LINK11

DDOS REPORT

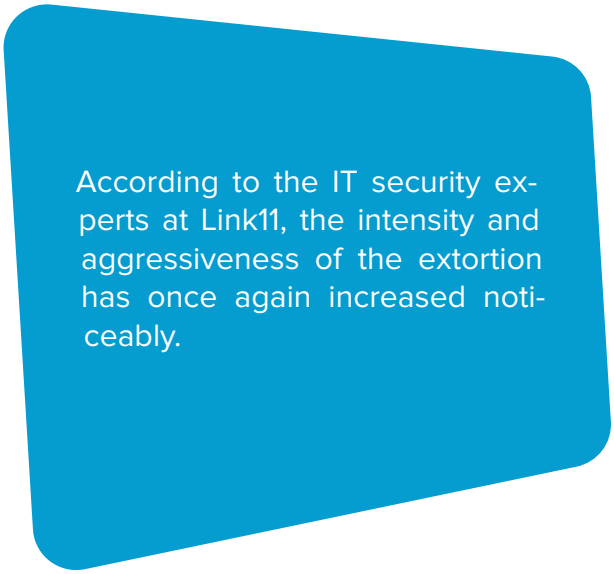
full year 2021

Table of Contents

Introduction and Summary	03
DDoS in the News	04
1st Half Year	04
2nd Half Year	05
Development of Total Numbers in the Link11 Network	06
Evolution of Attack Bandwidths	07
Multi-Vector Attacks	08
Reflection Amplification Attacks	09
Multiple Waves of DDoS Extortion	10
DDoS as a smokescreen to prepare for a data breach	11
Attacks From the Cloud	12
What We Will See More of in the Future	13
Sources	14

Introduction and Summary

Our everyday world is becoming more and more digital. The same applies to the private sphere, business, and industry. At the same time, **cybercrime** is increasing rapidly as a result of global networking across company and national borders. Data is stolen, entire systems are paralyzed, and ransoms are demanded. In October 2021, the German **Federal Office for Information Security** (BSI) declared a red alert due to increasing cyber-attack threats. The German digital association Bitkom is also concerned because cyber-attacks are not only becoming more international, but also more professional. For companies in particular, cyber threats are among the greatest risks. According to a **Bitkom** cybersecurity study published in August 2021, the damage to the German economy alone is valued at more than **220 billion euros**. As the second-biggest threat after infection with malware, **DDoS attacks** harmed 27% of companies. This is a rising trend. [1]



In 2021, a year that continued to be impacted by the Coronavirus pandemic, the Link11 Security Operation Center (LSOC) reported a 41% year-over-year increase in the number of attacks for the full year, up from the 33% increase reported in the H1 2020 to H1 2021 comparison period. Among these, **high-volume attacks** increased significantly. The average bandwidth peak over the past twelve months was 437 Gbps. The highest attack bandwidth measured on the Link11 network was over 1 Tbps, adding up to over 4.5 Tbps of volume on the same customer in just under 2 hours. At the same time, so-called **“carpet bombing”** attacks developed into a major challenge for hosting and cloud providers, ISPs, and carriers. In these technically complex attacks, the traffic per IP address is so low in contrast to the high-volume attacks that many protection solutions don’t recognize them as an anomaly. The attacks often fly under the radar and are difficult to mitigate. In addition, the attacker does not direct DDoS traffic to a specific system or server. It’s not just one IP address that is attacked, but an entire network block with several hundred or thousand addresses.

In addition to under-the-radar attacks, complex **multi-vector attacks** continue to rise. Multi-vector attacks target vulnerabilities at the transport, application, and protocol levels in parallel. The more vulnerabilities and protocols attackers abuse in an attack, the more difficult it is to detect and defend against the attack. The use of this methodology has increased from 59% of all attack types in 2020 to 71% in 2021. This means that multi-vector attacks have reached a new high.

In addition, **Ransom DDoS** strengthened as a trend in 2021: more and more cybercriminals are demanding ransom money in DDoS attacks. According to the IT security experts at Link11, the intensity and aggressiveness of the **extortion** has once again increased noticeably. The extent far exceeds the many cybercriminal DDoS activities observed so far in the protection of numerous customers in recent years. During a series of attacks on VoIP providers in North America, attackers demanded ransoms of up to $4.5 million in **Bitcoin**. Link11 believes this trend could also be amplified by the fact that **DDoS attacks** were often used as **smokescreens** last year. In the slipstream of a massive DDoS attack, hackers can infiltrate and attack network security through the back door and remain undetected. DDoS attacks drastically alter traffic profiles and create noise that masks, for example, a **data breach** that is the real target of these attacks. This makes a comprehensive and targeted risk analysis all the more important to identify the right security tools.

DDoS in the News

1st Half Year

January 30, 2021

Digital TV unavailable in Iceland

Icelandic telecom provider Siminn's streaming TV service was unavailable on a Saturday night and even more so during the pandemic. After about two hours, the DDoS attack was stopped and the service was again accessible. [2]

February 18, 2021

Internet outages across Austria

The fixed-line Internet of telecommunications provider A1 experienced a two-hour outage across the country, which was problematic when people were working at home because of the pandemic. DDoS attacks were to blame; they caused a routing problem. [4]

May 4, 2021

State institutions offline in Belgium

The services and websites of more than 200 state organizations and institutions in Belgium were digitally unavailable for several hours. This was triggered by attacks on the ISP Belnet, which provides the network for the Belgian government, among other things. [6]

June 9, 2021

Widespread power outages in Puerto Rico

The lights went out for slightly more than 700,000 residents in the Caribbean nation after a DDoS attack hit the utility. A substation went up in flames just hours later. [8]

