Distributed Denial of Service Report

First Half of 2020

The threat situation in the first half of 2020 at a glance

238

The **maximum number of attacks was 238** (June 7); the **lowest number of attacks registered was just 18**, on February 19.

406 GBPS

The largest DDoS attack was stopped at 406 Gbps.

Almost 500 attacks

In almost 500 attacks, the attack volume was over 50 Gbps. This is well over the external connection of most companies.

55 million packets

The **maximum** packet rate amounted to 55 million packets per second.

1.390 minutes

The longest **DDoS attack lasted 1,390 minutes – 23 hours**. Interval attacks, which are set like little pinpricks and which thrive on repetition, lasted an average of 13 minutes.

52%

One in two attacks (52%) combined several methods of attack, making them harder to defend against.

14

One attack included 14 methods of attack – the highest number of vectors registered so far.

47%

At 47%, the percentage of DDoS attacks from the cloud was at a high level.

Covid-19: Resurgence in DDoS attacks

Within days and weeks of the start of the coronavirus pandemic, millions of people's jobs were relocated into home offices. This resulted in a 40% rise in global internet traffic between the start of February and mid-April 2020. IT infrastructure operators such as DE-CIX and telecom providers such as Vodafone have also reported an increase in data traffic around the world since March. At a time when the data loads are already large, even smallest attacks can shut down companies and their home-office plans. Against this backdrop, the Link11 Security Operations Center (LSOC) has observed a resurgence in DDoS attacks. Since April, the number of attacks on the network registered by Link11 was significantly higher than the number recorded in the same period last year.

April 2020: + 85%
May 2020: + 108%
June 2020: + 97%

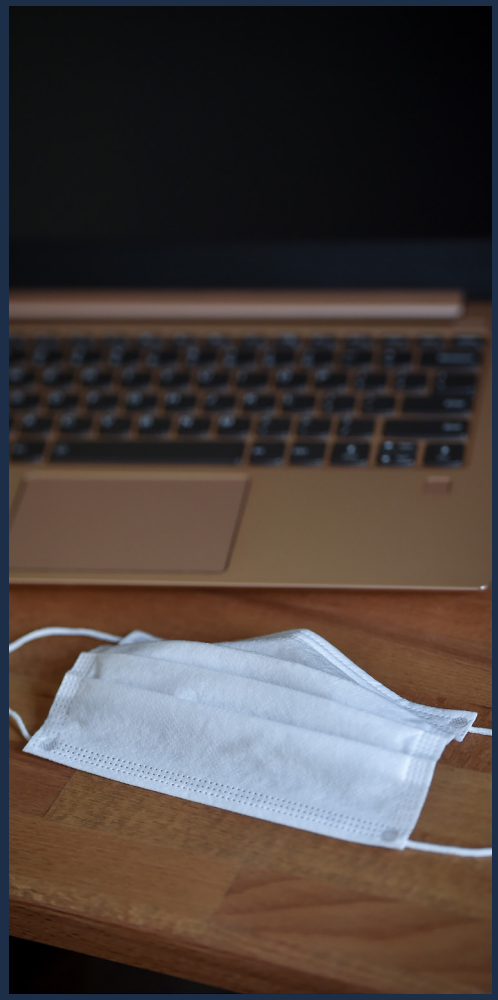
During Covid-19, DDoS attackers have largely concentrated on two components of in-house company infrastructure: VPN servers, and APIs and their accompanying web applications.

VPN servers act as a gateway to a company's internal network. Successful attacks can prevent remote workers from accessing it. A carefully planned TCP blend (DDoS) attack with an attack volume of just one Mbps is sufficient to crash a VPN server or a firewall. In addition, SSL-based VPNs are just as vulnerable to an SSL flood attack (DDoS) as web servers.

What makes things even harder is that many companies use either on-site hardware appliances or trust in their telecom provider's attack defense systems. These deployment models use a minimal level of automation and often require human interaction. When there is an attack, introducing defense measures can become a major undertaking when there are few or no IT personnel on site. These models also generally require 10 or even 20 minutes just to recognize the incident, which almost inevitably leads to a large outage.

Application programming interfaces (API), which act as one of the main elements of cloud services and web applications, can be just as insecure. If a business-critical application or API is compromised, all operations linked to the business are stopped, triggering a chain reaction. Suppressing application-level attacks – such as an HTTP/HTTPS flood – is particularly complex, since malign data traffic is hard to differentiate from normal traffic. Furthermore, attacks on the layer 7 level are highly effective, as they require little bandwidth to cause a blackout.

Companies must be alert and prepared for attacks to avoid losing time should they become a target. They should continue to opt for cloud services, as their scalability and higher bandwidth enables them to maintain redundancy. But the most important thing in times of remote work and social distancing is to opt for the radical automation of security processes, which guarantees immediate reactions to threats and eliminates human error.



DDoS attacks that hit the headlines in the first half of 2020

January 7, 2020

Online banking becomes offline banking

The second-largest online bank in Germany, Deutsche Kreditbank AG, is attacked by hackers over several days. The attacks compromise the availability of the website, online banking, and brokerage services.

