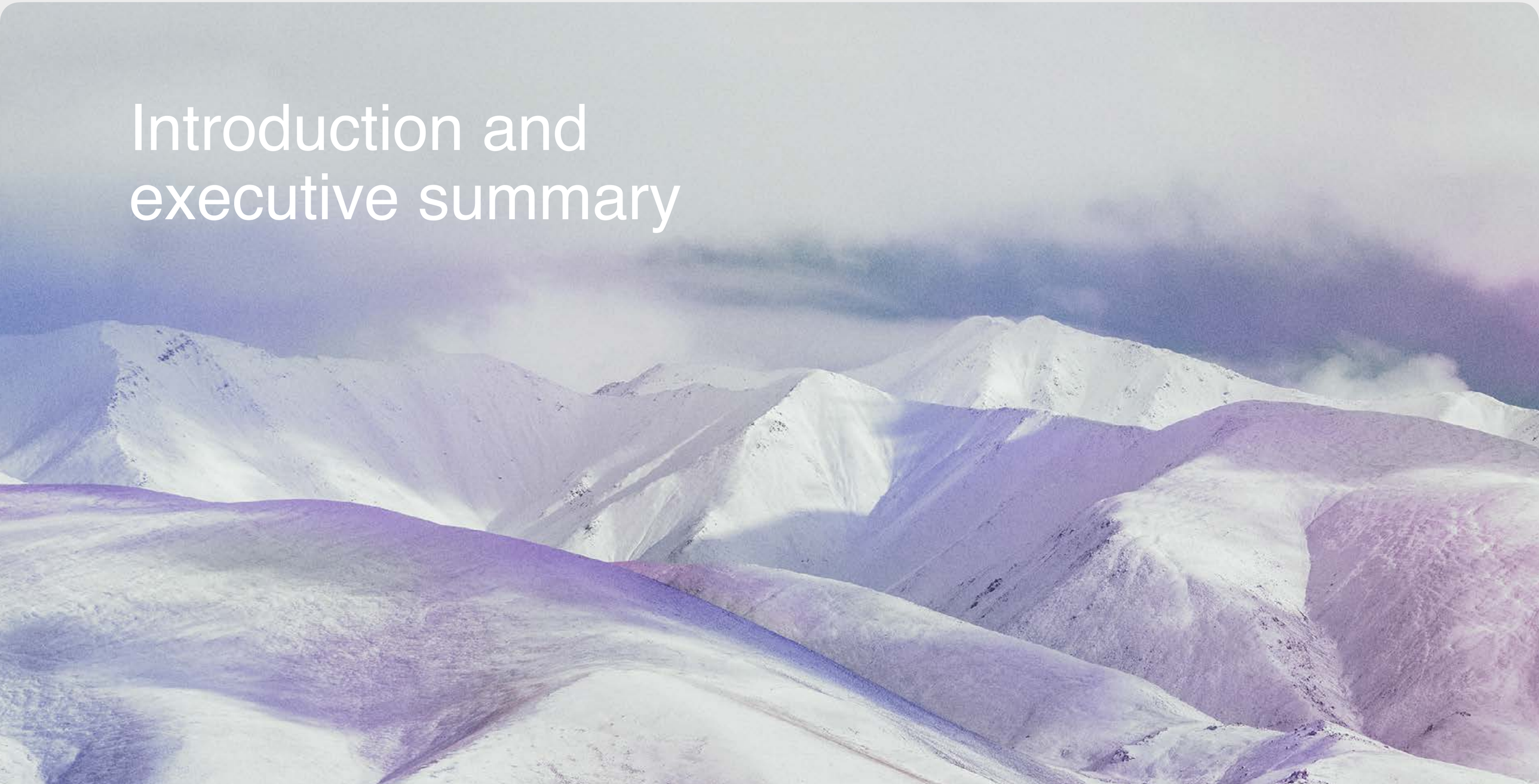
Key backbone security trends

DDoS threat landscape report 2022

Arelion

Introduction and executive summary



DDoS insights from the core of the Internet

As the world's #1 Internet backbone, we have a unique perspective on the constantly evolving DDoS threat landscape - from the core of the Internet.

This report highlights the key global DDoS trends we observed in 2021 – from the overall impact of DDoS attacks to the evolution of specific attacks vectors.

DDoS attacks larger than ever before

DDoS attacks were larger than ever in 2021, peaking at 1.71 Tbps – an increase of 45% from the previous year.

Attack intensity

Attack intensity continued to follow the main Covid-19 pandemic waves. We mitigated slightly less attack traffic overall in 2021 (50Pb) compared with 2020 (53Pb), but the number of attacks was roughly the same. While it is difficult to pinpoint exactly why, we believe there are a number of key factors at play. These include greater industry cooperation to track and mitigate attack sources and the closure of major botnets like Revil.

There was still a noticeable Covid-19 effect in 2021 and peaks again followed the main pandemic waves, but the correlation with DDoS activity was less pronounced – probably because lockdown timing & intensity varied more between different countries, and there was more social activity.

Multi-vector attacks

Multi-vector attacks and targeted extortion threats prevail. The multi-vector threat continued in 2021, fuelling sustained customer demand for auto-mitigation tools.

Our IP customers continued to face extortion-based attacks and notably, there were coordinated attacks on a number of major VoIP providers during October. Extortion attacks targeting bitcoin miners were also more prevalent.

Attack geography

The threat landscape continues to be influenced by geopolitical tensions. Geographically speaking, we continued to notice a direct relationship between the size of our IP customer base and the overall number of attacks across different regions. Simply put, more customer traffic meant more DDoS attacks.

Shifting geopolitical tensions also impacted attack size and frequency. In particular, we noticed more attacks within Europe and these became more frequent towards the end of 2021.

