CYBEROO

COMUNICATO STAMPA

PUBBLICATO L'OSSERVATORIO CYBEROO 2026: NUOVI TREND DI ATTACCO ALLE IMPRESE E STRATEGIE DI DIFESA PER IL 2026

- **L'evoluzione degli Agenti AI e i nuovi rischi per le imprese**
- **Identificati 320 nuovi *threat actor***
- **La sovranità digitale compete anche con le identità non umane**
- **Violazione dell'e-mail e MFA tra gli attacchi più comuni**

Reggio Emilia, 26 febbraio 2026 - Cyberoo S.p.A., Pmi innovativa quotata sul Mercato Euronext Growth Milan, specializzata in cybersecurity per le imprese, pubblica la seconda edizione del report annuale dell'Osservatorio Cyberoo, quest'anno dedicato al tema "Dentro la materia oscura del cyberspazio". Il documento analizza i principali trend e pattern di attacco emersi nel 2025 e traduce le evidenze raccolte in strategie operative di difesa per il 2026, grazie ai dati forniti dal team I-SOC, centro avanzato con oltre 100 specialisti operativi in Italia e all'estero, che combina monitoraggio e risposta h24 e *Cyber Threat Intelligence*, e dall'*Incident Response Team*. Il team, composto da *ethical hacker* e analisti, difende le aziende dalle minacce informatiche integrando fonti interne, quali i dati della Cyber Security Suite, e fonti esterne, come il *Surface*, *Deep* e *Dark web,* con l'obiettivo di prevenire e minimizzare i danni di un attacco informatico.

Numeri

Tra i dati più rilevanti emersi nel 2025, Cyberoo segnala:

- **320 nuovi *threat actor*** identificati, tra cui particolarmente aggressivi: Qilin, Akira, Sarcoma, Everest
- Oltre **1.300 segnalazioni alle autorità competenti** per *phishing*, *antispam* e antifrode da parte di Cyberoo
- Il rilevamento di **38.654 domini sospetti**
- L'identificazione di oltre **2.700 CVE[1] univoche** associate ai fornitori monitorati, confermando la criticità della gestione delle vulnerabilità nell'ambito della *supply chain*

Trend 2025

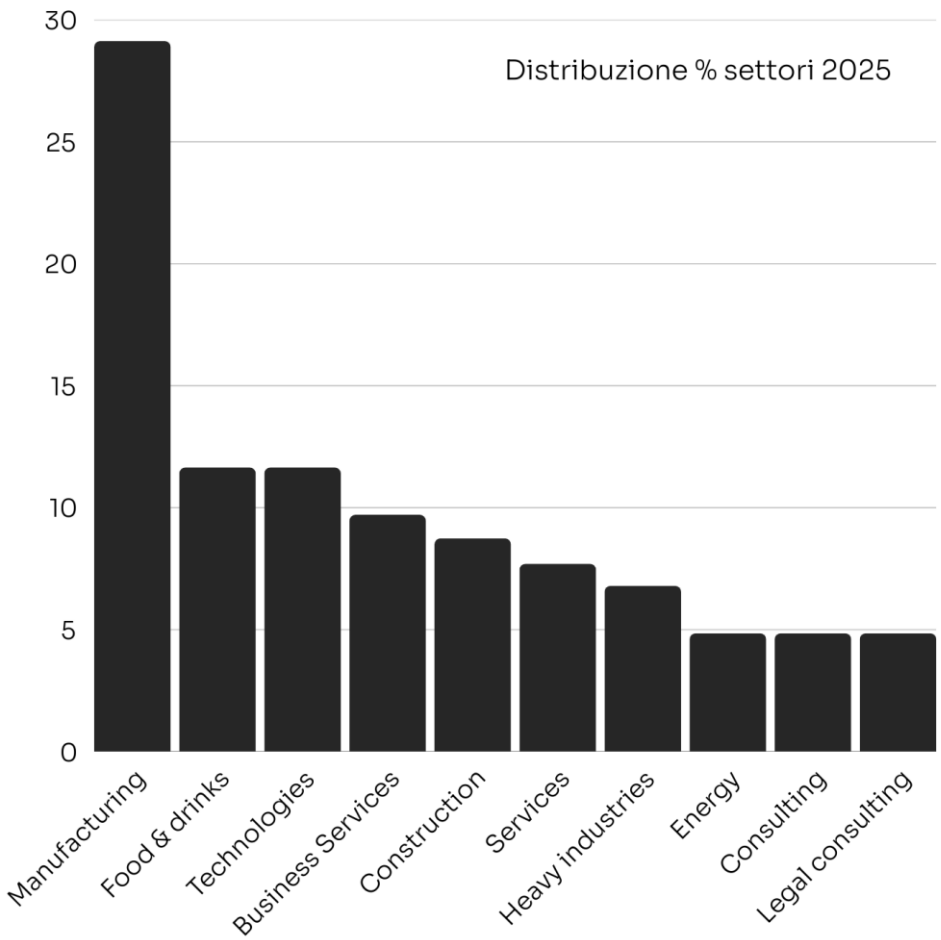
Il 2025 ha visto una crescita dello sfruttamento diretto delle vulnerabilità, incluse *zero-day*, e un'ulteriore espansione del mercato delle **credenziali rubate**. È tornato in auge l'uso degli **attacchi *DDoS***, cyberattacchi che rendono inaccessibili server e siti web inondandoli con traffico falso proveniente da migliaia di dispositivi infetti, come strumento di distrazione, impiegato per saturare i sistemi di difesa e facilitare attività parallele di ricognizione e infiltrazione.
Si è rivelato in forte evoluzione il ***phishing***, sempre più credibile e contestualizzato grazie all'uso dell'AI generativa, con casi di impersonificazione supportati da deepfake vocali e video.