February 8, 2020

Internet outages across Iran

Iran's internet infrastructure is hit by heavy and well-organized DDoS attacks, bringing 25% of it crashing down. Outages for ISPs across the country last for several hours.

March 16, 2020

DDoS attacks hit the US Department of Health

The Department of Health website is one of the most sources of information on the Covid-19 pandemic for Americans. DDoS attackers don't succeed in bringing the servers to its knees, but they do slow down response times.

March 18, 2020

Customers wait in vain for food orders

The German food delivery service Lieferando has experienced a boom during the coronavirus crisis. Hackers take advantage of this: they begin with DDoS attacks on Pizza.de, then attempt blackmail, which the company refuses to engage with.

March 22, 2020

Hospitals in Paris under attack

More than 40 hospitals in the French capital are disconnected from the network for many hours after a DDoS attack, making it impossible for staff to access emails and programs for working at home. Patient care is not endangered.

April 20, 2020

University website goes offline

The University of Luxembourg website (www.uni.lu) is targeted by DDoS attacks. The teaching program, with lectures and courses that are transferred to digital channels during the coronavirus crisis, is not affected.

June 27, 2020

Russian online voting becomes a DDoS target

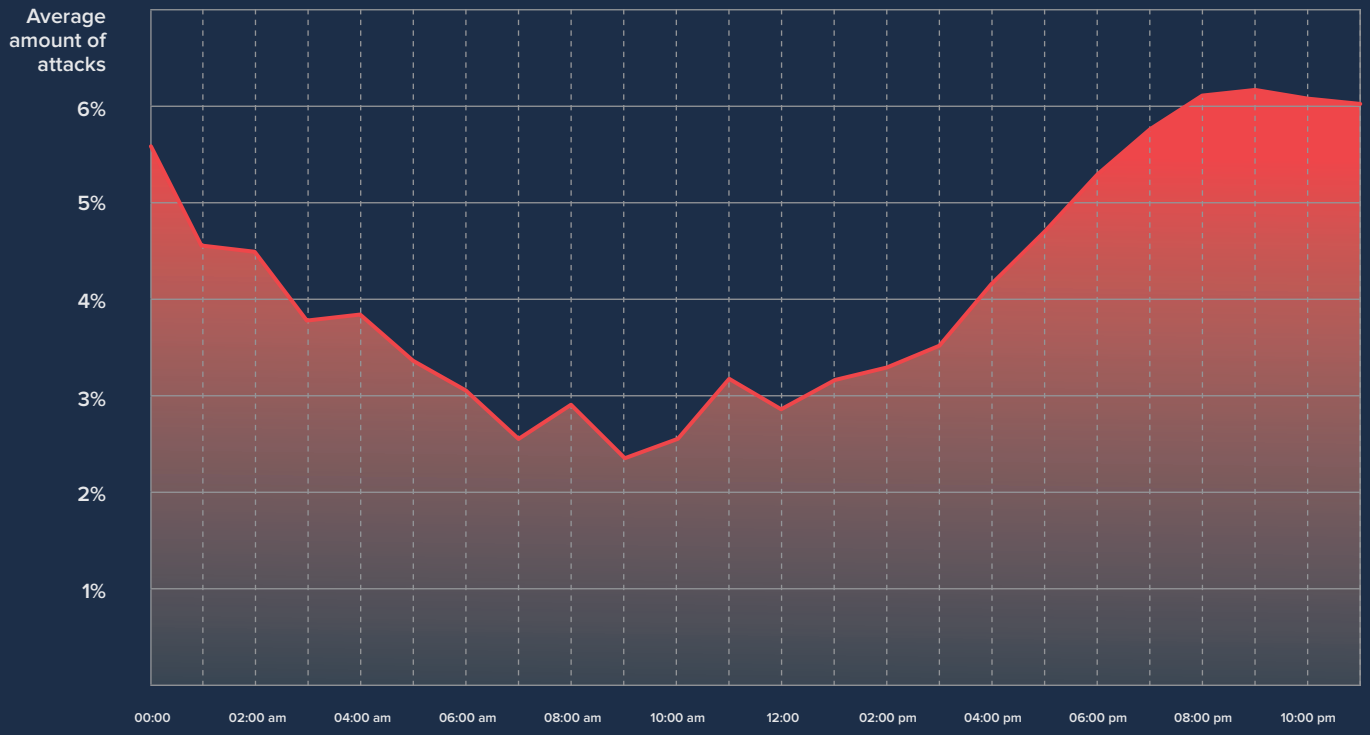
At the start of the one-week election period, during which votes are held on the Russian constitution, DDoS attacks hit the online voting system. The voting of more than a million registered voters from Moscow and Nizhny Novgorod is unaffected.

DDoS attacks around the clock

DDoS attacks have been launched at all times of the day and night, on weekdays, and on weekends. However, attack activity between late afternoon and after midnight was somewhat higher than it was during the day. During the course of the week, Saturdays and Sundays in particular experienced above-average numbers of attacks. Almost a third of all registered attacks hit on those two days.