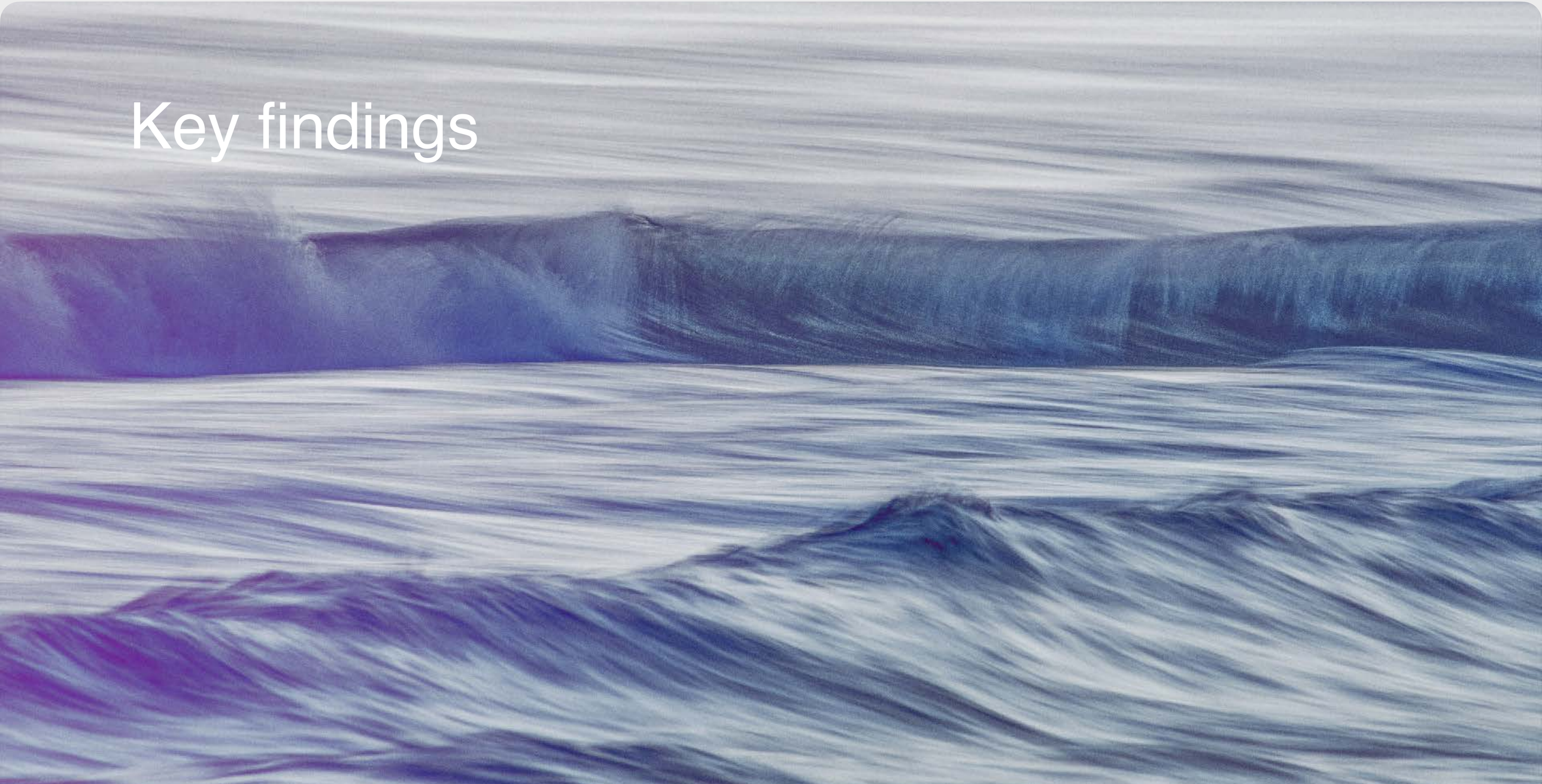
Attack vectors

DNS and NTP amplification attacks were again the most common and consistent attack vector in 2021. This is largely because open DNS & NTP vulnerabilities are relatively easy to find and exploit. Additionally, the spectacular results they yield and the amplification factor mean they continue to be a compelling opportunity for cybercriminals.

Carpet bombing

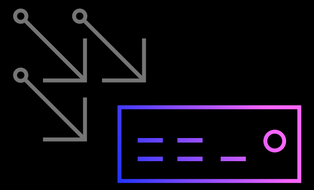
Carpet bombing is more sporadic, but still a significant threat. Carpet bombing activity peaked in January/ February 2021 and tailed off from May (excluding the well-documented VoIP attacks in October). Overall, there was a 14% increase in attacks. - to more than 42,000 in 2021.

Key findings



Attack distribution changed in 2021

Attack vectors have shifted from persistent, small-packet SYN attacks to less-frequent, but more spectacular large-packet attacks with amplification.



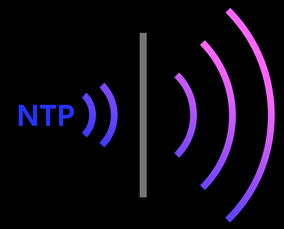
SYN attacks
An attacker rapidly initiates multiple SYN connection requests to a server without finalizing them. The server must wait for half-opened connections, which ultimately consume enough system resources to render the targeted system unresponsive to legitimate traffic.

Huge amounts of data and packets cleaned in 2021

We cleaned 50 petabits of malicious data and 13 x 10^{12} packets during the year – the equivalent of 1.3 million DVDs.

Activity peaks mirror covid restrictions

There was still a significant ‘Covid-effect’ in 2021, with an overall increase in attacks and activity peaks that appear to have mirrored the lockdowns in the US and Europe. However, this was less pronounced than in 2020.



NTP amplification
A type of DDoS attack where the attacker exploits publicly-accessible Network Time Protocol (NTP) servers to overwhelm a target with User Datagram Protocol (UDP) traffic. The server response is much larger than the request, amplifying traffic towards the server and degrading legitimate traffic.

Continuing trend towards auto-mitigation of attack traffic

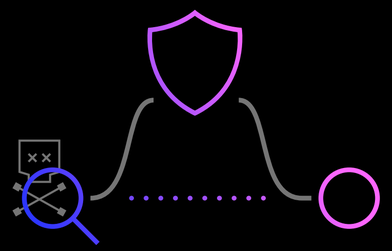
Due to an increase in multi-vector attacks, customers are continuing to move towards auto-mitigation of attack traffic.

