Distributed Denial of Service Report

First Half of 2021

The threat situation in the first half of 2021 at a glance

+ 33%

more DDoS attacks

555 GBPS

is the maximum value for attack bandwidth

+ 36%

increase in maximum attack volume

+ 100%

increase in high-volume attacks in Q2 2021 vs. Q1

+ 147%

increase in maximum packet rate

65%

of all attacks were complex multi-vector attacks

DDoS attacks that hit the headlines in the first quarter of 2021

January 4, 2021

School platforms under attack

In Germany, school servers and digital learning platforms such as Moodle, the Hasso Plattner Institute's school cloud, and Lernsax were affected by DDoS attacks in January. This made the implementation of distance learning in pandemic times more difficult. (1)

January 13, 2021

Slow internet in Malta

The Maltese internet provider Melita was extorted with DDoS attacks. The attacks caused a significant slowdown in internet connections across the country for several hours but were then successfully mitigated. [2]

January 30, 2021

Digital TV unavailable in Iceland

The Icelandic telecom provider Siminn's streaming TV service was unreachable on a Saturday evening (and in pandemic times to boot). After about two hours, the DDoS attack was stopped and the service was again accessible. (3)

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. [4]

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. [5]

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 motive remained unclear. [6]

DDoS attacks that hit the headlines in the second quarter of 2021

May 4, 2021

Government institutions offline in Belgium

The services and websites of more than 200 government 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. [7]

May 15, 2021

Insurer faces wrath from cybercriminals

After announcing cuts to cyber-insurance for ransomware attacks, insurance group AXA in France came under attack. Several branches in Southeast Asia fell victim to data encryption and DDoS attacks. [9]

June 9, 2021

Widespread power outages in Puerto Rico

Lights went out for just over 700,000 residents in the Caribbean nation after a DDoS attack hit the utility. A substation went up in flames just hours later. [11]

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. [8]

June 3, 2021

No online banking at German cooperative banks

The cooperative banking sector experienced major IT disruptions in online banking and apps lasting several hours. This was caused by DDoS attacks on the IT service provider's data centers. [10]

