COMUNICATO STAMPA

OSSERVATORIO CYBERSECURITY DI EXPRIVIA

NEL 2025 QUANTUM COMPUTING E ARTIFICIAL INTELLIGENCE RIDEFINISCONO LE MINACCE INFORMATICHE IN ITALIA

Secondo il Report annuale di Exprivia il cyberattacco ha cambiato qualità, diventando più selettivo, automatizzato e orientato al futuro

- Nel 2025 registrati oltre 1.000 attacchi informatici a trimestre, fatta eccezione per il primo
- L' 8,5% degli incidenti è già potenzialmente riconducibile a tecnologie quantistiche
- L'AI è impiegata nel 42% degli attacchi riusciti
- Il settore Finance è il più colpito dell'anno
- Al Sud maggior numero di fenomeni registrati per milioni di abitanti rispetto a Nord e Centro Italia

Molfetta, 10 marzo 2026 – Dodici ore al giorno sotto attacco, per tutto il 2025. È il quadro che emerge dal **Threat Intelligence Report** annuale rilasciato dall'Osservatorio Cybersecurity di Exprivia, basato sull'analisi di fonti aperte tra siti di aziende colpite, portali web di interesse nazionale, agenzie di stampa online, blog e social media. Nel 2025 l'Intelligenza Artificiale è entrata stabilmente nella cassetta degli attrezzi dei criminali informatici rendendo gli attacchi più precisi, più difficili da rilevare e più efficaci. E mentre questo avviene, si affaccia già una nuova minaccia, quella quantistica.

I numeri e la geografia del 2025

Nel corso del 2025 il numero di **attacchi informatici** si è mantenuto costantemente elevato, con oltre **1.000 eventi a trimestre**, fatta eccezione per i primi tre mesi, in cui sono stati registrati 630 fenomeni criminali. Gli **incidenti, ovvero gli attacchi andati a buon fine**, hanno superato stabilmente i 100 eventi ogni trimestre, mentre le **violazioni della privacy** si sono attestate su una media di circa 19 eventi per trimestre. Complessivamente, nel 2025 si sono verificati 3.732 attacchi, 676 incidenti e 75 violazioni della privacy, per un totale di 4.483 fenomeni rispetto ai 2.461 del 2024 **(+82%).**
Parallelamente, la distribuzione geografica vede il Nord Italia con il maggior numero di attacchi e incidenti, perché concentra infrastrutture digitali più estese e un tessuto produttivo più esposto; il Centro con un'esposizione rilevante ma inferiore, riflettendo la centralità dei poli amministrativi, istituzionali e dei centri direzionali che lo caratterizzano; **il Sud**, pur con numeri assoluti inferiori, **risulta proporzionalmente più impattato rispetto alla popolazione** a causa di una vulnerabilità legata a una minore maturità delle difese.

La frontiera quantistica: una minaccia già presente, con impatto futuro

Il dato più inedito del Report di Exprivia riguarda le tecnologie quantistiche. **L'8,5% degli incidenti del 2025 è già potenzialmente riconducibile al quantum computing** che - secondo gli esperti di Exprivia - nel medio-lungo periodo potrebbe modificare alcune dinamiche della sicurezza informatica. Ad esempio, le capacità di calcolo quantistico potrebbero potenziare significativamente in futuro la cifratura dei dati a scopo estorsivo o le operazioni di *privilege escalation,* cioè la capacità di ottenere livelli di accesso più alto. Il quantum computing non è ancora uno strumento operativo nelle mani del cybercrime, ma la sua influenza si fa già sentire nella strategia degli attaccanti. Un criminale informatico può sottrarre oggi dati cifrati con algoritmi tradizionali e conservarli in attesa che la potenza di calcolo

quantistico renda possibile decifrarli. È la strategia nota come "*harvest now, impact later*", ovvero raccogliere adesso, colpire dopo. Il rischio cresce ulteriormente nella combinazione AI-quantum, dove l'intelligenza artificiale seleziona i dati più preziosi da sottrarre e la computazione quantistica si prepara a scardinare le protezioni crittografiche.

