CYBEROO

PRESS RELEASE

CYBEROO OBSERVATORY 2026: NEW ATTACK TRENDS TARGETING BUSINESSES AND DEFENSE STRATEGIES FOR 2026

- **The evolution of AI agents and new risks for businesses**
- **320 new threat actors identified**
- **Digital sovereignty also competes with non-human identities**
- **Email and MFA breaches among the most common attacks**

Reggio Emilia, February 26, 2026 - Cyberoo S.p.A., an innovative SME listed on the Euronext Growth Milan Market, specialized in cybersecurity for businesses, publishes the second edition of the annual report of the Cyberoo Observatory, this year dedicated to the theme "Inside the dark matter of cyberspace." The document analyzes the main trends and attack patterns that emerged in 2025 and translates the evidence gathered into operational defense strategies for 2026, thanks to data provided by the I-SOC team, an advanced center with over 100 specialists operating in Italy and abroad, which combines 24/7 monitoring and response and Cyber Threat Intelligence, and by the Incident Response Team. The team, composed of ethical hackers and analysts, defends companies from cyber threats by integrating internal sources, such as data from the Cyber Security Suite, and external sources, such as the Surface, Deep, and Dark Web, with the aim of preventing and minimizing the damage of a cyber-attack.

Numbers

Among the most significant data emerging in 2025, Cyberoo reports:

- **320 new threat actors** identified, including particularly aggressive ones: Qilin, Akira, Sarcoma, Everest
- Over **1,300 reports to the competent authorities** for phishing, antispam, and antifraud by Cyberoo
- The detection of **38,654 suspicious domains**
- The identification of over **2,700 unique CVEs**[1] associated with monitored suppliers, confirming the criticality of vulnerability management within the supply chain

Trends for 2025

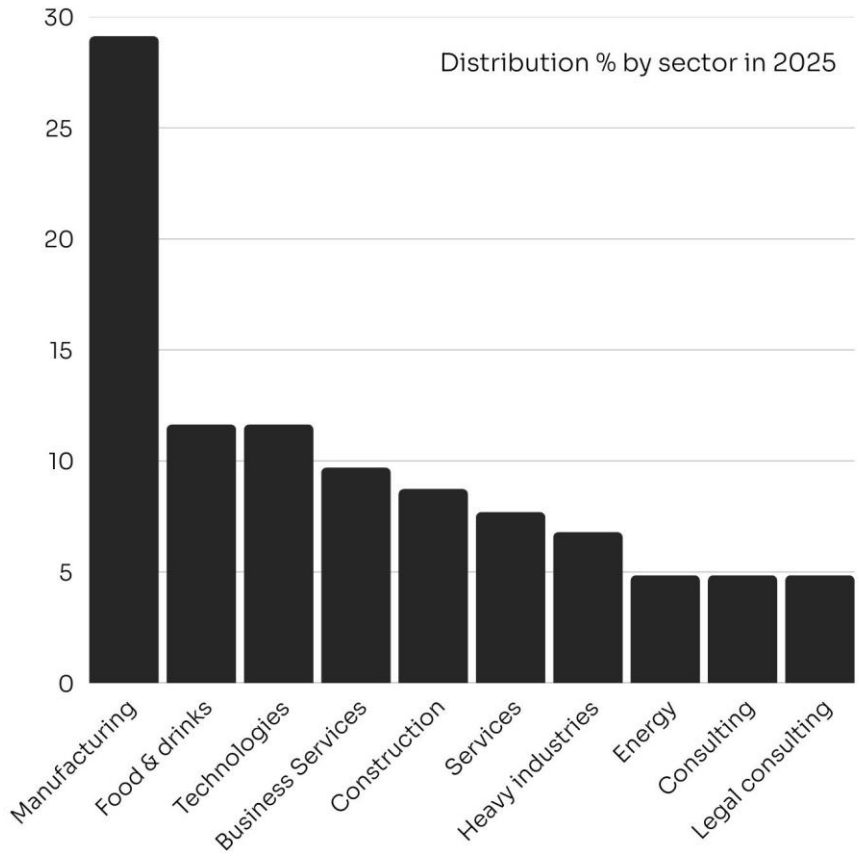
2025 saw an increase in the direct exploitation of vulnerabilities, including zero-day vulnerabilities, and further expansion of the market for **stolen credentials**.
DDoS attacks, cyberattacks that render servers and websites inaccessible by flooding them with fake traffic from thousands of infected devices, made a comeback as a distraction tool, used to saturate defense systems and facilitate parallel reconnaissance and infiltration activities.
Phishing has evolved significantly, becoming increasingly credible and contextualized thanks to the use of generative AI, with cases of impersonation supported by voice and video deepfakes.

