LINK11

DDOS-REPORT

2022

www.link11.com

Table of Contents

Current Threat Situation and Executive Summary

Adaptive, Complex, and Dangerous - DDoS Attacks and Their Metamorphosis

The Coronavirus pandemic has affected everyone's social life and business for more than two years. For Bitkom's "Digital Office Index 2022," one in two of the companies surveyed said that Covid-19 had accelerated digital transformation[1]. This is especially true for hybrid work models, migration to the cloud, and improvements to corporate IT services and web services that ensure everyday professional life.

Although cyber incidents have already increased significantly due to the Coronavirus pandemic and the associated digitalization surge, the situation has become even more acute with the start of the war in Ukraine on February 24, 2022. In its current situation report, the BSI states that the threat is "higher than ever."[2]

The pro-Russian hacker group "Killnet" has declared cyberwar on several countries, including Germany[3]. The consequences of this declaration have already been felt in Germany, Italy, Lithuania, Norway, and Poland. Hardly a month went by without a cyberattack on NATO countries, their public institutions, banks, or critical infrastructure[4].

Although cyber actors use sophisticated malware or complex DDoS attacks even in peacetime, the consequences can be far more devastating when used as a weapon in cyber warfare. The attackers are primarily concerned with weakening the morale of the combatants and the population and causing the greatest possible damage, as Microsoft also noted in the report "Defending Ukraine: Early Lessons from the Cyber War."[5]

Currently, we are experiencing a very dynamic situation: while the Link11 Security Operations Center (LSOC) observed a decline in 2022, hardly a day goes by since the German government announced its support for Ukraine with battle tanks in January 2023 without media reports of DDoS attacks, especially against critical infrastructure operators (CRITIS). The Dutch National Scrubbing Center (NaWas) has also registered fewer DDoS attacks since the end of 2021[6].

As before, the long-term trend of increasing cyberattacks continues unabated. According to the World Economic Forum experts, a real "cyber storm" is gathering. The latest "Global Cybersecurity Outlook" also reveals that 91% of the executives surveyed expect widespread and catastrophic cyber incidents in the coming years[7].

There are several reasons for the first temporary drop of more than three-quarters (79%) in attacks compared to the record DDoS year of 2021. The massive increase in politically motivated DDoS attacks - also due to further geopolitical tensions like those between China and Taiwan as well as between the US, Israel, and Iran - led to a shift in attacks. In addition, attackers looked for easy targets with unsecured or not effectively protected systems.

In addition, in April 2022, a successful collaboration between the BKA and the US Department of Justice led to the shutdown of the largest illegal online marketplace, "Hydra," on the Darknet[8]. In December 2022, the FBI and Europol struck again against DDoS crime by shutting down 48 illegal DDoS-for-hire services, so-called "booter services."[9] Such actions are brief breathers until hackers can make a name for themselves again with new platforms and become more active.

In 2020 and 2021, several waves of DDoS (RDDoS - Ransom Distributed Denial of Service) extortions by Armada Collective, Fancy Bear, Lazarus Group, or Fancy Lazarus were big drivers. However, since these peaks, there have been fewer RDDoS attacks as the usual players on the cybercrime playing field have focused their capabilities on other targets or politically motivated attacks.

While there are fewer attacks, at the same time, they are more dangerous. LSOC has observed that these attacks and the methods used are constantly changing. Instead of randomly attacking companies in hopes of success, advanced and sophisticated DDoS attacks are now being used in a very targeted manner. The attacks recorded in the period under review are shorter, more intense, and more demanding. For example, an analysis of

attacks recorded on the Link11 network shows that DDoS attacks in 2022 reached the critical load on average just 55 seconds after the attack began. In comparison, attacks in 2021 took an average of 184 seconds to reach their peak. These “turbo attacks” can cripple the network even before the defenses are effective without a high-performance defense system such as Link11‘s in terms of precision and speed of mitigation.

The trend toward high-volume attacks, which began to emerge at the end of 2021, has indeed stabilized in the first half of 2022. However, in direct comparison with the previous year, bandwidth peaks were larger on average. While bandwidths measured by LSOC exceeded 100 Gbps every month in 2021, 2022 is characterized by significant fluctuations. In October and November 2022, bandwidth peaks are well below 100 Gbit/s.

In the first half of 2022, the share of multi-vector attacks has decreased compared to the same period last year. While in 2021, the share of multi-vector attacks was 71%, in the first six months, only about one-third of the attacks (35%) were multi-vector attacks. Overall, the proportion of multi-vector attacks increased to 45% from July to December 2022, with the most significant increase seen in Q4.

To summarize: DDoS attacks are tremendously adaptable. Their DNA is continuously changing, and they are permanently adapted to the conditions in the cyber landscape. This makes them an unpredictable threat to organizations of all types and sizes. The vacuum left by “Hydra” and others is being filled by yet unknown parties, increasing uncertainty in the future.

DDoS in the News

January 2022

Multiple outages of Solana network - cryptocurrency suffers price losses

The Solana network fails multiple times due to DDoS attacks. The price of cryptocurrency falls as a result. The reason for this could be the use of the novel blockchain technology[10].

January 2022

No Internet in Andorra: attack on Minecraft player shuts down Internet

During a Twitch gaming tournament, DDoS attacks on the Internet Service Provider (ISP) in Andorra kicked several Minecraft players out and crippled the Internet across the country[11].

February 2022

DDoS attack wave on Ukraine

Before the Russian invasion of Ukraine, there were several DDoS attacks on state institutions such as the Ministry of Defense and state-owned banks[12].

February 2022

Russian government websites targeted with DDoS attacks

Following announcements by the hacker collective Anonymous, the Russian government and state media websites experienced repeated outages due to DDoS attacks[13].

March 2022

Attack on Ukrainian national Internet provider

The Internet in Ukraine has been down for 15 hours after an attack on Ukrtelecom, the national Internet provider[14].

April 2022

Attack on the websites of the Finnish Ministry of Defense

During Ukrainian President Zelenskyy's speech, a DDoS attack crippled the Finnish Ministry of Defense website. In addition, the Ministry of Foreign Affairs was also affected[15].

April 2022

Russian hacker group "Killnet" attacks Romanian government websites

Several public websites managed by government agencies in Romania were affected by DDoS attacks. These included the official website of the Romanian government and that of the Romanian Ministry of Defense[16].

May 2022

Attack on the Eurovision Song contest and subsequent attacks against Italian authorities

Following the pro-Russian attack on the Eurovision Song contest, which was successfully repelled by Italian police, there were attacks on Italian authorities[17].

May 2022

Hacker attack on German authorities

Several websites of German authorities and ministries were affected by DDoS attacks. This was probably a pro-Russian hacker attack[18].

May 2022

Port of London website under attack

A DDoS attack also hit the Port of London.
A pro-Iranian hacker group is believed to be behind it[19].

June 2022

Norway targeted in cyberattack

Several private and public institutions in Norway were victims of a so-called DDoS attack. According to Norwegian security authorities, a criminal pro-Russian appears to be behind the attacks[20].