January – March 2021

Vaccination portals disrupted by attacks worldwide

Reports of cyber-attacks on vaccination portals increased in several countries including the UK, Germany, and the US. The websites used to book COVID-19 vaccination appointments were overloaded by DDoS attacks. [3]

March 8, 2021

Parliament website offline in Italy

The institutional website of the Chamber of Deputies, which along with the Senate makes up the Italian Parliament, was down for over a day. The perpetrators behind the DDoS attack and their motives remained unclear. [5]

May 18, 2021

ISPs in Ireland targeted

In the first half of May, numerous ISPs in Ireland – including Blacknight, one of the country's largest web hosting providers – were the target of DDoS attacks. The attacks resulted in numerous outages lasting several hours. The attacks were often accompanied by DDoS extortion. [7]

DDoS in the News

2nd Half Year

September – November 2021

Series of attacks on international VoIP providers

Between September and November, several international VoIP providers were attacked. These included international industry giants Bandwidth, VoIP.ms, and Telnyx. For days, the attacks knocked out the services of the service providers. The hacker group REvil was responsible for a large part of the attacks and demanded up to $4.5 million in ransom. [9]

September 12, 2021

Meris botnet record attack paralyzes Russian internet giant

Russian Internet giant Yandex was the target of a massive DDoS attack consisting of up to 21.8 million requests per second. The largest attack on the Russian Internet to date, RuNet, was initiated by the novel botnet Meris. It is believed that the requests originated from up to 250,000 compromised Ethernet-connected computers. [10]

September 13, 2021

No online banking in New Zealand

Victims of a widespread DDoS attack included New Zealand banks, the national weather service, and the country's postal service and police. Access problems, Internet banking outages, and card payment problems occurred over a period of days. [11]

October 8, 2021

Educational portals in Switzerland offline for days

The targeted and massive attack on IP addresses hit the Swiss Service Center for Vocational Education (SDBB) with full force. For almost two weeks, several education platforms in Switzerland were unavailable. [12]

November 23, 2021

Alternative Spanish media victims of targeted hacker attacks

Spanish alternative media La Marea and El Salto became victims of a hacking campaign against the left and alternative media that started in mid-November. The websites completely collapsed due to the L7-type DDoS attack, which enormously increases page views. [13]

December 15, 2021

The Hague's computer systems unreachable

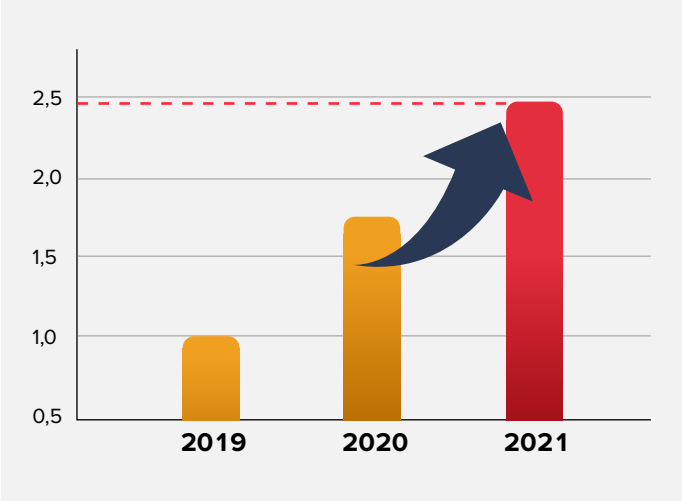
The computer systems of the city of The Hague were overloaded with traffic to such an extent that the municipality's services became inaccessible. [14]

Development of Total Numbers in the Link11 Network

New Work, New Life, and DDoS attacks continuing to rise

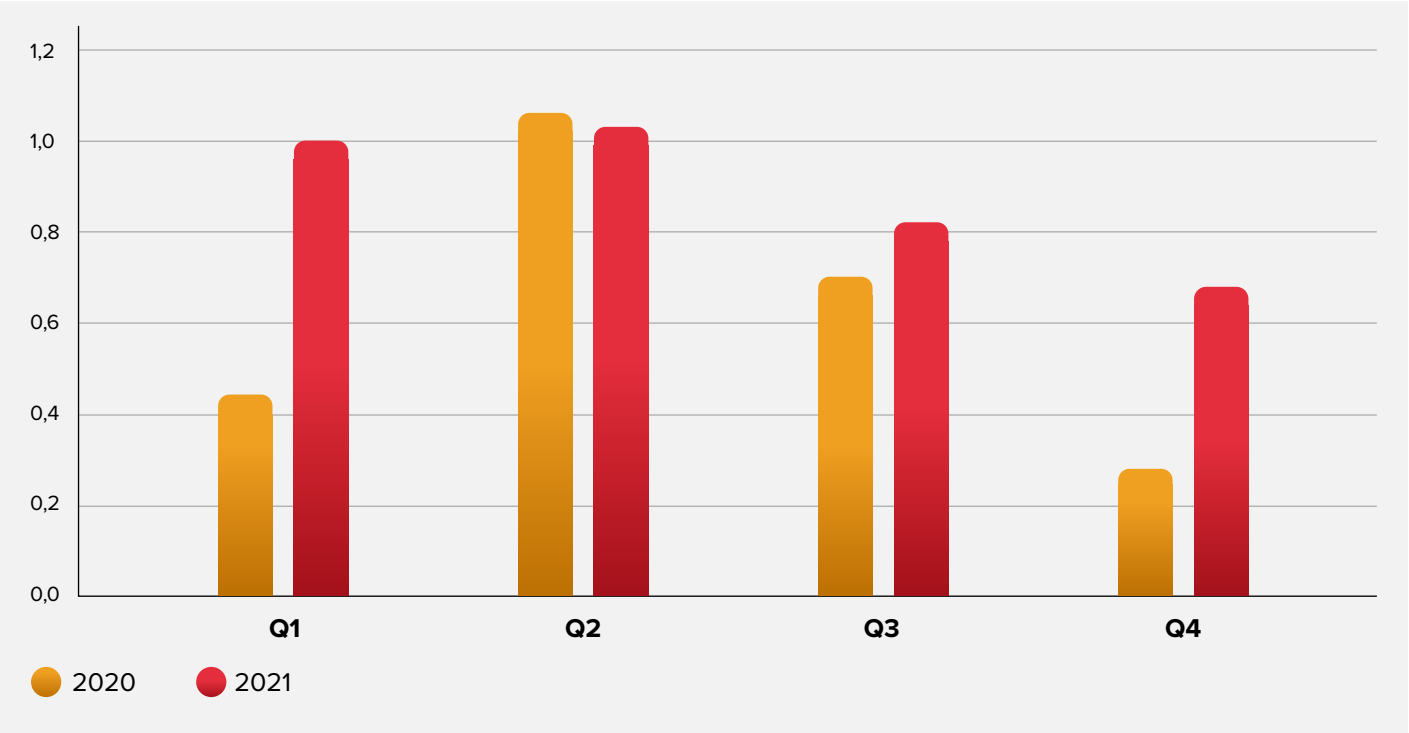
Since the beginning of the Coronavirus pandemic, a great deal of our lives has taken place online. Professionals worldwide have multiple video conferences a week. Microsoft Teams alone was used by 145 million people around the globe in April 2021 – 113 million more people than in March 2020. [15] Working via VPN access in the home office is now standard at many companies and could remain at a high level, according to Corona. E-learning, e-commerce, e-government ... more and more applications and services are being used digitally. The consequences: data traffic continued to increase in 2021, as announced by the world's leading Internet node operator, DE-CIX Frankfurt. In total, more than 38 exabytes of data have been exchanged, which corresponds to an increase of almost one-fifth (20%) compared to the previous year. With such a data volume, about 18,000 people could stream HD video for a lifetime. [16]

