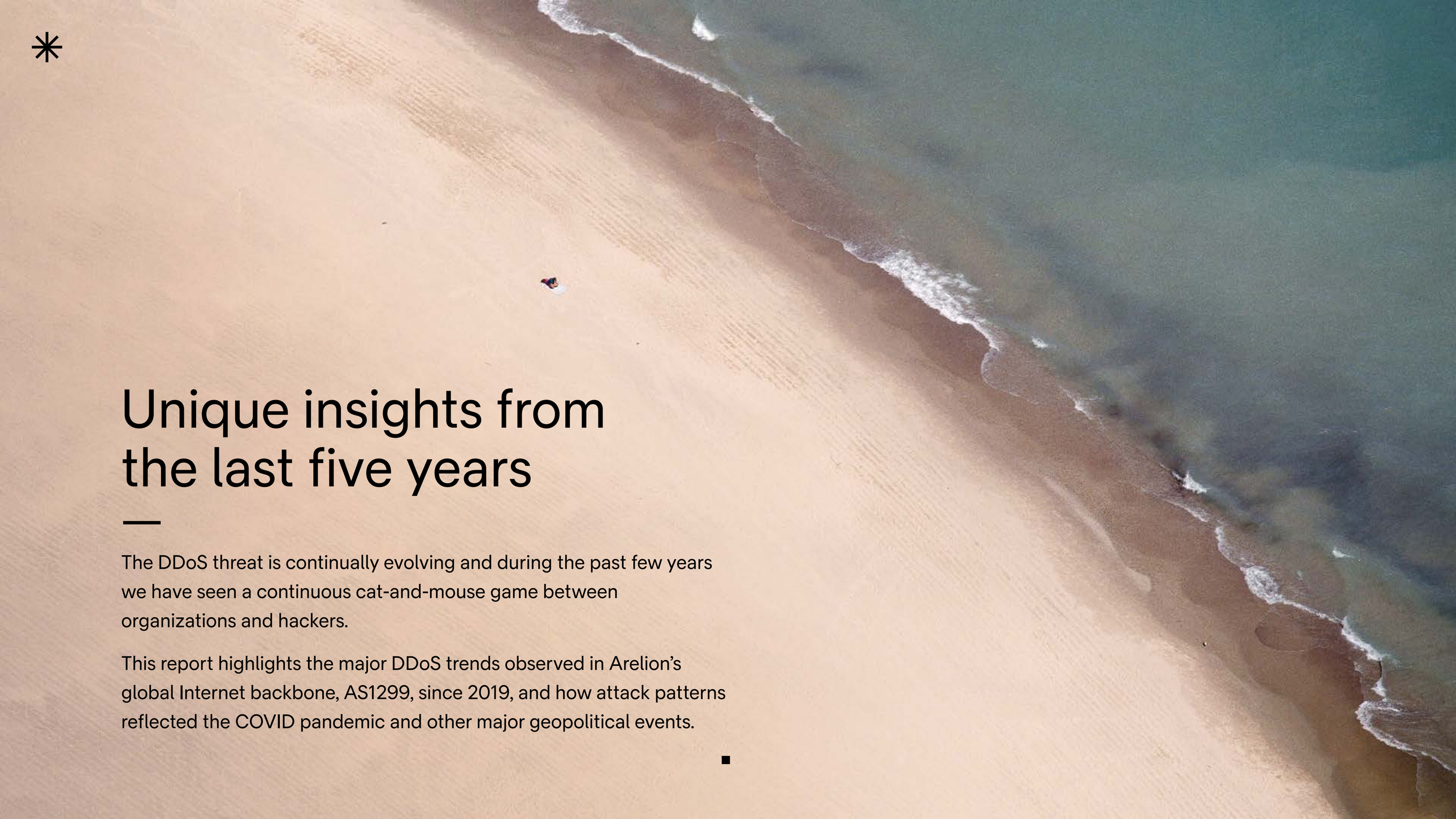
DDoS attack evolution since 2019

The shifting sands of the DDoS threat landscape



Arelion



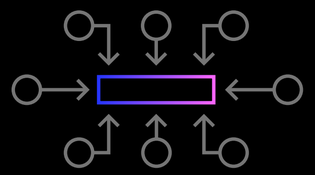
Unique insights from the last five years

The DDoS threat is continually evolving and during the past few years we have seen a continuous cat-and-mouse game between organizations and hackers.

