Distributed Denial of Service Report

for the Year 2020

The 2020 DDoS Threat Landscape at a Glance

50 million the estimated total number of DDoS attacks worldwide in 2020

14 the highest number of vectors recorded in a single attack

2.3 TBPS the new DDoS attack bandwidth record [5]

5,698 minutes length of the longest DDoS attack; equates to nearly 95 hours, or four full days of continuous bombardment

+ 98% average percentage increase in DDoS attacks during the Covid-19 pandemic

59% the share of attacks that combined multiple attack techniques and made systems harder to defend

Three new attack vectors that generate even more high-volume attacks were detected:

1. DVR DHCPDiscovery
2. Plex Media Server
3. Citrix Netscaler

COVID-19 Caused a Boom in DDoS Attacks

Data traffic changed dramatically during the Covid-19 lockdowns. The use of video conferencing services and home office access via VPNs increased sharply. The internet exchange DE-CIX in Frankfurt reported 120% more traffic because of video conferencing. [1] Furthermore, corporate use of cloud-based services increased. Other usage increases were recorded in:

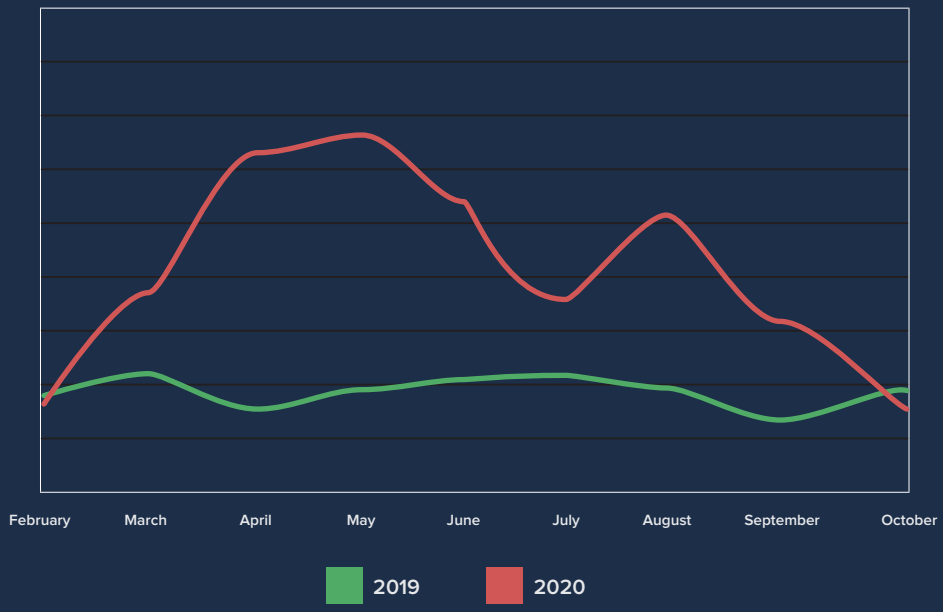
- Media outlets and official websites that provided information about the pandemic
- E-learning platforms for schools and universities, and
- Online retail
- Entertainment like streaming and online gaming

The growth of data traffic also accelerated significantly. Peak data throughput registered a 27% year-on-year increase.

Also, companies had to adapt their IT infrastructures for remote work and ensure their permanent availability for outside access. Because of remote work, VPN servers and interfaces to cloud-based applications became a business-critical element; at the same time, the BKA warned, they became attractive attack targets. [2] They could serve as a gateway for data theft, or manipulated overload attacks could block or disrupt data exchange and work processes throughout the company.

From February to September, the number of attacks recorded on Link11's network was significantly higher than in the same period last year. The increase averaged 98%, with a peak of over 197%. In addition to VPNs and APIs, the attackers also focused on CRMs, databases, email and web servers. The attacks affected all layers. Since there was already a high load on the attacked services, even relatively small attacks of several Gbps or low packet rates were enough to overload inadequately protected infrastructures.

Number of attacks since the beginning of the pandemic compared to the previous year



Number and Distribution of DDoS Attacks

DDoS attacks are increasing everywhere. For 2020, it can be assumed that there were more than 50 million attacks in total, of which LSOC has defended against a significant portion. The 50 million approximation is derived from LSOC's long-term observations in combination with OSINT analyses and represents an extrapolation.

Currently, no macroscopic view of the global DDoS threat landscape exists, as analyses of individual SOCs by protection vendors and university research teams tend to focus on individual regions or networks. That said, in 2017, researchers from several universities researched the total number of attacks on the Internet. [3] They concluded that nearly 21 million attacks – an average of 28,700 attacks per day – had been launched over a two-year period. For 2020, an average of 137,000 attacks per day can now be assumed. Most attacks targeted e-commerce, financial services, and hosting providers. However, healthcare and educational institutions have also become frequent attack targets.