June 25, 2021

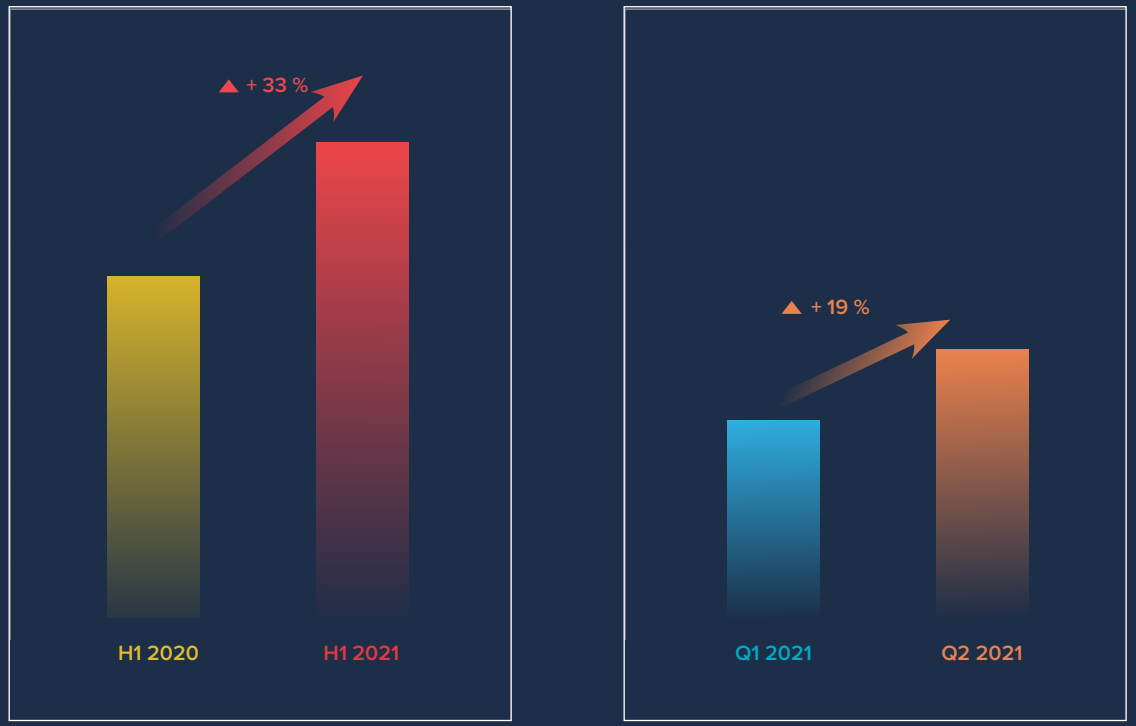
Banks in Israel under attack

Several banks in Israel have been targeted by DDoS attacks. On Telegram, a pro-Palestinian Malay hacker group claimed responsibility for the attacks as a sign of political protest against the Israel-Gaza conflict. [12]

Further increase in DDoS attacks

Cybercriminals launched a record-breaking number of attacks in the first half of 2021. LSOC recorded one-third (33%) more attacks than the same period for the record-breaking DDoS year of 2020, with more than one-fifth of attacks (27%) occurring on weekends. The number and volume of DDoS attacks increased once again from January to June. For example, LSOC recorded 19% more attacks in Q2 than in Q1 2021. This has added to the already high threat level posed by this form of attack. There is no end in sight to the boom in DDoS attacks.

According to IT security experts, this development is due to the ongoing pandemic conditions, which have accelerated digitization and opened up new gateways for attackers. Many attacks targeted web services that ensured living, learning, and working under pandemic conditions. These included vaccination platforms, learning portals, and IT infrastructures for remote working at home offices. Hosting providers and ISPs, which made express digitization in business and society possible in the first place, also came under attack.



