Cyber Security: Fastweb maps the main trends in the Italian cybersecurity landscape for the Clusit Report 2025

Cyberattacks on the rise (+23%), increasing in volume and complexity, with over 69 million security events detected in 2024. AI plays an increasingly key role in both attack and defense techniques

Milan, 25 February 2025 – For the year 2024 Fastweb, now Fastweb + Vodafone, once again contributed to capturing the state of cybercrime in Italy through its 24/7 active Security Operations Center (SOC) and its cybersecurity competence center.

The analysis, included in the Clusit Report 2025, the ICT security report by the Italian Association for Computer Security, highlighted a significant increase in cyberattacks in 2024, marking a sharp reversal from the previous year's findings and confirming the increasingly pivotal role of AI in shaping the global cybersecurity landscape.

From the analysis of Fastweb' s network infrastructure, consisting of over 7 million public IP addresses, each of which can communicate with hundreds of devices and servers, over 69 million security events were recorded in 2024, equal to a 23% increase compared to the events detected in the previous report.

After a 2023 in which the number of attacks remained substantially stable, the year 2024 saw an escalation of cyber-criminal activities in terms of volume, complexity, and diversification. Notably, malware infections (+131%) and botnet detections (+41%) increased in Italy, alongside a 7% rise in the number of malicious software families in circulation. In the field of DDoS (Distributed Denial of Service) attack, which involves flooding a website with requests until it becomes unreachable, there is an increase in the number and severity of attacks compared to 2023, with a 100% growth in attack volume and a marked increase in high-impact events with over 100 Gbps of bandwidth used.

In line with the trends detected in previous years, the most affected sectors remain the Public Administration and Finance&Insurance, which together account for almost 50% of cases. In particular, the Public Administration rises to first place, going from 560 attacks in 2023 to as many as 1430 in 2024, while Finance&Insurance, although remaining the second most affected sector, demonstrates greater resilience to attacks, recording a contained increase of 36% thanks to the effectiveness of the measures adopted to mitigate cyber threats compared to the average of other sectors, which exceeds 100%.

The most significant increase, however, is in the Services sector, which recorded a +250% increase compared to the previous report.

In response to these trends, the increasing pervasiveness of AI-driven technologies, now deeply integrated into both attack and defense strategies, along with greater awareness of cybersecurity risks, has helped mitigate the rise in malicious activities. Since 2019, the number of servers exposing critical services to the internet has been steadily declining (-11% in 2024). Additionally, the detection rate of unknown malware dropped from 0.18% in 2023 to 0.12% in 2024, demonstrating improvements in zero-day threat detection and prevention tools, largely thanks to AI advancements.

Also in 2024, the integration of AI into Fastweb' s cybersecurity infrastructures contributed to the identification of anomalies and malicious events with increasing effectiveness, reducing the detection of false positives by up to 70%, in line with industry trends. Thanks to AI's ability to gather more information about threat actors, more accurately distinguish threats, and recognize the characteristic signs of cyber-attacks in advance, a reduction in malicious events related to social engineering, which exploit the human factor and user browsing habits, is observed in 2024, reversing the upward trend observed in 2023. Among these, attacks related to "credential phishing" recorded a 17% reduction, although this type of attack remains stable in first place among email-based threats, which are becoming increasingly credible using AI.

Thanks to the collaboration with 7Layers, a cybersecurity firm acquired by Fastweb in 2020 and specialized in advanced cybersecurity solutions, the report also includes monitoring of the most sophisticated cyber threats detected and countered through the Managed Detection and Response (MDR) service. This has allowed the identification of macro trends in the attack techniques most used by cybercriminals. In first place, with 38% of the total, are 'Execution' attacks that allow malicious actors to run harmful code within victims' devices, followed by 'Initial Access' attacks at 12%, which are carried out to identify potential vulnerabilities. Meanwhile, 'Exfiltration' attacks, which aim to steal sensitive data, represent 9% of the attacks.

Per informazioni:
Fastweb + Vodafone Ufficio Stampa

Roberta Dellavedova
Tel. + 348 14 71 722
roberta.dellavedova@fastweb.it