The main reason for the growing number of attacks is the steady increase in the attack surfaces in society and the economy resulting from the ever-growing use of online services and digital transformation in industry. These developments were accelerated by the Covid-19 pandemic – as described by LSOC in the summer of 2020 – and have led to a resurgence of this form of attack.

At the same time, attackers are finding it much easier to obtain suitable DDoS weapons. In addition to freely available source code for DDoS attack tools, the operators of numerous platforms offer DDoS attacks as a paid service. Law enforcement agencies are waging an important but seemingly hopeless battle against these so-called DDoS-as-a-service or DDoS-for-hire services. Once a platform is taken down, several new online services sprout up, Hydra-like. The offer is large, and access is easy. The risk of getting caught is comparatively low. The probability that a cybercriminal will be detected and prosecuted in the US is 0.05%. [4]

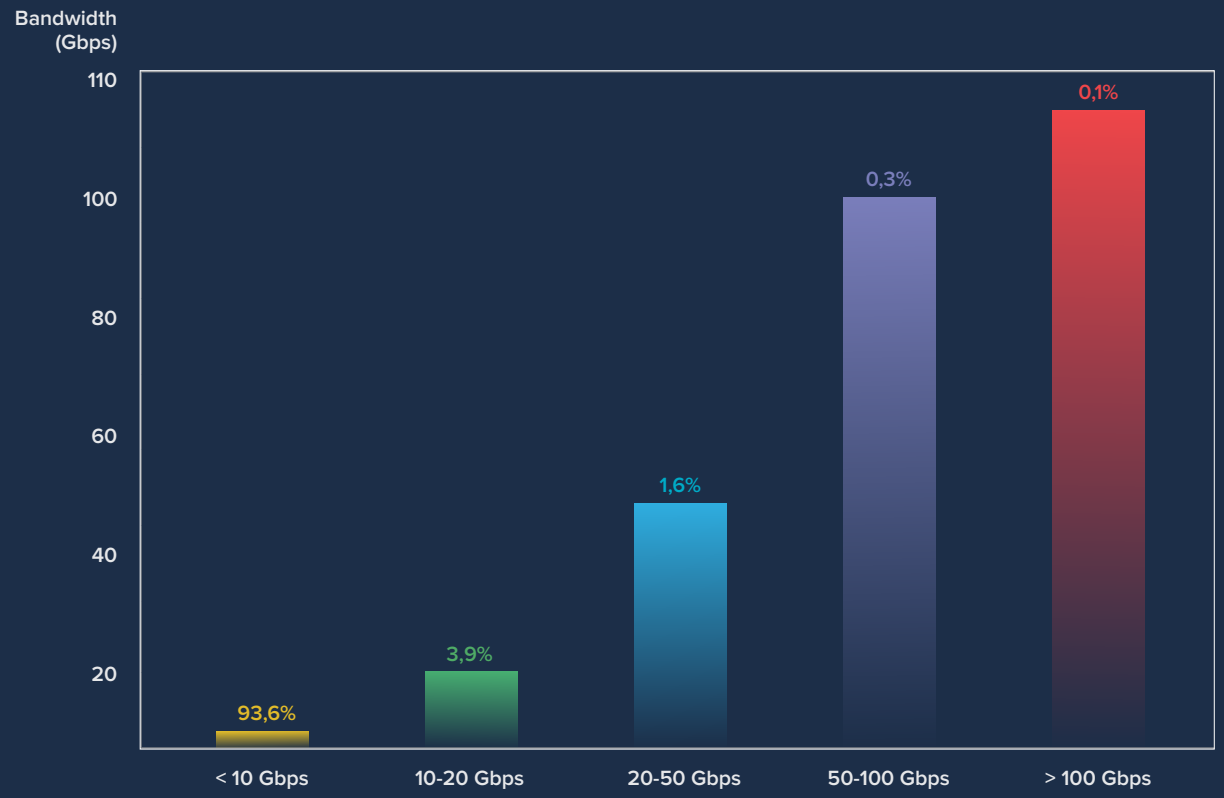
Volume of DDoS Attacks Continues to Rise

The number of high-volume attacks has continued to increase. In the period under review, LSOC recorded 48 attacks with bandwidth peaks above 100 Gbps. There were 175 other attacks with bandwidth peaks between 50 and 100 Gbps. Overall, 25% more high-volume attacks occurred than in the same period last year. The largest attack stopped at 406 Gbps.

In the majority of attacks (93.6%), the attack bandwidth was up to 10 Gbps. Another 3.9% of the attacks analyzed peaked between 10 and 20 Gbps, and 1.6% peaked at volumes between 20 and 50 Gbps.

From a public perspective, attacks of a few Gbps are essentially invisible. Many IT managers associate DDoS threats with high-volume attacks of more than 100 Gbps, which are often picked up in the media as new DDoS records. For example, in February 2020, AWS reported an attack of 2.3 Tbps. [5] The largest known DDoS attack occurred in March 2018. It measured 1.7 terabits per second.