Development of attack figures

High volume attacks of up to 555 Gbps

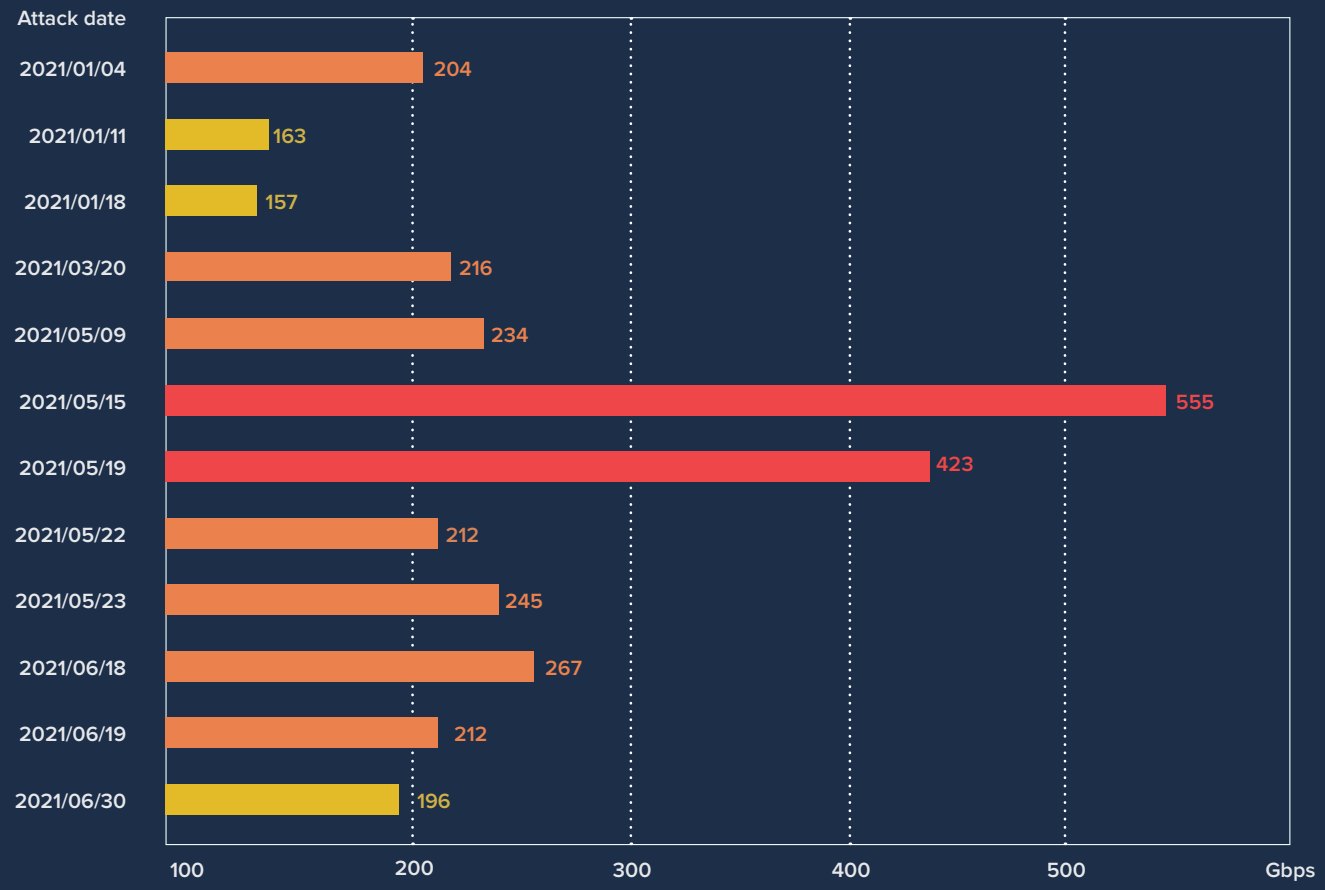
From January to June, LSOC recorded more than 40 attacks with a volume of more than 100 Gbps. In the same period last year, there were just under 30 attacks. Two-thirds of these attacks occurred in Q2 2021, along with 234 other attacks with bandwidth spikes between 20 and 100 Gbps across both quarters. The largest attack of the first half of the year stopped at 555 Gbps and exceeded the maximum attack bandwidth of the same period last year by nearly 38%.

The 555 Gbps attack, which took place in mid-May and targeted a company in the media/entertainment sector, was a DNS reflection attack. In addition to the large attack volume, the attack also stood out because of its long duration of 63 minutes. High-volume attacks usually end after a few minutes to reduce the strain on the attackers' resources. The first half of the year saw numerous other attacks with large attack volumes and very long durations:

204 Gbps and 173 minutes
163 Gbps and 724 minutes
102 Gbps and 62 minutes
93 Gbps and 75 minutes
80 Gbps and 500 minutes.

In no case did the very persistent attackers manage to reach his target and take his target offline.

Almost always, attacks of several 100 Gbps are oversized for the target at hand. Instead, attackers act resource-consciously and adapt their attacks and strategies to the connectivity of their targets, choosing bandwidths between 1 and 10 Gbps.



DDoS extortions: Bitcoin demands in the name of Fancy Lazarus

In 2021, several waves of DDoS (RDDoS - Ransom Distributed Denial of Service) extortions have created a tense threat situation. The peaks of extortionist activity were in January and June. The perpetrators posed as Fancy Lazarus. Their actions were largely identical to the criminal activities of DDoS extortionists that have been operating under the names Armada Collective, Fancy Bear, and Lazarus Group since the summer of 2020.

Businesses targeted

Companies from a wide range of business sectors have received Fancy Lazarus extortion emails, including finance, e-commerce, media and logistics, telecommunications, and hosting providers/ISPs. Reports of RDDoS attacks were received by LSOC from several European countries, including Germany, Austria, the UK, Ireland, as well as the US and Canada. Rather than being indiscriminate, ransom demands varied according to the size of the company and the industry of the victims. In many cases, 2 Bitcoins (as of June 2, 2021, approximately 75,000 euros) were demanded.