[1] **CVE**: *Common Vulnerabilities and Exposures*; refers to a standardized system used to uniquely identify known security flaws in software, hardware, and firmware.

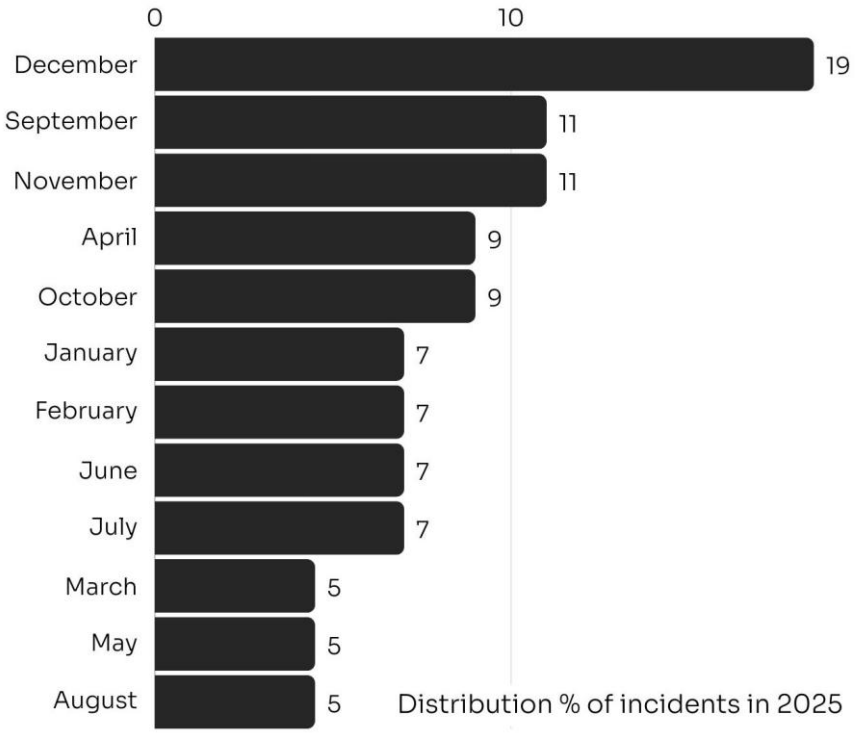
In general, **AI-powered attacks** represent a growing threat. Looking ahead to 2026 and beyond, the Observatory highlights the increase in AI-enabled threats, which make phishing, impersonation, and the spread of **fake news** more effective and scalable. The risk associated with credential theft and pressure on cloud and SaaS, which requires continuous monitoring, also remain central issues.
At the same time, supply chain incidents have shown a “chain” dynamic, in which a vulnerability in a supplier or shared component has often resulted in a blow to multiple organizations, extending to the supply chain with forms of pressure such as **triple extortion**, an advanced cybercriminal tactic and evolution of ransomware, whereby attackers do not just encrypt data, but apply three simultaneous levels of pressure to force victims to pay a ransom for their data.

Distribution of cyber-attacks: affected markets and critical periods

In the sample analyzed for the purposes of drafting the report, the manufacturing sector is the most exposed to cyber-attacks, accounting for 29% of the total examined, also considering the “volume” effect of the sector in the Italian and European markets.



In terms of timing, December is the month most affected by compromises in 2025, coinciding with the Christmas holiday period, when reduced security measures and staffing levels can increase companies' operational vulnerability.



