typical" case, however, it is far more moderate. This shows that a few extreme outliers are responsible for most of the growth while the "typical" attack develops more slowly but steadily.

Two Speeds of Threat

The longest documented attack in the first half of 2026 lasted 8,673 minutes, or around six days, and occurred in February. Although shorter than the previous year's record (12,388 minutes, or around eight days and 14 hours), it remained at a high level. The duration and intensity of the largest attacks are developing independently of one another.

However, the "typical" attack remained largely stable, contrary to what the simple average would suggest. While the simple average is skewed upward by a few very long campaigns (rising from 25.5 to 35.3 minutes, an increase of 38%), the mid-range average shows a moderate decline from 8.3 to 7.6 minutes (an 8% decrease).

The Real Shift Is Happening at the Short End

The percentage of attacks lasting two minutes or less increased from 16% in the first half of 2025 to 31% in the first half of 2026. Meanwhile, the percentage of attacks lasting between two and five minutes decreased from 30% to 20%.

For durations of around ten minutes or more, however, the distributions for the two periods are nearly identical. Thus, the shift is concentrated almost entirely on the shortest attacks, which are becoming ever shorter and moving toward "microbursts."

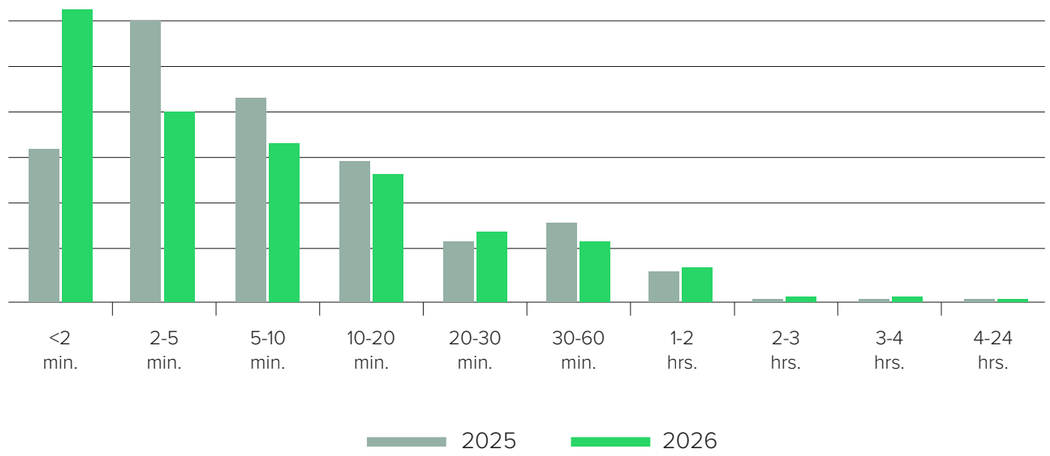
Two explanations seem plausible for this trend of increasingly fast, short attacks.

1. **Payload-first tactic:** Attacks are increasingly designed to take effect within seconds, knocking out a server before defensive measures can respond. Rather than relying on a long, resource-intensive assault, these attacks use automated blackholing or exploit server errors to keep a service offline even after the initial spike in attacks has ended, eliminating the need for a sustained attack.

2. **Early abandonment** Attackers are increasingly abandoning attacks that are not effective early on rather than investing further resources in failed attempts.

In both cases, the pattern suggests that today's attackers expect immediate results and can deploy massive amounts of traffic with surgical precision. This contrasts with the multi-day marathon campaigns that still exist at the upper end of the distribution. Therefore, both patterns occur simultaneously — a sprint and a marathon, so to speak — with neither one replacing the other.

Comparison of Attack Duration: First Half of 2025 vs. 2026



Recurring Attacks: Once Is Rarely Enough

Statistically speaking, once you have been attacked, it is unlikely that it will stay that way. In our analysis, we examine how many days pass between attack waves on the same customer and the likelihood that an attack will be followed by more.