How the perpetrators operated

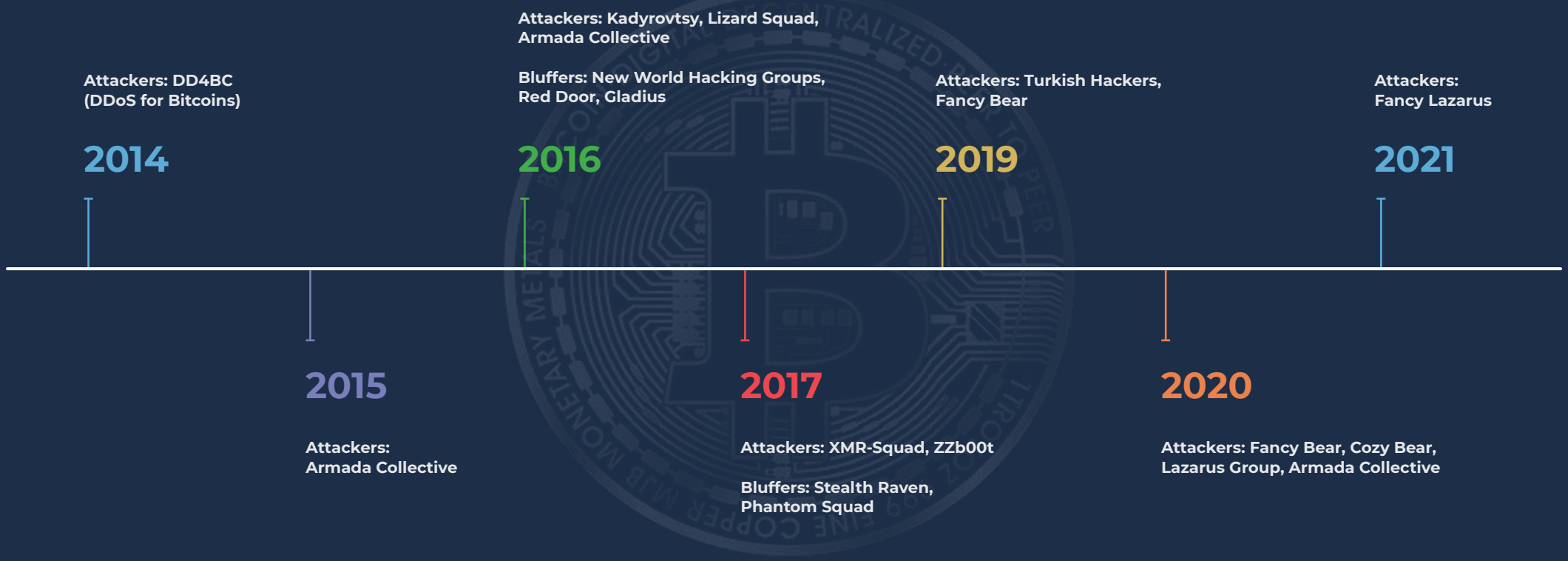
The perpetrators obtained information about the company's IT infrastructure in advance and provided clear details in the extortion e-mail about which servers and IT elements they would attack for the warning attacks. They also used routing information to check whether external DDoS protection is deployed in front of the company network to permanently analyze incoming data traffic for anomalies. If this was not the case, the attackers launched demo attacks, some of which lasted several hours and were 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 perpetrators used reflection amplification vectors such as DNS. If the demands were not met, massive high-volume attacks of up to 2 Tbps were threatened. The company was given 7 days to transfer the Bitcoins to a specific wallet.

Non-payment and follow-up attacks

Companies targeted by DDoS extortionists face the choice of paying up or entering into a dispute with the attackers. LSOC lacks information on whether crypto money has already flowed to Fancy Lazarus. However, there's no guarantee that payment will stop the attacks. One wave of extortionists followed the next. Although perpetrators have repeatedly appeared with new names to stress their demands, who is behind the attacks remains unclear. Those companies that chose the integration of professional DDoS protection solutions were well prepared and protected against the attacks when the set ultimatum expired, and the attacks subsequently went nowhere and were successfully repelled. The high number of emergency onboardings realized between January and June contrasts with zero DDoS-related downtime for protected infrastructures.

