LAVOCE.INFO – 14 APRILE 2026

Cybersecurity: anche l'Italia è un bersaglio degli hacker

di Gian Lorenzo Cosi

Gli attacchi informatici sono diventati uno strumento ricorrente di acquisizione di dati, estorsione e spionaggio. Colpiscono le grandi organizzazioni, ma anche imprese e individui. Cosa si fa in Italia per contrastare il fenomeno in crescita.

Tutti possono subire un attacco

Pochi giorni fa, un gruppo di hacker legato all'Iran ha violato l'account e-mail personale del direttore dell'Fbi Kash Patel, rendendo evidente che pure le figure istituzionali di altissimo profilo possono essere esposte ad attacchi informatici mirati. Anche in Italia il rischio è assai concreto: un attacco alle Gallerie degli Uffizi ha portato alla sottrazione di dati sensibili – tra cui codici di accesso, password e sistemi di sicurezza – con la richiesta di un riscatto per evitarne la diffusione sul dark web.

Sul piano economico, gli attacchi informatici generano costi rilevanti e spesso sottostimati. Secondo Ibm, nel report *Cost of a Data Breach* (realizzato con il Ponemon Institute), il costo medio di una violazione dei dati per azienda si attesta intorno ai 4 milioni di dollari.

Le stime aggregate suggeriscono inoltre che il cybercrime rappresenti ormai una componente significativa delle perdite economiche globali, soprattutto per gli effetti indiretti sulla produttività, sulla continuità operativa e sulla fiducia nei sistemi digitali.

Oltre gli stereotipi

Il fenomeno hacker è articolato e non è riconducibile esclusivamente a una dimensione individuale. Una quota crescente degli attacchi è infatti attribuibile a gruppi organizzati, spesso mossi da interessi economici, strategici o politici.

In alcuni casi, soggetti privati operano in connessione, diretta o indiretta, con apparati di sicurezza nazionale, contribuendo a rendere il fenomeno parte integrante delle dinamiche geopolitiche ed economiche.

Il termine "hacker" identifica un insieme eterogeneo di attori, competenze e finalità. Nel campo, per esempio, operano anche figure professionali legittime, come gli hacker etici, sempre più richiesti da imprese e istituzioni per individuare vulnerabilità prima che vengano sfruttate in modo malevolo. Tra queste polarità si colloca un'area intermedia in cui competenze tecniche e finalità non sono sempre chiaramente distinguibili.

Uno strumento di spionaggio

Gli attacchi informatici sono diventati uno strumento ricorrente di acquisizione di dati, estorsione e spionaggio. Gli effetti coinvolgono non solo grandi organizzazioni ma anche imprese e individui, spesso in modo indiretto.

In questo contesto cresce la domanda di competenze specialistiche in cybersecurity, mentre la disponibilità e il riutilizzo di dati sottratti alimentano dinamiche che travalicano la dimensione puramente criminale, assumendo rilevanza economica e geopolitica.

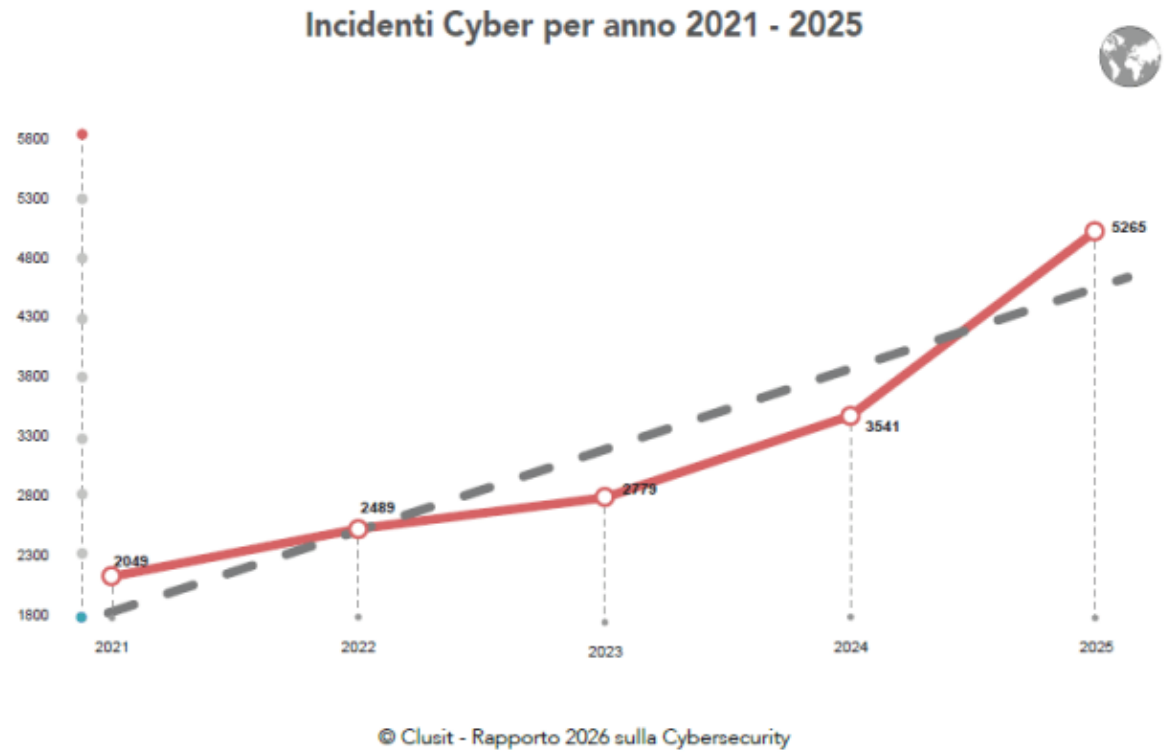
L'uso di strumenti digitali avanzati, inclusa l'intelligenza artificiale, contribuisce ad aumentare la scala e la sofisticazione degli attacchi, ma al tempo stesso rappresenta anche un fattore chiave per il rafforzamento delle difese.