Attack waves rarely come alone. In the first half of 2026, we recorded more than one attack wave on the same day on more than half of all attack days. The adjusted average is 58% (H1 2025: 49%). Thus, an "attack day" is increasingly not a one-off event for affected customers, but rather the norm, with several waves in succession.

And that is usually not the end of it. The probability that a customer will be spared for a certain period after an attack has decreased year over year across every examined time horizon.

Period without another attack

	H1 **2025**	H1 **2026**
1 Day	93%	89%
7 Days	78%	71%
30 Days	54%	44%
60 Days	33%	24%
90 Days	19%	12%

In other words, only 44% of affected customers managed to stay attack-free for 30 days after an attack wave ended in the first half of 2026, compared with 54% in the same period the year before. "Once and never again" is becoming less common — .not just in perception. But at every time horizon examined (1, 7, 30, 60, and 90 days), the recurrence rate in 2026 was higher than the previous year. Anyone who is attacked should expect a follow-up attack over a significantly longer period than before. Those hit once in 2026 should expect a significantly higher probability of facing further waves in the following weeks.

"We're seeing more and more microburst attacks — short, intense hits that end quickly. Attacks used to last three to four minutes, but now they're often just a minute or less. Attackers rely on automated fault conditions or server errors to keep a website offline even after the attack ends."



Sean Power, Solution Engineer

Bots, Botnets, and the Practice of Modern WAAP Defense

Bots are almost as old as the Internet itself. However, what falls under this term today bears little resemblance to the harmless IRC helpers of the early 1990s. This chapter examines this evolution in two steps. First, it illustrates how, over the course of more than three decades, bots and botnets have evolved from simple chat scripts into AI-powered attack tools. Second, it illustrates this evolution through specific examples from the first half of 2026. Real cyber-insight analyses from the Link11 Security Operations Center (SOC) demonstrate how volume, concealment, and legitimacy converge in practice and the implications for an effective Web Application and API Protection (WAAP) strategy.

From Eggdrop to Agent:
The Evolution of Bots and Botnets

Botnets are almost as old as the Internet itself, but their tools have changed radically. What began as an IRC prank—IRC stands for Internet Relay Chat, one of the oldest chat protocols on the internet—is today an industrialized, AI-powered attack economy. A look back shows why rigid defense concepts struggle to keep up with this ever-evolving threat.

1988 – 2000

The Beginnings: Chat Helpers Become a Weapon

The story begins harmlessly enough. In 1993, Jeff Fisher released "Eggdrop," one of the first IRC bots. These bots were designed to provide administrative assistance for chat channels.[8] However, because users who were kicked from channels wanted revenge, these tools gave rise to what became known as IRC wars. These wars are considered the forerunners of today's DDoS attacks. In 1999, "PrettyPark" and "SubSeven" followed as the first malware programs to steal passwords, redirect traffic, and be controlled remotely.[9] In 2000, "GTbot" established itself as the first bot with a dedicated DoS function.[10] That same year, researchers discovered EarthLink Spammer, one of the earliest commercial botnets used for mass phishing.[11]

What Is IRC?
Internet Relay Chat (IRC) is a text-based chat protocol created in 1988. Users connect to a server and join „channels" (e.g., #chat), where participants can write in real time.

Why This Matters for Bot History:
IRC bots were easy to build and control via chat commands, so the protocol became the preferred channel for botnets from the mid-1990s onward. Attackers hijacked machines, logging them into their own channel, and controlled them centrally — the blueprint for the command-and-control principle that still shapes botnets today. As of 2026, IRC still appears as a fallback channel, for example, in TuxBot v3.