A new approach to detection and mitigation

Carpet bombing is placing an increasing strain on customer network infrastructure. This requires a revised approach to traditional threshold-based detection and mitigation (from host-level to logical network-level).

DNS & NTP amplification attacks most common vector

DNS & NTP amplification attacks were again the most common attack vector in 2021.



Auto-mitigation of attack traffic

When a DDoS attack is detected, the impacted traffic flow is directed into DDoS scrubbing centers automatically, allowing attack mitigation to begin within a few seconds of attack detection.

Number of attacks

42,000

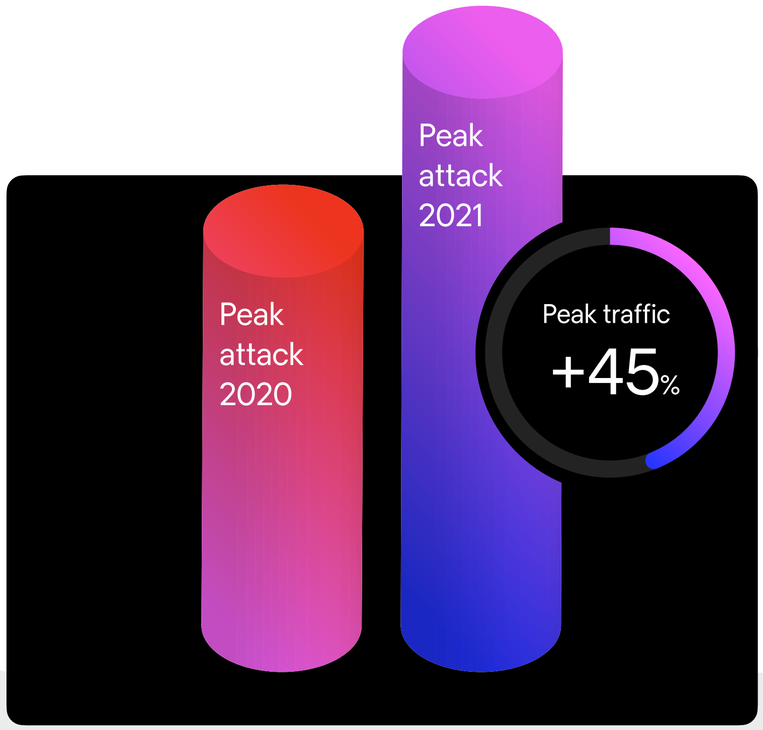
Carpet bombing attacks on the rise

Carpet bombing attacks has become more commonplace and frequent. We saw unprecedented levels during 2021, with an increase of 14% from 2020 to more than 42,000.

DNS amplification

A reflection attack which floods a target with large quantities of User Datagram Protocol (UDP) packets. These attacks exploit vulnerabilities in domain name system (DNS) servers to turn initially small queries into large data payloads which eventually take down a victim's servers.

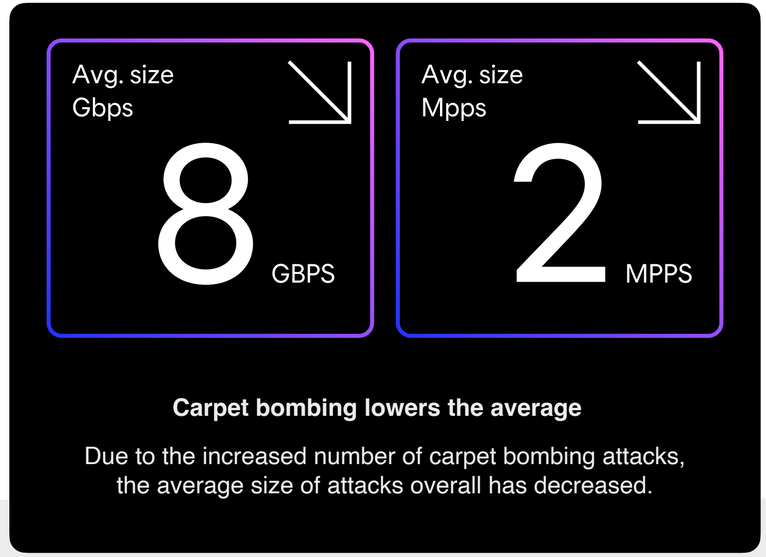
Peak traffic increased in size and was up 45% year-on-year



