LINK11

DDOS-REPORT

1st half year 2022

Inhalt

Introduction and Summary

In the eye of the storm

DDoS attacks are decreasing but becoming faster and more dangerous

The Corona pandemic has been affecting social life and business for more than two years. In many areas of life, it has accelerated the **digital transformation**. According to the SZ Digital Barometer, over 90% of people aged 14 and older in Germany are online, and 94% of professionals use the Internet.[1] Hybrid work models, migration to the cloud, and improvements to corporate IT services and web services that secured everyday professional life were the main drivers.

Even though a Bitkom study published in June 2022 concludes that the Russian war of aggression on Ukraine, the disruption of supply chains, rising energy costs and accelerated inflation are slowing down **digitization** in Germany.[2], the associated **cyber dangers** are consistently among the **most serious implications**. Increasingly, costly and damaging cyber incidents are occurring, affecting increasing numbers of government institutions, critical services and infrastructure.

According to the **World Economic Forum's** "Global Risks Report 2022," cyber security failure is one of the **top 10 risks** worldwide within the next five years.[3] This makes it understandable that around two-thirds (62%) of top managers surveyed by management consultancy Horváth consider cyber security one of the most important management challenges.[4] According to the Hiscox Cyber Readiness Report 2022, almost half (48%) of the companies surveyed worldwide were affected by at least one cyber attack in 2021.[5]

The **threat landscape** in the cyber space continues to **intensify**. According to PwC, cyberattacks are globally the most common cause of white-collar crime.[6] On the one hand, this is due to the ever-increasing influence of **cyber criminals**, who are becoming more **professional** and internationally **networked**, and more **innovative tools** and **sophisticated methods** are becoming available at relatively low cost.

Despite this threat, we are experiencing a **paradoxical situation**, particularly regarding the issue of DDoS: last year, the Link11 Security Operations Center (LSOC) registered a record-breaking number of DDoS attacks, and simultaneously, there was hardly any media attention for this very tense threat situation. Since the start of the Ukraine war and related cyber operations, media attention to DDoS attacks has increased significantly, while the hard facts - the numbers - show a different picture.

LSOC recorded a **temporary decline** in DDoS attacks on the network for the first time. During the period under review, the total attacks decreased by more than three quarters (80%) compared to the same period last year in the DDoS record year of 2021. 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**. After these peaks of ransomware activity, there have been significantly fewer Ransom DDoS attacks. In addition, several illegal **darknet marketplaces**, including the world's largest darknet hub, "Hydra-Market", have been **shut down** recently, draining the collection points of criminal energy.[7]

While there are **fewer attacks**, they are **more dangerous** at the same time. That's because LSOC has observed in recent years that the **DNA of attacks** is continually changing. Instead of attacking companies indiscriminately in hopes of success, companies are now targeted specifically with **sophisticated DDoS attacks**. In addition, the attacks recorded during the period under review are significantly shorter, more intense and more sophisticated.

Introduction and Summary

For the first time, DDoS attacks recorded on the Link11 network were analyzed regarding how many seconds must pass after the first bytes are transmitted before traffic reaches its maximum value. In the first half of 2022, a **critical payload** was reached on average just 55 seconds after the DDoS attack began. In comparison, attacks in 2021 peaked only after an average of 184 seconds. Instead of rising steadily, as in the main cases observed, these **“turbo attacks”** peak quickly. This means the attack can cripple network systems even before defensive measures take full effect.

The trend towards **high-bandwidth** DDoS attacks continues strong. The average maximum attack bandwidths continued to increase year on year from 266 Gbps in the first half of 2021 to 325 Gbps in the first half of 2022. The largest attack was stopped at 574 Gbps. The increase in **intensity** is also reflected in the volume increase in the number of packets transmitted. While the average number of packets per second during the period under review was 1.5 million packets, the packet rate in the first half of 2021 was significantly lower. In the attack case, only 277,000 packets per second were transmitted.

If we consider the correlation between the duration and intensity of DDoS attacks, there is an evident change: the attacks are **shorter** and **more intense**. The more concentrated, targeted and sophisticated attacks are, the more precision and speed are required in detecting and defending against them. This means that when dealing with DDoS attacks, time is becoming an increasingly essential factor.

DDoS in the News

1st Quarter 2022

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.[8]

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.[9]

February 2022
DDoS attack wave on Ukraine

Prior to the Russian invasion of Ukraine, there were several DDoS attacks on state institutions such as the Ministry of Defense and state-owned banks.[10]

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.[11]

February 2022
Moscow Stock Exchange website outage

The Moscow Exchange website was down on Monday, February 28, 2022. The stock exchange remained closed on that day.[12]

March 2022
Attack on Ukrainian national Internet provider

The Internet in Ukraine is down for 15 hours after an attack on Ukrtelecom, the national Internet provider.[13]

DDoS in the News
2nd Quarter 2022

April 2022
Attack on the websites of the Finnish Ministry of Defense

During Ukrainian President Zelenskyy's speech, the Finnish Ministry of Defense website was crippled by a DDoS attack. In addition, the Ministry of Foreign Affairs was also affected.[14]