Relative Development DDoS Attacks 2019 – 2021



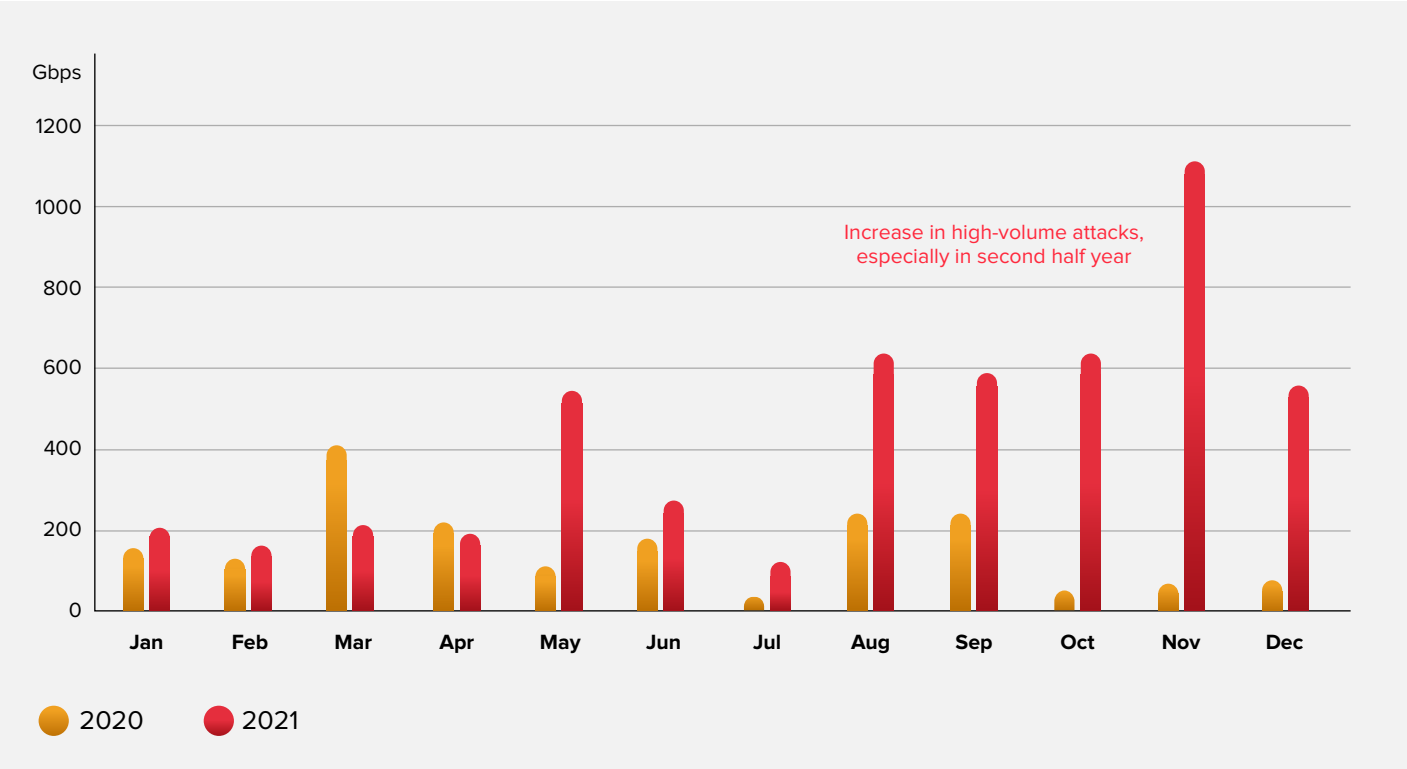
It's no coincidence that in an increasingly interconnected world, threat surfaces are increasing and, as a result, DDoS attacks are at an all-time high. The number of attacks registered on Link11's network in 2021 was again significantly higher than the same period last year. The 2021 vs. 2020 increase amounted to 41% in total. Compared to the same period last year, more than twice as many (108%) attacks occurred in Q1 2021, and nearly 2.5 times (148%) more attacks occurred in Q4 2021 than in the same period in 2020, despite a decrease compared to H1 2020. In addition to international hosting providers, banks, vaccination portals, learning platforms, and public institutions were also affected by DDoS attacks. There were also significantly more ransom DDoS attacks and higher ransom demands. According to the annual report of the European Organized Cybercrime Law Enforcement Agency (IOCTA), more advanced techniques and the relative ease of implementing DDoS attacks led to a 300% increase in ransomware attacks compared to 2019 and 2020. [17]