High-volume attacks do indeed pose a threat to almost any unprotected enterprise. However, LSOC estimates that for the majority of companies, even a fraction of this attack volume is enough to overload their IT infrastructures. Therefore, IT security should be designed to handle the widest possible range of attack bandwidths.



Duration of DDoS Attacks and Their Distribution

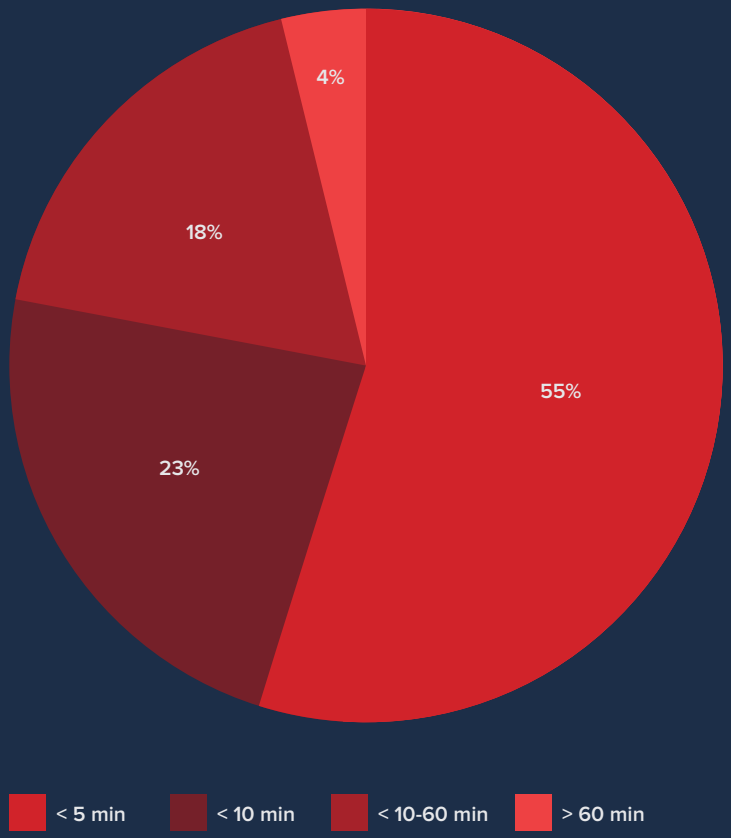
The analysis shows that attack durations varied from a few minutes to several days. The majority of attacks (78%) lasted up to ten minutes. Still, 18% of all registered attacks were between 10 and 60 minutes long, and another 4% were up to 300 minutes long. Several hundred attacks lasted longer than 300 minutes. The longest attack was 5,698 minutes, equivalent to nearly 95 hours or four full days of sustained fire.

The decisive factor in short or long durations is often the attack technique. Attackers often use short attacks of a few minutes to scan their target's IT infrastructure for vulnerabilities by briefly attacking individual IPs. Another tactic is to blast the target with short, high-frequency attacks, like pinpricks. The constant alternation between attack and attack pause can last for hours or days, blocking the bandwidth of the company. This is often the case when the attacks are ordered from DDoS-for-hire services. Most IP stressor and booter services offer attack packets of 600 to 1,200 seconds in duration.

Relatively small and short DDoS attacks are also used to disguise parallel hacker attacks on servers and networks. By flooding control systems with junk events at high frequency, attackers keep the IT team busy, tie up their resources, and provide the necessary distraction. As a result, external infiltrations of a network or data theft, for example, become less noticeable.

In many cases, however, DDoS attacks are short-lived because the attackers realize they can't reach their target. If the attacks are bounced off of well-protected infrastructures, the attackers usually pull back to save their resources.

In the case of long-lasting attacks, the attackers often aim to cause permanent disruption to the attacked infrastructures.