2002 – 2009

Professionalization: Malware Kits and Spam Armies

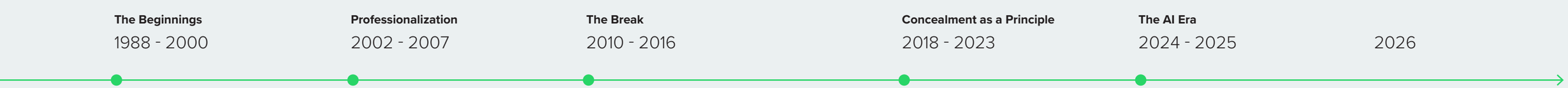
Between 2002 to 2004, "Agobot," "SDBot," and "Spybot" emerged as complete construction kits. Because their source code was openly available online, even less technically skilled individuals could create their own variants — an early precursor to today's malware-as-a-service models. During this time, "Sinit" and "Phatbot" emerged as the first peer-to-peer botnets, operating without a central command-and-control server, making them more difficult to shut down.[12] The largest expansion of the attack surface up to that point occurred in 2007 with the Storm botnet, which is estimated to have infected up to 50 million computers. It was used for sending spam, manipulating stock prices, and committing identity theft.

2010 – 2018

The Break: Web Bots, Browser Emulation, and the IoT Wave

As web-based services became more widespread, bots abandoned pure IRC channels. Attackers started using HTTP, SSL, and ICMP as communication channels. Meanwhile, a second generation of bots emerged on the web in the form of headless browsers, such as PhantomJS, which could process entire websites, including JavaScript, without requiring a graphical interface.[13] This made it possible to automatically fill out forms and try login credentials on a massive scale for the first time. Credential stuffing became a mass phenomenon.
The next breakthrough occurred in 2016 with the Mirai botnet. This malware scanned the internet for Internet of Things (IoT) devices with default factory passwords. It infected routers, cameras, and digital video recorders and generated attacks of

Timeline at a Glance



an unprecedented scale: over 600 Gbit/s were directed at security researcher Brian Krebs's blog, around 1 Tbit/s at French hosting provider OVH, and a multi-hour outage hit DNS provider Dyn, affecting large parts of the U.S. internet.[14] Shortly afterward, when the source code was released, it spawned an entire family of imitators that remain active to this day.[15]

2010 – 2023

Concealment as a Principle:
Browser Bots and Residential Proxies

In the years that followed, the focus shifted to a race for inconspicuousness. Bots built on Chrome or Chromium could imitate mouse movements, clicks, and scrolling behavior so convincingly that they were nearly indistinguishable from real users.

Meanwhile, attacks increasingly targeted hijacked home routers and private internet connections, also known as residential proxies. Consequently, traffic no longer originated from suspicious data centers, but rather from seemingly ordinary households.[16] Security vendors began classifying this evolution into generations, from simple scripts to headless browsers to full browser emulation, with each stage being harder to detect than the previous one.[17]

2024 – today

The AI Era: Generative, Agentic, Industrialized

Since 2024, generative AI has accelerated this development in two ways. First, the barrier to entry is decreasing. Bot-as-a-service platforms and AI code generators enable even those with limited technical expertise to develop functional attack tools. According to recent reports, the number of AI-generated bot attacks increased from approximately two million to 25 million per day in just one year.[18] That is a twelvefold increase. Currently, more than half of all web requests are said to come from bots, one-third of which are malicious.

Second, AI is changing the development of malware itself. In July 2026, Palo Alto Networks' threat intelligence team, Unit 42, documented TuxBot v3 Evolution, an IoT botnet framework. The author used a large language model to write much of the code, including an encrypted command-and-control channel, a domain generation algorithm, and its own exploit language.

The errors are particularly revealing. Among other things, the model left its own chains of reasoning as comments in the code and claimed to have implemented modern Argon2id encryption. In reality, however, it relied on a much weaker method. AI lowers the barrier to development but does not replace expert oversight, a pattern likely to repeat itself in the years ahead.

The IoT botnets Aisuru and Kimwolf demonstrate the direction in which operations are heading. In a campaign called "The Night Before Christmas," they launched an attack with a peak load of 31.4 terabits per second at the end of 2025. This attack triggered the largest publicly known DDoS attack at the time. The attack was launched via hijacked routers and increasingly compromised Android TVs.[19] In March 2026, Germany's Federal Criminal Police Office (BKA) dismantled a network of over three million hijacked devices belonging to this ecosystem, working together with US authorities and Canadian investigators.[20]

This is the most far-reaching case to date, going beyond classic botnets. In November 2025, Anthropic disclosed that a group believed to be state-sponsored had used its AI coding tool as a largely autonomous attack agent for several weeks. Reconnaissance, exploit development, and data analysis were carried out 80 to 90 percent without human intervention.[21]

Whether this degree of autonomy is already the norm or still the exception is a matter of debate among experts. In bot defense, the focus has shifted from traffic detection to determining whether a request originates from a script, human, or autonomously planning system.