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.[15]

May 2022
Attack on 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.[16]

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.[17]

June 2022
All systems down: cyberattack on the Italian city of Palermo

Italy's fifth largest city, Palermo, has suffered a cyberattack. It has greatly impacted all kinds of services for residents and tourists.[18]

June 2022
Lithuanian state and private websites hacked

Russian hackers attacked the Lithuanian state and private websites. The attack is said to be a retaliation for Vilnius' decision to stop the transit of some goods to the Russian exclave of Kaliningrad.[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]

Development of Total Numbers in the Link11 Network

Fewer DDoS attacks in the first half of the year

After the ever-increasing attack numbers in previous years and the all-time high in 2021, LSOC recorded a temporary decrease in DDoS attacks on the network for the first time. The number of attacks decreased by more than three quarters (80%) in the first half of 2022 compared to the same period last year. Especially in the first half of 2021, many attacks went down to several waves of DDoS extortion (RDDoS - Ransom Distributed Denial of Service). After this peak, there have been significantly fewer DDoS extortions.

In addition, in April of this year, the world's largest illegal darknet marketplace was shut down. German authorities such as the BKA cooperated with the U.S. Department of Justice in this operation. The joint German-US operation seized the servers of the "Hydra market," a Russian website, as well as $25 million in cryptocurrency.[22]

In addition, in the two record years of 2020 and 2021, many attacks targeted web services that ensured living, learning and working under pandemic conditions. These included vaccination platforms, learning portals and IT infrastructures for mobile working in the home office. Hosting providers and ISPs that enabled express digitization in business and society were also under fire.

Due to the Ukraine war and the parallel cyber war, many players on the cybercrime playing field could focus their capacities on other targets. A fluctuation in terms of the origin of DDoS attacks is also evident in Link11's network. Relatively speaking, more attacks are coming from Russia and fewer from the U.S. and China.

However, this may be the calm before the storm. The current situation is dynamic and unpredictable. Since the start of the Ukraine war, state-backed hacker groups have increasingly been on the move besides the usual players. For example, the pro-Russian hacker group "KillNet," has declared cyberwar on several states, including Germany. The consequences of this declaration of war have been observed in Italy, Lithuania, Norway and Poland.[23]

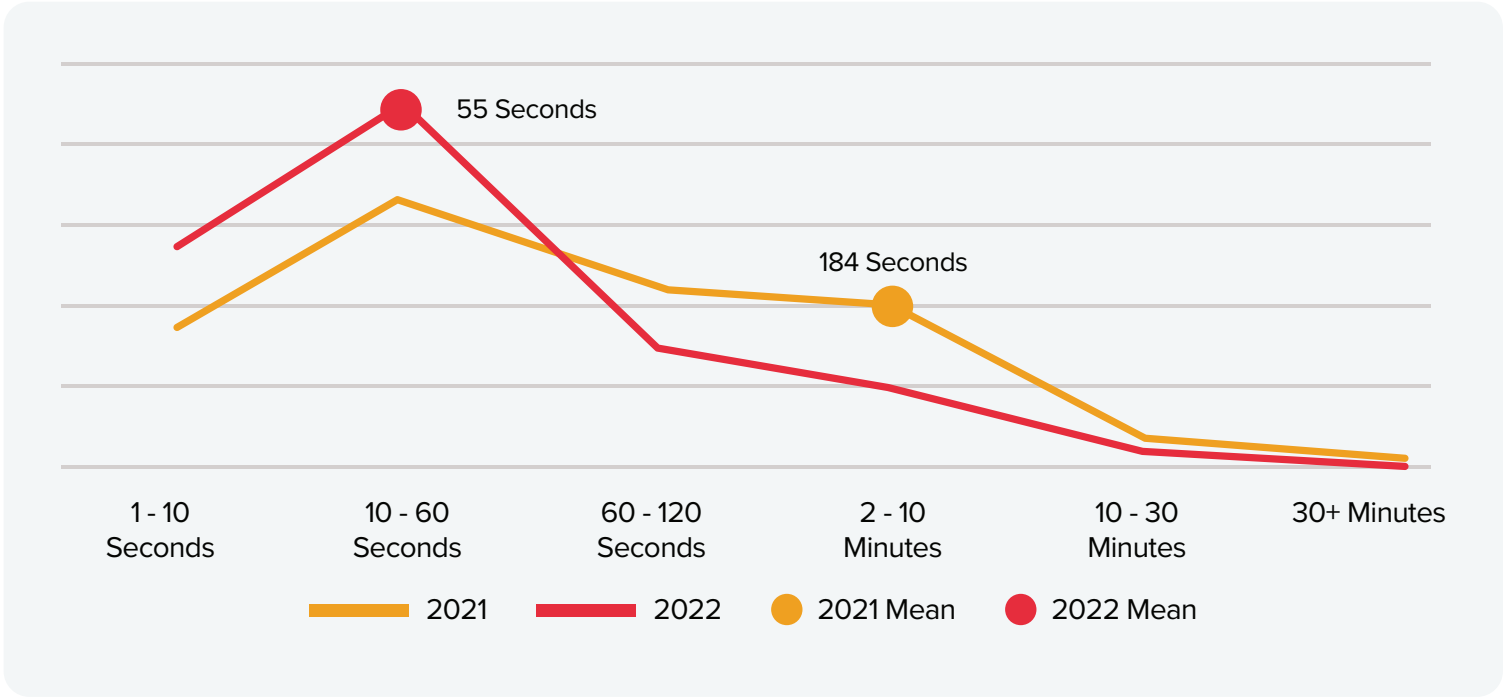
Even though the number of attacks has decreased significantly compared to the same period last year, they still pose a major threat. Their DNA is changing continuously. This makes it all the more important to take a close look at a sensible and effective IT security strategy.