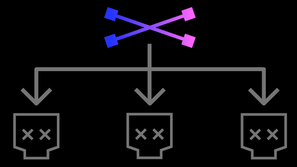
This report highlights the major DDoS trends observed in Arelion's global Internet backbone, AS1299, since 2019, and how attack patterns reflected the COVID pandemic and other major geopolitical events.

Evolution of DDoS:

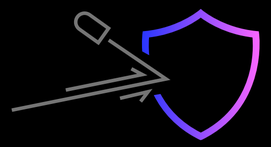
2019 — 2020 — 2021 — 2022 — 2023



Blunt volumetric attacks dominated the DDoS threat landscape. The emergence of Carpet-bombing spurred network operators to begin developing effective countermeasures.



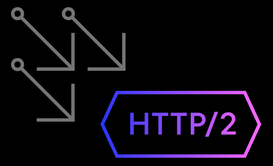
Botnets increased in complexity, capability and size, with the focus on infecting as many machines as possible to effectively distribute attacks.



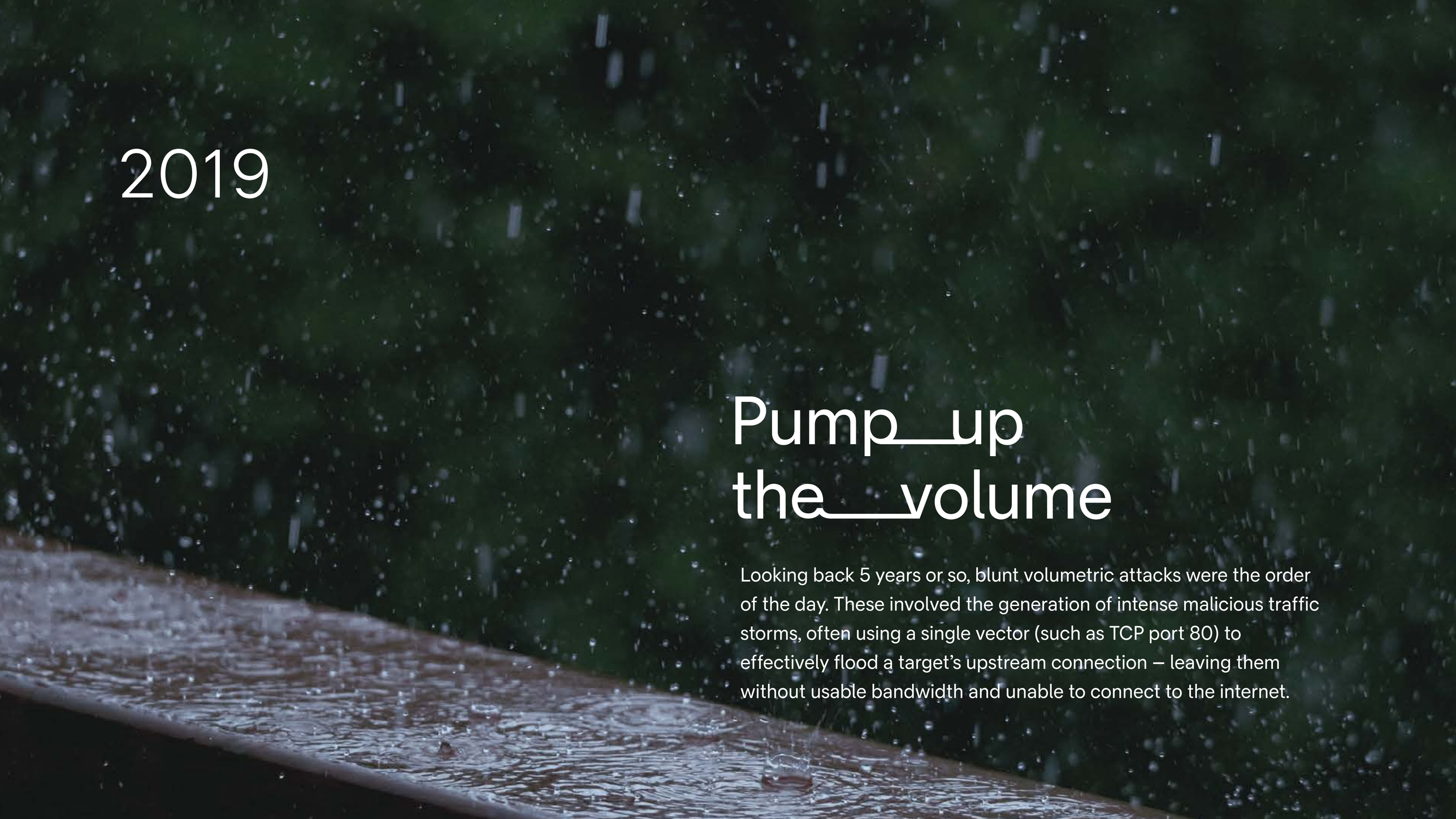
As DDoS security providers developed volumetric attack countermeasures, DDoS attacks became smaller but more intelligent.