This correlates with observations by the LSOC from previous quarters. Attackers often concentrate on off-peak hours, when administrators have finished work and IT teams are working on-call. This increases the chances that attacks will be detected later. DDoS protection solutions based on manual interventions often lose valuable time before the defense can begin. Companies that opt for fully automated and permanent filtering of the data stream to detect patterns of attack within seconds are at a clear advantage.

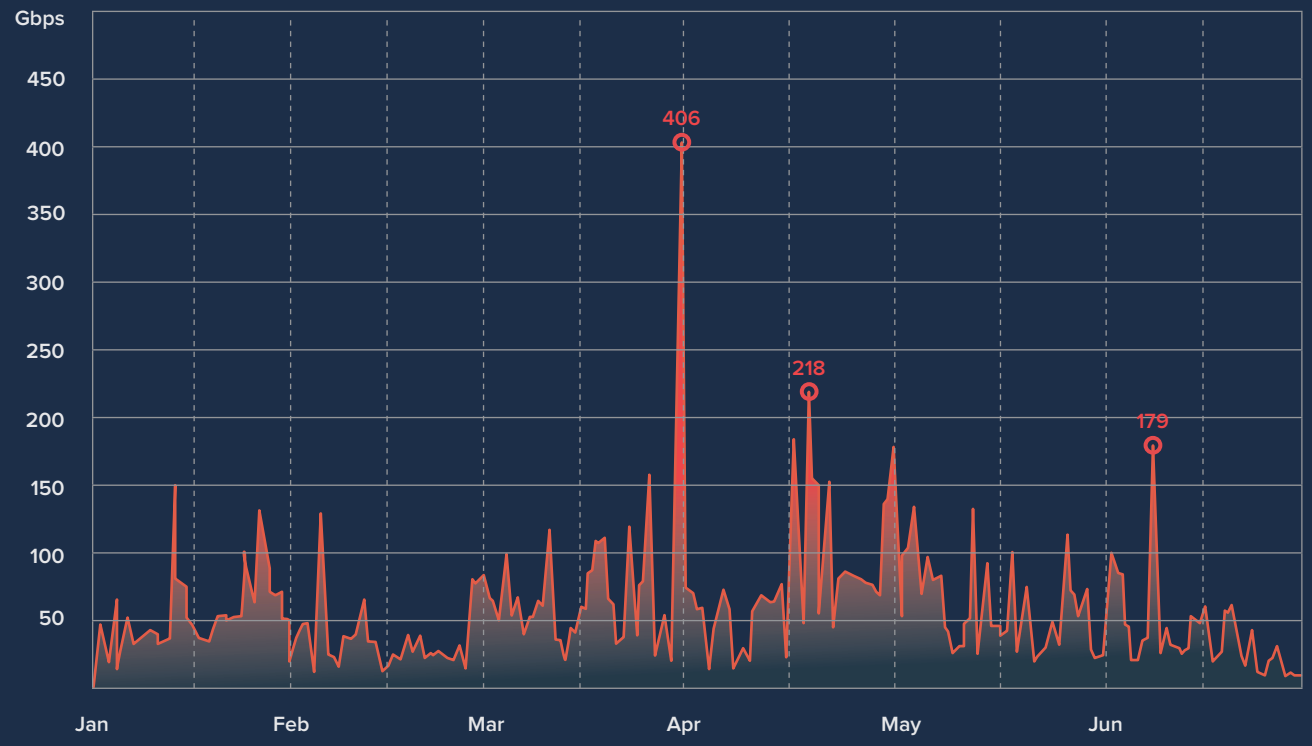
Another driver for attacks on evenings and weekends may be the high personal use of online services. Consumers often shop online between 6 pm. and midnight, and often on Saturday and Sunday. E-commerce retailers and providers of other digital services are particularly vulnerable to attacks during these peak times.



Wide range of attack bandwidths

The attack volume of DDoS attacks has stabilized at a high level, at an average of 4.1 Gbps. In the majority of attacks, fully 80% achieved levels of up to 5 Gbps. Companies should adjust their external connection accordingly if they want to stop attacks using their own default tools. One in five attacks that the LSOC registered in the first half of 2020 exceeded the 5 Gbps mark. Around 500 attacks saw an attack volume of more than 50 Gbps; 30 of them were larger than 100 Gbps. The highest attack volume was measured at 406 Gbps. The continuous provision of corresponding bandwidth connections to mitigate attacks using locally installed protection solutions is unrealistic for companies and typically exceeds available resources. Scalable scrubbing centers in the cloud offer a future-proof alternative to attacks amounting to several dozen or hundred Gbps. The graphic shows the distribution of the attack bandwidths in the first half of the year.