Relative Number DDoS Attacks Q1 – Q4, 2020 vs. 2021



Evolution of Attack Bandwidths

Bandwidth Peak per Month



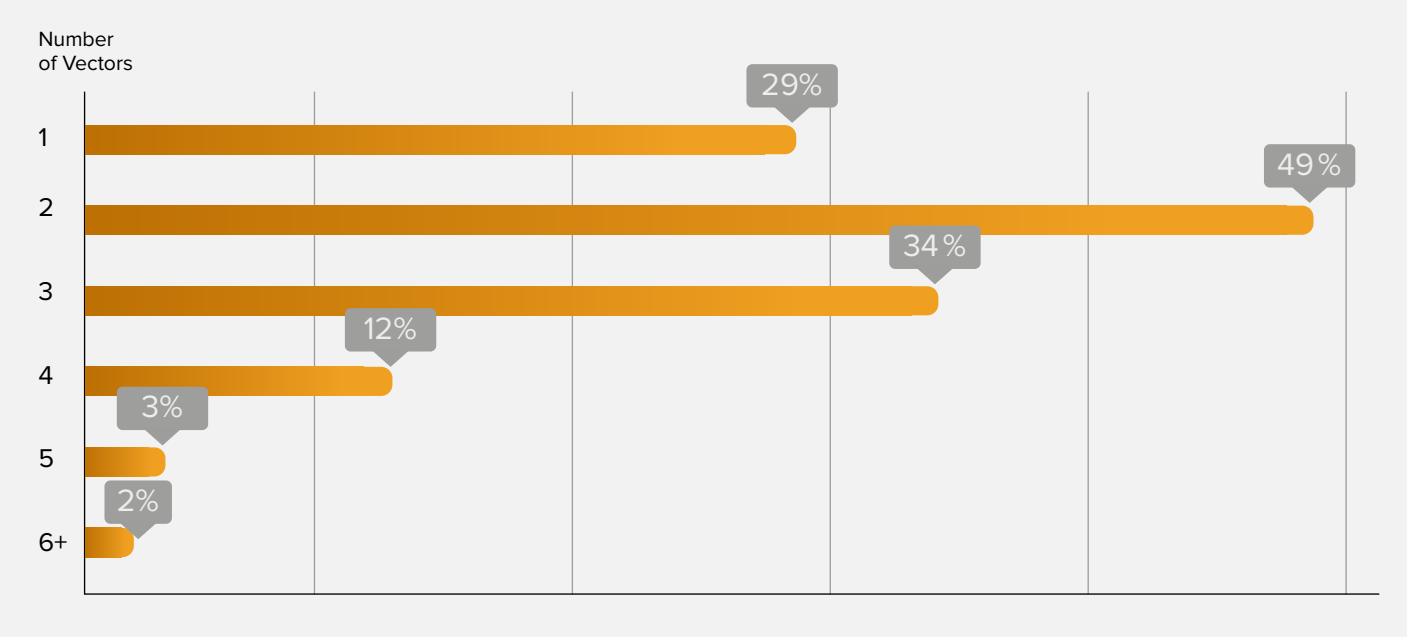
A massive increase in high-volume attacks

High-volume attacks increased significantly in 2021. In the past twelve months, the average bandwidth peak was 437 Gbps; in 2020, the attack bandwidth per month averaged 161 Gbps. In ten of the twelve months, the attack bandwidth of DDoS attacks exceeded the comparative figures from 2020, with bandwidths measured by LSOC exceeding the 100 Gbps mark every month. Especially in the second half of the year, Link11 recorded numerous high-volume attacks in the network. Between August 2021 and December 2021, high-volume attack bandwidths ranged from 546 Gbps to the highest single measured spike of 1.1 Tbps. The new and massive Meris botnet, named after the Latvian word for plague, may have been one of the factors responsible for the increase in high-volume attacks. Cybersecurity experts estimate that around 250,000 devices worldwide were compromised. Thus, Meris manages to disrupt even very robust networks through a large number of requests per second (RPS). Unlike the legacy Mirai DDoS malware, Meris relies on specialized modules that launch volumetric attacks instead of bandwidth-only attacks. [18]

In contrast, the average total bandwidth fell from 1.5 Gbps in 2020 to 1.4 Gbps in 2021 due to the increase in so-called “carpet bombing”. See the section “Carpet Bombing” on page 13.

Only a high-performance IT security solution can help defend against DDoS attacks from powerful botnets like Meris.

Shares of Single- or Multi-Vector Attacks



Complex multi-vector attacks on the rise

In recent years, the complexity of DDoS attacks has grown increasingly, according to LSOC's observations. Multi-vector attacks with at least two different attack vectors dominate. These target vulnerabilities at the transport, application, and protocol levels in parallel. The more vulnerabilities and protocols attackers abuse in an attack, the more difficult it is to detect and defend against the attack. All the individual vectors must be identified to detect a pattern. Such multidimensional attacks, therefore, mean that several attacks are running simultaneously. Their share increased from 59% in 2020 to 71% in 2021, reaching a new high. In this methodology, where attackers combine multiple techniques, the probability of success for the attackers increases. This is because the protection solutions widely available on the market are often not up to date, and their patch and update cycles lag behind the threat landscape. To reliably secure corporate IT, it is critical to rely on protection solutions that work effectively at all filter levels of multi-vector attacks. Attackers relied on a single vector for just under one-third (29%) of attacks in 2021. The highest number of simultaneously deployed vectors observed in the Link11 network was 12.