Faster and more intense - DDoS attacks become more sophisticated

The DDoS attacks registered in the Link11 network were the first to analyze how many seconds must pass after the first bytes are transmitted before the traffic reaches its maximum value. These fast-onset DDoS attacks or "turbo attacks" are usually of shorter duration. They peak quickly or reach a critical payload, instead of rising continuously, as has been observed in most cases in the past. This means that the attack might already bring the network systems to a standstill before the defensive measures can take full effect.

Based on the initial analysis, the full year 2021 was assumed as the comparison period. In the first half of 2022, a critical payload was reached on average 55 seconds after the onset of the DDoS attack. In comparison, attacks in 2021 peaked only after an average of 184 seconds.

Duration until Critical Payload of Attack | H1 2022 vs. 2021

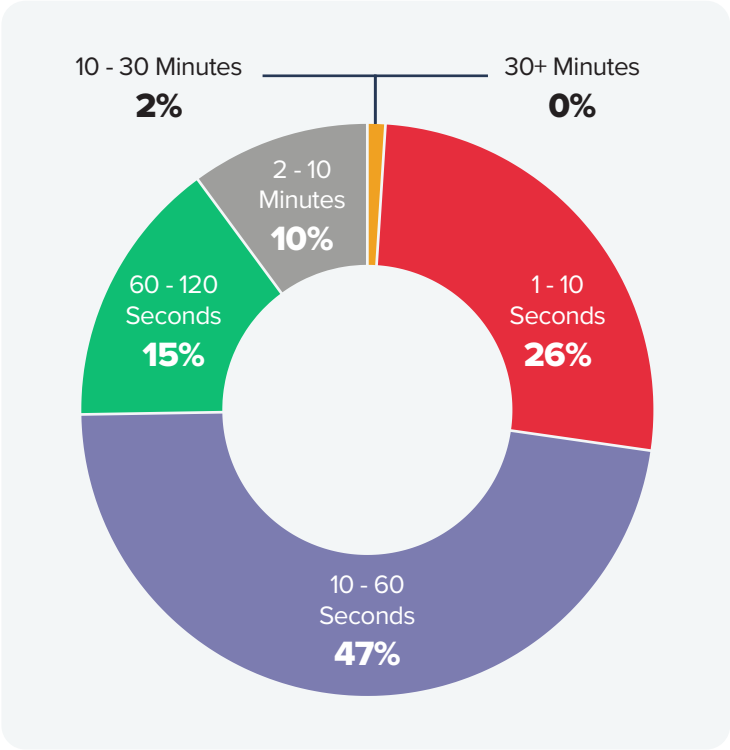


A look at the distribution of the time it takes for a DDoS attack to reach its peak shows the following results for the first half of 2022: In more than a quarter of attacks (26%), the critical payload is reached within the first ten seconds. Last year, this percentage was 17%. In the first half of 2022, attacks that reach 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 addition to long-lasting attacks that last more than 12 hours, there is also a trend toward fast-onset attacks. These attacks are shorter in duration but reach a critical payload very quickly before the protection mechanisms can take full effect.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

In only 15% of cases, it takes between one and two minutes for DDoS attacks in the first half of 2022 to reach the critical maximum level. For more than two minutes, the proportion is around one-tenth of the DDoS attacks recorded by LSOC. Compared with the previous year, major differences are evident 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.

Distribution of the Duration until Peak of the Attack



In the event of an attack, the most important thing is that no valuable time is wasted, for example, in the manual assessment of incidents, the often-associated reactive panning of data traffic and route changes. If, in addition, unforeseen routing problems occur or new attack methods have undercut the radar, such delays in defense can lead to significant damage.

Short attack times do not indicate the size and seriousness of an attack. Instead, one attack might peak quickly with barely any disruption, while another might have critical effects, such as a complete outage before maximum attack potential has been achieved. But with these fast-onset attacks, the time to mitigation, or time-to-mitigate (TTM), is critical. DDoS attacks have occurred on the Link11 network that was able to deliver twice the payload only 70% of the time. Even a TTM of just one minute is not enough in such a scenario to avoid a complete system failure.