Extortion with DDoS attacks: a chronology

DDoS extortion has been a serious problem for businesses for several years. LSOC first warned of the threat in 2014, when it was posed by the international group DD4BC. Since then, the incidents have increased, and companies of almost all sizes and in all industries, from SMEs to global corporations, have now become targets. Among the perpetrators, numerous imitators take their cue from seemingly financially successful extortion gangs and copy their business model – from contacting the victim to the extortion letter – but still call their bluff. However, many perpetrators are serious and invest much criminal energy and resources to obtain cryptocurrencies via their victims. In LSOC's experience, only dedicated protection solutions can help ward off persistent extortion and targeted DDoS attacks that put pressure on the attacked company. The following chronology shows which perpetrators LSOC has observed in the past.



The 5 most prominent DDoS extortions

Often, companies that become the target of DDoS extortion keep quiet about it to avoid damaging their reputation. However, for exposed services such as banking and finance, as well as e-commerce, the downtime is hard to hide. In contrast, other companies seek publicity to warn others about the danger.

November 2015

Protonmail

Swiss crypto webmail provider Protonmail was extorted on behalf of Armada Collective. The company paid a ransom of just over 5800 Swiss francs. The attacks nevertheless continued afterward. [13]

April 2017

DHL, Hermes, and eBay

DDoS extortionists using the name XMR Squad targeted German delivery service providers. In addition to DHL, Hermes, and the shipment pages of the marketplace eBay were also targets of the attacks. The attackers demanded 250 euros for testing the (DDoS) protection. [14]

October 2019

Banks in South Africa

Numerous major banks in South Africa were extorted with DDoS attacks, and online banking services went down. It was suspected that the attackers launched the attack specifically on payday to cause maximum damage. [15]

March 2020

Delivery service Lieferando

German food delivery service Lieferando was booming during the nationwide Covid-19 pandemic lockdowns, and hackers took advantage of it. They first launched DDoS attacks on Pizza.de and then demanded two Bitcoins (around 12,000 euros at the time) but the company refused to pay them. [16]