The average duration of each attack was approx. 11 min

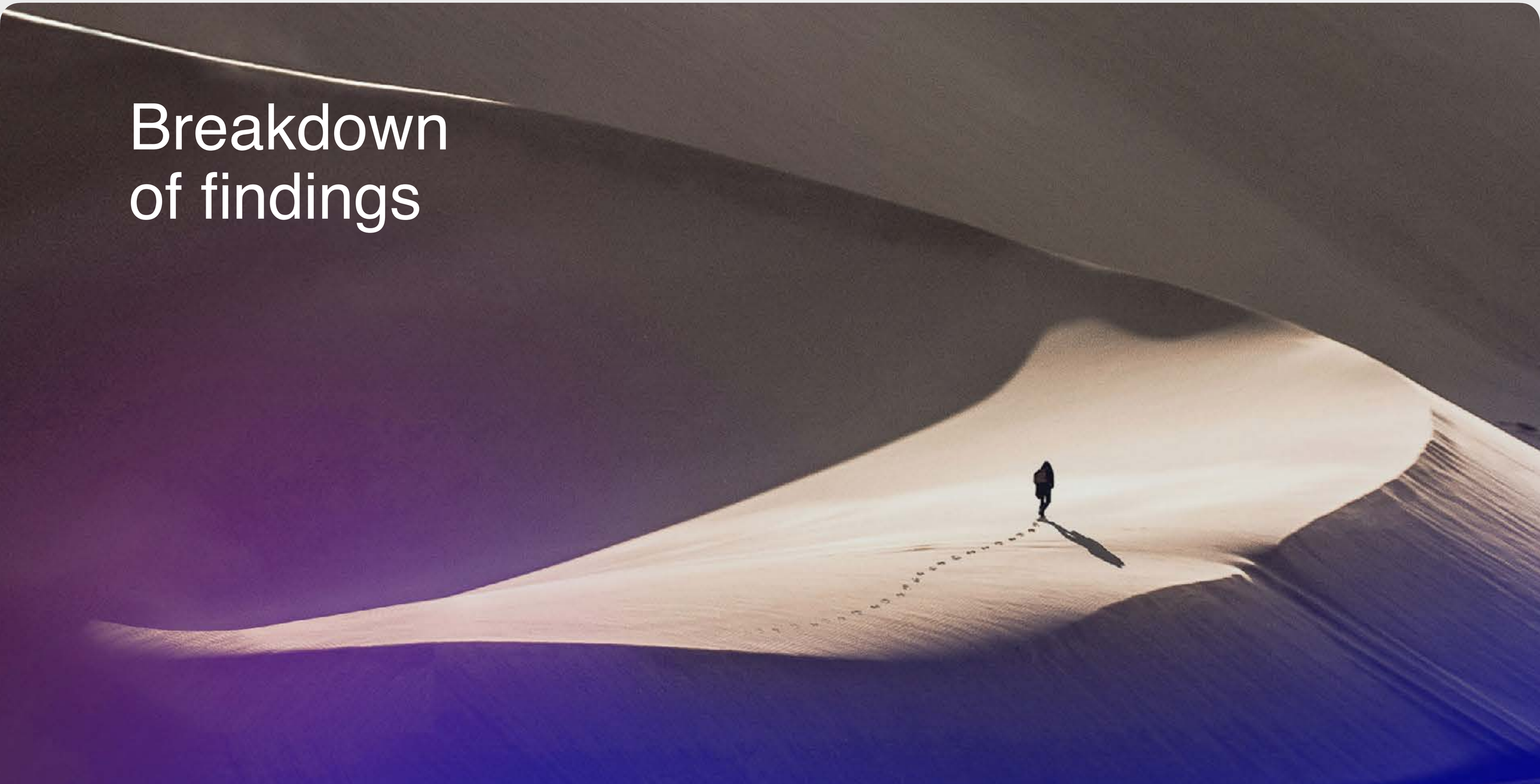
The average size of each attack was 8 Gbps or 2 Mpps

This was a significant drop compared with 2020 due to greater carpet-bombing activity in 2021. If we exclude carpet bombing attacks below 5 Gbps & 5 Mpps, the average attack size was 35 Gbps or 25 Mpps.



Arelion

Breakdown of findings



Overall network impact

DDoS attack traffic peaks continue to increase – in both size and scale, and with ever greater network impact.

Peak attack Gbps

1.71 GBPS

Peak attack Mpps

717 MPPS

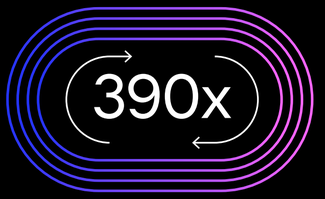
Peak attack size increase

Peak traffic

45%

Mitigation volume

We cleaned 50 Petabits and 13 Tera packets of malicious data in 2021 – the equivalent of 1.3 million DVDs.



The data cleaned is the equivalent of:

- 1,3 million DVDs. Lined up around a running track, they would stretch 390 laps (156 km).
- 2.5x more data than the total memory capacity of the human brain.
- Over 2 decades of uninterrupted 4K Ultra HD video recording.

Average attack size and duration

Whilst the largest attack size increased significantly year-on-year, there was a significant drop in the average attack size compared with 2020 due to increased carpet-bombing activity in 2021.

If we exclude carpet bombing attacks below 5 Gbps & 5 Mpps, the average attack size was 35 Gbps or 25 Mpps.