An effective IT security strategy analyses traffic in real-time using smart, fast and secure methods to achieve the greatest possible visibility across all network traffic. Probably the most effective way to defend against DDoS attacks is a mix of basic protection and intelligent and automated AI technology.

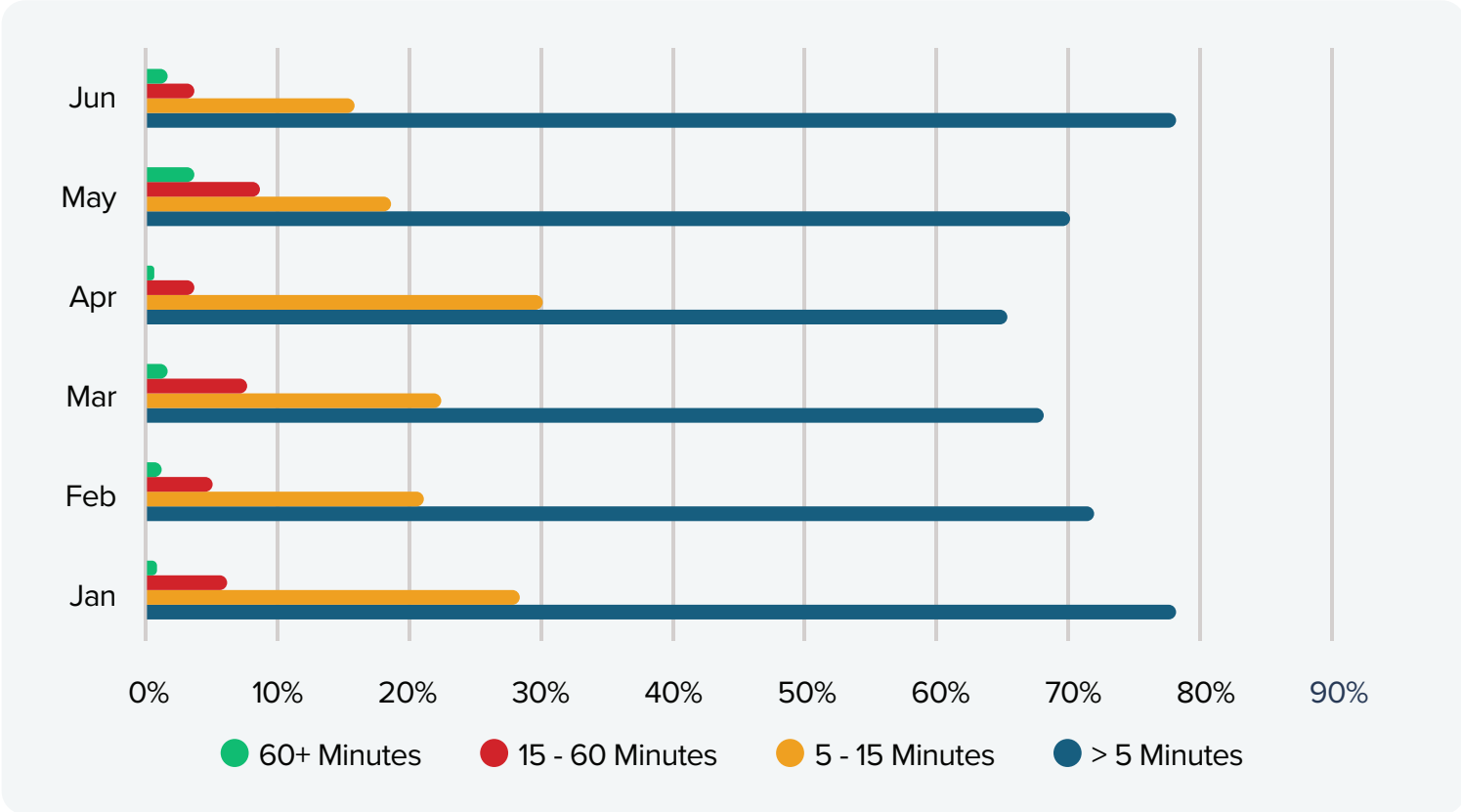
Evolution of Attack Duration

Brevity is the spice of life

The duration of DDoS attacks recorded on the Link11 network in the first half of 2022 has shortened compared to the same period last year. While there were significant outliers almost every month, overall attack duration has decreased. A look at the graph (above) clearly shows how the normal distribution of attack duration compares to the outliers. Despite their short span, the DDoS attacks recorded have seen a significant increase in volume, both in terms of packets and bits per second.