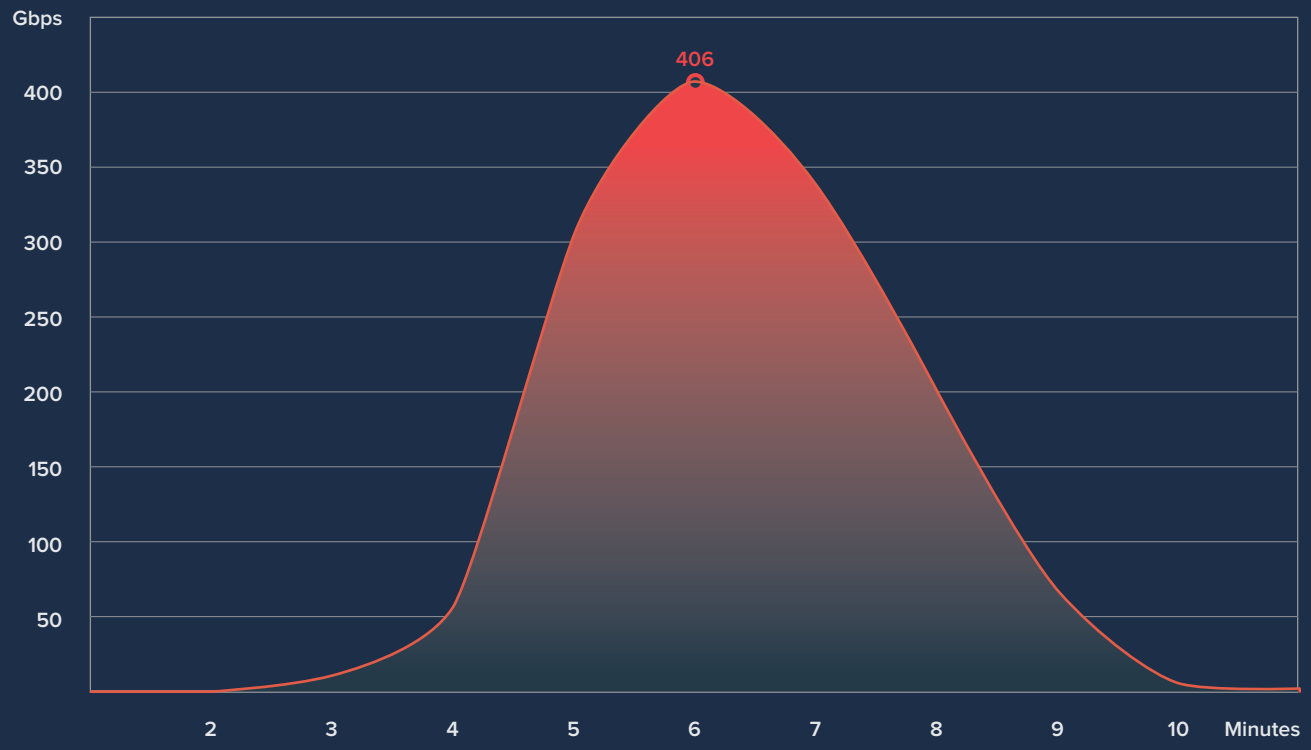
The peaks in packet rates were between 40 and 54 million packets per seconds. These values are many times higher than the permissible packet rates of firewalls and appliances.



The progress of a high-volume attack of 406 Gbps

In the first half of 2020, the largest attack volume measured was 406 Gbps. The attack lasted 11 minutes, during which the attack bandwidth slowly increased. The peak was achieved in the sixth minute.

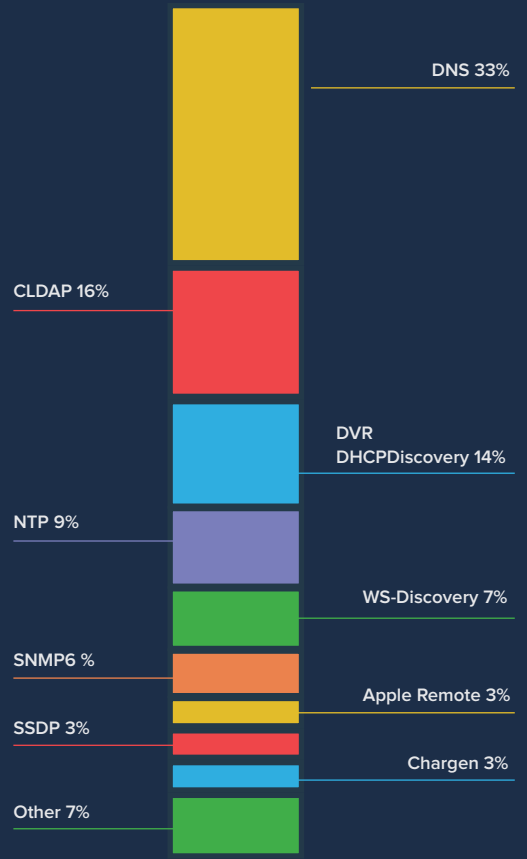
The attacker strengthened the UDP flood with two amplification vectors – DNS amplification and CLDAP amplification – to send the bandwidth upward. The amplification factor for DNS is between 28 and 54, and for CLDAP it is between 56 and 70. Most of the DDoS packets came from Russia, the USA, Ukraine, and the Netherlands.