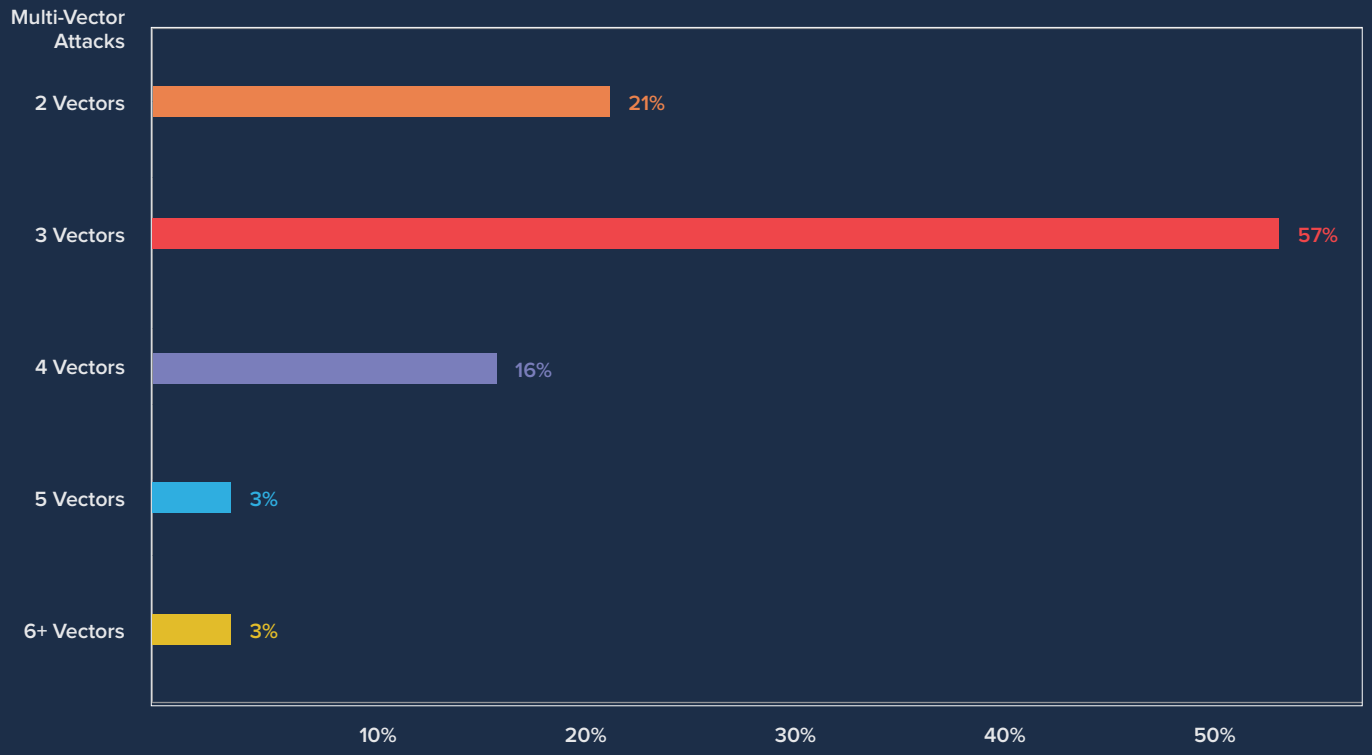


Multi-Vector Attacks Continue to Gain in Complexity

The majority of DDoS attacks (59%), were characterized by complex attack structures. The attackers simultaneously targeted various potential vulnerabilities in the IT infrastructure. In addition to flood attacks, they also used attacks at the application and protocol level as well as reflection amplification techniques. Multi-vector attacks are more complicated to defend against compared to attacks that rely on only one attack technique, such as pure UDP attacks or TCP floods.

Of the multi-vector attacks, attacks with three vectors were the most common. They accounted for one-third (57%) of all registered multi-vector attacks. This was followed by two-vector attacks (21%) and attacks with four vectors (16%). Attacks with five vectors accounted for 3%. The highest number of vectors was 14. That attack included the well-known amplification reflection vectors DNS, NTP, and CLDAP but also emerging attack techniques such as WS Discovery, Apple Remote Control, and Citrix Netscaler.

Combining multiple techniques increases the chances of attack success. Every port and every layer poses a risk to uninterrupted traffic or network operations. If requests and data are only selectively monitored at individual points without including all layers and ports, there is a risk that attacks will be detected too late.