June 2022

DDoS attack on cryptocurrency platform Tether

Requests to the cryptocurrency website Tether increased by over 400% from two thousand to eight million every five minutes due to a DDoS attack[21].

July 2022

Disruption of the US Congress website

Pro-Russian hackers claimed responsibility for a cyberattack that briefly disrupted access to a US congressional website Thursday night[22].

August 2022

DDoS attacks on Taiwanese websites

The visit of the Speaker of the House of Representatives, Nancy Pelosi, triggered a DDoS attack on Taiwanese websites[23].

September 2022

Cyber attack on Iran‘s central bank

Iran‘s central bank has confirmed a cyber attack on its systems. The bank had been the target of a DDoS attack[24].

September 2022

Poker tournaments cancelled

All six of PokerStars‘ WCOOP Main Events have been cancelled due to DDoS attacks and had to be postponed[25].

October 2022

US airport websites hit by cyberattacks

DDoS attacks by a pro-Russian hacker group affected the airport websites of several major U.S. cities, including Atlanta, Chicago, Los Angeles, New York, Phoenix, and St. Louis[26].

November 2022

Black Tuesday for trading bank Swissquote

The bank was under a DDoS cyber attack; customers were unable to access securities and receive quotes[27].

November 2022

Pro-Russian hacktivists cripple EU Parliament website with DDoS attack

The European Parliament website was shut down after a DDoS attack carried out by Anonymous Russia (part of the Killnet group)[28].

December 2022

Russia‘s second-largest bank VTB attacked

The state-owned bank VTB was the victim of a cyberattack. The bank was able to fend off the DDoS attacks[29].

Development of Total Numbers in the Link11 Network

Number of DDoS attacks reduced

DDoS attacks took a hiatus in 2022: After reaching an all-time high in 2021, LSOC recorded a decline in attacks on the network for the first time. In 2022, the number of attacks dropped by 79% compared to last year. The reasons for this are many.

During the Coronavirus pandemic, the global number of DDoS attacks increased as cybercriminals sought to exploit the digital vulnerabilities of enterprises and remote working populations. This particularly affected key web services such as vaccination platforms, learning portals, and home office IT systems. In addition to the increase in attacks on the infrastructures that ensured people could live and work during the Corona pandemic, DDoS attacks also extended to hosting providers and Internet service providers.

Since the start of the war in Ukraine in February 2022, politically motivated DDoS attacks have increased significantly due to the associated cyberwar. The pro-Russian hacker group “Killnet” has declared cyberwar on several countries, including Germany, amid the ongoing war in Ukraine. The consequences of this declaration were already felt in Italy, Lithuania, Norway, and Poland. Hardly a month went by without a cyberattack on NATO countries, their public institutions, banks, or critical infrastructure.

Even though the number of attacks has decreased compared to the same period last year, it shows the enormous mutability of DDoS attacks. Their DNA is constantly changing. This makes it more important to prepare for all potential attack modalities with an up-to-date AI-based and automated DDoS protection solution.

Killnet is a Russian-backed cybercrime syndicate that first appeared in January 2022 when it offered DDoS services on illegal forums. During the Russian invasion of Ukraine, the group pledged allegiance to the Russian government and stated that it would treat anyone who opposed the regime with hostility. Since then, Killnet has launched targeted attacks on websites in countries hostile to Russia, including several NATO member states.

The group is considered one of the most active hacktivist organizations, primarily aimed at attracting attention rather than serious harm or substantial financial gain. Killnet‘s new commander, Blackside, is reportedly an expert in phishing, ransomware, and crypto-theft, suggesting the group is looking to expand and improve its operational capabilities.

Killnet‘s tactics include DDoS attacks and disinformation campaigns that they use to alienate the public. The group has carried out attacks on critical infrastructure, airport websites, government services, and media outlets in NATO countries, as well as Ukrainian supporters in Eastern Europe, Nordic, and Baltic countries. Typically, Killnet attacks do not involve ransomware, and the group disseminates its campaigns and potential attack targets through its more than 90,000 Telegram subscribers.

Killnet has a structured organizational hierarchy and has reportedly collaborated with other pro-Russian hacktivist groups, including XakNet Team or Anonymous Sudan. The Latvian government classified Killnet as a terrorist organization after the group was blamed for a cyberattack that temporarily crippled the country‘s parliamentary web services. Killnet has also had public run-ins with the hacktivist group Anonymous[30].

2022 showed how dynamic and unpredictable the attack landscape is. Politically motivated DDoS attacks dominated as a component in cyberwarfare. While it may look like a breather, the threat is not gone - DDoS attacks resemble shapeshifters. They are becoming more diverse, complex and sophisticated.

Jens-Philipp Jung, Managing Director, Link11

The massive increase in politically motivated DDoS attacks led the usual players on the cybercrime playing field to focus their capacities on other targets. In addition to the Ukraine war, other geopolitical tensions include those between China and Taiwan and between the U.S., Israel, and Iran. This also caused a fluctuation in the origin of attacks in the Link11 network. In relative terms, the number of attacks from Russia has almost doubled. On the other hand, there were also significantly more attacks from Ukraine and Taiwan and fewer DDoS attacks from the USA and China. In addition, attackers looked for easy targets in unsecured or not effectively protected systems.

In April 2022, the world experienced an unprecedented blow to Darknet crime: the largest illegal online marketplace was shut down. German and US authorities worked hand in hand to secure the Russian “Hydra market” servers and seize $25 million in cryptocurrency. Successful cooperation between the BKA and the US Department of Justice led to a breakthrough in the fight against criminal activity on the Darknet.

In early December, the FBI and Europol struck again against DDoS crime: 48 Internet domains offering illegal DDoS-for-hire services were seized. Six suspected perpetrators responsible for operating so-called “booter” platforms were arrested. These websites allowed users to launch massive DDoS attacks that can block access to the Internet.

Already in 2020 and especially in the first half of 2021, several waves of DDoS extortion (RDDoS - Ransom Distributed Denial of Service) by Armada Collective, Fancy Bear, Lazarus Group, or Fancy Lazarus were a major driving force. However, after these peaks of ransomware activity, there have been significantly fewer Ransom DDoS attacks.