This historical development from chat script to an autonomously planning agent is more than just a retrospective. It explains why the attacks observed by the Link11 Security Operations Center (SOC) in the first half of 2026 hardly resemble the traditional concept of a botnet. The following five cases demonstrate how this manifests in the day-to-day reality of real customers.

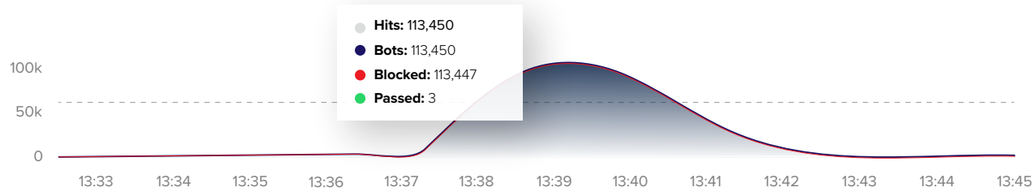
WAAP in Practice: When Traffic Is No Longer What It Seems

The classic DDoS attack — loud, massive, and easy to spot — is still around, but it's no longer the norm. Instead, we now face a threat landscape in which the volume, origin, and target of an attack are increasingly decoupled. Those who only monitor bandwidth and known signatures often only see half the truth.

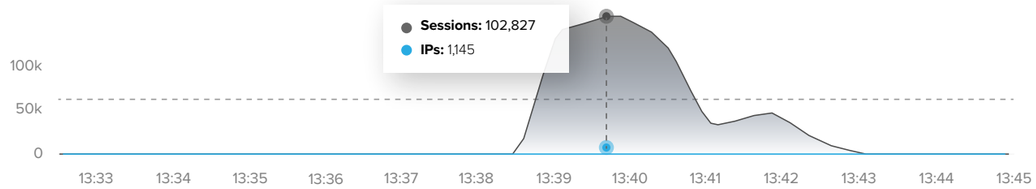
Small Numbers, Real Impact

Not every effective attack requires a botnet of millions of devices. One case involving around three million GET requests against a single root domain initially appeared harmless compared to record attacks in the double-digit terabit range. Only the combination of geo-filtering and rate limiting exposed the pattern: a small, inconspicuous botnet that deliberately tied up server resources without ever tripping an alert threshold for "large" attacks.

Passed vs. Blocked



Unique Sessions & IPs



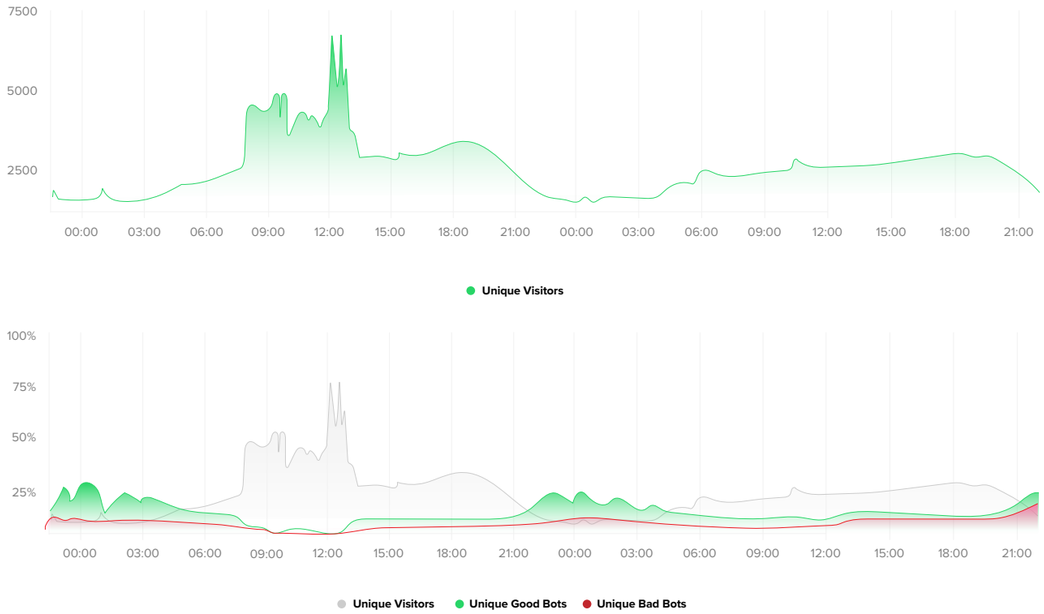
The most dangerous attacks are no longer the loudest ones. Those who only monitor bandwidth and known signatures miss the attacks that can cause the most damage because they are designed to be inconspicuous."