> **"Fighting multi-vector attacks is like fighting the Hydra: mitigate one vector, and you find it replaced by two more. In the future, be on the lookout for even more varied and complex multi-vector attacks and prepare for them as best you can.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

Reflection Amplification Attacks

What are reflection amplification attacks?

Reflection amplification attacks are a class of multi-vector attack that similarly exploit various misconfigured open servers and services on the Internet. The target system is not attacked directly, but services such as DNS or NTP are misused for this purpose. The attacker first sends small numbers of data packets to the intermediate servers, which act as amplifiers. They mirror the requests (reflection) and forward them, amplified many times, to the actual attack target.

New vectors appear on the scene

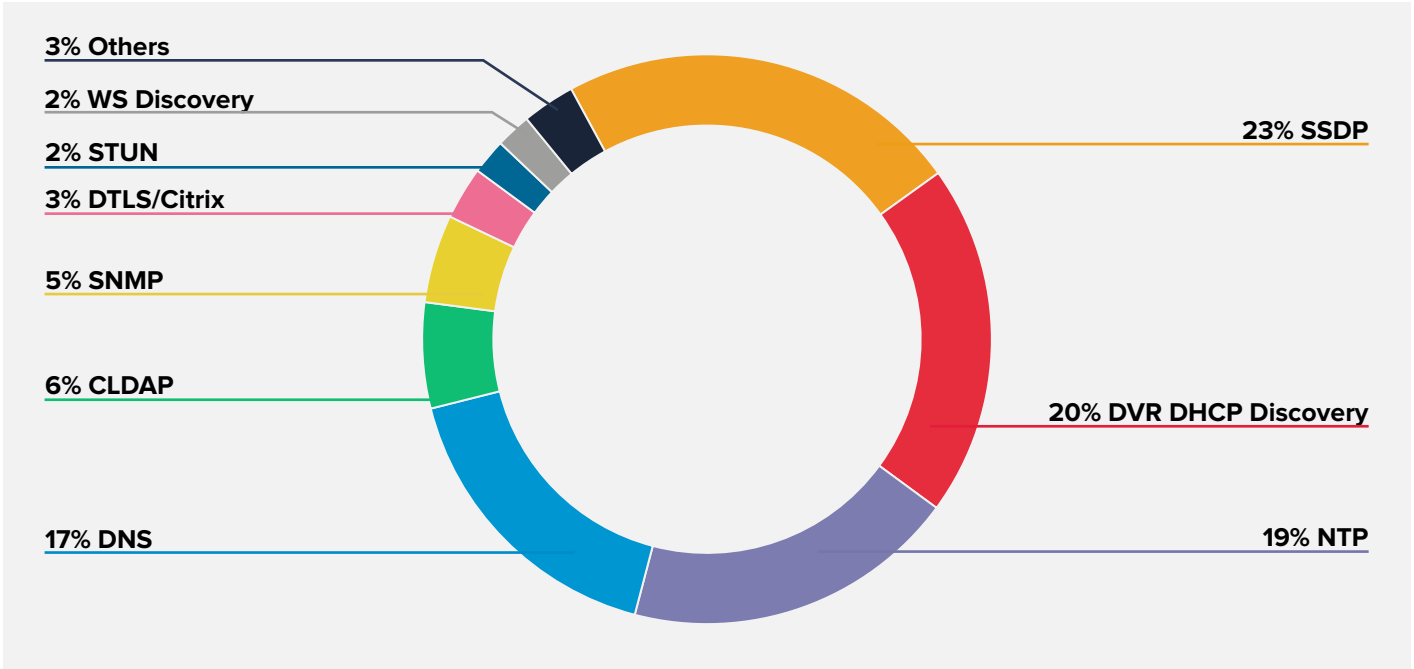
The first reflection amplification vectors appeared in 2013 and involved DNS and NTP. Since then, the range of vectors has grown much wider. Currently, there are over 20 techniques, including memcached reflection amplification and CLDAP. In the first half of 2021, LSOC identified new vectors through its global network and AI-based mitigation technology: Datagram Transport Layer Security (DTLS) via Citrix Netscaler and Session Traversal Utilities for NAT (STUN). DTLS is designed to allow encrypted data to be transmitted not only over secure, connection-oriented transport protocols such as TCP but also over connectionless UDP. A STUN server ensures that end devices such as computers or VoIP telephones, which are hidden behind a router or firewall in the local network, can communicate with VoIP providers on the Internet. Attackers are constantly discovering new vulnerabilities such as inadequately protected Internet services and open services. At the same time, most of the attacks in 2021 used already known and proven vectors.

The Internet service most frequently exploited for attacks and misused as an amplifier in 2021 was SSDP (23%), followed by DVR DHCP Discovery (20%), NTP (19%), and DNS (17%).

Earlier this year, DVR DHCP discovery attacks were the most widespread reflection amplification attacks. This protocol is used for network management of DVR recorders. In the second quarter, DNS was the most important protocol for amplification attacks. DNS is one of the first and most frequently used protocols for this form of attack. SSDP and NTP caused the most reflection amplification attacks in the second half of the year. Simple Service Discovery Protocol is used for plug-and-play device discovery. Network Time Protocol is used for time synchronization between devices.

Even though their potential for abuse has been long recognized, the vulnerabilities are inadequately patched. This makes it all the more important to ensure that the DDoS protection solution used is generally capable of detecting new, previously unknown attack vectors and defusing them within a few seconds.