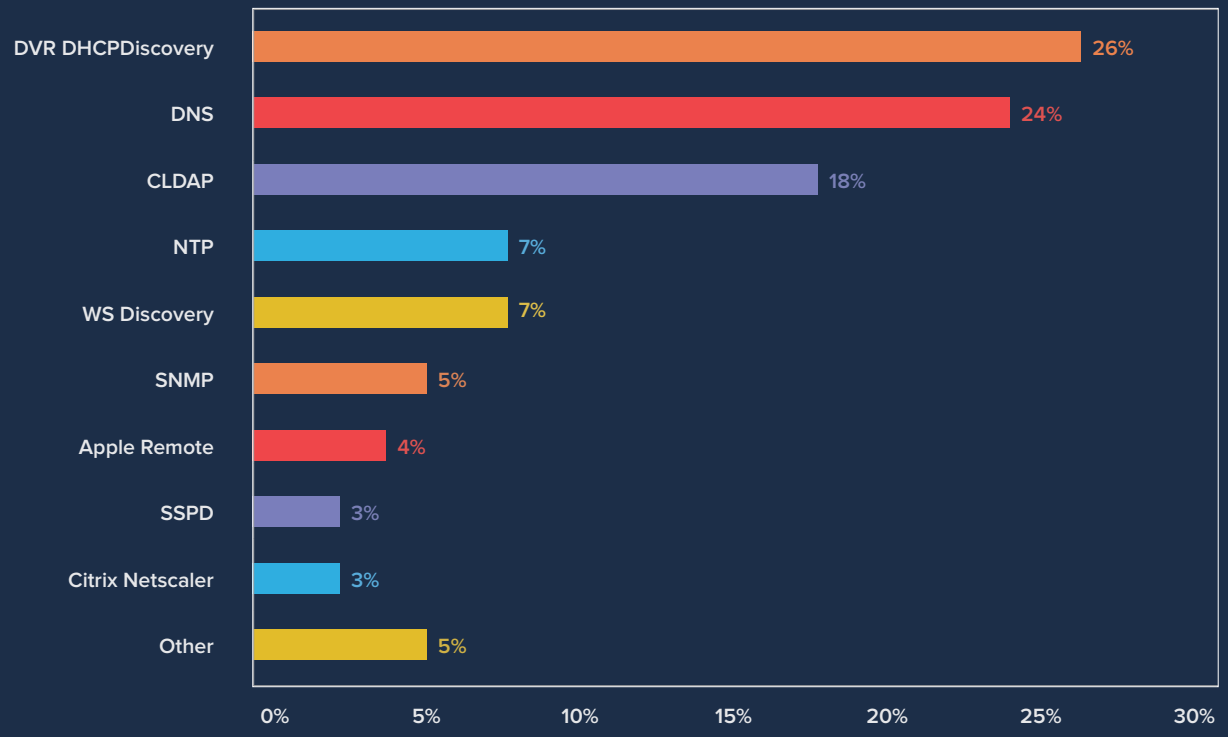


The Most Important Reflection Amplification Vectors

Reflection amplification techniques based on UDP have played a large part in the increase in multi-vector attacks. These vectors, which are designed to increase bandwidth or packet rates, can be combined in any number of ways. Reflection amplification was used in two-thirds of all attacks with a bandwidth greater than 100 Gbps.

LSOC recorded nearly two dozen amplification techniques in 2020. Among them were attack techniques such as DNS or NTP reflection amplification, which have been a part of DDoS attackers' arsenal since as early as 2013. They are characterized by high amplification factors – a maximum of 54 for DNS and 556 for NTP – and high availability in the global Internet infrastructure. Vectors such as CLDAP, SSDP, and SNMP, which have also been used for several years, also played an important role.

LSOC also registered new vectors such as DVR DHCPDiscovery, Citrix Netscaler, and Plex Media. Almost every year, DDoS attackers identify new vulnerabilities for DDoS attacks. Many of them, such as CoAP or Memcached, enjoy high popularity for a few months before being replaced by other techniques. 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 be used to overload corporate IT infrastructures.



New Reflection Amplification Vectors in 2020

LSOC observed new attack vectors in 2020 in the area of reflection amplification. Among them, three particularly stood out: DVR DHCPDiscovery, Plex Media Server, and Citrix Netscaler. Strikingly, two of the three new vectors originate from the private-use IT sector, many of which have weak or no protection against cyber-attacks.

DVR DHCPDiscovery

The technique exploits a vulnerability in digital video recorders (DVR devices). Hard-disk recorders that record footage from web-cams or regular television programming can be controlled and configured over the web. The <get-config> command can be used to query information about storage space utilization, recording times, and operational readiness. The amplification factor of the new DDoS vector is between 20 to 30.

LSOC registered the first attack with the new vector in November 2019, at which time the attack technique was used sporadically. Over the course of the year, the vector became the most commonly used amplification technique; it was used in 26% of all reflection attacks. Attacks relying on DVR DHCPDiscovery as a reflection amplification vector, among others, reached bandwidth peaks of up to 118 Gbps.

Plex Media Server

The media server makes it possible to stream music, videos, or pictures to a wide variety of devices. The remote access required for this is via port 32400 with the SSDP protocol enabled. The amplification factor is 4. LSOC saw sporadic abuse of Plex Media Servers as early as Q2 2020 but did not pay further attention to them because the attacks were successfully stopped by fully automated DDoS mitigation. In the second half of the year, the number of attacks increased to as many as 100 a month, bringing them into the focus of network monitoring. Plex media server is mostly combined with other reflection amplification vectors. The attacks can then reach 36 Gbps at their peak.

Citrix Netscaler

DDoS attacks against Citrix Application Delivery Controller (ADC) systems with Enlightened Data Transport (EDT) enabled began to increase worldwide in late December 2020. Citrix systems are an integral part of many corporate IT infrastructures, as they allow employees to access corporate networks when they are working remotely. EDT is used to improve the performance of applications and services. To use EDT, the Datagram Transport Layer Security (DTLS) protocol (port 443) must be enabled.