August 2020

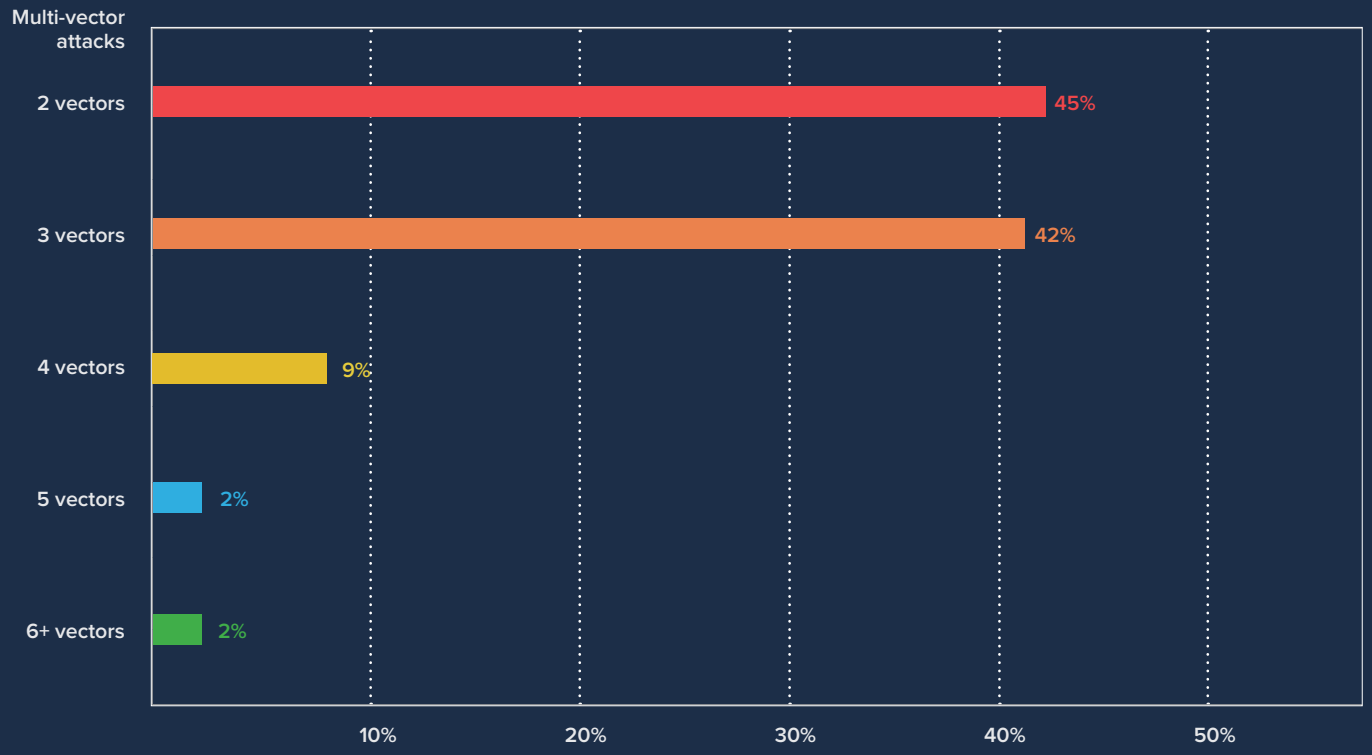
New Zealand Stock Exchange

The multi-day outages on the New Zealand Stock Exchange in August 2020 were attributed to DDoS extortionists. Another 100 banks, stock exchanges, insurance companies, and other financial companies around the world, including PayPal and MoneyGram, were also attacked. [17]

Complex attack patterns prevail

Attackers used a single vector such as UPD or TCP in 35% of attacks in H1. In the same period last year, the figure was 48%. In contrast, most attacks (65%) featured complex attack structures in which the perpetrators combined several techniques. According to LSOC observations, the trend in DDoS attacks has for several years been toward significantly more complex attacks that target vulnerabilities at the transport, application, and protocol levels in parallel. Each attack technique and the protocol abused for it requires a special detection and mitigation strategy, so that in multi-vector attacks not only one attack, but several attacks running synchronously, can be defended against simultaneously. Therefore, for reliable protection of corporate IT, it's important to rely on protection solutions that work effectively at all filtering levels of multi-vector attacks.

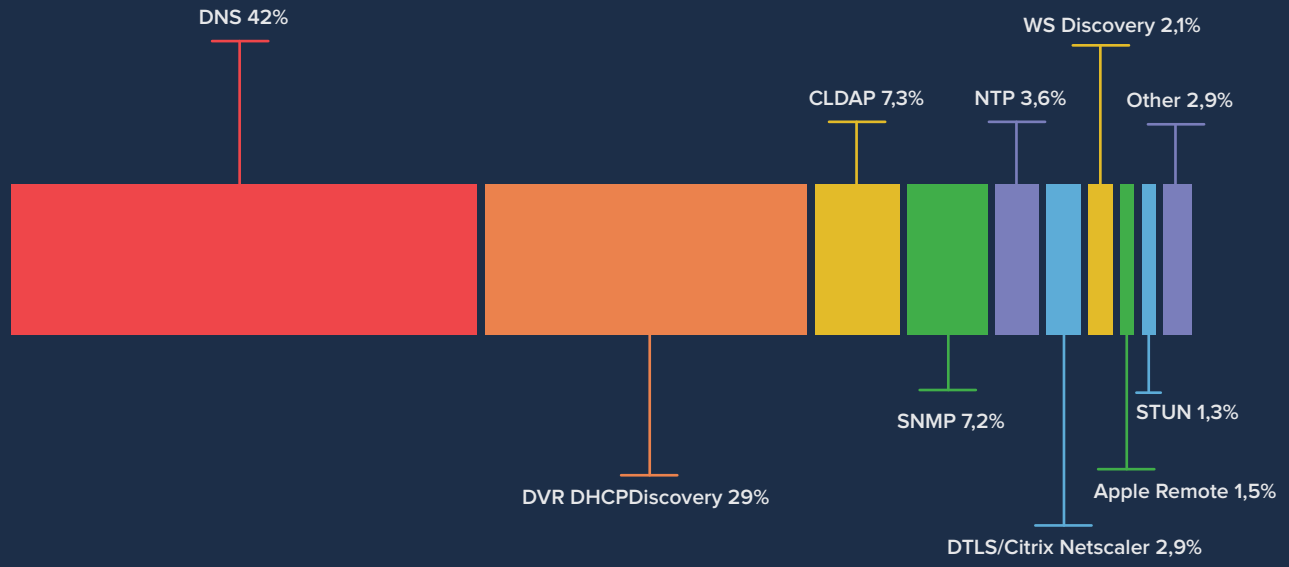
Among multi-vector attacks, attacks with two vectors (45%) were the most common. This was followed by attacks with three vectors (42%) and attacks with four vectors (9%). Attacks with five vectors made up 2% of all registered attacks. The highest number of vectors within was 12. This maximum number of vectors was used in 21 attacks.