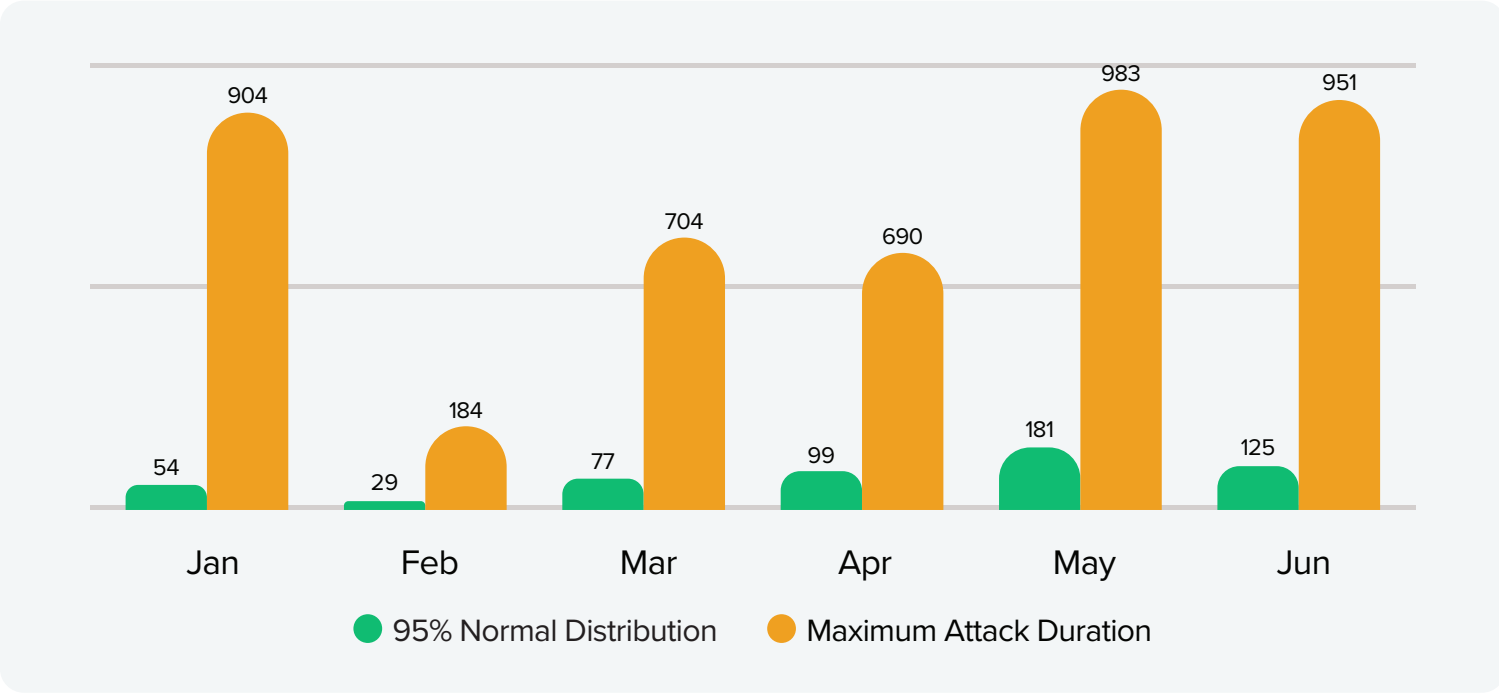
Further analysis shows that the length of the attacks varied from a few minutes to several hours. The majority of attacks (70%) lasted less than 5 minutes. Just under a quarter of all registered attacks (22%) were between 5 and 15 minutes long, with another 6% lasting up to 60 minutes. Only about 2% of attacks were longer than 60 minutes. The peak in attack duration was 981 minutes, or just under 16.5 hours. In the same period in 2021, the longest attack lasted 1,440 minutes, corresponding to one day.

Overview Attack Duration in H1 2022



Evolution of Attack Duration

Normal and Maximum Attack Duration Trend in Minutes | H1 2022



Whether an attack is short or long is often related to the attack technique. With short attacks of a few minutes on individual IP addresses, attackers tap the IT infrastructure of their target for vulnerabilities. In addition, small and short DDoS attacks are frequently used to mask simultaneously running hacker attacks on servers and networks.

However, in the slipstream of a DDoS attack, hackers can penetrate and attack network security through the backdoor without being noticed. To defend against the DDoS attack, existing IT resources are mobilized in the shortest possible time to minimize system downtime and further damage.

In addition, there are short DDoS attacks because the attackers realize they will not reach their target. If the attacks bounce off well-protected infrastructures, the attackers usually retreat to conserve their resources. Long-lasting attacks are usually the means of choice if the attackers are concerned with permanently torpedoing or disrupting the attacked infrastructures.