Top 10 Reflection-Amplification-Vectors



Multiple Waves of DDoS Extortion

Extortion attacks continue to increase in 2021

Since the beginning of 2021, repeated and ever-increasing waves of DDoS extortion attacks have also created a tense threat situation. Blackmail emails with changing senders such as Fancy Bear, Lazarus Group, or Fancy Lazarus have targeted companies with ever-increasing frequency. Instead of being indiscriminate, ransom demands now vary depending on the size of the company and the industry the victims operate in. In fact, throughout the year, companies from a wide range of industries (including finance, e-commerce, media, and logistics) were affected. Between September and November, several international VoIP providers were attacked. Among them were international industry giants Bandwidth, VoIP.ms, and Telnyx. For days, the attacks knocked out the services of the service providers. The hacker group REvil was responsible for a large part of the attacks and demanded ransoms of up to $4.5 million. [9]

According to the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), the payment of ransom money may even be declared illegal in the United States. The reason for this is that the criminal proceeds could fund activities that run counter to the national security and foreign policy goals of the United States. Moreover, the statement said, ransom payments in no way guarantee that stolen data will be returned. For U.S. companies affected by DDoS extortion, the situation is twice as bitter. [19]

According to Link11's IT security experts, the intensity and aggressiveness of the extortions have increased noticeably. The scale far exceeds the many cybercriminal DDoS activities observed so far in the protection of numerous customers in recent years. With each passing day, more companies are reporting that they are unable to withstand the DDoS warning attacks and are experiencing severe outages and seeking protection via short-term emergency integrations. Costly business interruptions, production losses, data losses, and lengthy restorations of systems are sometimes the result.

The DDoS extortionists' approach

The criminals gather information about the company's IT infrastructure in advance and provide clear details in the extortion e-mail about which servers and IT elements they will attack for the warning attacks. As leverage, the attackers launch demo attacks, some of which last several hours and are characterized by high volumes of up to 200 Gbps. To achieve these attack bandwidths, which are generally only withstood by dedicated protection solutions from specialized protection providers, the attackers use reflection amplification vectors such as DNS. If the demands are not met, massive high-volume attacks of up to 2 Tbps are imminent. The company has seven days to transfer the Bitcoin to a specific Bitcoin wallet. The EU law enforcement agency Europol has also increasingly observed cybercriminals launching smaller DDoS attacks and showing the damage they can do before threatening larger attacks and making ransom demands.

LSOC's observation of the perpetrators has shown that companies that use professional and comprehensive DDoS protection can significantly reduce their downtime risks. As soon as the attackers realize that their attacks are going nowhere, they stop them and withdraw.

DDoS as a smokescreen to prepare for a data breach

Just before Christmas 2021, 3.7 million customer data from the U.S. digital appointment and calendar service FlexBooker surfaced on a hacker forum. A group of cybercriminals calling themselves the “Uawrongteam” traded the stolen data, including email addresses, names, phone numbers, and password hashes, and credit card information, on the dark web. According to reports from FlexBooker, a massive DDoS attack on the Amazon AWS server enabled the data theft. Only after working through the DDoS attack with Amazon did the digital calendar service discover that more than three million customer records had been stolen. [20]

DDoS attacks as diversionary tactics are not new. At the same time, they are not usually an inherent part of such data theft. However, in the slipstream of a massive DDoS attack, hackers can penetrate and attack network security through the back door undetected.

DDoS attacks drastically alter traffic profiles and create noise that obscures the data exfiltration, which is the real goal in these attacks. The intrusion detection systems and intrusion prevention systems (IDS/IPS systems) needed to detect and prevent data theft are extremely sensitive to DDoS attacks. Because they need to perform computationally expensive checks on every packet in and out, they are one of the first systems to be overwhelmed by a DDoS attack.

> **“It’s best to additionally protect your intrusion detection systems and intrusion prevention systems (IDS/IPS systems) with a cloud-based DDoS defense service.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

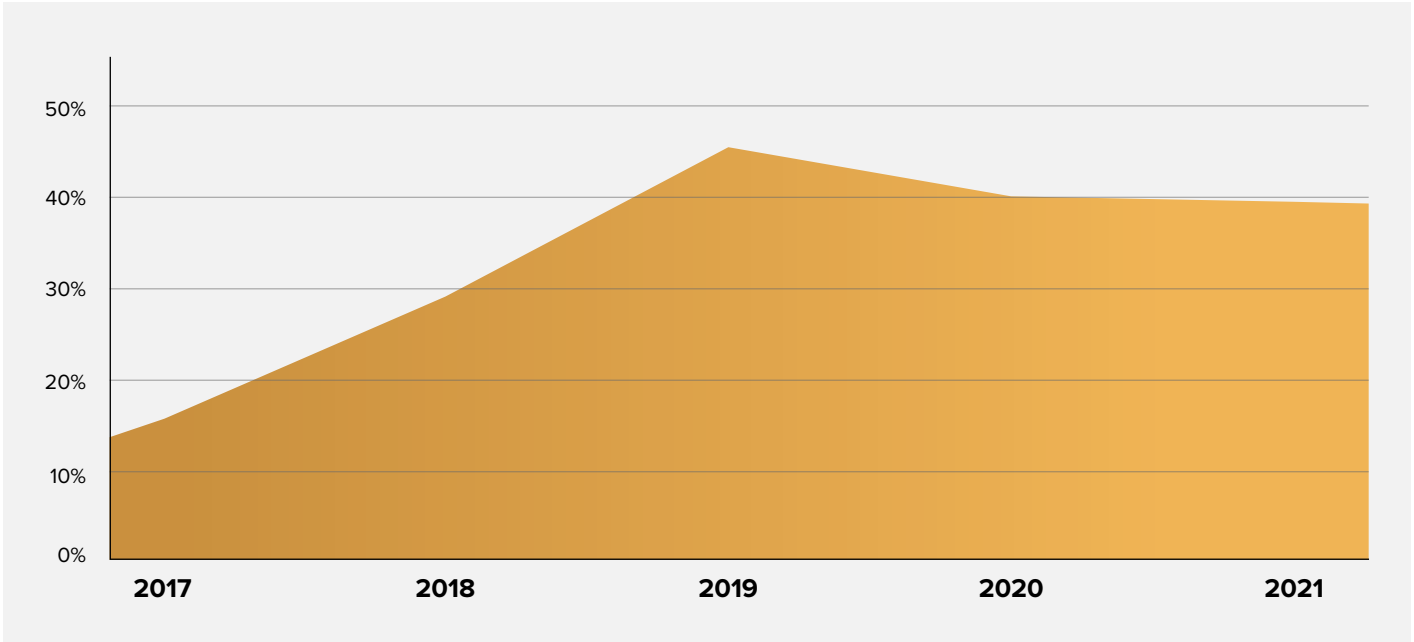
To defend against the DDoS attack, existing IT resources are mobilized in the shortest possible time to minimize system downtime and further damage. This means that IT managers are primarily concerned with defending against the attack and restoring normal operations. Since DDoS attacks also result in prolonged outages, the potential financial losses or reputational risks for companies can be considerable.