Threat from reflection amplification attacks

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 misused for this purpose. The attacker first sends small numbers of data packets to the intermediate servers, which act as amplifiers: They reflect the requests and forward them, amplified by many times, to the actual target of the attack.

The Internet service most frequently exploited for attacks and misused as an amplifier in the first half of the year was DNS (42%), followed by DVR DHCPDiscovery (29%) and CLDAP (7%). The spectrum of these services, also called reflection amplification vectors, is growing with each passing year and currently includes over 20 vectors. In H1, new vectors such as Datagram Transport Layer Security (DTLS) over Citrix Netscaler and Session Traversal Utilities for NAT (STUN) were added to the criminal's stockpile.
DTLS was 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 hidden behind a router or firewall in the local network can communicate with VoIP providers on the Internet.



The most relevant source countries for reflection amplification attacks

The devices and servers that attackers abuse for DDoS attacks are distributed around the world. In H1, most DDoS attack requests came from the US, followed by Germany. DDoS traffic from Russia and China, which accounted for most of the traffic in previous years, has decreased significantly.

USA	27%
Germany	18%
China	7%
Russia	5%
Brazil	5%
Great Britain	4%
Ukraine	3%
Netherlands	3%
India	3%
France	2%

The source countries represented the location of the device used for the attack, not the location of the attackers themselves. The IP address of compromised devices is spoofed in reflection amplification attacks, making it very difficult to determine the origin of the attack.

DDoS threat from attacks from the cloud

DDoS attackers regularly get bandwidth and computing power for their attacks from the cloud. In H1 2021, attackers relied on cloud resources for one in three DDoS attacks (35%). They compromised server instances of public cloud service providers by gaining access via vulnerabilities or exploits. They then uploaded a pre-written script that turns the server into a DDoS bot within minutes. The companies that have used the instances usually do not notice this third-party access, or only when it's too late. In addition, criminals gain access via stolen credit card data and rent cloud instances under false names.

The misuse of cloud servers fluctuated and ranged from 16% in February to 56% in May 2021. The cloud instances from the three major providers – Amazon Web Services (AWS), Microsoft Azure, and Google Cloud – were most frequently detected. In addition, attackers also used cloud offerings from the B2B space such as Oracle Cloud, DigitalOcean, and IBM Cloud.

As cloud usage continues to grow in both private and corporate environments and cloud providers expand their infrastructure, attackers have more and more resources at their disposal. DDoS attacks from the cloud must therefore be classified as a persistent threat.