The war in Ukraine and rising global tensions made state-sponsored DDoS attacks a significant and more conspicuous element of hybrid warfare.



An emerging type of DDoS attack based on HTTP/2 was widely used to bring down web sites. This type of attack presents new mitigation challenges.



2019

Pump up the volume

Looking back 5 years or so, blunt volumetric attacks were the order of the day. These involved the generation of intense malicious traffic storms, often using a single vector (such as TCP port 80) to effectively flood a target's upstream connection – leaving them without usable bandwidth and unable to connect to the internet.

50%

Increase of average attack size (bits/s) globally in 2019

The way this malicious traffic was generated varied, but was largely based on the reflection of traffic from various public servers distributed across the Internet. This allowed botnets to fully exploit the relatively small amounts of bandwidth available to them and punch well above their weight, causing major issues throughout the Internet as a result.

It is also during this time that Carpet-bombing first reared its ugly head, and in turn, network operators began developing effective countermeasures. It has continued to evolve and is still a serious threat that needs to be taken seriously by network engineers and vendors alike.





2020

The rise of botnets

In response to the industry’s defensive actions, bad actors on the internet shifted their focus to the botnets themselves.

These botnets became cheaper to activate and increased in complexity, capability and size, with the focus on infecting as many machines as possible to effectively distribute attacks.



DNS amplification
NTP amplification

The most common attacks in 2020

As security manufacturers closed off major servers, and increasingly even home computers, hackers shifted their focus to less protected and vastly prolific machines.

These were often IoT devices, widely deployed, often with little or no inbuilt security to keep costs and processing power down. Initially these devices were used heavily in reflection attacks — something for which they were widely suited, and attack complexity began to grow.

However, there was no universal response. IoT has become an integral part of the modern ecosystem, and it cannot be easily filtered or secured. The main approach was to identify botnets through a system of analysis and honey traps — isolating devices when compromised, but allowing them to function during normal operation.