DTLS was developed to allow the transmission of encrypted data not only via secured, connection-oriented transport protocols such as TCP but also via the connectionless UDP. It turns out to be a disadvantage that DTLS, like all UDP-based protocols, can be spoofed and that the reply packages can be significantly larger than the requests. Initial analyses assume an amplification factor of 35 for DTLS attacks.

The maximum value in the attack bandwidth for reflection amplification attacks via Citrix Netscaler was 107 Gbps.

Increases in DDoS Extortion

In the 2nd half of the year, there were several globally distributed waves of DDoS extortions. The attackers claimed to be Fancy Bear, Cozy Bear, Armada Collective, and Lazarus Group. LSOC believes they were copycats and not the original perpetrators. However, that did not make them any less dangerous. On the contrary, the perpetrators were extremely aggressive. The New Zealand Stock Exchange, which had to suspend trading for several days at the end of August due to DDoS attacks, gained sad notoriety in this regard.

The Method

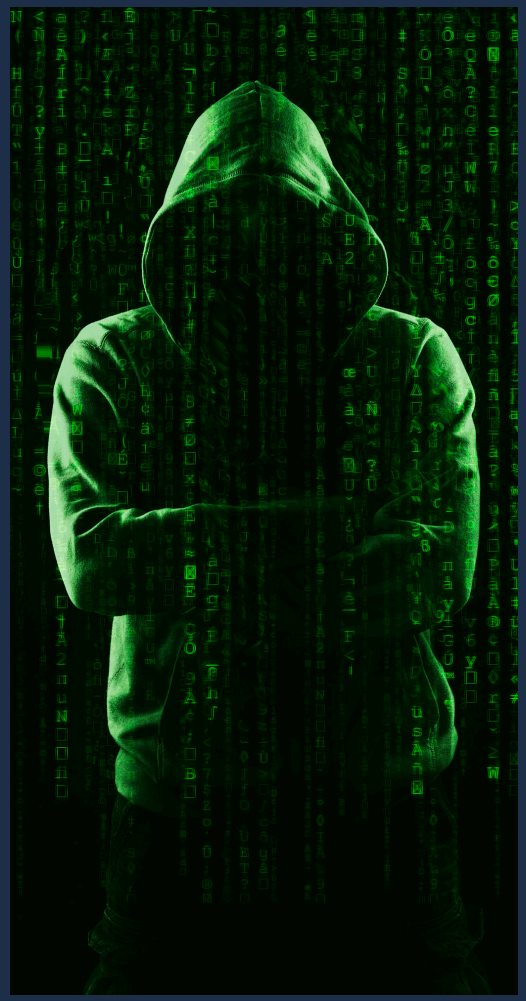
Cybercriminals often used DDoS attacks to force the victim to pay a ransom. The perpetrators launched an initial DDoS attack as a clear warning to the target company to underline the severity of the protection-money demand. Essentially, the demand was: Pay us what we're asking, or we'll attack you and take your company offline. In some ways, the strategy was similar to that of ransomware attacks. The company can no longer continue business operations or adequately protect its threatened systems or data, forcing it to pay.

Intimidation through Warning Attacks

In DDoS extortions from H2 2020, the perpetrators relied on high-volume warning attacks ranging from 10 to over 100 Gbps. In extortion letters emailed to multiple individuals and distribution lists in the attacked company, the attackers announced attacks of up to 2 Tbps: *"Our attacks are extremely powerful, sometimes over 2 Tbps per second" or "our attacks are extremely powerful (peak over 2 Tbps)."* The extortion email also included IP addresses of the company targeted by the demo attacks.

Ransom in Bitcoin

The extortionists' demands ranged from 5 to 15 bitcoin. As of mid-August, 15 bitcoin was equivalent to about 150,000 euro. The cryptocurrency was to be transferred to a victim-specific Bitcoin wallet to monitor receipt of payment. The anonymous crypto-currency helps cybercriminals disguise the payment channels of their extorted money. On the other hand, the extortionists themselves pay with cryptocurrencies when they rely on DDoS-for-hire services to carry out their attacks.



Scale of the Extortions

The global campaigns primarily targeted operators of critical infrastructure, financial service providers, online retailers, and hosting providers. More than 100 banks, stock exchanges, insurance companies, and other financial firms worldwide were targeted by the same type of DDoS extortion that crippled the New Zealand Stock Exchange in August, although the scale of the damage was smaller.

Response Options

In their extortion emails, the perpetrators pointed out in many cases that basic protection solutions would not prevent the threatened high-volume attacks: *"no cheap protection will help"*. The blackmailers quickly backed away from companies where the demo attacks bounced due to the presence of appropriate protection measures.

DDoS Extortionists Target Hosting Providers and ISPs

In the context of DDoS extortion waves in the 2nd half of 2020, attacks on hosting providers and ISPs all over Europe also increased. For example, on August 28, more than a dozen ISPs in France, Germany, the Netherlands, and Belgium reported DDoS attacks targeting their DNS infrastructure. Not all providers could withstand the attacks, which lasted several hours and peaked at nearly 300 Gbps, causing outages. In the following months, hosting providers in other European countries were also targeted by extortionists.