New Developments

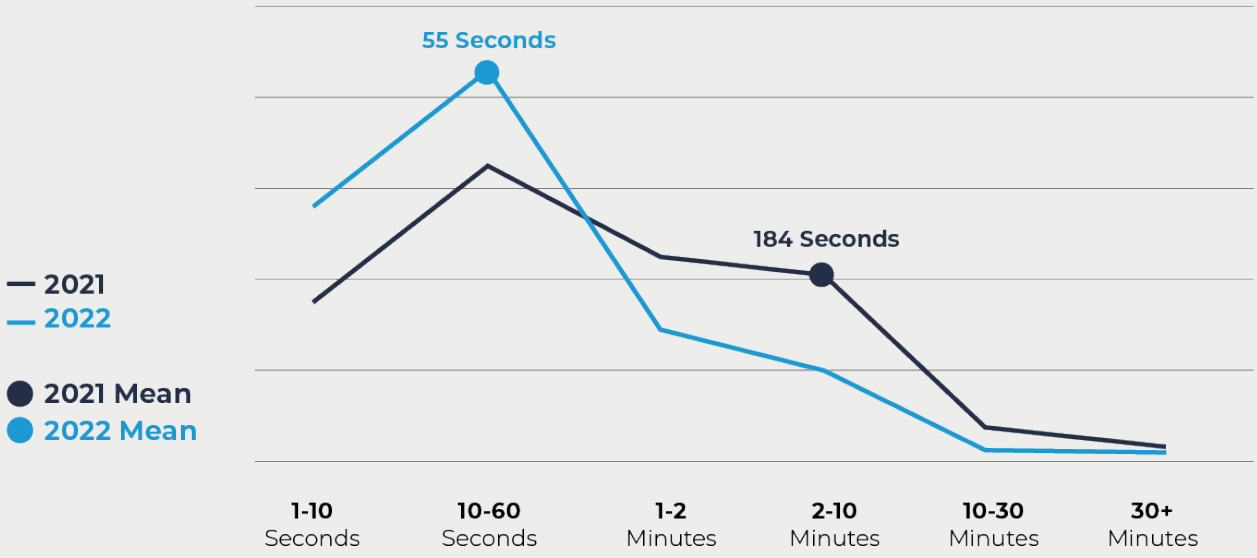
Increasing complexity - DDoS attacks become more challenging

LSOC has analyzed for the first time how long it takes for DDoS attacks to reach their maximum value. This is referred to in English as the “onset,” i.e., the beginning of the attack. The onset is the time it takes for an attack to reach a critical volume.

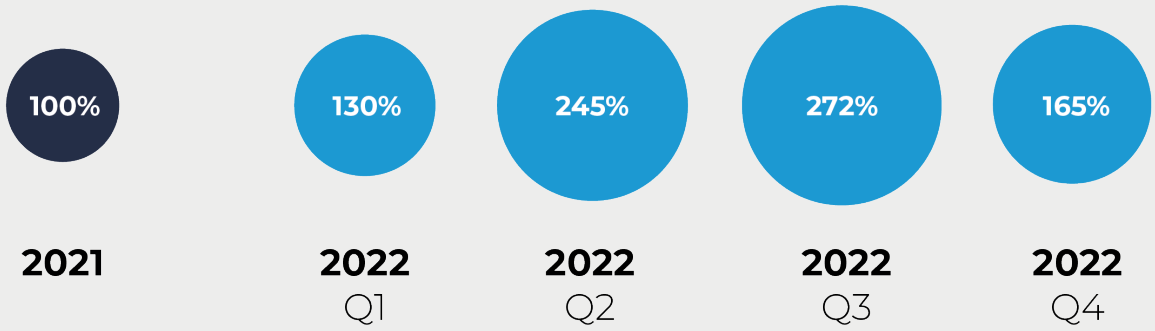
It was analyzed how many seconds must pass after the transmission of the first bytes before the traffic reaches its maximum value. These fast-onset DDoS attacks, or “turbo attacks,” are usually shorter but reach a critical payload quickly instead of continuously increasing. As a result, network systems can be crippled before defensive measures take effect.

On average this year, DDoS attacks reach critical levels after only 55 seconds. However, compared to the 2021 average of 184 seconds, these turbo attacks reach critical volumes 3 times faster.

Duration until the peak of an attack| 2021 vs. 2022



Speed to critical attack volume | 2021 vs. 2022



Especially in the second and third quarters of 2022, attacks escalated much faster than the previous year. DDoS attacks in the second quarter reached their maximum value 245% faster than in 2021, and particularly fast "turbo attacks characterized the third quarter." The critical volume was achieved by fast-onset attacks 272% faster than in the previous year. This also enormously shortened the time for the targets of such an attack to take the appropriate defensive measures.

The short duration of an attack alone is not an indicator of the strength of a DDoS attack. One attack may reach its peak without causing much damage. Another attack may already have critical effects, such as a complete outage before the maximum attack potential is exhausted. Therefore, time-to-mitigate (TTM) is critical, especially for fast-onset attacks.

In the Link11 network, attacks were recorded in 2022 that could transfer twice as much payload only 70% of the time. In this case, a one-minute TTM is not enough to avoid a complete failure.

Time is one of the most important factors in the event of an attack, because every passing second can lead to major damage - through manual assessments of incidents, unforeseen routing problems or outwitted defense mechanisms.

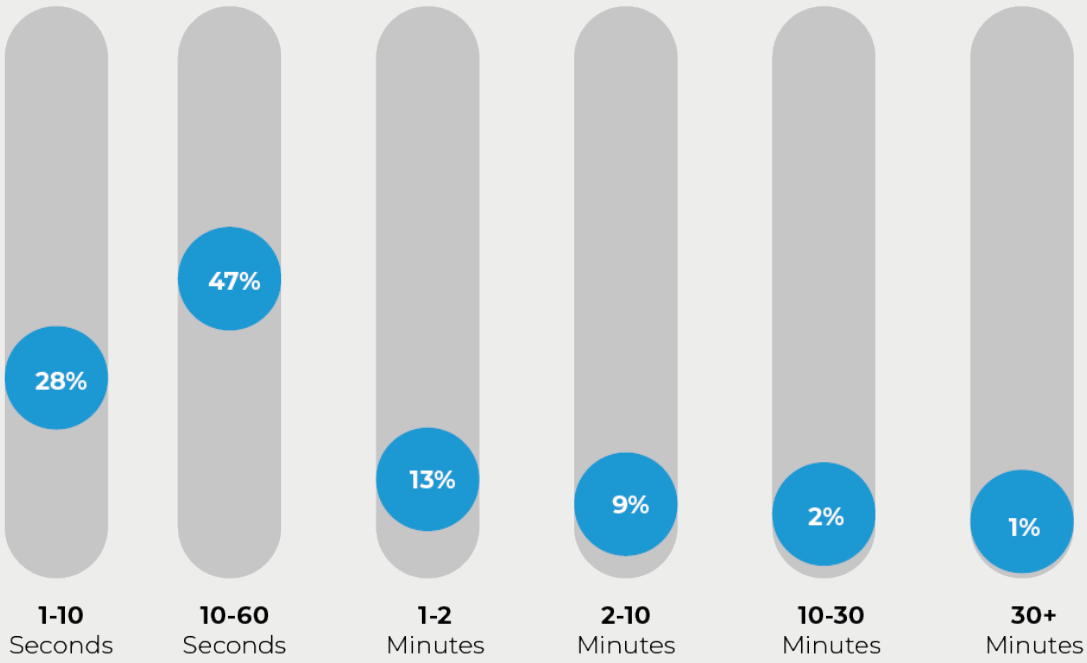
Jag Bains, Vice President Solution Engineering, Link11

A look at the distribution of the time it takes for a DDoS attack to reach its peak in 2022 shows the following results: In more than a quarter of attacks (28%), the critical payload was reached within the first ten seconds. Last year, this percentage was 17%. In the first half of 2022, attacks that reached their maximum value in ten to 60 seconds accounted for almost half of all attacks registered in the network (47%). In comparison, one-third of attacks (34%) in 2021 approached their peak simultaneously.