Jag Bains, VP Solution Engineering

Low-and-Slow: Invisible in the Noise

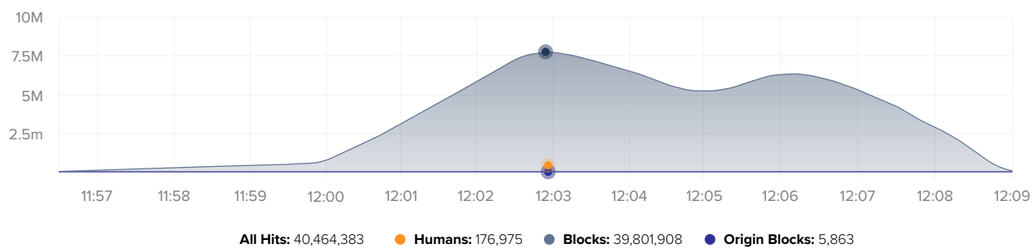
An attacker acted even more subtly against an European e-commerce provider. The number of unique IP addresses doubled for no apparent business reason. Although bandwidth and requests per second remained unremarkable, response times and conversion rates suffered. This was caused by real, compromised end devices with fully functional browsers that barely stood out individually, but had an effect en masse — a classic low-and-slow pattern that hid within the statistical noise of normal usage. After geo- and ASN filters failed to make a difference, only human-machine verification proved effective.



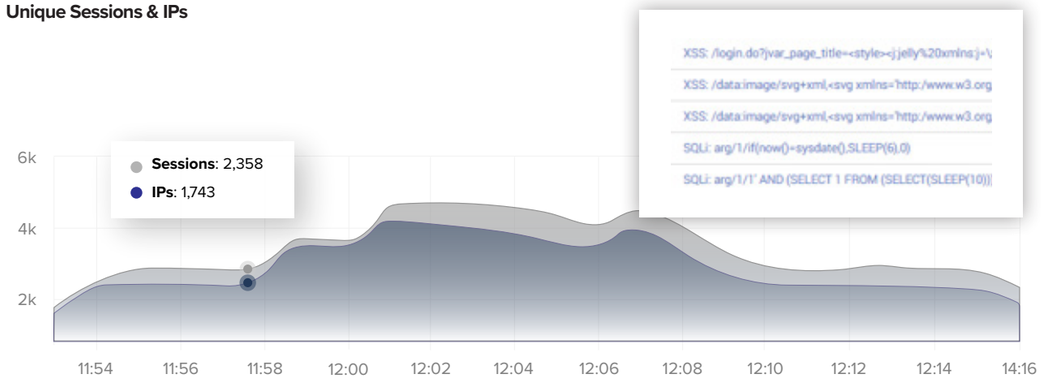
Noise as Camouflage

A second pattern shows that an attack does not necessarily target a traffic peak. In one case, two domains, including a booking platform, were hit with 14 to 40 million requests. At the same time, targeted SQL injection and XSS signatures appeared in the WAF analysis. The logic behind such „smokescreen“ attacks is simple: the volumetric noise is meant to flood monitoring systems and bloat log files while quiet exploits are planted in its wake. In this case, however, the attackers revealed their identity by using the same IP addresses for DDoS traffic and infiltration attempts. Consequently, both vectors were blocked by the same block rule. A more sophisticated actor would have used separate IP pools, making them considerably harder to stop.