> **The attack landscape has radically evolved: The denial-of-service attack of ten years ago has nothing much to do with the sophisticated, highly complex and intelligent DDoS attacks of today.**
>
> **– Marc Wilczek,** Geschäftsführer, Link11

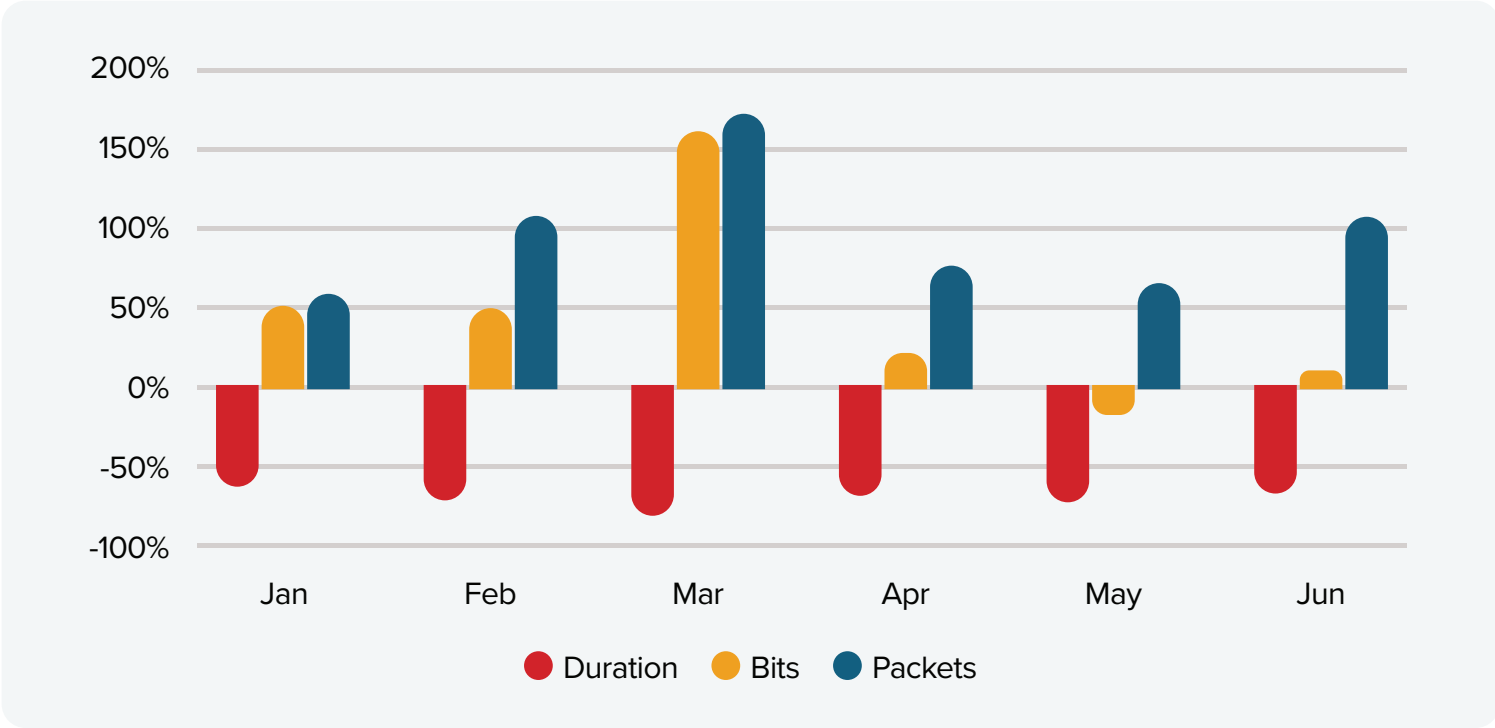
Evolution of Attack Bandwidths

The intensity of attacks continues to increase

The trend toward high-volume attacks, which was already evident in the same period last year, has become more pronounced in the first six months of 2022. The intensity of DDoS attacks increased further in the period under review compared to last year. Average maximum attack bandwidths have increased year on year from 266 Gbps in the first half of 2021 to 325 Gbps in the first half of 2022. The trend toward high-bandwidth DDoS attacks continues unabated. The largest attack was stopped at 574 Gbps.

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 transmitted. While the average number of packets per second was 1.5 million during the period under review, the packet rate was significantly lower in the first half of 2021. In the attack case, only 277,000 packets per second were transmitted.

Attack Volumes and Duration | H1 2021 vs. H1 2022



If we look at the correlation between the duration and intensity of DDoS attacks, we can see a clear change: the attacks are shorter and more intense. Time is becoming an increasingly important factor in dealing with DDoS attacks. The decisive factor here is how much time elapses before the first reaction to the attack and the start of damage limitation, the Time-to-Mitigate (TTM), and how long it takes to restore the original state, the Mean-Time-To-Repair (MTTR).To see how Link11 and other competitors are positioned on this critical factor, see the Frost & Sullivan study, **"The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough."**

The more concentrated, targeted and sophisticated attacks, the more precision and speed are required to detect and stop them. This is because protection solutions are relentlessly tested, especially with the fast-occurring and intense attacks with large bandwidths and high packet rates. Some of the on-premises solutions can defend against simple and uncoordinated attacks. Primarily, the protection covers network-type attacks (e.g., ICMP-UDP floods) on Layer 3 or 4. At the same time, more complex and particularly intense attacks can overwhelm local devices.