Growing number of reflection amplification vectors

During volume attacks, DDoS attackers often relied on reflection amplification vectors, whose spectrum is broad. The perpetrators used almost two dozen different techniques to increase the bandwidths (amplification) and to falsify the sender (reflection). The most commonly used vectors included DNS, CLDAP, and NTP, which have been among the tools deployed by DDoS attackers for many years. Both WS Discovery and the Apple Remote Control protocols, which the LSOC registered and described for the first time in the first half of 2019, were also frequently used.

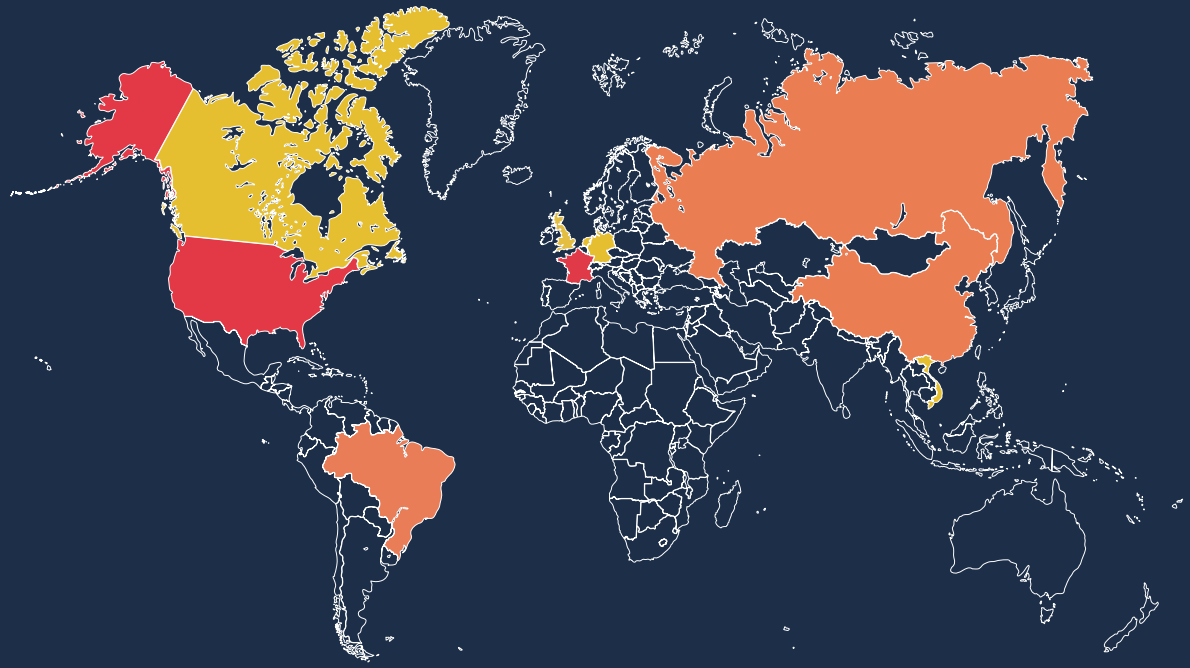
Since the beginning of the year, the vector set for DDoS attackers has also been expanded by DVR DHCPDiscovery. The LSOC has discovered a new vector that exploits a vulnerability in digital video recorders (DVR devices). These hard-drive recorders, which record digital images from webcams or from standard TV programs, can be controlled and configured via the internet. The command <get-config> enables information on the available storage space, recording times, and operational availability to be queried. The response produced by the device is approx. 20 to 30 times larger (amplification factor) than the query. A query of 50 bytes becomes a response of several kilobytes. DDoS attackers use this by redirecting the response to the IP address of the victim, quickly using up their bandwidth. The first attack with the new vector was registered by the LSOC back in November 2019, when the technique was still used sporadically. Attacks that rely only on DVR DHCPDiscovery as a reflection amplification vector achieve bandwidth peaks of up to 10 Gbps.



Reflection amplification attacks: servers are globally distributed

DDoS attackers abuse a multitude of Internet protocols to reinforce their attacks. Most techniques, also called vectors, belong to the reflection amplification category. DDoS reflection involves guiding the reply of a service to the IP address of the victim. The side effect is that the attack is virtually untraceable. This is called spoofing. Popular reflectors are DNS resolvers and NTP servers, but SSDP- and SNMP-based devices, as well as smart devices with CoAP, are also used as attack tools.

The DDoS sources of reflection amplification attacks were distributed around the globe. The top three most important source countries so far have been the USA, China, and Russia. However, in the first half of 2020, more and more attacks could be traced back to France. Other countries that were sources of attacks were Brazil, the UK, and Germany.