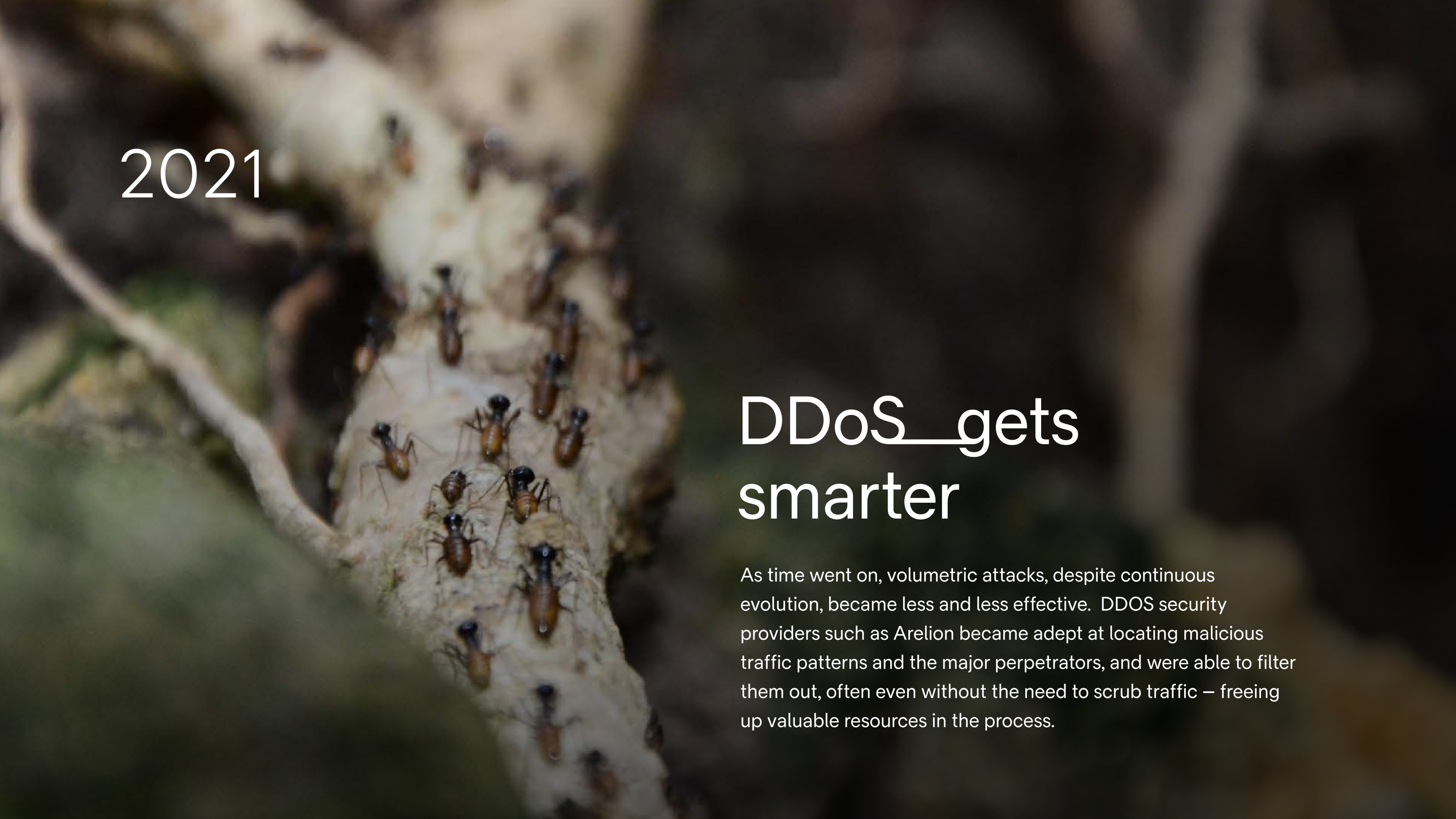
> In 2020, there appeared to be a distinct correlation between the two main COVID pandemic waves (lockdown phases) and the number of DDoS attacks targeting Arelion DDoS customers.

Botnets remain a threat to this day, and many have been monetized with ‘Stress Test’ websites that are effectively ‘DDOS-as-a-Service’.

These offer various levels of attack, and often even a free tier of attacks which, whilst not posing serious problems to those who have invested in solid DDoS defence, will cause problems for an unprotected target, especially if multiple parties co-ordinate free services to either chain them together, or attack all at once.

Keeping botnets out should remain a key IT priority for any organization.





2021

DDoS gets smarter

As time went on, volumetric attacks, despite continuous evolution, became less and less effective. DDOS security providers such as Arelion became adept at locating malicious traffic patterns and the major perpetrators, and were able to filter them out, often even without the need to scrub traffic – freeing up valuable resources in the process.



Security procedures for keeping botnets out began to ensure that locations and IP ranges became more predictable and more easily cordoned off. The attack vectors had to change to be effective, and so they did.

Moving up the OSI model, DDOS attacks became generally smaller, but more intelligent: targeting vulnerabilities in the servers themselves, exhausting resources in target computers and causing them to crash even with sufficient network bandwidth available.

'Carpet-bombing', where the target IP address is switched up frequently, has proved especially effective at bypassing 'old-school' systems of defence.

Carpet-bombing attacks became more commonplace and frequent. 2021 saw unprecedented levels, with an increase of 14% from 2020 to more than **42,000.**