[1] **CVE**: *Common Vulnerabilities and Exposures* (Vulnerabilità ed Esposizioni Comuni); si riferisce a un sistema standardizzato utilizzato per identificare in modo univoco le falle di sicurezza note in software, hardware e firmware.

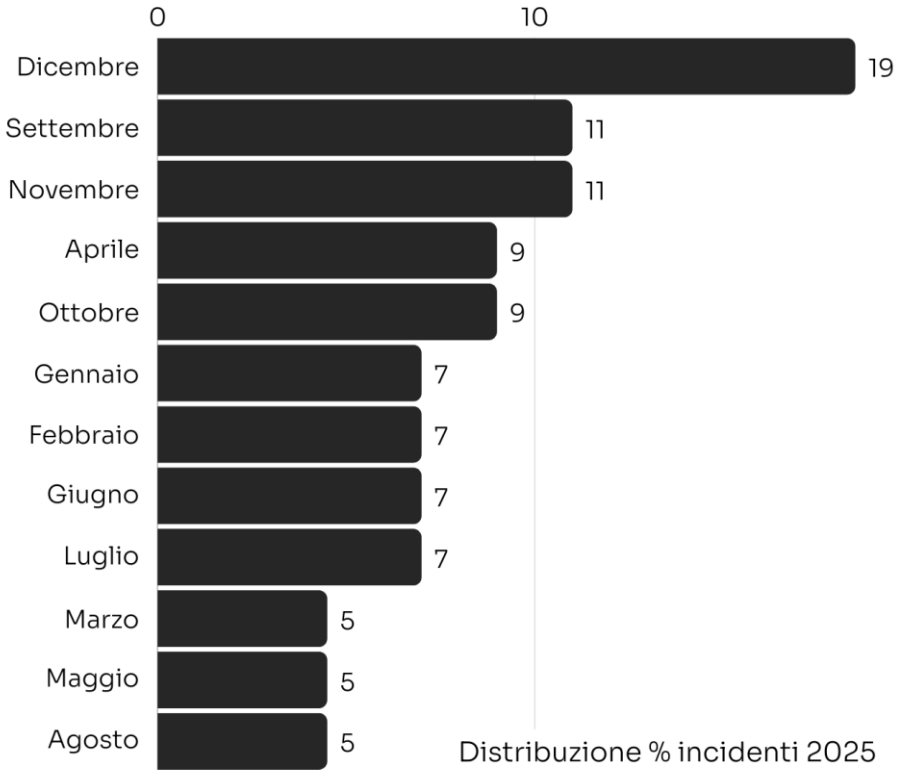
In generale, gli ***attacchi AI-powered*** rappresentano una minaccia in ascesa. Guardando al 2026 e al futuro, l'Osservatorio evidenzia l'aumento delle minacce abilitate dall'AI, che rende più efficaci e scalabili, oltre al *phishing*, impersonificazioni e diffusione di ***fake news***. Restano centrali anche il rischio legato al furto di credenziali, la pressione su *cloud* e *SaaS* che richiede controlli continui.
Parallelamente, gli incidenti legati alla *supply chain* hanno mostrato una dinamica "a catena", in cui una vulnerabilità su un fornitore o un componente condiviso si è spesso tradotta in un colpo a più organizzazioni, fino a estendersi alla filiera con forme di pressione come la ***triple extortion***, tattica cybercriminale avanzata, evoluzione del *ransomware*, con cui gli aggressori non si limitano a cifrare i dati, ma applicano tre livelli di pressione simultanei per costringere le vittima a pagare il riscatto dei dati.

Distribuzione degli attacchi cyber: mercati colpiti e periodi critici

Nel campione analizzato ai fini della stesura del report, il settore manufacturing risulta il più esposto agli attacchi cyber, avendone registrata una percentuale pari al 29% del totale esaminato, considerando anche l'effetto "di volume" del settore nel mercato italiano ed europeo.