If a massive DDoS attack like the one reported by FlexBooker occurs, all possible defense mechanisms and security measures are initiated immediately. The outages associated with DDoS attacks torture normal business operations and require a prompt solution. If the big picture is missed in the rush of action, or the possibility of a multi-layered attack is ignored, the damage to the business can be significantly greater. The range and impact of DDoS attacks have increased continuously in recent years. Attacks in which DDoS is used as a smokescreen in particular show that the danger is becoming even greater. It is therefore all the more important for companies to take these security risks seriously and create a strategic plan to detect and defend against DDoS attacks. The faster and more accurately DDoS attacks are detected and defended against, the more time IT staff will have to track down other anomalies and threats in the network.

Cloud as an established attack tool

Cloud usage in the private and corporate environment is growing steadily. Cloud providers are expanding their infrastructures accordingly. DDoS attacks from cloud resources misused for this purpose to generate corresponding bandwidth and computing power have now become firmly established. In LSOC analyses of the use of cloud servers in DDoS attacks in 2017, the proportion was 16%. In the long-term view, the share of DDoS traffic routed through abused cloud servers has steadily increased and is now established at a level of 40-45%, with monthly peaks of up to 56%. This means that over one-third to one-half of DDoS attacks in 2021 used the cloud as an attack tool. The attackers compromised the server instances of public cloud service providers by gaining access via vulnerabilities or exploits. They then played a pre-written script that turned the server into a DDoS bot within minutes. The companies that have rented the instances usually don't notice this third-party access, or only very late, when the bill arrives. In addition, criminals gain access via stolen credit card data and rent cloud instances under a false name. The perpetrators use a wide variety of public cloud service providers for their attacks. Most frequently, abused servers were registered with the three major international providers: Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. In addition, the attackers also used cloud offerings from the B2B sector such as Oracle Cloud, DigitalOcean, and IBM Cloud.

Share of Cloud Abuse



What We Will See More of in the Future

Carpet Bombing

Carpet bombing attacks can become a major challenge for hosting and cloud providers. These attacks are technically complex. The traffic per IP address is so low that many protection solutions do not detect it as an anomaly, which means that attacks often fly under the radar. In addition, the attacker does not direct DDoS traffic to a specific system or server. It is not just one IP address that is attacked, but an entire network block with several hundred or thousand addresses. Insufficiently protected, it is almost impossible for hosting and cloud providers to mitigate “carpet bombing”.

According to LSOC’s assessment, this form of attack has reached a new level of quality.

Complex attacks require intelligent solutions

Attack techniques that attack the volume layer as well as the network and application layers are becoming increasingly sophisticated. Complex and combined forms of attack make it difficult for companies to defend against them. Off-the-shelf protection solutions whose patch and update cycles lag behind the threat landscape cannot keep up. Instead, companies should rely on systems with multi-layered anomaly detection and networked security mechanisms.

Precision in detection and speed in mitigation via intelligent, adaptive systems are key success factors.

DDoS as a smokescreen

In the slipstream of a massive DDoS attack, hackers can penetrate network security unnoticed through the backdoor and, for example, place malware before forcing the web servers to reboot. The diverse attack surfaces offered by our digital life, work, and business are likely to be exploited even more effectively in the future. This makes it even more important for organizations to take these security risks seriously and create a strategic plan to detect and defend against DDoS attacks.

The faster and more accurately DDoS attacks are detected and defended against, the more time IT staff will have to detect other anomalies and threats in the network.

Extortion with DDoS attacks becoming the norm

In the coming months, we can expect to see a further increase in ransomware attacks, as seen in newer and shorter waves since the summer of 2020. As enterprises continue to digitize, they provide more and more attack surfaces and, unless they have adequate protection, become more vulnerable to downtime and business interruptions.

The low cost and ease of execution of DDoS attacks ensures that extortion attacks will continue to increase.