DDoS Attacks Put Hosting Services at Risk

Hosting providers and ISPs are a profitable target for DDoS criminals. For example, in the B2B sector, providers supply dozens or hundreds of companies with data center services at the same time. In addition to the floor space in the data center, the customers usually also share the connection to the Internet. A successful attack on the data center affects all customers that share this Internet link. For example, a November 2020 extortion email supposedly from Fancy Bear stated: *"All customers hosted with you will suffer."*

Customers expect the hosting provider to fulfill the SLAs for service availability and external connectivity. If outages occur, they will open support tickets by the hundreds in a very short time, complain to the company, and even take legal action for damages. Ultimately, the hosting company will probably lose customers due to the incident, and its reputation will certainly be damaged. The extortionists play on this fear, saying, in effect: *We will destroy your reputation and make sure your network will remain offline until you pay.*

Danger from High-Volume Attacks

Data centers that are inadequately protected against high-volume attacks and do not respond to extortion must act quickly. The payment period set by the perpetrators is usually between 2 to 5 days. Dropping all traffic, as a practice known as black-holing, does not solve the problem of the blocked line, as no traffic reaches customers. Likewise, installing more appliances is not enough in the face of attacks of several hundred Gbps. The new appliances could quickly reach their capacity limits due to the flood of requests.

Experience shows that data centers are only protected against high-volume DDoS attacks if all the data center traffic is redirected and cleaned by multi-stage filtering processes conducted by an external protection solution provider. Cloud-based protection solutions can also scale easily.

Under the Radar: Carpet Bombing

Carpet bombing attacks are another DDoS weapon against hosting providers. In contrast to high-volume attacks, DDoS attackers here rely on a large number of small attacks. Instead of targeting individual IP addresses, they target the entire network block. The data volume of each DDoS bomb is so small that it evades the DDoS radar of most protection solutions and is therefore not filtered. However, in total, the attack bandwidth of all attacks equals that of a high-volume attack. For secure detection and immediate filtering, all traffic on a network must be brought together and considered as a whole.

DDoS Attacks that Hit the Headlines in 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. [6]

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. [7]

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. [8]

March 18, 2020

Customers wait in vain for food orders

The German food delivery service Lieferando has experienced a boom during the corona-virus crisis. Hackers take advantage of this: they begin with DDoS attacks on Pizza.de, then attempt blackmail, which the company refuses to engage with. [9]

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. [10]

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. [11]

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. [12]

DDoS Attacks that Hit the Headlines in Second Half of 2020

August 2, 2020

Internet outages in parts of Australia

On the east coast of Australia, customers of the local telecommunications provider Telstra were unable to go online for four hours. DDoS attacks overloaded the company's DNS infrastructure. [13]

August 31, 2020

SwissSign battles DDoS attacks

From August 31 to September 8, 2020, Swiss-Sign Group had to fend off DDoS attacks. Products and services of the company, such as the digital certificate SwissID, were therefore only available to a limited extent. [15]

September 24, 2020

Financial and telecom infrastructure disrupted in Hungary

Numerous banks in Hungary and Hungarian Magyar Telekom were targets of DDoS attacks that came in several waves. Some financial institutions experienced disruptions, and the Magyar Telekom network was also partially overloaded. [17]

November 3, 2020

British online broker offline

Trading 212, a fintech company based in the UK, reported problems with its platform. For about an hour, access to the trading portal, which manages about 1 billion pounds in customer assets, was disrupted due to DDoS attacks. [19]

August 25, 2020

Stock exchange trading suspended in New Zealand

The New Zealand Stock Exchange struggled with massive problems as a result of DDoS attacks. Trading in the $135-billion market had to be suspended for four days. The attacks were part of an extortion attempt. [14]

May 9, 2020

US teenager took schools offline

A Florida teenager allegedly attacked several schools using a simple open-source tool for DDoS attacks. As a result, educational institutions near the city of Miami were unable to hold online classes for three days. [16]

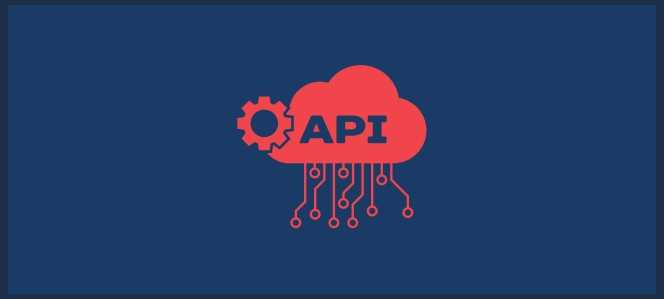
October 22, 2020

Mega attack against Norwegian telecom blocked

Telecom provider Telenor Norway successfully mitigated a three-hour DDoS attack of 400 Gbps. The company did not respond to the extortion email for 20 bitcoin that arrived shortly after the attack. [18]

5G will ensures growth in DDoS attack size

In executing attacks, cybercriminals will benefit from the network expansion provided by 5G, which ensures continuous evolution of Internet infrastructure in terms of bandwidth strength. The fast transmission rates and low latency will give a further boost to the trend of high-volume attacks. Once the standard is rolled out across the board to billions of networked devices, new volume peaks in attacks can be expected. Also, expect to see a greater number of attacks exceeding 50 Gbps.