→

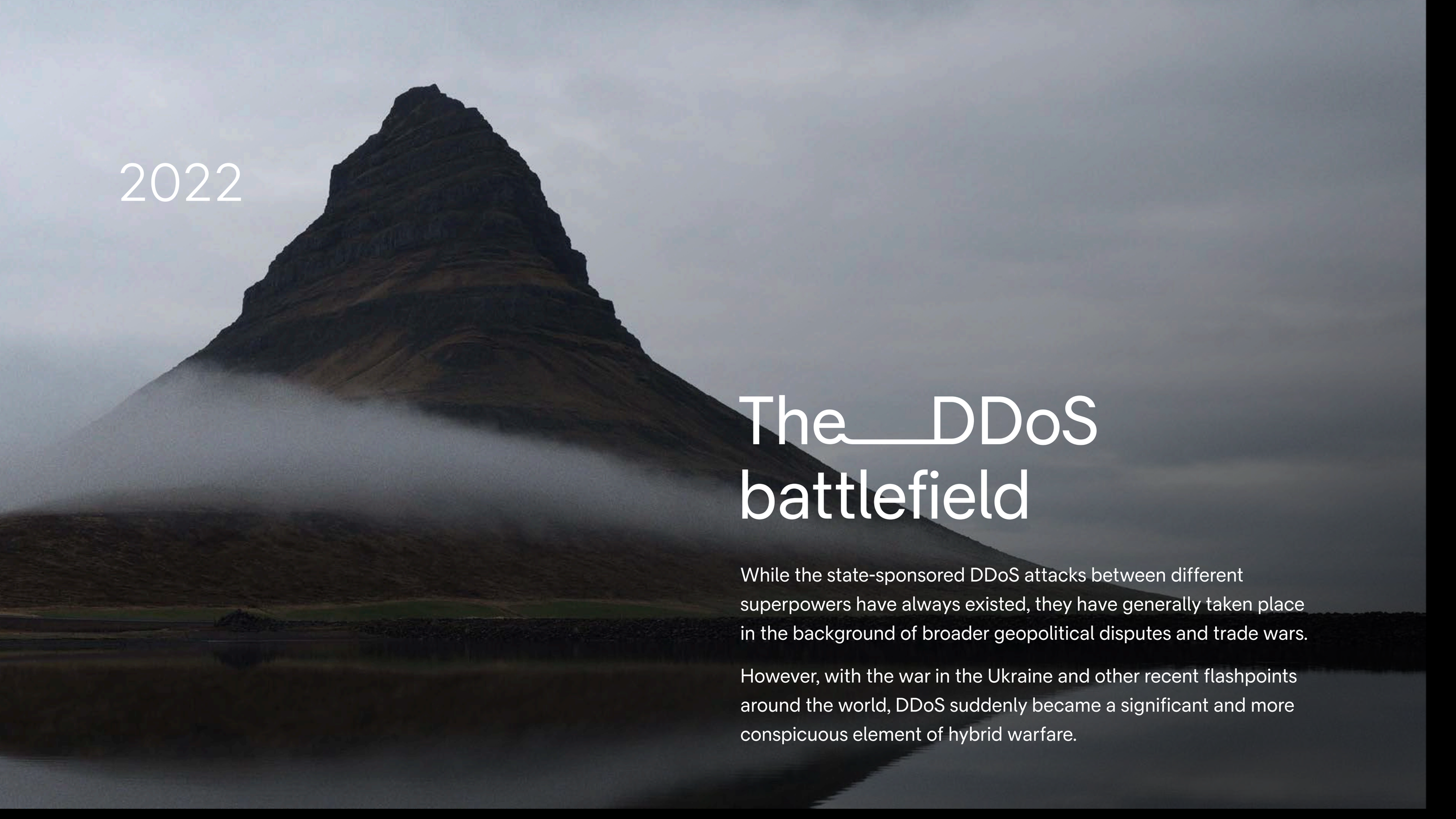


DDoS defences continue to evolve

Profiled detection and mitigation is effective at countering Carpet-bombing by learning to recognise legitimate traffic. Layer 7 attacks require a multi-layered approach, but as new attack vectors are created, a combination of ISP level filtering and on-site capabilities aid mitigation.

Patching is critical

Many of these attacks imitate but are not identical to legitimate queries, and software updates can often mitigate the “Layer 7” part of the attack, leaving ISPs with an underwhelming amount of traffic which their volumetric systems should be able to handle.



2022

The DDoS battlefield

While the state-sponsored DDoS attacks between different superpowers have always existed, they have generally taken place in the background of broader geopolitical disputes and trade wars.

However, with the war in the Ukraine and other recent flashpoints around the world, DDoS suddenly became a significant and more conspicuous element of hybrid warfare.



In part, because many of the countries that invested heavily in this capability began to actively to use them, but also because our growing dependence on connectivity and the digital ecosystem has made the consequences more tangible.

In contrast to attacks generated by criminal gangs and lone wolves, state-sponsored DDoS attacks are well-funded and can be sustained for longer. They are also intended to create maximum damage, rather than generate a stream of illicit revenue.

If this trend continues, the private firms who provide DDOS protection will increasingly find themselves in a grey zone of conflict with nation state capabilities, and a new front will be opened in the struggle to keep the Internet functional and secure.

→

Innovative DDoS financial models also emerged, such as NoName057(16) which incorporates gamification and cryptocurrency rewards to cultivate a community of cyber volunteers. Also, The DDoSia project, launched in July 2022, encourages individuals to participate in its crowdsourced botnet, offering financial compensation based on contribution and combat merit.