Avg. size >5 Gbps

35 GBPS

Avg. size >25 Mpps

25 MPPS

Avg. size Overall

8 GBPS

Avg. size Overall

2 MPPS

Avg. duration of DDoS attacks

Duration

11 MIN

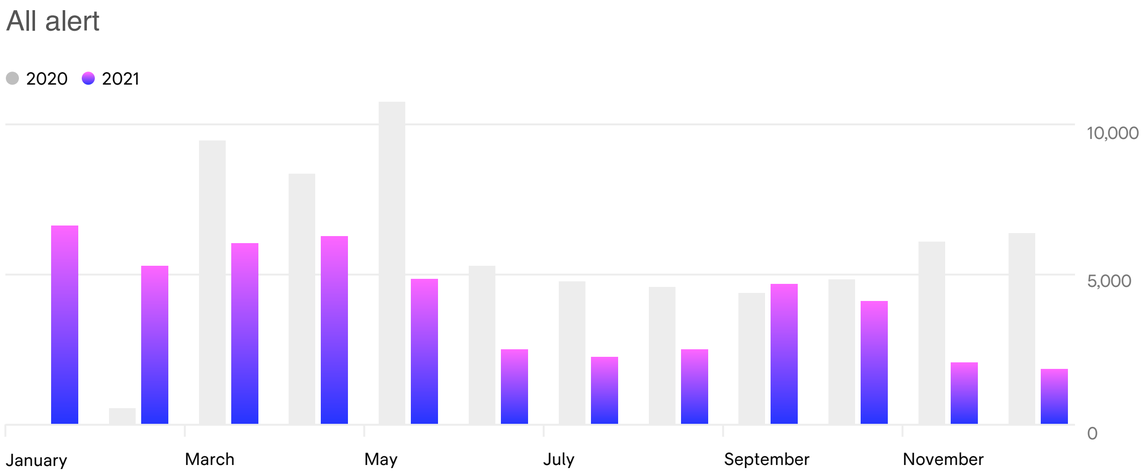
Arelion

Attack frequency and duration

The Covid-19 effect

—

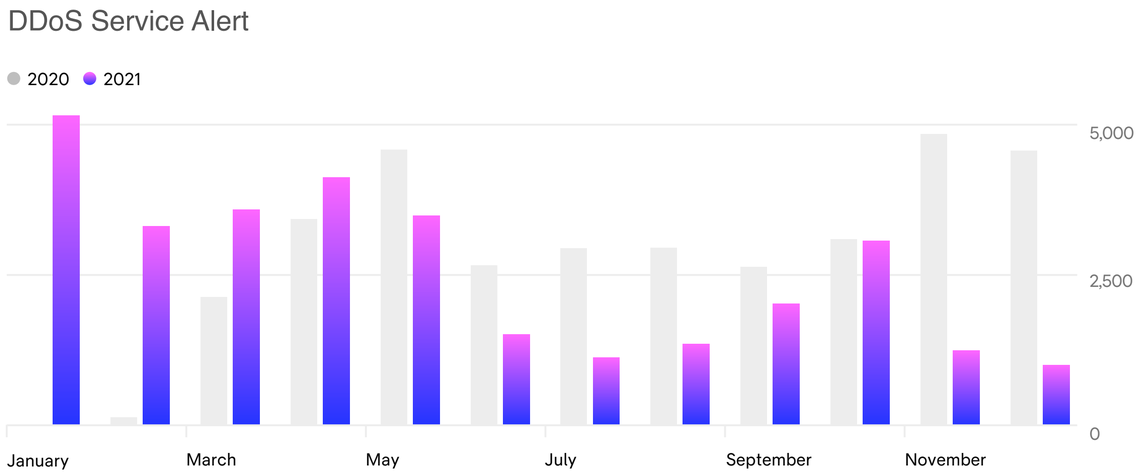
There was still a noticeable Covid-19 effect in 2021 and peaks again reflected the pandemic waves, but this was less pronounced than in 2020. Whilst it is difficult to pinpoint exactly why, we believe this was largely a result of softer restrictions, as testing/quarantine replaced blanket lockdowns (i.e. fewer people were home at the same time).

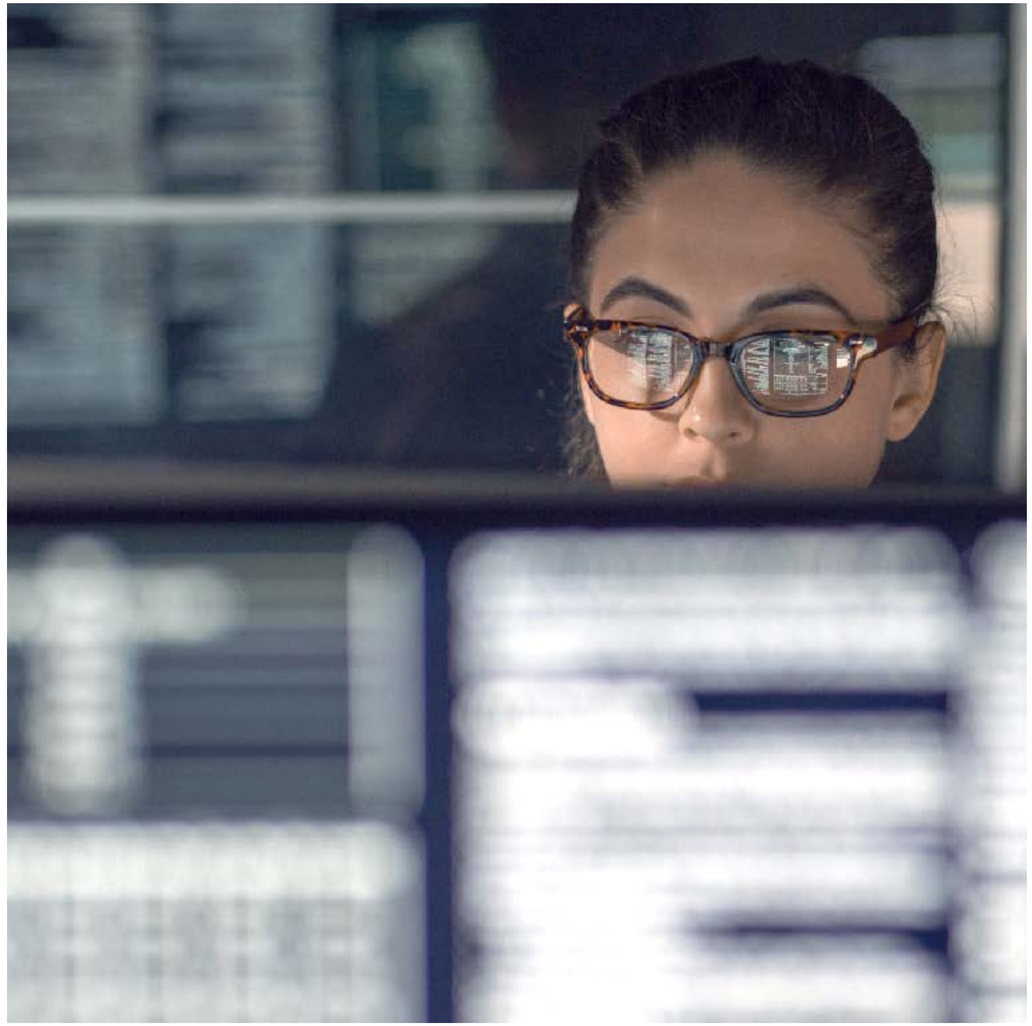


Greater protection means fewer attacks

—

In 2021, we noticed a slight decrease overall in attacks targeting customers with our DDoS protection compared to 2020. We believe this is because customers are more conscious of the threat landscape and are taking greater steps to protect themselves.



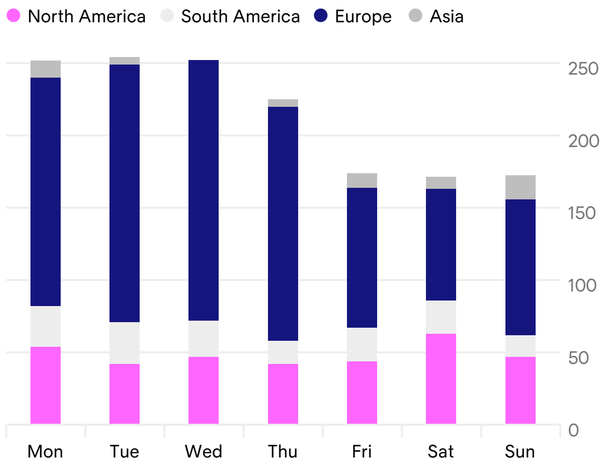


DDoS is never out-of-office

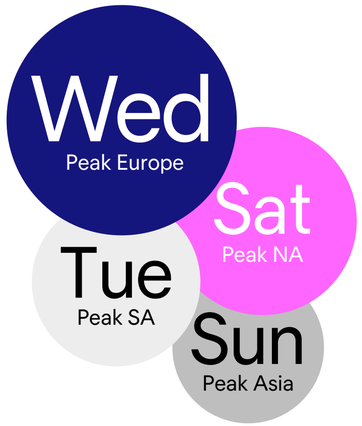
—

Attacks were constant and affected customers on every day of the week. Customers need to remain vigilant at all times.