Sources

1 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

2 Telecompaper.com: Siminn reports DDoS attack hitting television service on 30 January, 03.02.2021

3 Lfpress.com: ‚Bot' attack slowed London area COVID-19 vaccine booking site: top doc, 22.03.2021

4 ORF.at: DDoS-Attacke: Österreichweite Ausfälle bei A1-Internet, 18.02.2021

5 Weirditaly.com: Lower House website under attack, 09.03.2021

6 Futurezone.at: Massive Cyberattacke legte Internet in Belgien weitgehend lahm, 06.05.2021

7 Illinoisnewstoday.com: Irish Internet Service Provider Hit by Cyber Attack, 17.08.2021

8 Securityaffairs.co: Major blackouts across Puerto Rico. Are the DDoS and the fire linked?, 14.06.2021

9 https://www.ispreview.co.uk/index.php/2021/09/ddos-attack-disrupts-voip-and-internet-services-at-voipfone-uk.html

10 https://www.bleepingcomputer.com/news/security/yandex-is-battling-the-largest-ddos-in-russian-internet-history/

11 https://www.newstalkzb.co.nz/news/business/cyber-attack-kiwibank-customers-still-having-access-issues/

12 https://www.inside-it.ch/de/post/heftiger-ddos-angriff-auf-berufsbildungszentrum-sdbb-20211008

13 https://taz.de/Hacker-Attacken-in-Spanien/!5813776/

14 https://www.rtlnieuws.nl/tech/artikel/5274188/ddos-aanval-gemeente-den-haag

15 https://de.statista.com/statistik/daten/studie/1189929/umfrage/anzahl-der-taeglich-aktiven-nutzer-von-microsoft-teams-welt-weit/

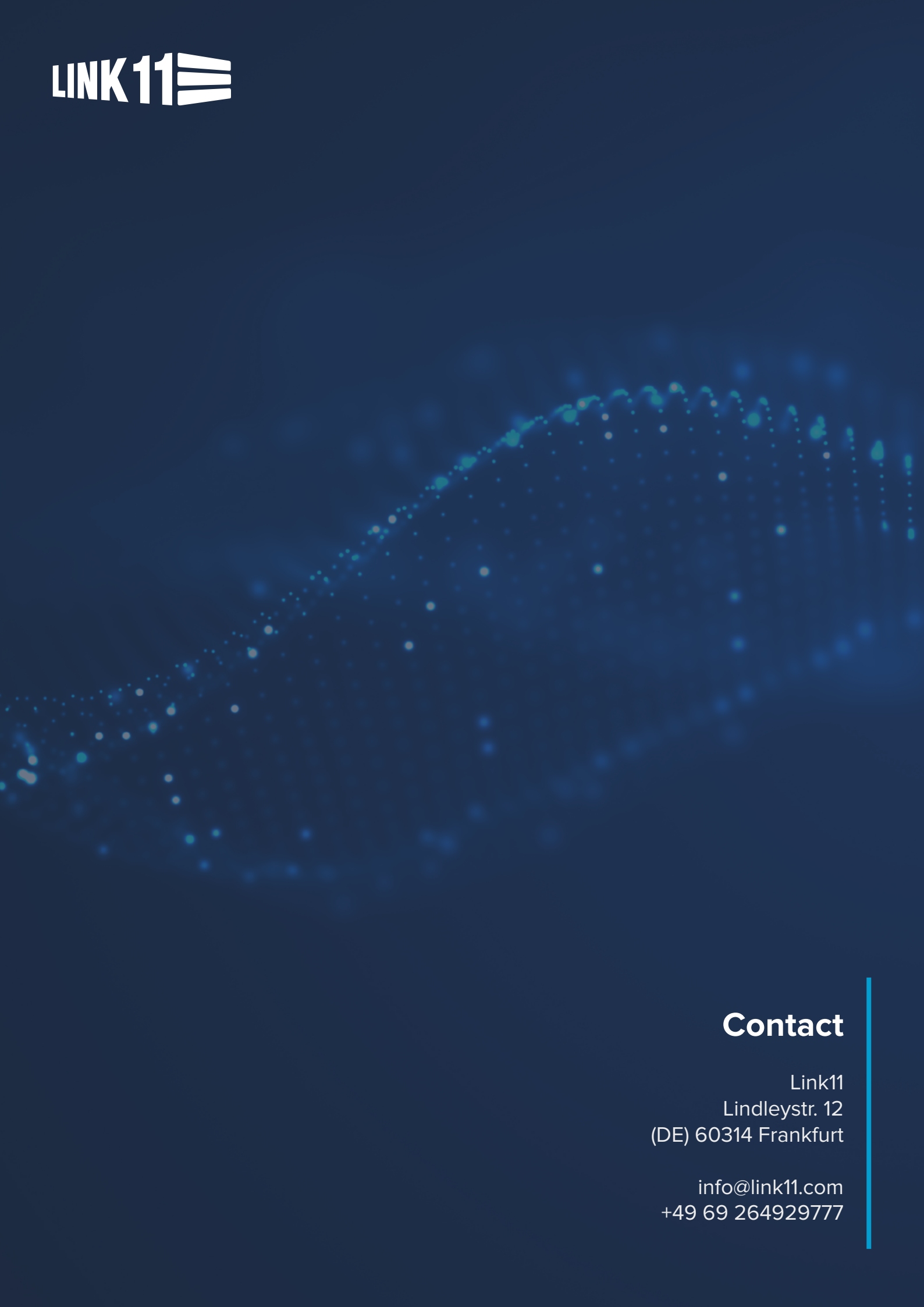
16 https://www.de-cix.net/de/unternehmen/medien/pressemitteilungen/datenverkehr-an-de-cix-internetknoten-macht-sprung-auf-ueber-38-exabyte

17 https://www.itpro.co.uk/security/cyber-crime/361523/europol-report-ddos-ransomware-gangs-evade-capture

18 https://www.cybertalk.org/2021/09/13/250000-strong-ddos-botnet-record-shattering-attacks/

19 https://www.gma-cpa.com/technology-blog/paying-ransom-on-a-ransomware-attack-is-illegal

20 https://www.cpomagazine.com/cyber-security/3-7-million-flexbooker-accounts-leaked-to-hacker-forum-after-ddos-attack/



Contact

Link11
Lindleystr. 12
(DE) 60314 Frankfurt

info@link11.com
+49 69 264929777