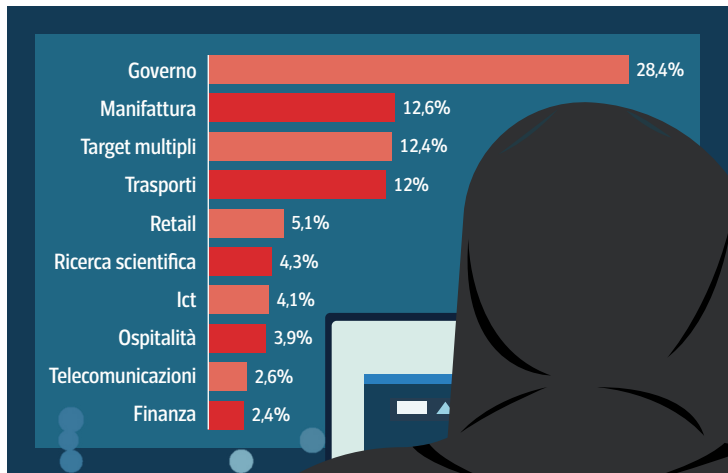


VOCI CLONATE, VISI CONTRAFFATTI NELLA GUERRA DEI ROBOT IL PIRATA È UN ALGORITMO

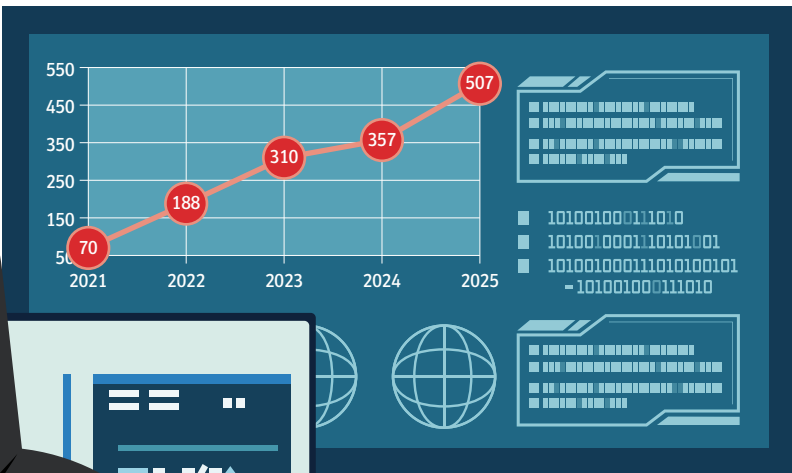
I più colpiti

Le principali vittime di cyber attacchi in Italia nel 2025



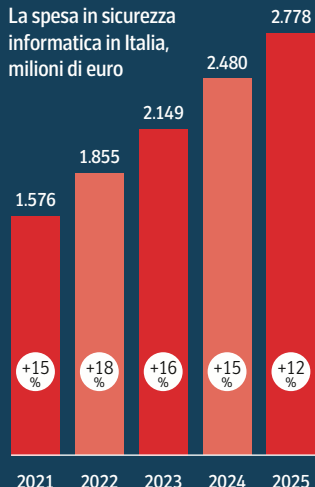
L'impennata

I cyber incidenti di maggiore impatto economico e reputazionale* in Italia negli ultimi 5 anni



Il prezzo dello scudo

La spesa in sicurezza informatica in Italia, milioni di euro



1.432

I gravi incidenti da attacchi informatici in Italia fra il 2021 e il 2025

+76%

La spesa in sicurezza informatica in Italia fra il 2021 e il 2025

Fonte: Clusit - rapporto sulla cybersecurity 2026

* Attacchi andati a buon fine, con conseguenze gravi e sistemiche, confermati e di dominio pubblico

Fonte: Osservatorio cybersecurity & data protection - Polimi 2026

S. A.

Nella perenne lotta tra pirati informatici e cyberpoliziotti si è inserito un terzo attore: i sistemi di intelligenza artificiale. Usati dai primi per mettere in atto nuove modalità di incursioni, dai secondi per difendersi. L'Italia non si sottrae al crescente trend di attacchi, sempre più sofisticati e intensi. Si tratta, in particolare, di deepfake, con immagini e video manipolati, e di ransomware, il software dannoso che blocca l'accesso a computer, documenti o dispositivi mobili crittografandoli, con la richiesta di riscatti economici in cambio delle informazioni rubate. Il Rapporto Clusit 2026, l'associazione italiana per la Sicurezza informatica, rivela che il 2025 ha segnato il record storico per la criminalità informatica.

Nel mondo gli attacchi sono cresciuti del 49% rispetto all'anno precedente, arrivando a 5.265 casi gravi. Il maggior numero registrato fino a oggi. L'Italia si conferma un bersaglio in primo piano nel panorama globale.