In only 13% of cases, it took between one and two minutes for DDoS attacks in 2022 to reach the critical maximum level. At more than two minutes, the proportion was around one-tenth of the DDoS attacks recorded by LSOC. Compared to the previous year, large differences can be seen here. In 2021, just under a quarter of attacks (23%) peaked in one to two minutes, and in one-fifth of cases (21%), it took more than two minutes.

Every second counts in a DDoS attack. This makes it more important to avoid wasting time, such as manually reviewing incidents or unforeseen routing issues. If unforeseen routing problems occur or new attack methods slip through the security net, such delays in defense can lead to major damage.

Distribution of the duration until the peak of the attack



Therefore, an effective IT security strategy relies on analyzing data traffic in real-time using smart, fast, and secure methods to ensure maximum transparency in the network. A promising defense against DDoS attacks consists of basic protection and a combination of intelligent and automated AI technology.

The Development of Attack Duration

First short and heavy, then again long-lasting DDoS attacks

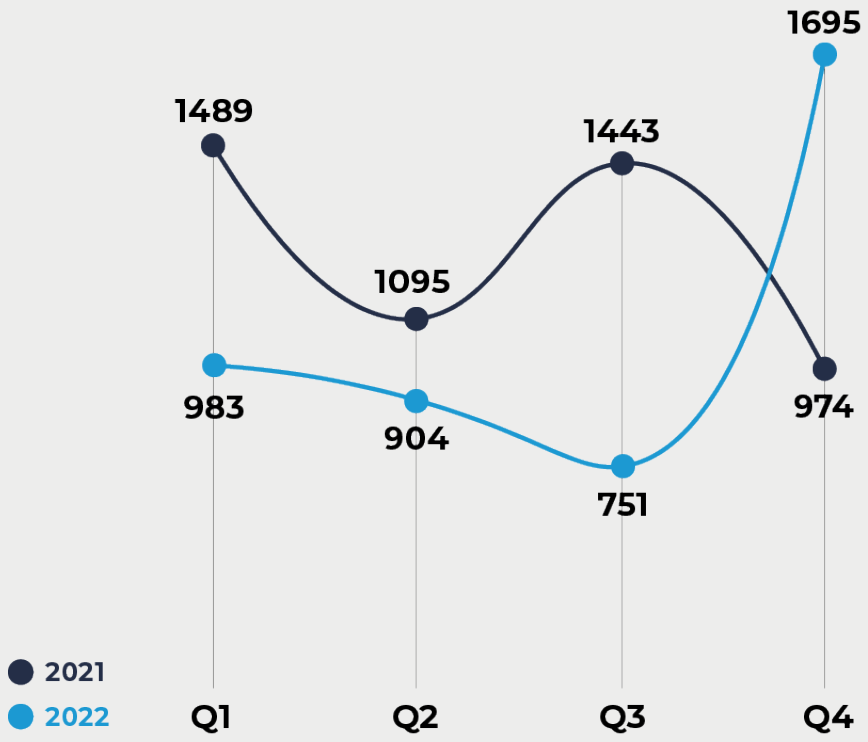
The duration of DDoS attacks recorded on the Link11 network in 2022 has shortened compared to the same period last year. While there were significant outliers almost every month, the overall attack duration decreased. A look at the graph below clearly shows how the duration of DDoS attacks compares to the same period last year.

Overall, the longest attacks in each case differ significantly from one another. The trend towards shorter DDoS attacks was already apparent in the fourth quarter of 2021. This has continued into the third quarter of 2022. The attacks had a particularly short duration in the second and third quarters. This is characteristic of the short, fast-onset DDoS attacks increasingly observed in these two quarters.

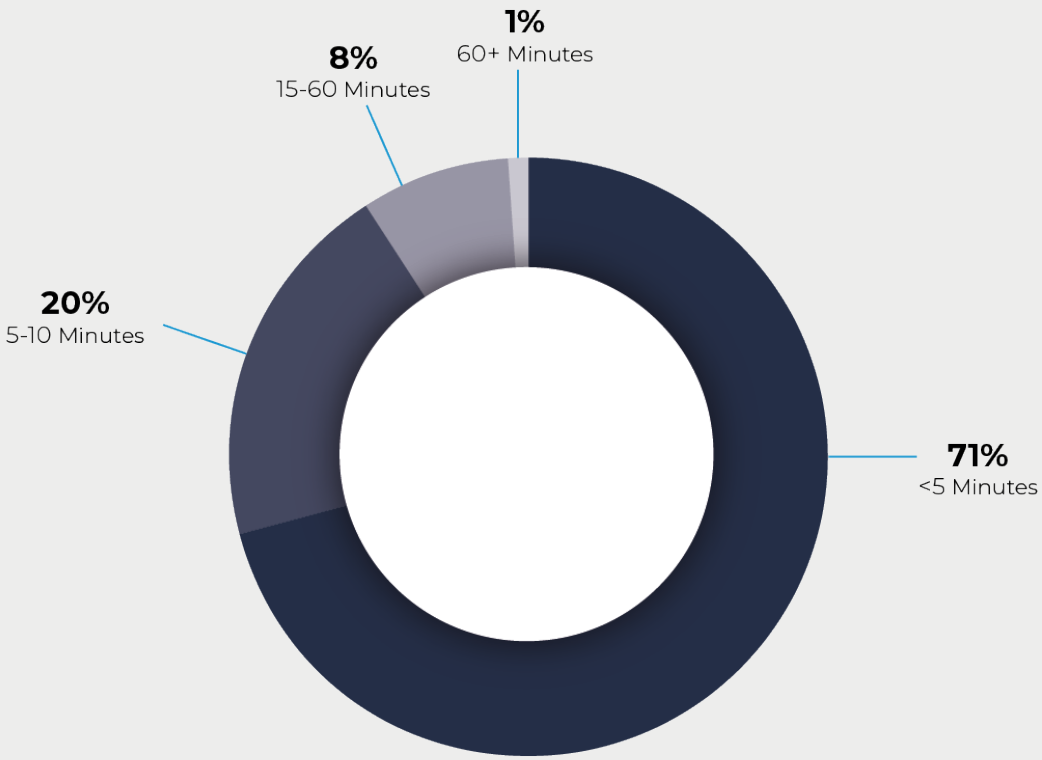
In the fourth quarter, the duration of attacks increased significantly again. The longest attack in 2022 was 1,695 minutes long, or 28 hours and 15 minutes, well above the longest DDoS attack in the same period last year. This was only 1,489 minutes, or 24 hours and 49 minutes.

This shows how changeable the attack landscape is. For example, while fast-onset "turbo attacks" predominated in the middle of the year, the fourth quarter of 2022 again saw longer-lasting multi-vector attacks.