The challenges of 2026

In light of the data highlighted, the biggest challenge concerns what remains invisible: there is a gap between the perception of security and the real risk to information systems. Cyberoo defines this unobserved area as “cyber dark matter”: it is the combination of unmapped assets and surfaces, incomplete controls, obsolete systems, poor awareness, inadequately managed tokens and APIs[2], and non-human identities outside the monitoring perimeter.
That is why, among the priority actions recommended for 2026, the first is to strengthen internal governance and accountability, combine training, culture, and awareness with the orchestration of technologies, processes, and human skills, adopt identity-first controls, apply risk-based patch management, and ensure continuous supervision of cloud and SaaS with backups and incident response playbooks. The goal must be to move from reactive security to proactive and strategic defense, especially in larger companies that manage longer supply chains.
In addition, it is essential to increase transparency and control over AI: managing artificial intelligence is critical to avoid falling into digital traps.

[2] **API**: *Application Programming Interface* is a set of rules and protocols that allows different software and applications to communicate, exchange data, and share functionality automatically and securely.

	Problem	Impact	Priorities for 2026
Governance and Management	Absent governance and security underestimated by the Board	High costs, operational downtime, and reputational damage	Structured governance and consistent investments
Infrastructure obsolescence	Outdated systems and insufficient investment	Accelerated emergency measures	Training and skills alignment
Human variable	Poor security culture and social engineering	Amplification of technical vulnerabilities	Evolution of behaviors and responsibilities

"2025 has reminded us that the attack surface is no longer just technical: identity, AI, and suppliers determine the real risk. Investing in governance, continuous monitoring, and operational resilience is the choice that protects value, business, and the people who make up the company. Protecting activities and services requires an approach that combines advanced technologies, governance, and, above all, continuous training. The Cyberoo Observatory 2026 was created with the aim of increasing awareness and helping to make risk measurable and manageable, increasing visibility and prioritization capabilities, and transforming the evidence gathered into repeatable decisions and actionable strategies to reduce the operational impact of incidents" - said **Veronica Leonardi, CMO & Board Member of Cyberoo**.

***

SOURCE: The Observatory is based on the continuous monitoring and analysis of billions of security events detected in 2025 (over 61,000 events per second) through Cyberoo's proprietary systems and the operation of its MDR (Managed Detection & Response), which includes Cyber Threat Intelligence activities. The scope of observation includes over 700 midsize European customers from different sectors. Cyberoo publishes the Observatory's findings with the aim of promoting greater awareness of cyber dynamics and risks, helping companies to strengthen their cyber resilience through timely and measurable choices, in line with the evolution of the regulatory framework and the latest European guidelines on the subject.

The complete document in Italian is available at the following link Download the Report – CYBEROO Observatory 2026.

***

Cyberoo S.p.A., a company listed on the Euronext Growth Milan stock exchange of Borsa Italiana, is an innovative Reggio Emilia-based SME specialized in cybersecurity for businesses, intended not only to protect IT systems from external attacks but also to implement a real strategy capable of protecting, monitoring and managing IT ecosystem information. Cyberoo addresses the medium-sized enterprise market with a broad and deep portfolio of enterprise solutions developed using the most advanced technologies and with a value chain that allows it to set prices that are in line with our customers' spending power.

***

FOR INFORMATION:

CYBEROO
Chief Marketing Officer & Investor Relations Manager
Veronica Leonardi | veronica.leonardi@cyberoo.com +39 0522 388111

EURONEXT GROWTH ADVISOR
EnVent Italia SIM S.p.A.
Via degli Omenoni, 2 - 20121 Milan
Giancarlo D'Alessio| gdalessio@envent.it

INVESTOR RELATIONS ADVISOR
CDR Communication S.r.l.
Vincenza Colucci | vincenza.colucci@cdr-communication.it
Marika Martinciglio | marika.martinciglio@cdr-communication.it

MEDIA RELATIONS ADVISOR
CDR Communication S.r.l.
Maddalena Prestipino | maddalena.prestipino@cdr-communication.it