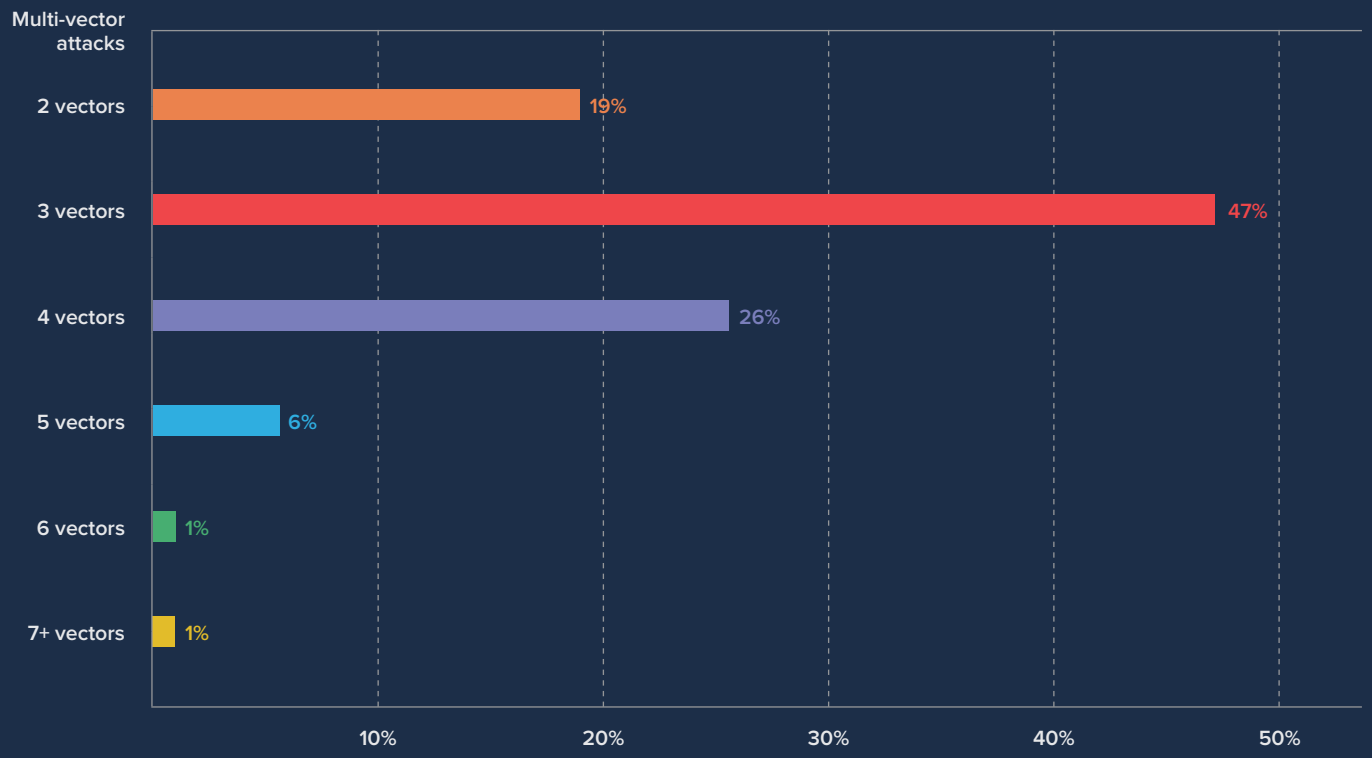
24% USA	14% France	10% China	6% Russia	5% Brazil
4% Great Britain	4% Germany	3% Vietnam	3% Canada	2% Netherlands

Multi-vector attacks create complex threats

In absolute numbers, the attacks were slightly less complex than in the same period in the previous year. Forty-eight percent of the attacks were based on a single vector, while the other 52% combined several methods. In the first half of 2019, the average value for these so-called multi-vector attacks was almost 55%. The long-range view shows that the value fluctuates between 40% and 70%. What is certain is that, due to multi-vector attacks, the threat situation is becoming more complex for companies.