The introduction of its cryptocurrency, dCoin, adds another element of complexity to its pay-out platform, emphasizing the group's commitment to a unique brand of DDoS.



2023

Key trends in 2023





The big DDoS attacks just get bigger. Peak attacks continue to grow – reaching 960Gbps in 2023. This demonstrates the continued importance of volumetric protection.

A global decrease in the number of large volumetric DDoS attacks. Although we've seen a global decrease in large volumetric DDoS attacks of late, we also noticed an increase in these locally – on a national level. Large amplification attacks are now harder to carry out successfully, especially in view of recent cooperation across our industry.

An overall decline in packets-per-second – it seems that hackers are increasingly working "smarter not harder". As DNS amplification has improved, fewer packets-per-second are needed for an effective attack, which is one less thing that could trip existing defences.

Attack duration is down, but this doesn't mean attacks are less serious. Larger, more intensive attacks over shorter periods ultimately cause the same overall damage. It appears that average duration is being dragged down by unsuccessful attacks being called off quicker, with resources being reassigned to alternate, unprotected targets.

→



DDoS attack avg. ↘
Duration -12%
8.7 min

The fight continues to prevent hackers using the internet infrastructure against itself. The ongoing decline in open ports is evidence that the Internet community continues to actively limit the resources available to hackers.

DNS Amplification is back – after a brief dip and a period of relative calm in 2022, brute force is in vogue again and was the dominant attack vector in 2023.

DNS Water Torture Attacks are on the rise. This attack vector was first publicly disclosed in February 2020 and although it isn't new, we saw an uptick in DNS Water Torture Attacks toward our customers in Q1 and Q2 2023.

DDoS attack average size (2Y) ↗ +6%
11.7 Gbps

DDoS attack average size (2Y) ↘ -16%
5 Mpps

Attack duration is down, but this doesn't mean attacks are less serious. Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall.

→

An ongoing Cyber-tug-of-war. As a result of the industry-wide push to shutdown or restrict networks used for, or potential used for, spoofing networks, DDoS attacks continue to evolve towards direct path attacks sourced directly from botnets.

New DDoS attack vectors are targeting web sites. Towards the end of the year in Q4 a new type of DDoS attack based on HTTP/2 has been widely used to bring down web sites – in particular, within the banking sector in Sweden and other countries.

The ebb and flow of the ground war in Ukraine reflects attack trends in countries such as Russia and Ukraine – and neighbouring countries like Poland. Cyber warfare is now an established part of nation state conflict.

Peak attack Gbps

960

Peak attack Mpps

343

The largest volumetric attack in 2023 peaked at 960 Gbps (up 18% from the 2022). This came from a UDP-based attack in Europe.

At 343 Mpps, the largest pps attack came from a multi-vector TCP SYN, SSDP amplification attack in North America.



DDoS is a complex, ever-changing, and often unpredictable challenge for businesses today. In order to achieve a robust level of DDoS protection, we recommend a multi-faceted approach which includes the following key components:

1. Network-based DDoS protection: Implementation of strong network-based DDoS protection with an upstream service provider is a powerful defence mechanism which can stop attacks before they reach you

2. CDNs: Use a CDN to distribute content across multiple servers globally, helping to absorb large volumes of traffic and protecting your services.

3. Network Segmentation: Segment your network to keep critical services separate from public-facing systems - minimizing the risk of a successful attack affecting the entire network.

4. DNS Resilience: Distribute DNS queries across multiple servers in different locations to mitigate the impact of DNS-based DDoS attacks, and balance the traffic between multiple servers on your side.

5. Web Application Firewalls (WAF): Use a WAF to defend against attacks targeting web applications, preventing low bandwidth attacks at Level 7 from slipping through and redlining your servers.

6. Rate Limiting: Implement rate limiting on servers and applications to control the number of requests from each IP address, helping to reduce the impact of large-scale attacks.

Arelion

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 75,000 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 X (formerly Twitter)
Discover more at www.arelion.com

This information set forth herein is intended for general informational purposes only and is provided "as is" without any representation, warranty or condition of any kind, either express or implied. There is no assurance as to the accuracy or completeness of such information and circumstances may change. Use of the information is entirely at the consumer's risk, and nothing herein constitutes an offer to sell any service or product or is intended to imply, create or modify a contractual or other relationship. No part of this document is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of Arelion.

©Arelion AB. 2024. All Rights Reserved.