



DDoS attacks are getting more and more frequent in Europe

With attacks becoming more sophisticated and harder to detect, intelligently automated DDoS protection is critical when it comes to preventing unwanted downtime.

Expectations for Internet response and resilience come down to seconds, not minutes.



5x increase in DDoS attacks in parts of Europe in February 2022 alone

Increased risk of DDoS attacks worldwide

Although we have yet to register a significant increase in DDoS activity in other global regions, Corero is predicting that the increasing global sanctions against Russia **will trigger DDoS attacks towards the countries imposing them.**

Multi-Vector Attacks Remain a Significant Threat

13% of all attacks were multi-vector and they still remain a significant threat to internet availability for organizations that are not using the latest generation protection. In order for a multi-vector attack to be completely mitigated, each vector must be recognized and responded to dynamically, in real-time, in order to prevent legitimate traffic from being impacted.

29% probability of a repeat DDoS attack

The overall trend still shows an increase. The only way to avoid repeat outages as a result of these attacks is to deploy active **real-time protection against DDoS** that can detect and mitigate in seconds or less.

82%

of Attacks are Less than 10 Minutes

Short Duration Attacks Require Automated DDoS Protection

The percentage of attacks with durations less than 10 minutes remains high at 85%. Cyber criminals continue to use shorter duration attacks to dodge legacy DDoS solutions. If a disruption in the network goes on for just a few minutes it is likely that it will fly under the radar, making these short duration attacks especially dangerous. By the time a staff member has been alerted, the damage has been done.

A successful DDoS attack brings the risk of significant downtime to your business operations, revenue loss, and damage to brand reputation. This makes using an intelligently automated DDoS protection platform essential. There are a variety of protection options available, on-premises, in the cloud or a combination of the two commonly referred to as hybrid DDoS protection. However, be sure to assess your risk tolerance and that of your customers. If any amount of downtime cannot be tolerated, you should invest in an always-on solution.

For more information, visit www.corero.com

EMEA HEADQUARTERS

Corero Network Security (UK) Ltd.
St Mary's Court, The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com

US HEADQUARTERS

Corero Network Security Inc.
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

SCOTLAND OFFICE

53 Hanover Rd
Edinburgh EH2 2PJ, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com