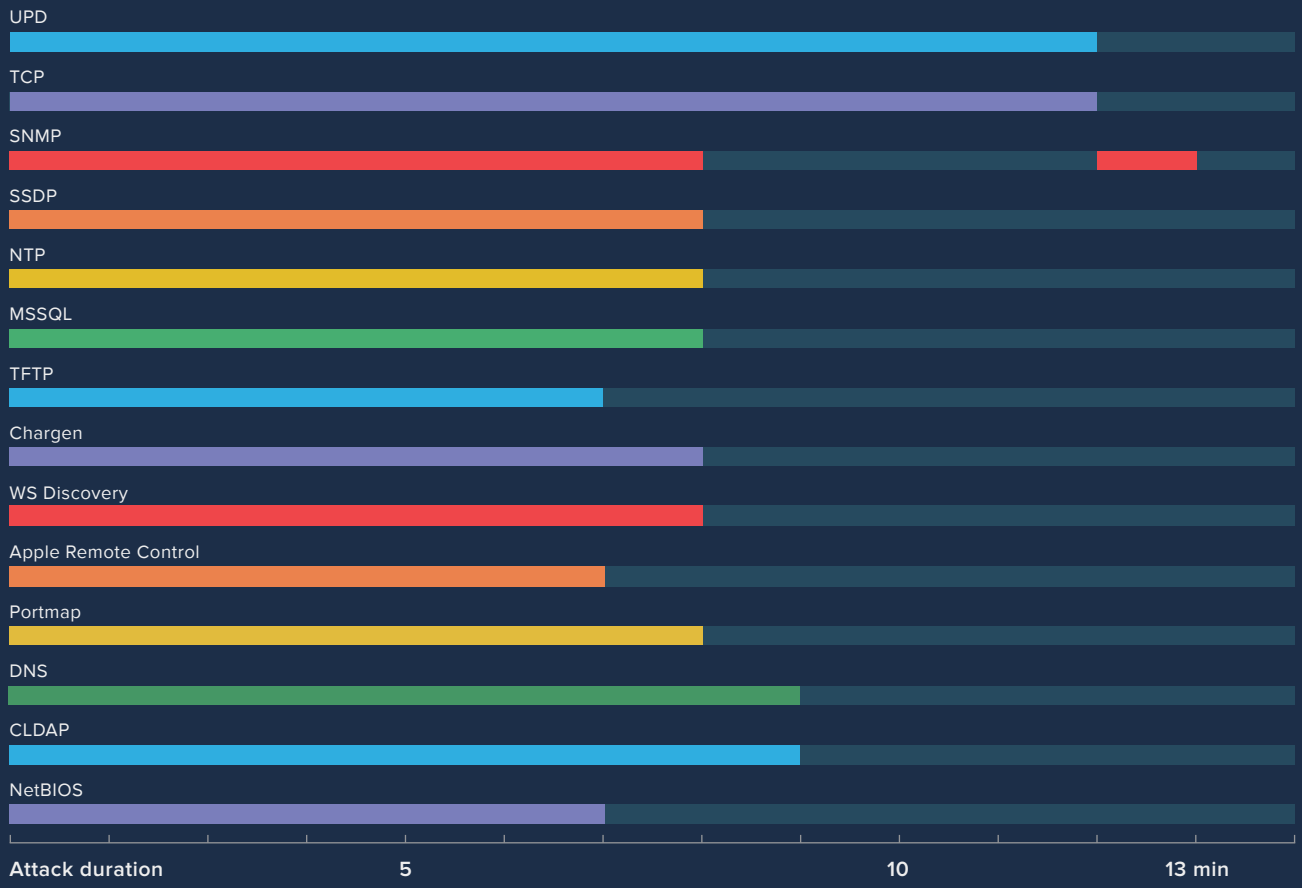
Most frequently, the attackers combined two to four vectors. They made up the majority (in fact, 92%) of all multi-vector attacks. The deployment of five or more vectors was more rare, making it all the more remarkable that the LSOC registered 23 attacks with ten or more vectors in the first half of the year. If the number of attack methods rises, it will become harder for companies to block them. When detecting many improperly deployed protocols that are attacking various infrastructure areas and applications, established protection solutions such as firewalls or hardware appliances often reach their limits.

The graphic shows the distribution of the number of vectors for all multi-vector attacks.



Analysis of a DDoS attack with 14 vectors

On May 16, 2020, the LSOC registered a multi-vector attack whose attacker combined 14 techniques. The vectors were implemented in parallel and were not staggered. The attack lasted 12 minutes, during which the attack bandwidth slowly built up and reached its peak of 4.6 Gbps in the seventh minute. The attack volume then rapidly fell within two minutes. The DDoS traffic came largely from North America, Asia, and Europe. The main source countries were the USA, China, Korea, Japan, Brazil, the UK, India, and Italy. AWS and Microsoft Azure were traced as misused cloud providers.



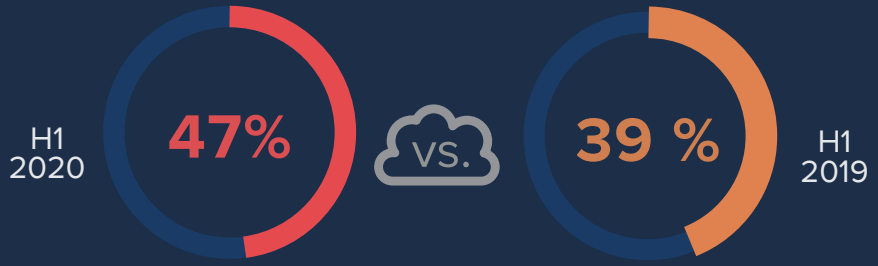
DDoS attacks from the cloud

In recent years, the misuse of cloud services has become the norm for DDoS attackers. The share of DDoS attacks instigated via cloud servers averaged 47% in the first half of the year. It was, however, subject to fluctuations: In April the figure was 52%, but in June it was only 41%. In the same period of the previous year, the average value was 39%.