Il Rapporto Clusit 2026

Il panorama delle minacce informatiche è in continua evoluzione e crescita, come conferma il *Rapporto Clusit sulla Cybersecurity 2026*, che analizza i principali incidenti di sicurezza informatica del 2025 a livello globale, inclusa l'Italia, in confronto con gli anni precedenti.

Nel periodo tra gennaio 2021 e dicembre 2025, il Rapporto ha censito 16.123 incidenti informatici a livello globale.

Figura 1



Nel 2025 la criminalità informatica ha rappresentato quasi nove incidenti su dieci (89,3 per cento, +3 punti rispetto al 2024), indicando una possibile crescente convergenza tra

criminalità tradizionale e digitale e un rafforzamento delle risorse disponibili per gli attori malevoli.

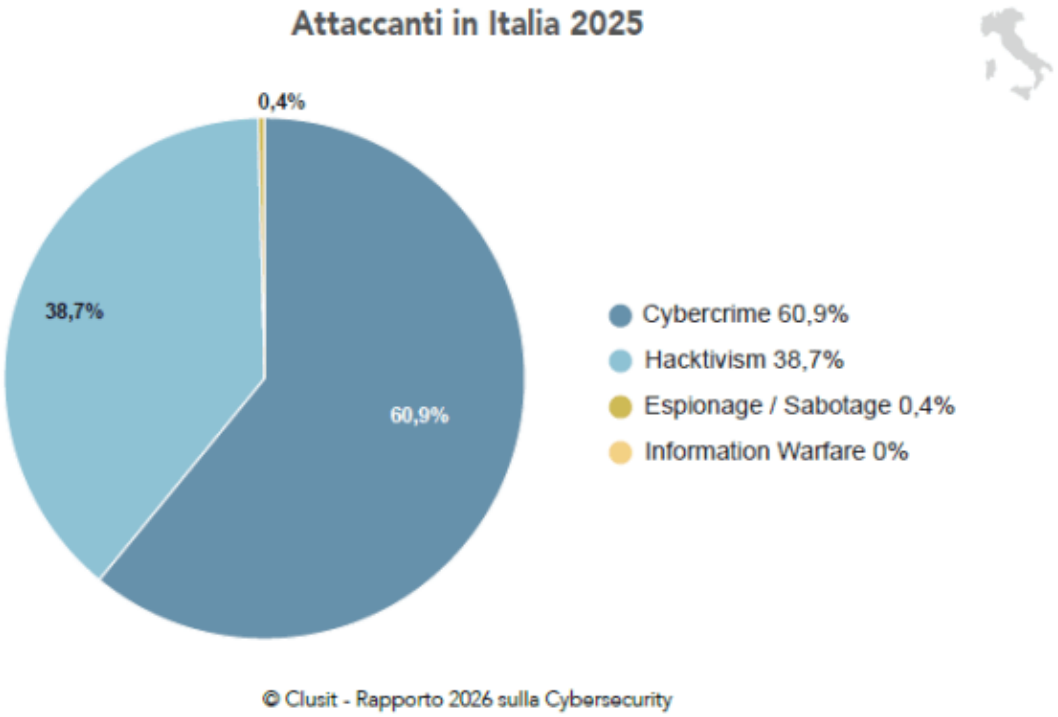
Quasi la metà degli incidenti (46 per cento) si concentra su tre categorie principali di vittime: attacchi a bersagli multipli (23 per cento), istituzioni governative e militari (12 per cento) e settore sanitario (11 per cento). Le campagne più trasversali, che colpiscono simultaneamente più settori, si confermano le più efficaci in termini di conseguenze. Particolarmente esposto risulta anche il settore finanziario, con banche, assicurazioni e operatori dei pagamenti stabilmente nel mirino degli attaccanti, a conferma del rischio sistemico per la stabilità economica.