Overview attack duration| 2021 vs. 2022



Overview attack duration 2022



Further analysis shows that the attacks‘ length varied from a few minutes to several hours. Most attacks (71%) lasted less than 5 minutes. One-fifth of all registered attacks (20%) were between 5 and 15 minutes long, and another 8% were up to 60 minutes long. Only about 1% of attacks were longer than 60 minutes.

Whether attacks are short or long is a question of the attack technique. On the one hand, hackers scan their target‘s IT infrastructure for vulnerabilities with lightning attacks on individual IP addresses. On the other hand, small and fast DDoS attacks are used in high frequency as a cover for parallel hacker attacks on servers and networks. However, behind this DDoS curtain, hackers can enter unnoticed through the back door. To defend against the DDoS attack, existing IT resources are mobilized in the shortest possible time to minimize system downtime and further damage.

Short attacks that are suddenly aborted often indicate that attackers could not reach their target. If the attacks bounce off well-protected infrastructures, the attackers usually retreat to conserve their resources. But they resort to long-lasting attacks if they want to permanently impair the targets and successfully cause damage.

Evolution of Attack Bandwidths

DDoS attacks: complex and powerful

The trend toward high-volume attacks that were already apparent in the same period of the previous year became more pronounced in the first six months of 2022. Even in the first half of the year, the bandwidth peak in a direct year-on-year comparison was above the values from 2021. While in 2021, the bandwidths measured by LSOC exceeded the 100 Gbit/s mark every month in the process, the chart below shows clear fluctuations in the further course of the year. In October and November 2022, the bandwidth peaks are even significantly below 100 Gbit/s.

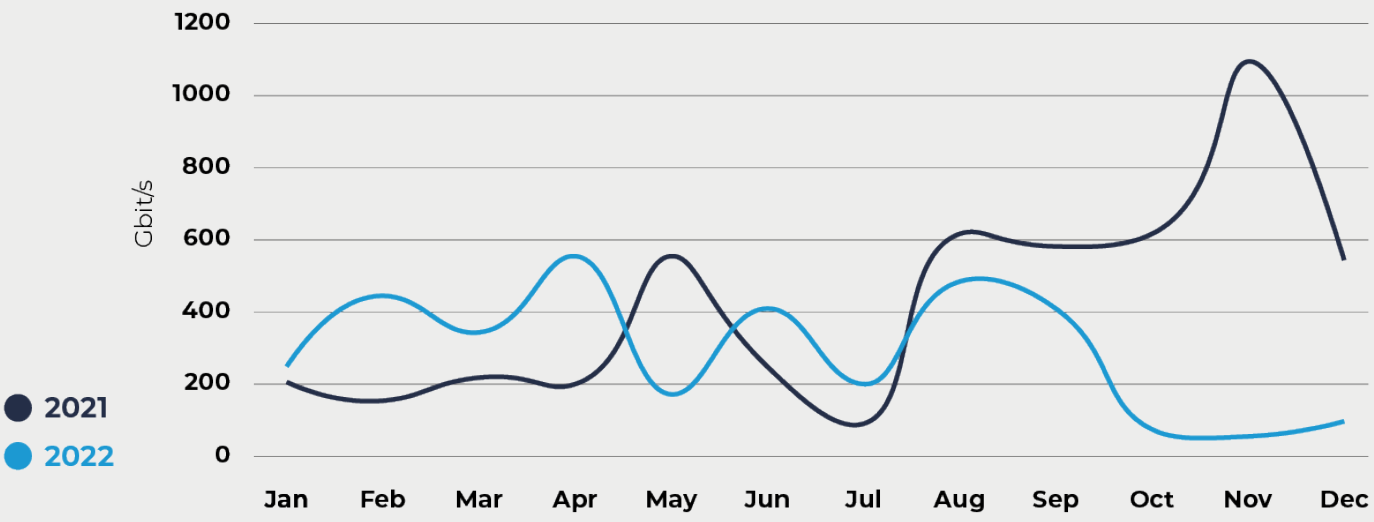
The largest attack in 2022 was stopped at 574 Gbit/s, which is very low compared to 2021. Between August 2021 and December 2021, bandwidths of high-volume attacks ranged from 546 Gbit/s to the highest single measured peak of 1.1 Tbit/s. In the fourth quarter of 2022, the largest DDoS attack was stopped at just 110 Gbit/s.

In contrast, the average total bandwidth has increased from 1.4 Gbit/s in 2021 to 2.6 Gbit/s. The reason for this is less "carpet bombing" in the attacks registered on the Link11 network. These technically complex DDoS attacks are difficult to detect because they have very low traffic per IP address. Instead of targeting a single IP address, attackers will divide the attack across a range of IPs within the same network with hundreds or thousands of addresses, which is almost impossible to mitigate for inadequately protected hosting and cloud providers. Often, protection solutions do not recognize this traffic as an anomaly.

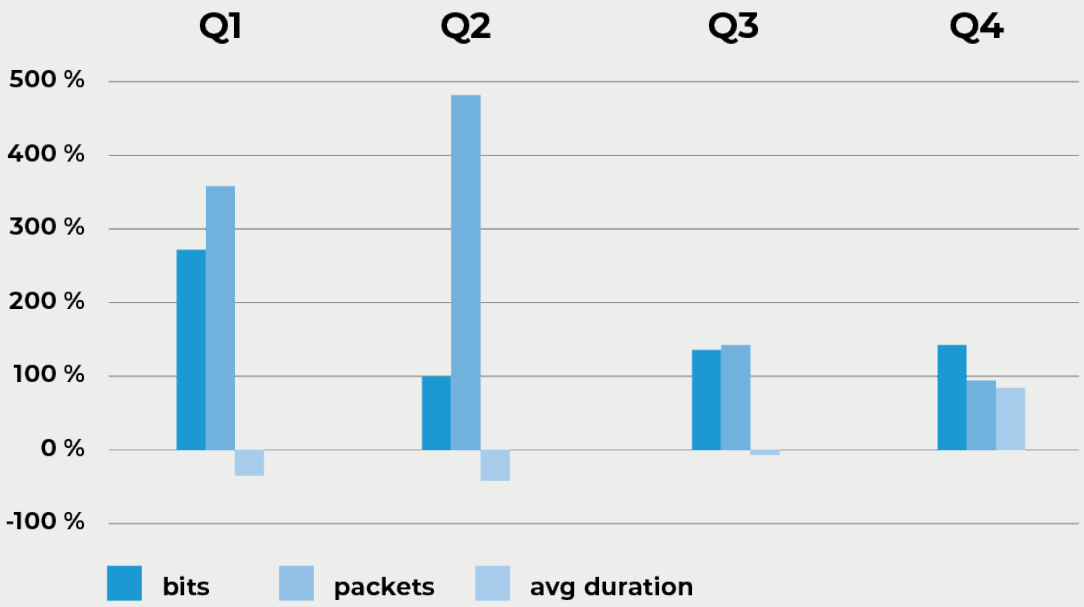
However, the increase in intensity is reflected not only in the increased average bandwidth but also in the volume in terms of the number of packets transferred. While the average number of packets per second was 3.3 million during the review period, the packet rate was significantly lower in 2021. In the attack case, only 990,000 packets per second were transmitted.

