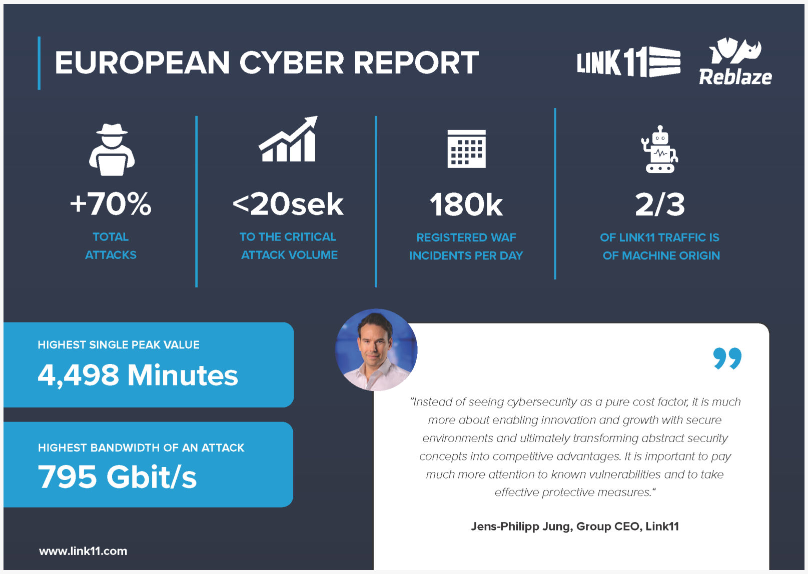
EINPRESSWIRE

# European Cyber Report 2023 from Link11 - 70% increase in DDoS attacks: speed and intensity of attacks at new highs

FRANKFURT AM MAIN, DEUTSCHLAND, March 13, 2024 /EINPresswire.com/ --
- Turbo attacks on the rise: In 2023, DDoS attacks reached critical level after just 14 seconds on average. Compared to the average of 55 seconds in the same period in 2022, these "turbo attacks" reached critical volume significantly faster.
- Attacks last longer: The longest attack in 2023 lasted 4,489 minutes, which corresponds to 74 hours and 49 minutes. The longest DDoS attack in 2022 lasted just 1,695 minutes, or 28 hours and 15 minutes.
- Good bots, bad bots, botnets: Two thirds of observed traffic is machine-based. Link11 records around 180,000 WAF events in its network every day.


EUROPEAN CYBER REPORT
LINK11
Reblaze
+70%
TOTAL ATTACKS
<20sek
TO THE CRITICAL ATTACK VOLUME
180k
REGISTERED WAF INCIDENTS PER DAY
2/3
OF LINK11 TRAFFIC IS OF MACHINE ORIGIN
HIGHEST SINGLE PEAK VALUE
4,498 Minutes
HIGHEST BANDWIDTH OF AN ATTACK
795 Gbit/s
www.link11.com

"Instead of seeing cybersecurity as a pure cost factor, it is much more about enabling innovation and growth with secure environments and ultimately transforming abstract security concepts into competitive advantages. It is important to pay much more attention to known vulnerabilities and to take effective protective measures."

Jens-Philipp Jung, Group CEO, Link11

Highlights of the Link11 European Cyber Report

Frankfurt am Main, March 13, 2024: The new European Cyber Report for 2023 not only highlights the increasing complexity of the threat landscape, but also shows how AI-based and automated security solutions offer comprehensive security while increasing cyber resilience. The in-depth analysis of DDoS attacks registered in the Link11 network is supplemented by additional content from the areas of web protection and web performance to offer a holistic view of the current landscape.

In 2023, the Link11 network recorded a drastic increase of more than 70% in DDoS attacks compared to the previous year, with politically motivated attacks contributing significantly to this. These attacks targeted well-known entities worldwide, such as German federal states and authorities, the European Investment Bank, and Microsoft.

Military conflicts led to a rapid increase in DDoS attacks worldwide
Geopolitical tensions are increasing worldwide, meaning that the threat of DDoS attacks

continues to grow. Many of these DDoS attacks target critical infrastructure (CRITIS), public institutions, and political organizations. Hardly a month has gone by without cyberattacks on NATO countries and their critical infrastructures. In addition to the ongoing war between Russia and Ukraine, the conflict in Israel has triggered a further increase in politically motivated DDoS attacks by well-organized attackers. Prominent actors include the pro-Russian groups NoName057(16) and Anonymous Sudan. What they all have in common is that they use DDoS attacks as their preferred means of ideologically motivated cyberattacks.

Web applications and APIs pose a major security risk
Every critical security vulnerability found in unpatched software is a potential gateway for cybercriminals. Web applications in particular pose a major security risk. The recent decision by the EU that Apple must open its interfaces to third-party providers in order to comply with the Digital Markets Act in the EU also increases the pressure for security solutions in the area of web applications. A conventional firewall is often not enough to effectively protect web applications. This is where the Web Application Firewall (WAF) comes into play. Around 180,000 weakened WAF events are registered in the Link11 network every day.

Increasing danger from AI-driven bots
Every year, companies are confronted with considerable damage caused by attacks from bad bots on their digital assets. According to Juniper Research, online fraud by bots is expected to increase by 131% by 2027. The rapid development of generative AI technologies could even accelerate this further. This trend affects companies in all industries, as automated attacks are an increasing threat.
Automated traffic on a website means greater consumption of computing resources. Depending on who is requesting the data, this can be both positive and negative: Bots and software from partners and known organizations can be a benefit, while unknown bots are a gray area. In the Link11 network, two thirds of the observed traffic is machine-based.

Jens-Philipp Jung, Group CEO at Link11: "The observations of the Link11 Security Operations Center (LSOC) in 2023 make it clear that the impact of cyber incidents requires a risk-based, holistic cybersecurity strategy. Instead of seeing cybersecurity as a pure cost factor, it is much more about enabling innovation and growth with secure environments and ultimately transforming abstract security concepts into competitive advantages. It is important to pay much more attention to known vulnerabilities and to take effective protective measures."

The full report is available for download on the Link11 website.

About Link11

Link11 is a specialized global IT security provider that protects infrastructures and web applications from cyberattacks. Its cloud-based IT security solutions help organizations worldwide to strengthen the cyber resilience of their networks and critical applications and avoid business disruption. Link11’s product portfolio includes security services in Network Security, Web Protection and Web Performance.

With the strategic acquisition of Reblaze Technologies, a leading provider of cloud-native web application and API protection, Link11 strengthens its own position in the WAAP space to offer customers an even more comprehensive protection package in the future.

Link11 is a BSI-qualified provider for DDoS protection of critical infrastructure. With ISO 27001 certification, the company meets the highest standards in data security.

Press contact

Lisa Froehlich
Link11
email us here
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/695588574