In Italia rischi dal cyberattivismo

L'Italia rappresenta il 9,6 per cento degli incidenti informatici a livello mondiale, una quota alta rispetto al Pil e alla popolazione, con una crescita significativa nel tempo. Nel 2025 gli attacchi nel nostro paese sono infatti aumentati del 49 per cento rispetto all'anno precedente, secondo il Rapporto.

È dunque necessario rafforzare ulteriormente le difese digitali, in un sistema caratterizzato da Pmi, per le quali le conseguenze in termini di operatività, costi e competitività non sono indifferenti.

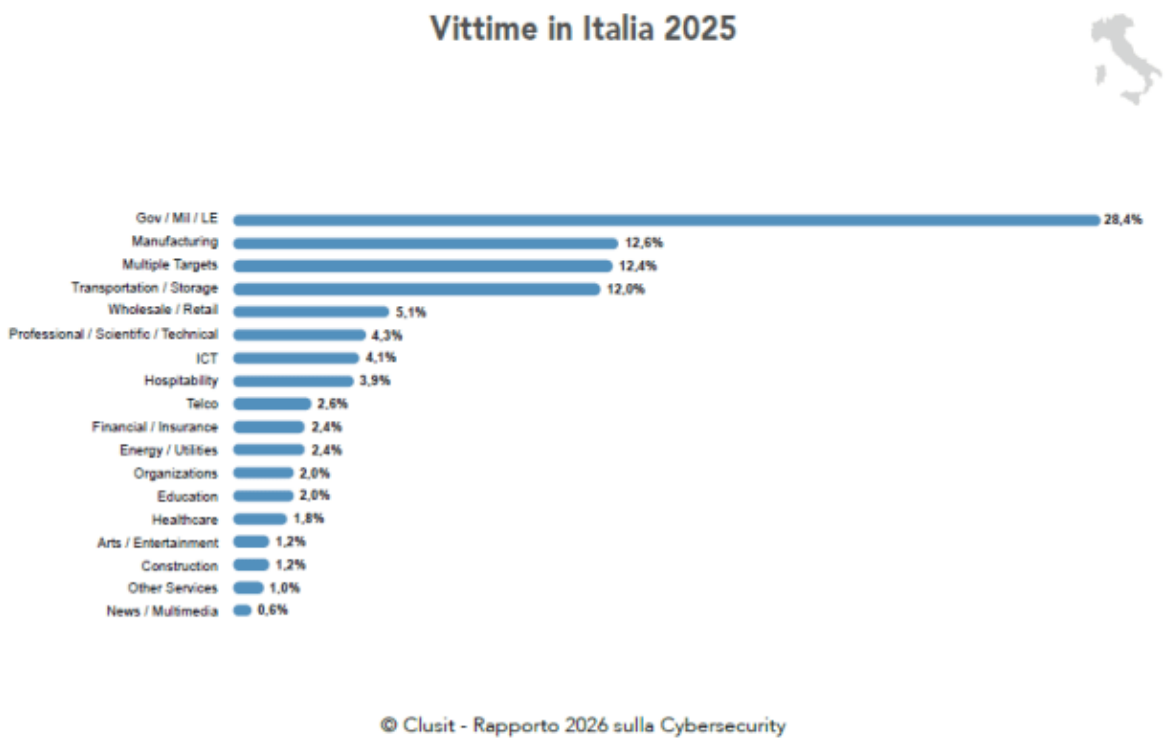
Figura 2 – Distribuzione degli attaccanti in Italia



La distribuzione si discosta significativamente da quella del campione globale, dove il cybercrime rappresenta circa l'89 per cento degli incidenti.