DDoS Customer Continent Weekday



Peak DDoS Weekday

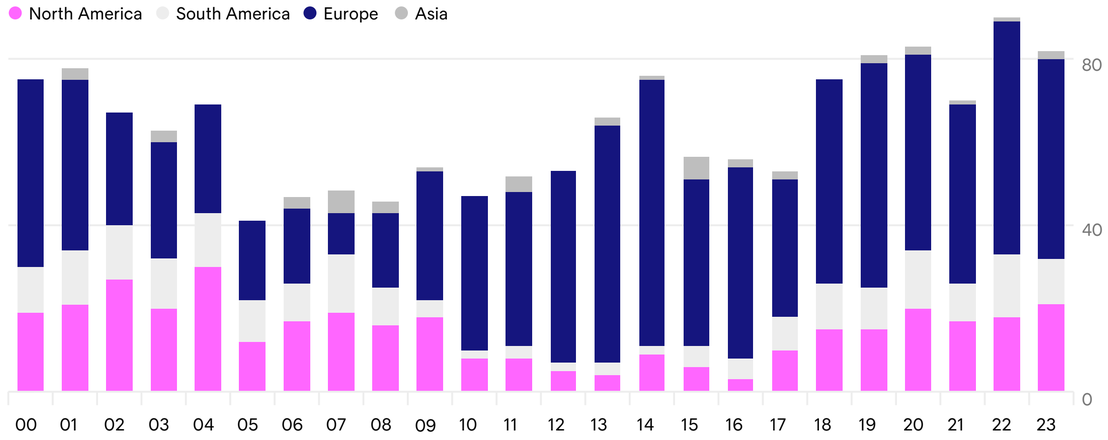


Attacks ’follow the sun’

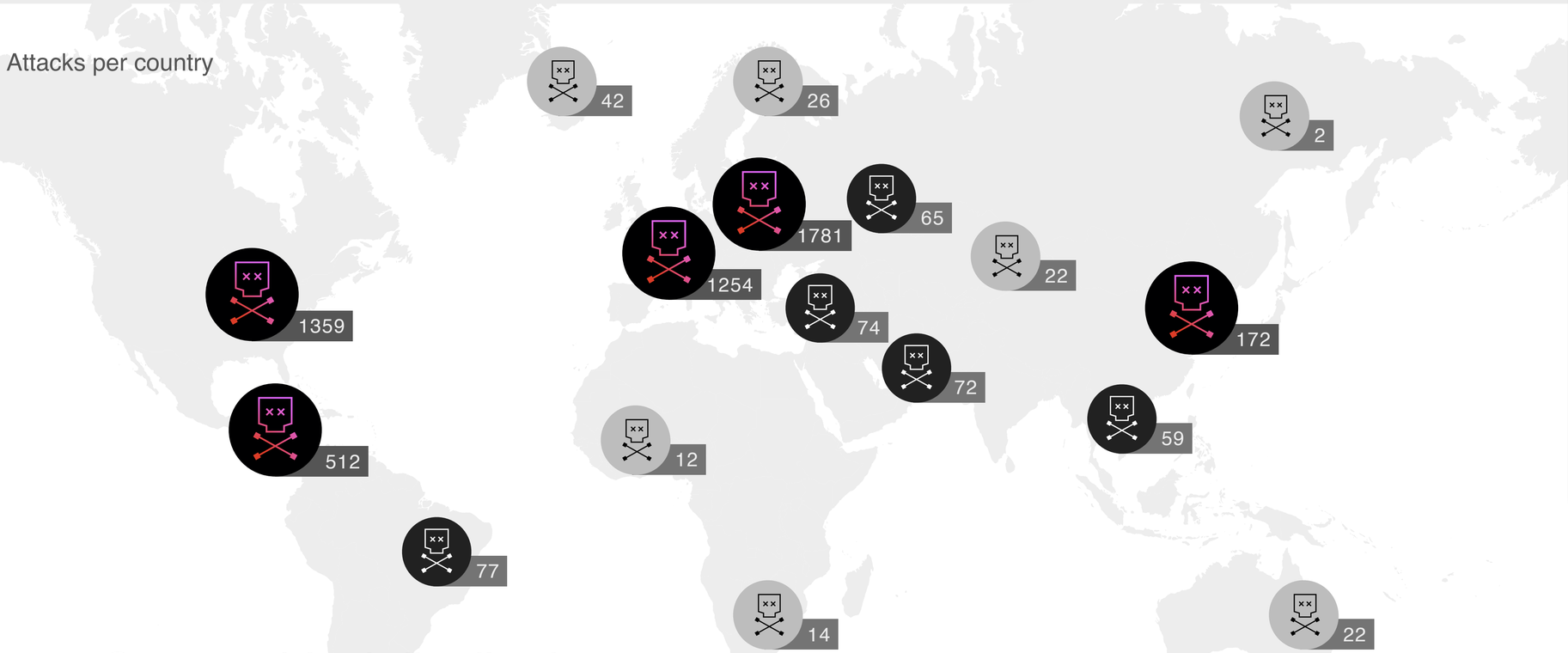
—

Attacks continue to 'follow the sun' across different continents, decreasing on one continent as day becomes night, only to increase on another after the sun rises.

DDoS Customer Continent Hour CET



22:00
CET
Peak DDoS Hour



NTP amplification

A type of DDoS attack where the attacker exploits publicly-accessible Network Time Protocol (NTP) servers to overwhelm a target with User Datagram Protocol (UDP) traffic. The server response is much larger than the request, amplifying traffic towards the server and degrading legitimate traffic.