Passed vs. Blocked



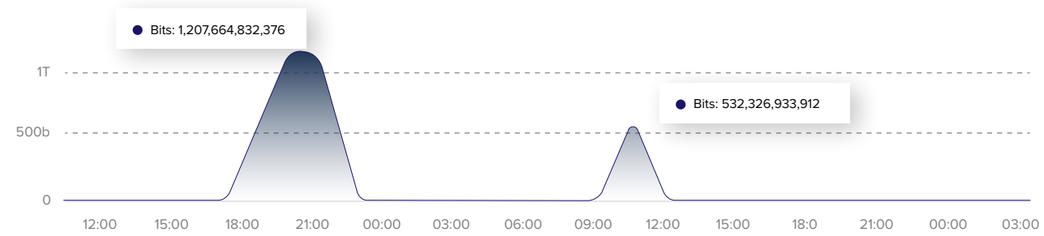
Unique Sessions & IPs



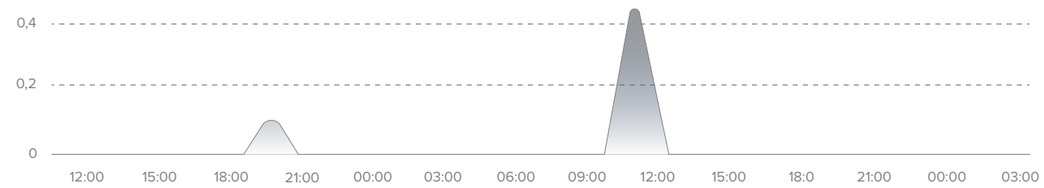
Request Rate Exceeds Bandwidth

An even more complex variant emerged in a two-wave attack involving over 335 million requests and a peak load exceeding one terabit. The second, smaller wave was particularly revealing. With only half the bandwidth of the first wave, it produced stronger latency effects due to a higher request rate per second. This is evidence that CPU load driven by request frequency is often more critical than bandwidth alone.

Total Bandwidth (bits)



Latency (milliseconds)



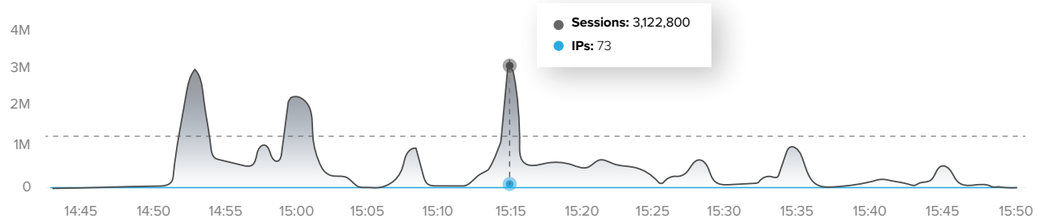
“In a two-wave attack, the second wave had only half the bandwidth of the first, yet it caused stronger latency effects simply because the request rate was higher. This shows that bandwidth alone often says little about how much damage an attack actually causes.”



Sean Power, Solution Engineer

When Real Traffic Becomes a Weapon

The most difficult attacks to understand are those that use legitimate infrastructure or data as a cover. For example, in a case involving a defense contractor, the majority of the attack traffic — over 50 million requests — came from known cloud and hosting environments, not a diffuse IoT botnet. Just 73 IP addresses generated over three million parallel sessions, which is a level of computing power that a home router could not produce. The geopolitical context—an active conflict between two states—suggested a political motive. Since cloud capacity is inexpensive, easily accessible, and technically reliable, the threat is shifting from bandwidth to application logic and from compromised end devices to cloud-native attack infrastructure.