Proportion of DDoS attacks abusing cloud servers

These cloud providers are particularly well-liked by DDoS criminals

27% aws	15% Google Cloud	11% Microsoft Azure	8% Alibaba Cloud
4% ORACLE DATA CLOUD	4% DigitalOcean	2% IBM Cloud	28% Other cloud providers

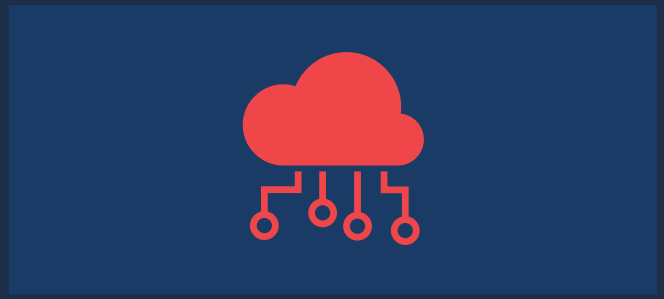
Extortion with DDoS attacks will become the new normal

In the coming months, we can expect to see a further increase in extortion attacks, as seen in the new and shorter waves since the summer of 2020. As enterprises continue to digitize, they provide more and more attack surfaces and become more vulnerable to downtime and business interruptions – unless they have adequate protection. In addition, the low cost and ease of execution of DDoS attacks ensure that extortion attacks will continue to rise.

Sophisticated attacks make playing defense more difficult

Attackers are improving their methods and rarely limit themselves to just one attack technique. Instead, they are increasingly using methods that attack both the volume and the network and application layers at the same time. The misuse of other protocols is also considered safe.

The mixed forms of attack pose new challenges for companies in terms of defense. Protection solutions that only defend against individual types of attack are not enough. Systems with multi-layered anomaly detection and networked security mechanisms must take their place.



The cloud is becoming one of the most effective DDoS weapons

DDoS attacks will continue to be carried out in large measure using compromised cloud servers. Perpetrators are using these with traditional botnets of infected home or corporate servers, as well as IoT devices, broadening their choice of attack tools. At the same time, they benefit from a booming infrastructure. The reasons are obvious: in terms of connectivity, cores, and attack vectors, cloud instances are far superior to other bots such as IoT devices. Their attack volume is up to 1,000 times higher. DDoS attacks and cloud infrastructures are becoming a dangerous combination.

Sources

(1) Berliner-Zeitung.de: Schul-Cloud in Brandenburg von Hackern angegriffen, 11.01.2021

(2) Independent.com: Melita services returning to normal after company faces cyber-attack, 13.01.202

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

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

(5) Telecompaper.com: A1 apologises with 10% discount on accessories for network collapse after DDoS attack, 19.02.2021

(6) Weirditaly.com: Lower House website under attack, 09.03.2021

(7): Threatpost.com: Massive DDoS Attack Disrupts Belgium Parliament, 06.05.2021

(8) Illinoisnewstoday.com: Irish Internet Service Provider Hit by Cyber Attack, 17.08.2021

(9) Infosecurity-magazine.com: AXA faces DDoS after ransomware attack, 18.05.2021

(10) Reuters.com: German cooperative banks hit by DDoS hack attack on IT provider, 04.06.2021

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

(12) Jewishpress.com: Mammoth Cyber Attack on Israel's Banking System Fails, 27.06.2021

(13) Forbes: ProtonMail Pays Crooks $6,000 In Bitcoin To Cease DDoS Bombardment, 05.11.2015

(14) T3n: Erpressergruppe zielt mit DDoS-Attacken auf DHL, Hermes und Ebay, 22.04.2021

(15) Thesslstore.com: Cyber Attacks Hit the City of Johannesburg and South African Banks, 29.04.2021

(16) Bleepingcomputer.com: Food Delivery Service in Germany Under DDoS Attack, 19.03.2020

(17) Zdnet.com: New Zealand Stock Exchange suffers day four disruption following DDoS attacks, 28.08.2020

About the report

Methodology

The Link11 DDoS report for the first half of 2021 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 June 30, 2021. 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 43 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

iStock 962404026 (Cover)
Unsplash / André François McKenzie (page 7)
Pixabay 3374479 (page 8)
Pixabay 4700815 (page 9)

Graphics

Link11 GmbH