Geographical distribution

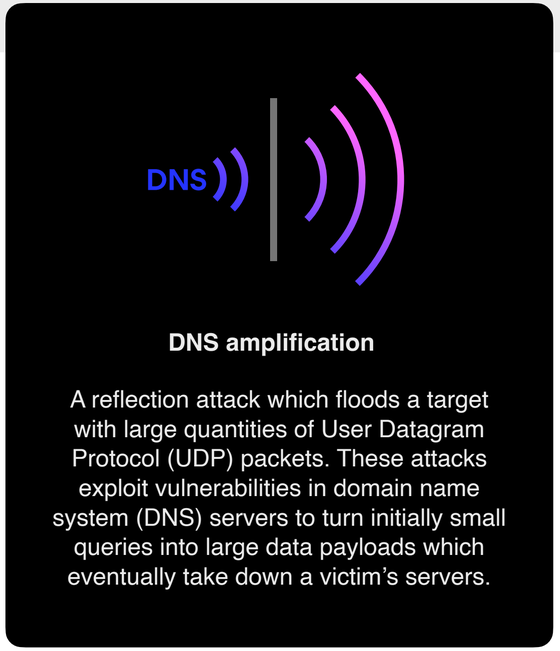
—

We saw the highest concentration of DDoS attacks in our key markets. In other words, DDoS attack intensity correlated directly with customer traffic volumes. Notably, we saw more attacks in Europe compared with 2020. The map shows attacks per country, as detected in our systems.

Customer attack trends

—

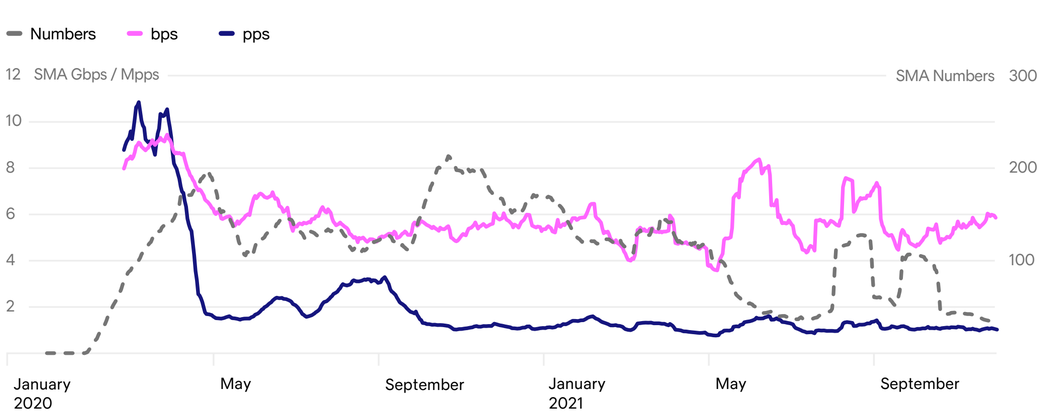
There appears to be a distinct correlation between the main pandemic waves (lockdown phases at the beginning and end of the year) and the number of DDoS attacks targeting our customers, although this was less pronounced than in 2021. DNS & NTP amplification were the most common attack-vectors in 2021.



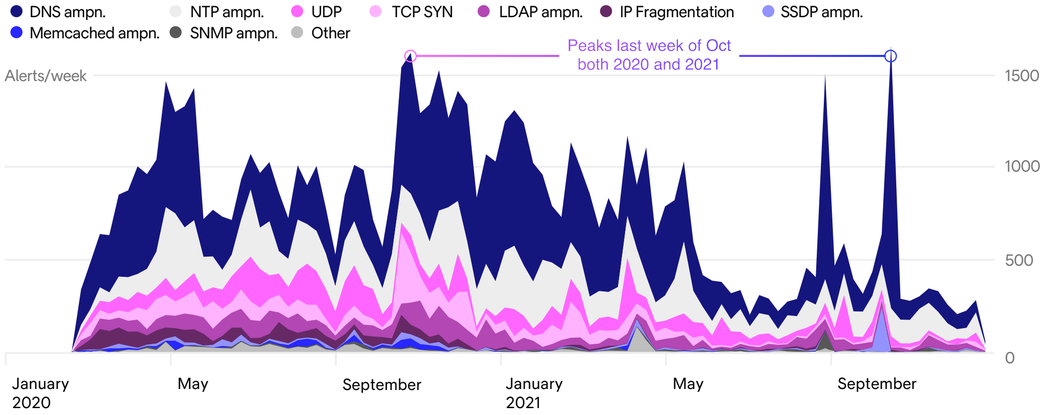
DNS amplification

A reflection attack which floods a target with large quantities of User Datagram Protocol (UDP) packets. These attacks exploit vulnerabilities in domain name system (DNS) servers to turn initially small queries into large data payloads which eventually take down a victim's servers.

Attack Size DDoS Customer per Day



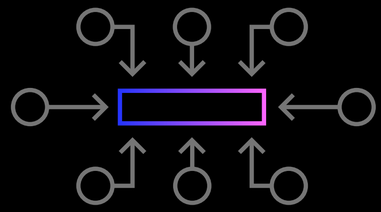
Alert Types DDoS Customer per Week



Scale and intensity

—

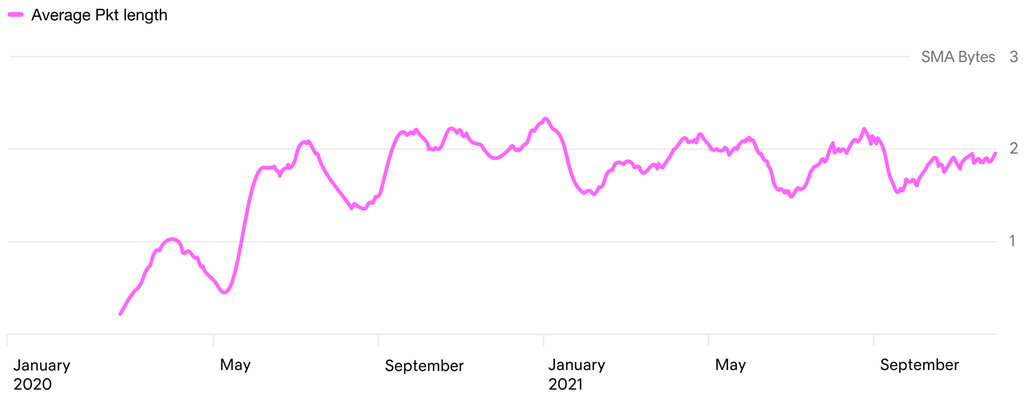
Attack Distribution changed in 2021 Attack vectors have shifted from persistent, small-packet SYN attacks to fewer, but more spectacular large-packet attacks with amplification. DNS & NTP are still the most common type of amplification attack and NTP attacks, in particular, increased in 2021.