A look at the correlation between the duration and intensity of DDoS attacks reveals a change, especially for the first half of 2022: the attacks are simultaneously more intense and shorter. This shows that time is increasingly important in combating DDoS attacks. What is important is how quickly the attack is responded to, damage mitigation is started (time-to-mitigate), and how long it takes for everything to get back to normal (mean-time-to-repair). Link11 and other vendors' performance on this critical factor can be seen in the Frost & Sullivan study, *"The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough."*

Bandwidth peak per month | 2021 vs 2022



Change in duration and intensity of attacks



When protecting against increasingly focused and sophisticated attacks, precision and speed in detecting and stopping attacks are especially important. Once attackers have launched one of these sophisticated and dangerous DDoS attacks, there is only a very narrow window of opportunity to limit the potential damage. This is because protection solutions are tested, especially in the case of fast-occurring and intense attacks with large bandwidths and high packet rates.

Some on-premises systems can defend against simple and uncoordinated attacks. Primarily, protection covers network-type attacks (e.g., ICMP-UDP floods) at Layer 3 or 4, but more complex and particularly intense attacks can overwhelm devices.

In such a scenario, a time-to-mitigate of just one minute is not enough to avoid a complete system failure. Instead, it's a matter of analyzing traffic in real-time with cloud-based automated AI technology to fend off DDoS attacks in the shortest possible time.

”

Fast TTM is essential for critical infrastructure operators, and a hybrid system can provide the critical advantage - but only if it is regularly reviewed to ensure protection solutions are working effectively at all levels.

Jag Bains, Vice President Solution Engineering, Link11

Multi-Vector Attacks

Multi-vector attacks are becoming more complex

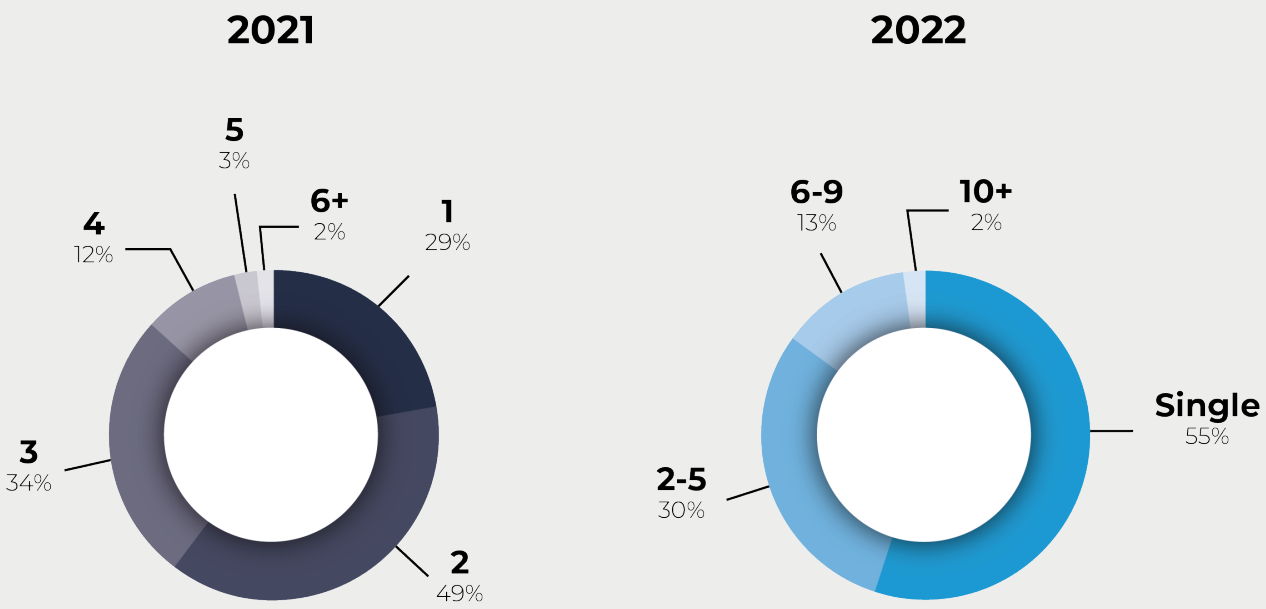
Multi-vector attacks are a particularly dangerous type of DDoS attack. Unlike traditional attacks that use only one attack vector, multi-vector attacks target multiple transport, application, and protocol vulnerabilities in parallel. In addition, using multiple attack vectors makes it more difficult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

Combining multiple techniques increases the likelihood of success for attackers, as many protection solutions are not up to date. It is, therefore, important to use protection solutions that work effectively against multi-vector attacks at all filtering levels.

In the first half of 2022, the share of multi-vector attacks decreased compared to the same period last year. While multi-vector attacks accounted for 71% of attacks in 2021, only about one-third (35%) were multi-vector attacks in the first six months.

Thus, implementing a specialized DDoS protection solution is advisable to ensure continuous monitoring and defense to protect against multi-vector attacks. Such a system can detect and defend against attacks in real-time to minimize the risk of prolonged downtime.

Number of single and multi-vector attacks | 2021 vs 2022



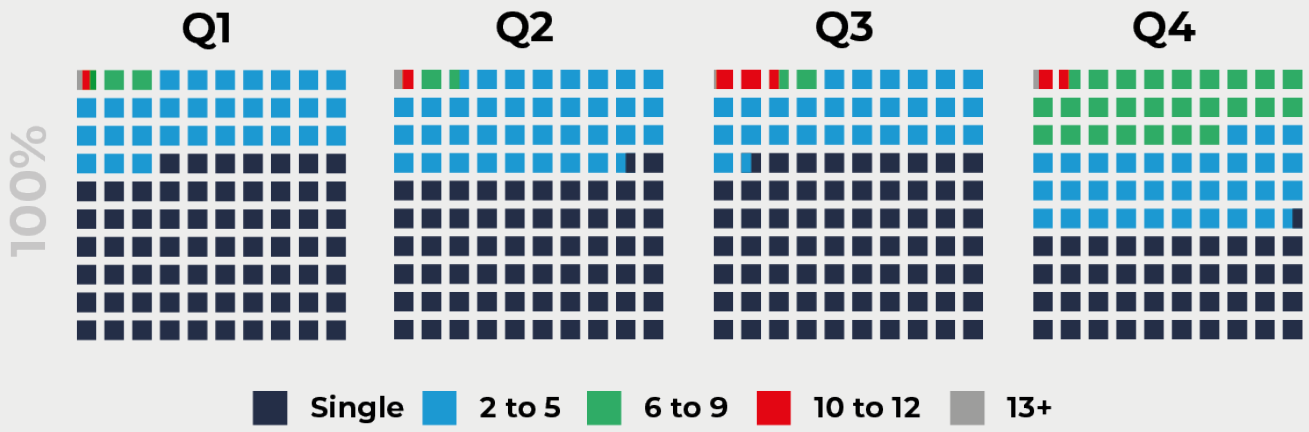
However, this trend did not continue in the second half of 2022. Instead, multi-vector attacks increased, especially in Q4. Overall, the percentage of multi-vector attacks increased to 45% from July to December 2022, with the most significant increase seen in Q4.