Il picco nazionale

Nel nostro Paese infatti si sono verificati lo scorso anno il 9,6% degli incidenti totali del mondo, con un aumento del 42% sul 2024. In assoluto, ne sono stati rilevati 507, in confronto ai 357 del 2024. Con l'AI presente come moltiplicatore di rischio per nuovi attacchi. Dal rapporto emerge come in Italia siano apparse nel 2025 due tipologie di hacker. I cybercriminali per il 61%, raggruppati ora in organizzazioni diffuse in più nazioni, con la possibilità di aggregazione dei compiti. E

Nel 2025 c'è stato il record delle intrusioni informatiche: 5.265 i casi più gravi nel mondo e il 10% è in Italia, +42% in un anno

La novità è che ora le frodi vengono direttamente dagli agenti Ai, senza l'intervento dell'uomo o quasi. E chi le frena? Altri agenti Ai...

di UMBERTO TORELLI

poi gli attivisti per il 39%, i cosiddetti hacktivist, che sfruttano tecniche hacking per promuovere online cause politiche, sociali e ideologiche.

Spiega a proposito Luca Bechelli, del comitato direttivo Clusit: «Spesso i fenomeni di cyber attivismo presentano finalità dimostrative e impatti economici limitati, ma gli attacchi colpiscono nel segno, attirando l'attenzione mediatica, con lo scopo di ledere la reputazione delle organizzazioni colpite».

Il ransomware, con l'obiettivo di estorcere denaro, si conferma la causa di nove incidenti su dieci, in crescita del 55% rispetto all'anno precedente. Questo andamento, secondo gli esperti, conferma l'emergente commistione tra criminalità tradizionale e digitale. Fenomeno che porta a reinvestire i proventi dei riscatti per aumentare le risorse economiche degli attaccanti.

L'analisi evidenzia come nel 2025 quasi un incidente su cinque sia avvenuto a danno di obiettivi multipli. Si tratta di attacchi che hanno colpito organizzazioni a prescindere da settore e dimensioni, in crescita del 96%. Un segnale preoccupante, secondo gli esperti Clusit, dovuto alla capacità degli hacker di gestire ope-

razioni su larga scala. Ma anche alla fragilità delle infrastrutture tecnologiche delle vittime.

I settori governativi e militari sono i più colpiti con il 12% del totale degli attacchi subiti. Segue la sanità (11%), con incidenti in crescita del 19% rispetto al 2024. Ma c'è anche una buona notizia: a fronte di minacce sempre più aggressive, aziende e istituzioni italiane hanno risposto incrementando gli investimenti.

Secondo l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, nel 2025 il mercato della cybersecurity in Italia ha raggiunto il valore di 2,78 miliardi di euro. In crescita del 12% rispetto al 2024. Un incremento per contrastare i nuovi sistemi di attacco dell'AI. «L'intelligenza artificiale ha portato all'automazione e potenziamento delle attività offensive — dice Gabriele Faggioli, responsabile scientifico dell'Osservatorio —. D'ora in avanti dobbiamo aspettarci cyberminacce autonome, messe in atto senza l'intervento dell'uomo».

Ecco perché l'83% delle grandi imprese italiane dichiara di presidiare stabilmente gli attacchi.

Le previsioni per il 2026 delineano uno scenario ancora più comples-

so, dominato dalla convergenza tecnologica. Secondo le analisi di Check Point Software, assisteremo all'alba dell'«Ai agentica». Il termine indica sistemi autonomi capaci di pianificare ed eseguire strategie con un intervento umano minimo. Questo trasformerà la sicurezza cybernetica in campo di battaglia tra avversari autonomi e difensori altrettanto autonomi.

Le nuove tecniche

Di fatto, a governare saranno dispositivi Ai. L'identità di persone e informazioni diventerà il nuovo perimetro di attacco. Grazie a deepfake e frodi vocali, i criminali saranno in grado di clonare voci e video in tempo reale per autorizzare trasferimenti di denaro e aggirare l'autenticazione a più fattori.

Un altro pericolo emergente è rappresentato dagli attacchi rivolti direttamente agli algoritmi.

Trend Micro nel Security Predictions 2026 valuta le reali nuove offensive come la *prompt injection* e il *data poisoning*. Il primo con l'attaccante che inserisce istruzioni testuali malevole (prompt) per ingannare l'intelligenza artificiale e bypassare le regole di sicurezza.

Il secondo, l'avvelenamento dei dati, colpisce i sistemi informatici dall'interno, intervenendo durante la fase di addestramento e aggiornamento dei programmi.

Stiamo assistendo alle prime schermaglie di cyberattacchi portati avanti da macchine contro macchine. Arriva la nuova era degli attacchi cyborg.

+49

Per cento

Gli attacchi informatici gravi nel mondo nel 2025 (a quota 5.265) rispetto al 2024 (fonte: Rapporto Clusit 2026)