What This Means for WAAP Practice

The conclusion is the same in all these cases: volume, origin, and known signatures are not reliable early indicators today. An effective defense requires endpoint-specific baselines that define normal traffic on a given path at a given time. Generic thresholds are insufficient for transaction-critical APIs. Second, behavior-based detection is needed rather than signature-based detection since replay attacks, low-and-slow patterns, and cloud-native floods can appear structurally „clean.“

The central lesson from the first half of 2026 is that a traffic peak does not automatically indicate a capacity problem, nor is inconspicuous traffic necessarily harmless. Therefore, resilience means not only staying online but also being able to recognize what is behind your own traffic at all times.

Conclusion

Analysis of attacks in the first half of 2026 shows that the DDoS threat landscape has intensified and diversified. Although the total number of attacks decreased by 42% compared to the same period the previous year, the bandwidth and packet rates of individual attacks increased significantly. Thus, attackers are increasingly focusing on fewer but far more powerful attacks

An Overview of the Five Key Findings

- Fewer but significantly more powerful attacks:
  42% fewer attacks but new records for bandwidth (2.3 Tbit/s) and packet rate (322 million pps).
- Superbotnets and cloud resources are responsible for these records.
  Aisuru/Kimwolf and compromised cloud servers serve as efficient attack vectors.
- Two speeds of the threat: microburst attacks and marathon campaigns occurring simultaneously.
- Once targeted, you remain in the crosshairs due to rising recidivism rates across all time frames.
- Attacks are becoming more sophisticated rather than just larger,
  with examples including Layer 7, obfuscation, and cloud-native infrastructure.

Notable as well is the bandwidth and packet rate of some attacks. They ranged from terabit-scale traffic to over 1.6 billion packets per second during the first half of 2026. This illustrates the potential impact on companies, institutions, and infrastructures. At the same time, more precise Layer 7 attacks demonstrate that concealment and deception pose risks in addition to sheer scale.

Companies must prepare for highly complex attacks of this kind. Essential components of this preparation include emergency plans, real-time monitoring, and AI-supported defense systems that can detect and automatically block suspicious traffic. Only rapid response mechanisms and the continuous adaptation of security strategies can mitigate the consequences of such massive attacks. Therefore, effective DDoS protection requires more than just bandwidth management to counter increasingly hybrid threats.

Your Contact Person

Rolf Gierhard
Chief Revenue Officer

+49 69 58004926-200
r.gierhard@link11.com



Sources

[1] https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026.pdf

[2] https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/global-digital-trust-insights.html

[3] https://www.bleepingcomputer.com/news/security/aisuru-botnet-sets-new-record-with-314-tbps-ddos-attack/

[4] https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down

[5] https://www.techradar.com/pro/security/europol-announces-takedown-of-major-ddos-for-hire-network

[6] https://unit42.paloaltonetworks.com/tuxbot-v3-evolution-iot-botnet/

[7] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[8] https://www.aic.gov.au/publications/tandi/tandi333

[9] https://arxiv.org/pdf/1706.05143

[10] https://abusix.com/blog/bots-and-how-theyve-shaped-the-internet/

[11] https://www.imperva.com/company/press_releases/bots-are-taking-over-the-internet-automated-threats-are-a-growing-risk-for-organizations/

[12] https://www.usenix.org/legacyurl/peer-peer-botnets-overview-and-case-study

[13] https://www.imperva.com/learn/application-security/what-are-bots/

[14] https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

[15] https://www.cyber.nj.gov/threat-landscape/malware/botnets/mirai

[16] https://www.imperva.com/blog/2025-imperva-bad-bot-report-how-ai-is-supercharging-the-bot-threat/

[17] https://www.clickfortify.com/glossary/bot-detection

[18] https://lyrie.ai/research/research/2026-05-02-bad-bot-report-2026-internet-no-longer-human

[19] https://www.cloudflare.com/learning/ddos/glossary/aisuru-kimwolf-botnet/

[20] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2026/Presse2026/260320_PM_Botnetze.html

[21] https://www.anthropic.com/news/disrupting-AI-espionage


LINK11