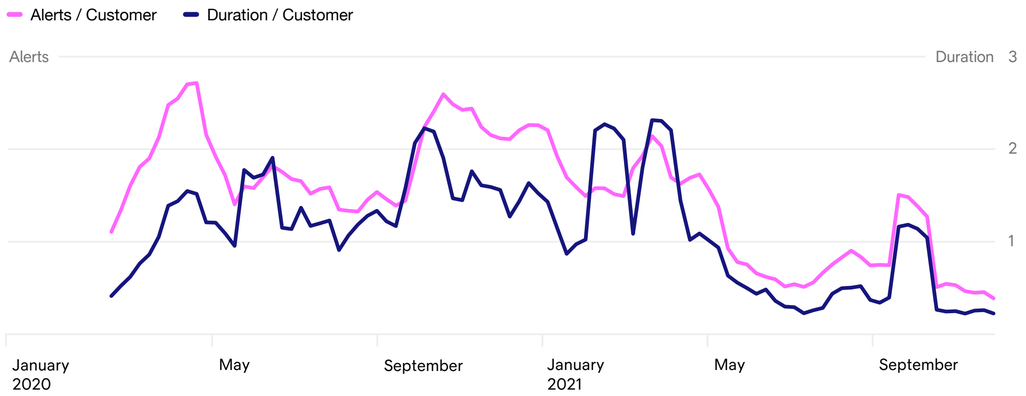
Attack-vector

A term used to describe the particular method or pathway used by cybercriminals to instigate a cyber attack. There are many types of attack vector – some more common than others – and cybercriminals today often employ multiple attack vectors simultaneously for maximum impact.

Attack Average Packet Length per Day



Alerts & Duration per DDoS Customer



Carpet bombing

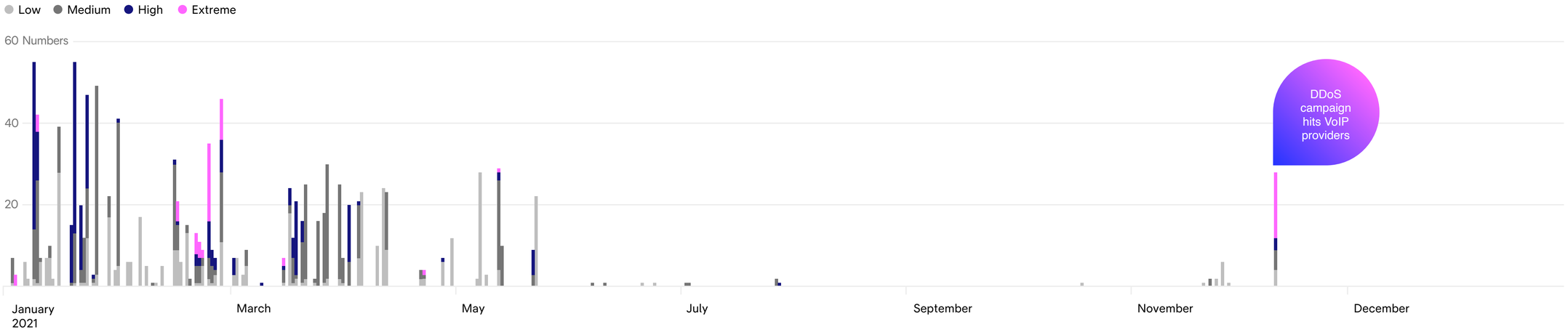
—

Carpet bombing is an ever-increasing problem, and here to stay. In 2021, we saw sustained activity, although there were greater peaks and less consistency than 2020. Most notable were the coordinated VoIP attacks in October 2021.

Carpet bombing

Carpet bombing is a term used to describe attacks that target a range of addresses or subnets, potentially affecting hundreds or even thousands of destination IP addresses. Carpet bombing attacks can impact a service provider's ability to deliver service overall, or to specific customers and are difficult to mitigate.

Global Carpet Bombing Severity



DDoS mitigation with superior precision

The Arelion DDoS protection service applies surgical scrubbing techniques to automatically detect and mitigate attacks.

Malicious traffic is dropped within our global backbone network, before it reaches your Internet connection. Network based mitigation provides a powerful shield for DDoS traffic, ensuring that only legitimate traffic passes through.

Scale to the number of managed objects

We provide a high-capacity solution throughout our global IP backbone that can be scaled to add more Managed Objects (MOs) and mitigation capacity to support evolving threats and to support your growing protection needs.

Flexible pricing

Our pricing model is designed in accordance with your risk profile, making it more economical than in-house edge solutions.

Features

- Protection against evolving attack vectors: volumetric, protocol, application
- Surgical host-level mitigation
- Manual or automatic protection
- 24/7/365 protection

Security highlights

- Physical and logical security from design to deployment
- A network-wide Acceptable Use Policy (AUP)
- Customer Service authentication procedures
- Transparent customer data handling policies

Arelion

About us

Formerly Telia Carrier, Arelion is a leading light in global connectivity services. We've been keeping the world connected since 1993 and today our global IP backbone, AS1299, is ranked number one in the world.

Our network spans Europe, North America and Asia, with 70,000 km of optical fiber and 1,700 MPLS end points. Our award-winning customer service team supports our expansive customer base, who rely on us for their business-critical services.

Follow us on LinkedIn and Twitter
Discover more at www.arelion.com