The highest number of concurrent vectors observed in the Link11 network was 18, the largest multi-vector attacks observed in Link11's network to date. In 2021, the number of vectors deployed simultaneously was only 12.

An attack with 18 different vectors can cause significantly greater damage. Multi-vector DDoS attacks are characterized by their ability to simultaneously attack multiple vulnerabilities in a system. As a result, the load on IT systems can increase enormously, leading to overload and ultimately prolonged downtime and complete failure in the worst case.

Thus, implementing a specialized DDoS protection solution is advisable to ensure continuous monitoring and defense to protect against multi-vector attacks. Such a system can detect and defend against attacks in real-time to minimize the risk of prolonged downtime.

Change in single and multi-vector attacks 2022



If IT security lags behind the threat landscape, it only takes a single vector that is targeted and concentrated to cause major damage.

Jag Bains, Vice President Solution Engineering, Link11

Reflection Amplification Attacks

New vulnerabilities despite known threats

Reflection amplification attacks are malicious multi-vector attacks that rely on exploiting misconfigured servers and services on the Internet. Instead of attacking the target directly, they abuse services such as DNS or NTP. There are many Internet services where sender verification is not supported or required. By forging the sender (also known as spoofing), an attacker tricks services into sending unsolicited responses to a target (reflection).

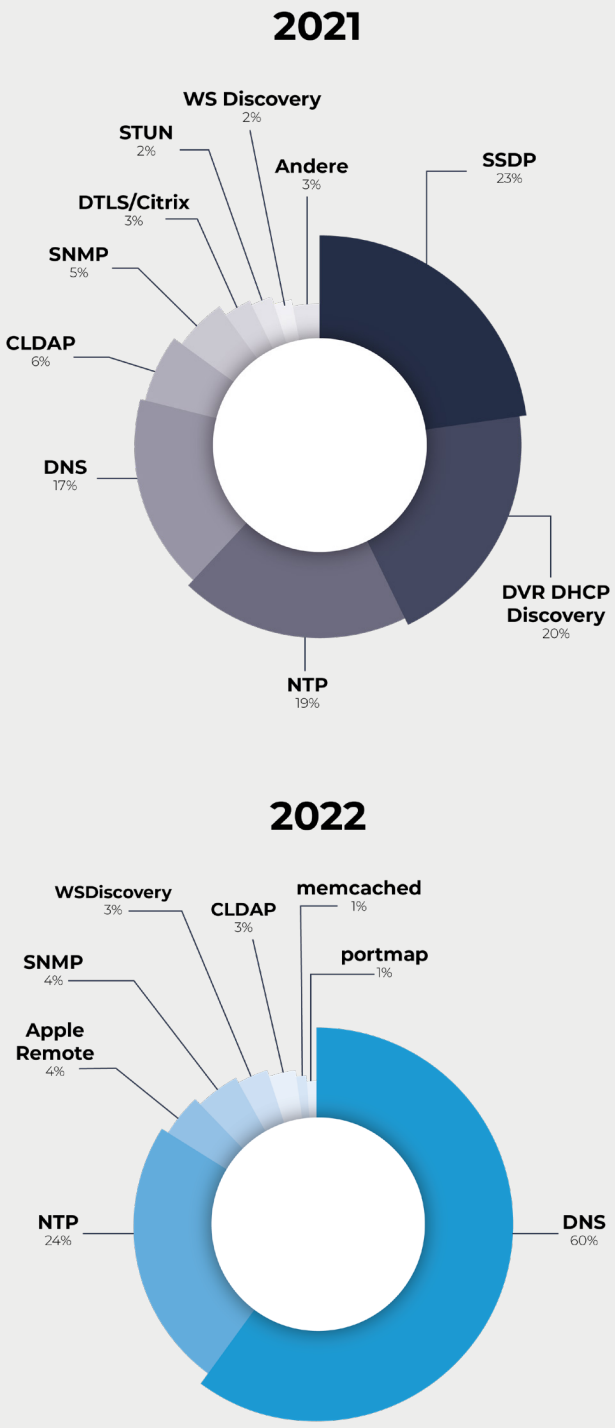
In doing so, attackers send small amounts of data to intermediary servers serving amplifiers. As a rule, attackers choose such services with many times larger responses than the actual request. Thus, they increase the amount of traffic sent. The abused servers mirror the requests and forward them many times, amplified (amplification) to the actual attack target.

In 2022, LSOC recorded a flood of amplification techniques. Many attack techniques, such as DNS Reflection Amplification and NTP Reflection Amplification, have been standard equipment for DDoS attackers since 2013. These techniques feature immense amplification, such as 100x amplification for DNS attacks and up to 200x amplification for NTP attacks.

Attackers constantly discover new vulnerabilities, such as inadequately protected Internet and open services. At the same time, most of the attacks during the period under consideration used already known and proven vectors. The Internet service most frequently exploited for attacks and abused as an amplifier in 2022 was DNS (60%), followed by NTP (24%), SNPM (4%), and Apple Remote (4%).

In 2022, there was a sharp increase in the popularity of DNS and NTP being used as amplifiers. DNS is one of the first and most frequently used protocols for this form of attack.

The most important reflection amplification vectors
2021 vs 2022



NTP (Network Time Protocol) synchronizes computer clocks over the Internet. NTP was first used about ten years ago and is still very powerful due to its large potential amplification factor. Within NTP, there is a function to return the last 600 hosts that polled the system. This response can be up to 200 times larger than the query that generated it. This means that an attacker can send 1 Gbps of spoofed requests, and the NTP servers will send the target up to 200 Gbps of unsolicited responses.

In contrast, compared to last year, Simple Service Discovery Protocol (SSDP), used for plug-and-play device discovery, and Connectionless Lightweight Directory Access Protocol (CLDAP), a connectionless directory protocol, no longer play a major role.

Attackers constantly exploit new vulnerabilities in Internet services and unprotected systems for 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.

One of the biggest gainers is Memcached, with a 50,000-fold gain. However, there is a new TCP middleware attack that has the potential to surpass this under certain circumstances. In theory, an August 2021 research paper showed that attackers could abuse middleboxes such as firewalls over TCP to amplify denial-of-service attacks with this amplification technique. The researchers also identified hundreds of thousands of IP addresses that amplify attacks hundreds of times using firewalls and content filters[31].

A well-functioning DDoS protection solution is essential as attacks become more advanced and evolve. Organizations must ensure that their protection measures are regularly updated to counter the latest threats. Good protection means responding quickly to attacks and mitigating them within the shortest possible time.

”

Attack methods continue to evolve, and cybercriminals are able to add increasingly sophisticated amplification techniques to their repertoire. With cloud-based and automated DDoS protection solutions, enterprises can keep pace.