Sul piano temporale, dicembre risulta il mese più colpito dalle compromissioni del 2025, in coincidenza con il periodo di ferie natalizie, quando la riduzione dei presidi e del personale può aumentare la vulnerabilità operativa delle aziende.



Le sfide del 2026

Alla luce dei dati evidenziati, la sfida più grande riguarda ciò che resta invisibile: esiste un divario tra la percezione di sicurezza e il rischio reale che grava sui sistemi informativi. Cyberoo definisce questa area non osservata "materia oscura cibernetica": si tratta dell'insieme di asset e superfici non mappate, controlli incompleti, sistemi obsoleti, scarsa consapevolezza, token e API[2] non adeguatamente gestiti, e identità non umane fuori dal perimetro di monitoraggio.
Ecco perché, tra le azioni prioritarie consigliate per il 2026, c'è innanzitutto rafforzare governance e responsabilità interne, unire formazione, cultura e consapevolezza all'orchestrazione di tecnologie, processi e competenze umane, adottare controlli *identity-first*, applicare una gestione delle *patch risk-based*, garantire supervisione continua di *cloud* e *SaaS* con *backup* e *playbook di incident response*. L'obiettivo deve essere passare da una sicurezza reattiva a una difesa proattiva e strategica, soprattutto nelle aziende più grandi che gestiscono *supply chain* più lunghe. Inoltre, è fondamentale aumentare trasparenza e controllo sull'AI: gestire l'intelligenza artificiale è fondamentale per evitare di cadere in trappole digitali.

[2] **API**: *Application Programming Interface* (interfaccia di programmazione delle applicazioni) è un insieme di regole e protocolli che consente a diversi software e applicazioni di comunicare, scambiarsi dati e funzionalità in modo automatico e sicuro.

	Problema	Impatto	Priorità 2026
Governance e Management	Governance assente e sicurezza sottovalutata dal Board	Costi elevati, fermi operativi e danni reputazionali	Governance strutturata e investimenti coerenti
Obsolescenza infrastruttura	Sistemi obsoleti e investimenti insufficienti	Interventi emergenziali accelerati	Formazione e allineamento competenze
Variabile umana	Scarsa cultura di sicurezza e social engineering	Amplificazione delle vulnerabilità tecniche	Evoluzione di comportamenti e responsabilità

"Il 2025 ci ha ricordato che la superficie d'attacco non è più solo tecnica: identità, AI e fornitori determinano il rischio reale. Investire in governance, monitoraggio continuo e resilienza operativa è la scelta che protegge valore, business e tutela le persone che formano l'azienda. Per proteggere attività e servizi è necessario un approccio che unisca tecnologie avanzate, governance e soprattutto formazione continua. L'Osservatorio Cyberoo 2026 nasce con l'obiettivo di incrementare consapevolezza e contribuire a rendere il rischio misurabile e gestibile, aumentando visibilità e capacità di priorità, e trasformando le evidenze raccolte in decisioni ripetibili e strategie attuabili per ridurre l'impatto operativo degli incidenti" - ha detto **Veronica Leonardi, CMO & Board Member di Cyberoo**.

***

FONTE: L'Osservatorio si basa sul monitoraggio e sull'analisi continuativa di miliardi di eventi di sicurezza rilevati nel 2025 (oltre 61.000 eventi al secondo) tramite i sistemi proprietari di Cyberoo e l'operatività del proprio MDR (Managed Detection & Response), che include attività di Cyber Threat Intelligence. Il perimetro di osservazione comprende oltre 700 clienti *midsize* europei appartenenti a settori differenti. Cyberoo rende pubblici i risultati dell'Osservatorio con l'obiettivo di favorire una maggiore consapevolezza delle dinamiche e dei rischi cyber, aiutando le aziende a rafforzare la propria *cyber resilience* attraverso scelte tempestive e misurabili, in linea con l'evoluzione del quadro regolatorio e con le più recenti indicazioni europee in materia.

Il documento completo è disponibile al seguente link Scarica il Report - Osservatorio CYBEROO 2026.

***

Cyberoo S.p.A., società quotata sul Mercato Euronext Growth Milan di Borsa Italiana, è una Pmi Innovativa emiliana specializzata in cyber security per le imprese, intesa non solo come protezione dei sistemi informatici dagli attacchi esterni ma come realizzazione di una vera e propria strategia in grado proteggere, monitorare e gestire le informazioni dell'ecosistema IT. Cyberoo si rivolge al mercato delle medie imprese con un portfolio di soluzioni enterprise ampio e profondo, sviluppate tramite l'utilizzo delle più avanzate tecnologie e con una catena del valore che permette di proporre a questo mercato prezzi in linea con le capacità di spesa.

***

PER INFORMAZIONI CYBEROO:

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

EURONEXT GROWTH ADVISOR
EnVent Italia SIM S.p.A.
ega@envent.it +39 02 22175979

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