Multi-Vector Attacks

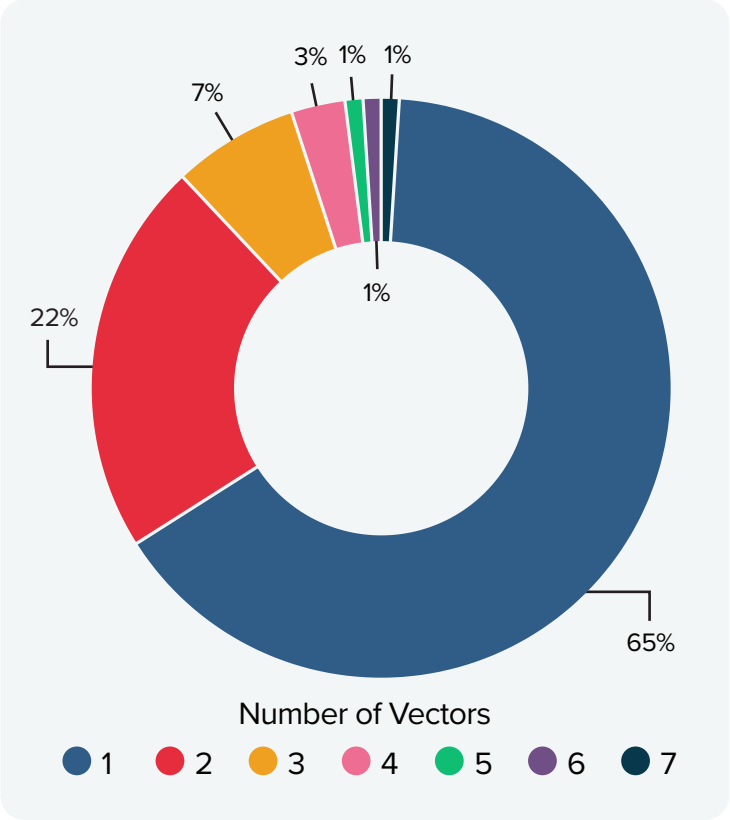
True to the motto: saving resources

After the complexity of DDoS attacks increased steadily in recent years and peaked in 2021, the proportion of multi-vector attacks decreased in the first half of 2022 compared to the same period last year. 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 attacks.

Instead of such multidimensional attacks, which are effectively multiple attacks running simultaneously, attackers preferred targeted, concentrated and resource-efficient attacks in the past six months. During the period under review, one-third of attacks (35%) were multi-vector attacks, while in the first six months of last year, two-thirds (65%) of attacks used multiple vectors. The highest number of vectors used simultaneously observed in the Link11 network was 11.

If IT security lags behind the threat landscape, a single vector used in a targeted and concentrated manner is enough to cause significant damage.

Multi-Vector Attacks



Although fewer multi-vector attacks were recorded in the Link11 network, the threat situation remains tense. Multi-vector attacks are still a major threat. Different attack vectors can complicate defense efforts and slow down TTM overall. Only with a protection solution whose patch and update cycles are adhered to and therefore up to date can the enterprise IT reliably secure. If IT security lags behind the threat landscape, a single vector used in a targeted and concentrated manner is enough to cause significant damage.

Reflection Amplification Attacks

Old acquaintances and a new vulnerability

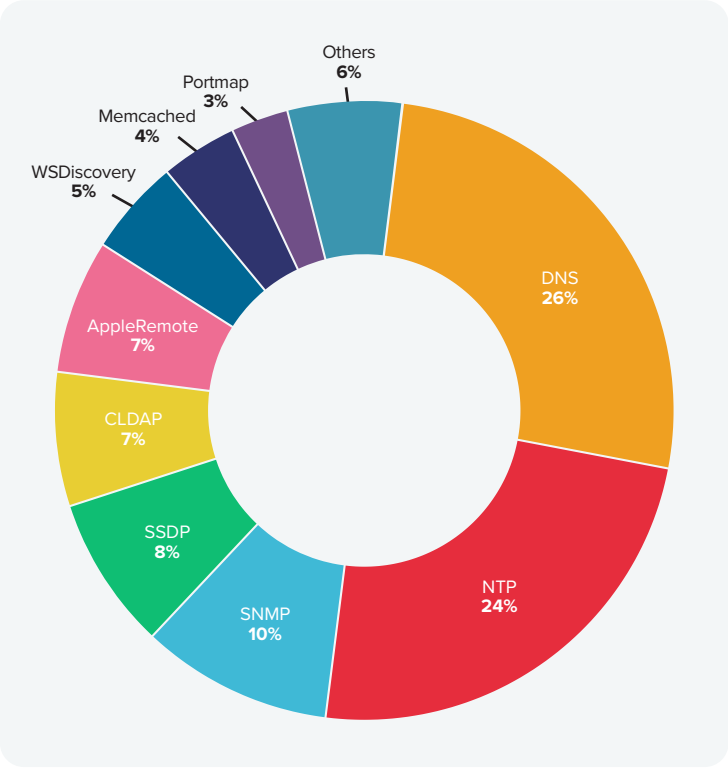
Reflection amplification attacks are a class of multi-vector attacks that similarly exploit various misconfigured open servers and services on the Internet. The target system is not attacked directly, but services such as DNS or NTP are abused. The attacker first sends small amounts of data packets to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

LSOC registered more than a dozen amplification techniques in the first half of 2022. Among them were attack techniques such as DNS or NTP reflection amplification, which have been part of DDoS attackers' tools of the trade since 2013. High amplification factors characterize them. The increase is 100 times for DNS attacks and up to 200 times for NTP attacks. Vectors such as SSDP and SNMP, which have also been in use for several years, played an important role.