Jens-Philipp Jung, Managing Director, Link11

Outlook

Cyber warfare: DDoS attacks as a strategic tool

DDoS attacks on critical infrastructure will become increasingly common in cyber warfare[32]. Unlike conventional wars, cyber warfare uses digital weapons such as viruses, malware, or DDoS attacks. As more and more information technologies are used everywhere, this way of waging wars is becoming increasingly important.

Cyber attacks, some of which are cost-effective, range from destroying computer networks to disrupting energy and transportation systems. The goal is to damage or cripple a country or company‘s infrastructure. Since the invasion of Ukraine, attacks have been recorded there and in various NATO countries in areas such as energy, banking and finance, and health.

The threat to German companies is great when hackers attack critical infrastructure. Although it is difficult for these attacks to reach control systems, the recent attacks are a worrying sign. They prove that Russian hacker groups in military service or intelligence agencies are ready to attack critical infrastructure. These attacks are expected to rise with increasing digitalization and further escalating geopolitical conflicts.

Head-to-head race between hackers and defenders

Volumetric DDoS attacks, one of the most widespread attack variants, have lost efficiency in the infrastructure sector. This is because the attacks, which flood a network exclusively with a lot of bandwidth, can be easily detected and defended against traditional DDoS protections. Nevertheless, due to politically motivated attacks, the threat level remains high, especially for critical infrastructure operators.

In the first half of 2022, the world‘s largest darknet platform, “Hydra-Market,” and providers of “booter services” offering DDoS-as-a-service were shut down. In the short term, this will reduce the number of attacks. However, the demand for DDoS attacks continues to grow. Therefore, it is not a question of if but only when criminal actors establish new platforms and eagerly make a new name for themselves.

Attackers are increasingly using artificial intelligence to improve their methods and attack types. As a result, the race between attackers and defenders is heating up. Intelligent and robust DDoS protection solutions like Link11‘s AI-powered, cloud-based solution can help defenders gain the upper hand in this race.

The *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 smarter, faster, and more secure.

But how does our AI handle AI-based attacks? Machine learning is a function of the amount of data it has access to. Our system can learn from hundreds of thousands of attacks every year. As the number of offensive AI systems increases, our training data will multiply accordingly, making our system smarter and faster and our protected systems more secure.

Cyber security standards tightened by new guidelines

Lawmakers worldwide are tightening cybersecurity standards and requiring full disclosure of security incidents under the threat of stiff penalties. On January 16, a new EU legislative package went into effect[33]. The revised “EU Network and Information Security Directive,”[34] or NIS2 Directive, is intended to increase the common level of security of network and information systems in the EU.

Like the first EU-wide cybersecurity legislation, NIS, NIS2 is intended to protect critical infrastructures from hacker attacks. The directive also aims to make management more accountable. However, it could be difficult for many German companies to comply by Fall 2024, as the requirements are considerable.

Regulation by the EU NIS2 directive is based on certain size criteria for companies. Medium-sized companies with 50 or more employees and a turnover of 10 million euros and large companies with 250 employees and a turnover of 50 million euros are affected by the regulation.

Small and micro businesses are typically not affected by the regulations, but some select companies may still be required to address cybersecurity risks in their supply chains. It is estimated that

80% of companies are unaware that they are affected by the “NIS2 Directive”.

Particularly strict requirements apply to sectors with high criticalities, such as energy providers, transport companies, Internet and cloud providers, banks, healthcare providers, space organizations, and public administration. In parallel, the EU is also introducing the Cyber Resilience Act, which contains specifications for the design of products “with digital elements” such as hardware and software. The draft EU NIS2 directive includes detailed regulations on reporting requirements, which can be punished with heavy fines of several million euros. Legislation modeled on the European data protection model (GDPR) is also being planned in Canada[35], with similar penalties.

The EU justifies its initiative by saying that digital infrastructure has become an important part of everyday life and cross-border exchanges, making cybersecurity more important than ever for the smooth operation of the single market.

Sources

[1] https://www.cas-crm.com/about-us/news-events/news/news/article/digital-office-index-2022-how-digitally-do-german-companies-work.html?cHash=8b44b412e6efd846023023025255 72fe67

[2] https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

[3] https://www.emcrc.co.uk/post/killnet-declare-war-on-the-uk-and-nine-other-nations

[4] https://zero.bs/ddos-as-attackvector-for-state-sponsoredhacktivist-groups-in-times-of-crisis.html#evolution_of_killnet

[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[6] https://www.nbip.nl/en/news/ddos-attacks-q4-2022/?utm_campaign=General&utm_content=LinkedIn&utm_medium=social&utm_source=LinkedIn

[7] https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/

[8] https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

[9] https://krebsonsecurity.com/2022/12/six-charged-in-mass-takedown-of-ddos-for-hire-sites/

[10] https://hackernoon.com/has-solana-encountered-another-ddos-attack

[11] https://therecord.media/ddos-attacks-on-andorras-internet-linked-to-squid-game-minecraft-tournament/

[12] https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/

[13] https://thebarentsobserver.com/en/security/2022/02/anonymous-takes-down-websites-defense-ministry-rt-and-kremlin

[14] https://www.cshub.com/attacks/news/iotw-ukraine-suffers-15-hour-internet-outage

[15] https://news.err.ee/1608559405/finnish-defense-and-foreign-ministries-hit-by-cyberattack

[16] https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/

[17] https://www.reuters.com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/

[18] https://www.bloomberg.com/news/articles/2022-05-06/german-government-sites-hit-by-pro-russian-hackers-spiegel-says

[19] https://www.hackread.com/pro-iran-altahrea-hit-port-of-london-website-ddos-attack/

[20] https://thebarentsobserver.com/en/security/2022/06/pro-russian-hacker-group-says-it-attacked-norway

[21] https://cryptoslate.com/tether-confirms-ddos-attack-on-tether-io/

[22] https://edition.cnn.com/2022/07/08/politics/congress-website-disrupted/index.html

[23] https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144

[24] https://www.reuters.com/world/middle-east/iran-says-it-foiled-cyberattack-central-bank-2023-01-06/

[25] https://www.pokernews.com/news/2022/09/pokerstars-ddos-attack-caused-wcoop-outage-rescheduled-42164.htm

[26] https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks

[27] https://www.financemagnates.com/forex/swissquote-confirms-massive-ddos-attack-works-on-solution/

[28] https://www.bleepingcomputer.com/news/security/pro-russian-hacktivists-take-down-eu-parliament-site-in-ddos-attack/

[29] https://www.bleepingcomputer.com/news/security/massive-ddos-attack-takes-russia-s-second-largest-bank-vtb-offline/

[30] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet
https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/
https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

[31] https://www.usenix.org/conference/usenixsecurity21/presentation/bock

[32] https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape

[33] https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[34] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[35] https://www.torys.com/our-latest-thinking/publications/2022/12/data-protection-enforcement

Contact

Link11 GmbH
Lindleystr. 12
60314 Frankfurt