"Quello che i dati del 2025 ci indicano è che, per la prima volta, gli attaccanti stanno preparando il terreno a scenari ancora inesistenti – commenta **Domenico Raguseo, direttore Cybersecurity di Exprivia** – *Questo cambia profondamente la prospettiva, in quanto non stiamo più parlando di difendersi solo dagli attacchi imminenti, ma di costruire oggi una resilienza capace di reggere a minacce per le quali verranno usati strumenti ancora in via di sviluppo. Le aziende e più in generale la collettività, che aspettano di vedere il problema prima di agire, rischiano di arrivare impreparate a una partita già iniziata. Appare così sempre più importante integrare la threat intelligence con analisi prospettiche, considerando la sicurezza come investimento strategico e non solo come funzione reattiva".*

L'AI impiegata stabilmente negli attacchi: più precisione, meno rumore

L'uso dell'intelligenza artificiale nei cyberattacchi, in particolare negli incidenti di sicurezza, si assesta al **42%** in chiusura dell'anno. Il contributo dell'AI non è nella forza bruta, ma nella precisione, poiché permette di costruire campagne di phishing personalizzate e credibili. Inoltre, rende i ransomware più selettivi e capaci di identificare e cifrare solo i file davvero critici (come contratti, dati contabili, informazioni strategiche) riducendo il rischio di essere intercettati e massimizzando il danno.

Il settore più colpito: Finance

Il **settore Finance** è nel 2025 il **target privilegiato dei criminali informatici** con 1.432 fenomeni (più che raddoppiati rispetto ai 709 del 2024) ed effetti significativi su processi core e dati sensibili. Questo mostra la forte pressione che banche e istituzioni finanziarie subiscono, dovuta soprattutto all'elevato valore economico delle informazioni gestite. A seguire, il settore **Software/Hardware**, con 1.348 casi (+77% rispetto ai 760 del 2024), segno che i fornitori di tecnologie digitali sono bersagli frequenti, anche per sfruttare eventuali vulnerabilità nei prodotti distribuiti su larga scala. Il **Retail** registra invece 521 fenomeni (nel 2024 erano stati 218), numero legato alla forte digitalizzazione del settore e alla gestione di dati sensibili come pagamenti e credenziali degli utenti. La **Pubblica Amministrazione**, con 351 casi (221 nel 2024) rimane un obiettivo rilevante per la grande quantità di dati sensibili gestiti e la presenza di infrastrutture IT spesso eterogenee e in parte non ancora protette adeguatamente o obsolete.

Come attaccano e impattano: le minacce dell'anno

Le tecniche più utilizzate nel 2025 sono **phishing/social engineering** e, a poca distanza, i **malware, che totalizzano insieme circa l'84% dei fenomeni complessivi.** Tra i malware, i RAT sono particolarmente insidiosi perché invisibili, forniscono agli attaccanti un accesso silenzioso e persistente ai sistemi colpiti, permettendo di muoversi lateralmente nelle reti, sottrarre dati e installare ulteriori malware senza lasciare tracce evidenti. Il **furto di dati si conferma il danno più frequente**, rappresentando il 70% degli eventi, a conferma di un cybercrime sempre più orientato al valore economico e strategico delle informazioni.

I dispositivi connessi: telecamere e dispostivi medici i più vulnerabili

Sul fronte **IoT, le telecamere** (il 31% dei dispositivi analizzati dagli esperti di Exprivia) **risultano i**

dispositivi meno sicuri, seguite da PLC e **dispositivi medicali**, dei quali il 29% del totale preso in esame è risultato vulnerabile. Un dato che segnala come la superficie di attacco si stia allargando ben oltre i sistemi informatici tradizionali, richiedendo un approccio alla sicurezza che includa tutti i device connessi, indipendentemente dalla loro funzione.

°°°

Exprivia

Il Gruppo Exprivia, specializzato in Information and Communication Technology, è tra i principali protagonisti della trasformazione digitale. Forte di un bagaglio di competenze maturate con una presenza costante sul mercato nazionale e internazionale, Exprivia opera in nove Paesi del mondo avvalendosi di un team di esperti in diversi ambiti della tecnologia e della digitalizzazione: dall'Intelligenza Artificiale alla Cybersecurity, dai Big Data al Cloud, dal Networking al BPO, dal CRM all'ERP, con particolare riferimento al presidio dell'offerta SAP. Exprivia supporta i propri clienti nei settori Banking, Finance & Insurance, Aerospace & Defense, Energy & Utilities, Healthcare, Manufacturing & Distribution, Telco & Media, Public Sector. La capacità progettuale del gruppo è arricchita da una solida rete di partner, soluzioni proprietarie, servizi di design, ingegneria e consulenza personalizzata. Maggiori informazioni al sito www.exprivia.com

Contatti per la stampa
Exprivia
Luca Vittorio Mario Ferraris
marketing.exprivia@exprivia.com
T.: +39 080 3382070
F.: +39 080 3382077

SEC Newgate Italia | Ufficio stampa Exprivia
Martina Trecca
martina.trecca@secnewgate.it
+39 334 1019671
Alessio Costa
alessio.costa@secnewgate.it
+39 340 3442329
Teresa Marmo
teresa.marmo@secnewgate.it
+ 39 335 671821