Attackers are constantly discovering new vulnerabilities such as inadequately protected Internet services and open services. At the same time, most attacks during the period under review used already known and proven vectors.

> **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 will be able to keep pace.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

Amplification Attacks by Occurance | H1 2022



The Internet service most frequently exploited for attacks and abused as an amplifier in the first six months of 2022 was DNS (26%), followed by NTP (24%), SNPM (10%) and SSDP (8%).

Almost every year, DDoS attackers identify new vulnerabilities for DDoS attacks. LSOC warns that no UDP service is safe from abuse by DDoS attackers. Long-term observation shows that attackers are constantly scouring the Internet for new ports and protocols that can overload corporate IT infrastructures. One of the biggest amplifiers is Memcached, with a 50,000x amplification. However, there is a new TCP middleware attack with the potential to surpass this under certain circumstances. Theoretically, a research paper in August 2021 showed that with this amplification technique, attackers could abuse middleboxes such as firewalls over TCP to amplify denial-of-service attacks. The researchers also identified hundreds of thousands of IP addresses that strengthen attacks hundreds of times using firewalls and content filters.[24]

What We Will See in the Future

Time becomes an increasingly critical factor in defending against DDoS attacks

Almost everywhere - at work or home - we are more dependent than ever on the digital world. Some companies are a single DDoS attack away from bringing business units to a standstill or threatening to bring production facilities to a halt. That's because, depending on the form of attack, only a few seconds pass before the DDoS attack can have its full effect.

Based on LSOC's observations, time plays an essential role in defending against these attacks. DDoS attacks have occurred on the Link11 network, able to deliver twice the payload only in 70% of the time. DDoS attacks have become shorter and more intense. In addition, attackers are more targeted and act prudently, testing the network and its protection first.

Once the attackers have launched one of these sophisticated and dangerous DDoS attacks, there is only a narrow window of opportunity to limit the potential damage. This is because protection solutions are put to the test, especially in the fast-occurring and intensive attacks with large bandwidths and high packet rates. In such a scenario, a time-to-mitigate of just one minute is not enough to prevent a complete system failure. Instead, the goal is analyzing traffic in real-time with cloud-based automated AI technology to fend off DDoS attacks in the shortest possible time.

New attack techniques are evolving

In the Link11 network, we monitor more than a dozen amplification techniques for DDoS attacks at any given time. Besides the many old familiar attack techniques such as DNS or NTP reflection amplification, used since 2013, there is a new TCP middleware attack that can abuse "middleboxes" such as firewalls. The attacks target the Transmission Control Protocol (TCP), a protocol responsible for secure communication between networked machines on the Internet.

The attack takes advantage of network middleboxes that do not conform to the TCP standard. The University of Maryland researchers scanned the entire IPv4 Internet for their research. In the process, they discovered hundreds of thousands of IP addresses that offer amplification factors more than a hundred times. According to the research team, network phenomena exist that can cause some TCP-based attacks to be so effective that they technically have an infinitely large amplification factor. After the attacker sends a constant number of bytes, this reflector generates infinite traffic.[25]

What was only considered theoretically possible until early March 2022 has now been observed in reality.[26] Therefore, it can be assumed that in the future, this attack method will find its way into the repertoire of cybercriminals and will be further developed.

Sources

1 https://www.bidt.digital/wp-content/uploads/2022/01/Analysen-Studien-bidt-SZ-Digitalbarometer.pdf

2 https://www.bitkom.org/Presse/Presseinformation/Daempfer-Digitalisierung-Weltlage-bremst-digitale-Transformation-Wirtschaft

3 https://www.weforum.org/reports/global-cybersecurity-outlook-2022

4 https://www.horvath-partners.com/en/media-center/studies/cxo-priorities-2022-managing-overlapping-crises

5 https://se.myconvento.com/public/get_file.php?id=enc2_YTNST1VFTXJObVJxZEdvM1RFWTVWbTlNVldKblVUMDk&download=1

6 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

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

8 https://hackernoon.com/has-solana-encountered-another-ddos-attack

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

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

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

12 https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=38adc2e677ca

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

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

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

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

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

18 https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/

19 https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/

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

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

24 https://www.usenix.org/conference/usenixsecurity21/presentation/bock

25 https://www.usenix.org/conference/usenixsecurity21/presentation/bock

26 https://www.akamai.com/blog/security/tcp-middlebox-reflection

LINK11

Contact

Link11 GmbH
Lindleystr. 12
60314 Frankfurt

info@link11.com
+49 69 264929777