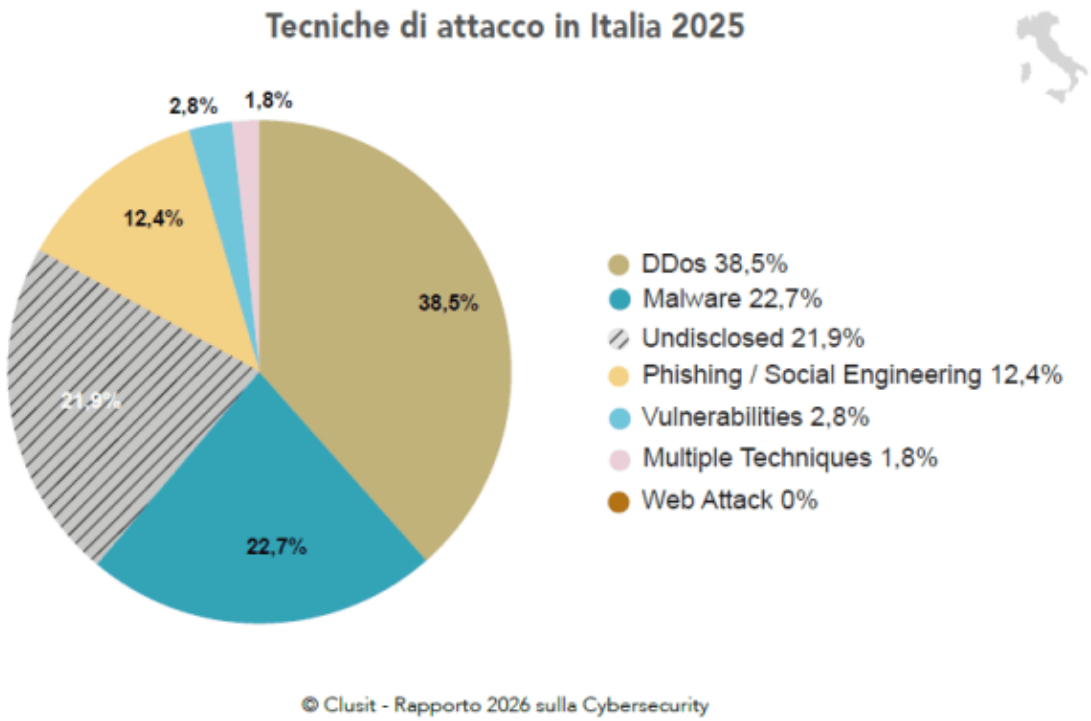
Nel contesto italiano, la quota scende al 60,9 per cento, mentre gli episodi riconducibili all'hacktivism, ossia motivati da finalità ideologiche o politiche, raggiungono il 38,7 per cento, registrando un aumento di 16,7 punti percentuali rispetto al 2024.
Questa crescita riflette il peso crescente delle dinamiche geopolitiche nello spazio digitale, con azioni di attivismo informatico sempre più spesso correlate ai principali conflitti internazionali in corso. Nel loro insieme, questi dati indicano come il rischio cyber in Italia non sia riconducibile esclusivamente alla criminalità a fini di lucro, ma risenta in misura crescente anche di fattori geopolitici, contribuendo a rendere il quadro delle minacce meno prevedibile.

Figura 3 – Distribuzione vittime per categoria



Il settore più colpito è quello governativo e militare, dove si concentra oltre il 28 per cento degli incidenti, in aumento di 12 punti percentuali rispetto all'anno precedente. A distanza significativa seguono il comparto manifatturiero, con il 12,6 per cento degli attacchi, e la categoria dei bersagli multipli, che rappresenta il 12,4 per cento del totale.
Nel complesso, la distribuzione conferma la forte esposizione delle infrastrutture pubbliche e dei settori industriali strategici, evidenziando come il rischio cyber si concentri in aree ad alto valore economico e istituzionale.

Figura 4 – Le tecniche di attacco



© Clusit - Rapporto 2026 sulla Cybersecurity

Tra le tecniche di attacco, il malware scende al secondo posto, al 22,27 per cento (dal 38 per cento del 2024) mentre gli incidenti DDoS (Distributed Denial-of-Service), che rendono inaccessibili siti web o risorse di rete, raggiungono il 38,5 per cento, partendo dal 21 per cento del 2024. Il dato è coerente con il forte aumento degli incidenti subiti dalla pubblica amministrazione ed è altrettanto coerente con l'impennata di incidenti di tipologia hacktivism.

Acn e direttiva NIS2

L'Agenzia per la cybersicurezza nazionale (Acn) – istituita nel 2021 – ha l'obiettivo di difendere gli interessi strategici digitali dell'Italia e della pubblica amministrazione. Mira a rendere il paese più sicuro e resiliente di fronte alle nuove sfide poste dall'incessante sviluppo tecnologico e dalla trasformazione digitale: identificare, prevenire e mitigare il più possibile le conseguenze derivanti da attacchi di natura cibernetica può rendere poco vantaggiose, per gli attaccanti, eventuali attività offensive.

In questo contesto si inserisce la direttiva NIS2, che rafforza la cybersecurity nell'Unione europea, introducendo requisiti più stringenti in materia di gestione del rischio e notifica degli incidenti ed estendendo gli obblighi a un numero maggiore di settori essenziali e strategici.

In Italia, la direttiva è stata recepita con il decreto legislativo n. 138/2024, entrato in vigore nell'ottobre 2024. Tuttavia, la sua attuazione è ancora in corso e rappresenta un passaggio cruciale per rafforzare in modo strutturale la sicurezza cibernetica del sistema paese.