Instances from all established providers were misused, but most commonly those of Microsoft Azure, AWS, and Google Cloud. The attackers rely on various strategies to gain access. One way consists of opening cloud accounts with false identities and paying for them with stolen credit card data (which are often traded in dark web forums). Alternatively, they hack into the management consoles of company-operated cloud installations. Within this cloud environment, they set up a private cloud with the desired number of servers. When the attacks have finished, the hacker switches off the servers and resets everything to zero. At the end of the month, companies get an unwanted surprise with their cloud service credit card bill in the form of a significantly higher billing amount.

For cloud providers, who explicitly prohibit misuse of their service in their terms and conditions, tracing reported abuse is difficult. The perpetrators only use the cloud server for a limited period. By the time companies point out the misuse, they have long since moved on to the next account.

Proportion of DDoS attacks using cloud servers



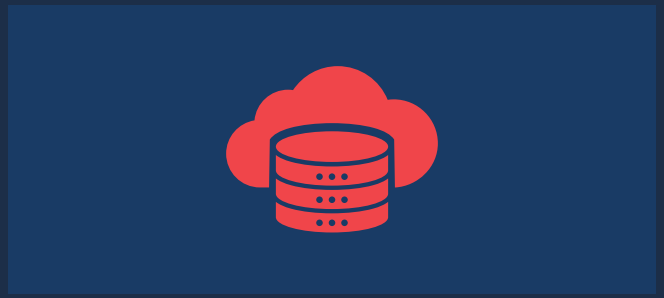
These cloud providers are particularly well-liked by DDoS criminals.

29% Microsoft Azure	26% aws	9% Google Cloud	6% Alibaba Cloud
6% ORACLE DATA CLOUD	5% DigitalOcean	4% SOFTLAYER	16% Other Cloud-Providers

Threat situation outlook for second half of 2020

Coronavirus changes the demands on company IT

The pandemic has massively accelerated digital transformation for states, administrations, and businesses, but also accelerated unwanted side effects. Wherever business or communication processes are being digitally transformed, DDoS attacks and other cyber attacks are never far away. The home office will continue to represent a major security risk for many companies. Much still needs to be done to secure networks and systems and to ensure the masterful tackling of disruptions such as attacks from the internet. After all, the push toward digitalization comes with a growing dependence on services and service providers.



Attackers take advantage of IoT and cloud growth

DDoS attackers are increasingly misusing the connected everyday world, as well as elements from company IT, for their own ends. They are continuously finding weak points in internet-enabled devices and systems to expand their botnets or to develop new methods of attack. In so doing, they are benefiting in particular from the expansion of the global IT infrastructure via public cloud providers. First, this facilitates their access. Second, the accounts, with high-bandwidth connections, offer perfect conditions for starting high-volume attacks. The potential impact of the attacks is greater than ever before.

Rethinking IT security in the direction of automation

In the face of highly developed threats from cyber attacks and a rising dependence on digital services, many established protection solutions are no longer up to date. The growing data streams are accompanied by a rise in the number of suspicious and dangerous incidents. Security concepts that rely on static rules and patterns as well as the human factor offer only a partial defense. Continuous monitoring demands automated protection solutions that rely on automation, artificial intelligence, and machine learning to increase the quality of prevention, detection, and reaction.

About the report

Methodology

The Link11 DDoS report 2020 is based on data from the monitoring of Link11's global network. The staved-off attacks targeted websites and servers that are protected against DDoS attacks by Link11. The data were collected between January 1 and June 30, 2020. Due to a change in the methodology for identifying and counting attacks in 2019, the total number of attacks in this report is not comparable with attack numbers in previous reports. In addition to network analyses and the evaluation of DDoS attack data, the Link11 DDoS report also makes use of open source intelligence (OSINT) analyses.

About LSOC

The Link11 Security Operation Center (LSOC) comprises a team of experienced DDoS protection experts. Running 24/7, it helps well-known companies globally to protect themselves against cybercrime and DDoS attacks. The LSOC is also responsible for the further development of the Link11 DDoS Filter Clusters and the permanent expansion of the necessary infrastructures. The LSOC publishes the results of its work and an analysis of attacks on a regular basis in the form of reports and alerts; it also analyses current DDoS security incidents on Link11's IT security blog https://www.link11.com/en/blog/.

About Link11

Link11 is the leading European IT security provider in the field of cyber-resilience. The global protection solutions of the Cloud Security Platform are fully automated, react in real-time and defend against all attacks, including unknown and new patterns, in under 10 seconds. According to unanimous analyst opinion (Gartner, Frost & Sullivan) Link11 offers the fastest mitigation (TTM) available on the market. To ensure cyber-resilience, web and infrastructure DDoS protection, bot- mitigation, API protection, secure DNS, zero touch WAF, secure CDN, and threat intelligence services, among others, ensure holistic and cross-platform hardening of corporate networks and critical applications. International customers can thus concentrate on their business and digital growth. Since the company was founded in 2005, Link11 has received multiple awards for its innovative solutions.

Editors

Link11 / Katrin Gräwe
k.graewe@link11.com

Photo credits

iStock ID: 1032524414 (Cover)
iStock ID: 1217986221 (Page 3)

Contact

info@link11.com
+49 (0) 69-264929777

Graphics

Link11 GmbH