More attacks on cloud services and APIs

DDoS attacks are no longer limited to local IT infrastructure. The use of cloud services in the B2B sector has intensified in recent months and will continue to grow. This means that more and more companies are using cloud-native applications, which often communicate via APIs. The interfaces through which personal data, payment information, or measurement data are exchanged are particularly vulnerable to DDoS and bot attacks, as they can easily become clogged and create a bottleneck. To prevent this, proper safeguards must be implemented.

Danger of DDoS extortion for companies of all sizes and industries

As organizations become increasingly dependent on IT, cybercriminals will continue to launch extortion campaigns such as those seen since the summer of 2020 on behalf of Armada Collective and Fancy Bear. More than any other type of cyberattack, DDoS attacks can bring digital business processes to a quick and long-lasting standstill. In doing so, the perpetrators will not only attack enterprises whose financial resources are large but also smaller and medium-sized companies, as they often lack sufficient protection and thus represent a worthwhile target.

Sources

1) DE-CIX: The Internet defies the pandemic, bearing the protracted global burden of Corona – monumental growth in 2020, December 2020

(2) BKA: Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, September 2020

(3) M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti: Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem, in ACM Internet Measurement Conference (IMC), November 2017

(4) World Economic Forum: The Global Risks Report 2020, Januar 2020

(5) AWS Shield: Threat Landscape Report - Q1 2020

(6) Handelsblatt: Externer Angriff legte DKB-Homepage lahm, 07.01.2020

(7) Forbes: Powerful Cyber Attack Takes Down 25% Of Iranian Internet, 09.02.2020

(8) Bloomberg: Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak, 16.03.2020

(9) Der Westen: Lieferando: Hackerangriff! Kunden warten vergeblich auf ihr Essen, 19.03.2020

(10) Teller Report: Hospital systems Paris inaccessible for hours on end due to DDOS attack, 23.03.2020

(11) Tageblatt Letzebuerg: Hacker legen die Website der Universität Luxemburg per DDos-Angriff lahm, 21.02.2020

(12) TASS: DDoS attack on online voting system registered on Saturday - mayor's office, 27.06.2020

(13) Techguide: What caused the major Telstra NBN outage and disconnected customers, 02.08.2020

(14) CSO: NZX New Zealand stock exchange suffers multi-day DDoS attack, 30.08.2020

(15) The Daily Swig: DDoS attacks against SwissSign prompt temporary CA switch for ProtonMail, 09.09.2020

(16) Wired: A Florida Teen Allegedly Shut Down Remote School With a DDoS Attack, 05.09.2020

(17) Reuters: Hungarian banks, telecoms services briefly hit by cyber attack: Magyar Telekom, 26.09.2020

(18) telecompaper: Telenor Norway thwarts DDoS attack without paying NOK 2 mln ransom, 22.10.2020

(19) Cryptovibes: UK Brokerage Trading 212 Restores Trading, Recovers from DDoS Attack, 04.11.2020

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 was collected from January 1 to December 31, 2020. Due to a change in the methodology used to identify and count attacks in the second half of 2020, the data is not comparable to statistics cited 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 headquartered in Germany, with sites worldwide in Europe, North America, Asia and the Middle East. The cloud-based security services 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, Forrester) Link11 offers the fastest detection and mitigation (TTM) available on the market. The German Federal Office for Information Security (BSI) recognizes Link11 as a qualified DDoS protection provider for critical infrastructures.
To ensure cyber-resilience, web and infrastructure DDoS protection, Bot Management, Zero Touch WAF and Secure CDN Services among others provide holistic and cross-platform hardening of business' networks and critical applications. The 24/7 operated Link11 Security Operation Center, which is located at sites in Germany and Canada according to the follow-the-sun principle, provides the reliable operation of all systems and manages the expansion of the global MPLS network with 41 PoPs and more than 4 Tbps capacity. Guaranteed protection bandwidths of up to 1Tbps provide maximum reliability. 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 and business growth.

Editors

Link11 / Katrin Gräwe
k.graewe@link11.com

Photo Credits

shutterstock 1421446100
shutterstock 709660042
iStock 1206098096
iStock 1060638540
iStock 1144149567

Graphics

Link11 GmbH