ANNO 2025

Cyber Security Report

Analisi delle minacce ed evoluzione dello scenario

CYBER SECURITY FOUNDATION

TIM

Cyber Security Report

Analisi delle minacce ed evoluzione dello scenario

anno 2025

Realizzato da:

Cyber Security Foundation e TIM

In collaborazione con

Insikt Group – Recorded Future

Analisi ed elaborazioni grafiche

Centro Studi TIM

Cyber Security Report
anno 2025

On. Alessandro Colucci
Presidente Intergruppo Parlamentare per la Sicurezza Informatica e Tecnologica

Desidero innanzitutto ringraziare tutti coloro che hanno contribuito alla realizzazione di questo Rapporto di Cyber Security, giunto alla sua seconda edizione. È un lavoro prezioso, perché non si limita a raccogliere dati e analisi, ma contribuisce a far crescere una consapevolezza ormai indispensabile: la sicurezza digitale riguarda la vita quotidiana dei cittadini, la tenuta delle nostre istituzioni, la competitività delle imprese e la sovranità tecnologica del Paese.

Vale, anche in questo ambito, l'antico principio di Cicerone: «Salus populi suprema lex esto», il bene, la salvezza, del popolo sia la legge suprema. Nel tempo della trasformazione digitale, questo significa riconoscere che proteggere le reti, i dati e le infrastrutture è un dovere pubblico: una forma concreta di tutela dei cittadini e dell'interesse nazionale.

Per molto tempo abbiamo considerato la cybersicurezza come una materia per tecnici, specialisti, addetti ai lavori. Oggi non è più così. Ogni volta che un cittadino accede a un servizio sanitario online, prenota una visita, utilizza un'app bancaria, comunica con la pubblica amministrazione o affida i propri dati a una piattaforma digitale, entra in uno spazio che deve essere protetto. La sicurezza informatica non è più un tema distante: è una condizione concreta di libertà, fiducia e tutela della persona.

La cybersicurezza riguarda ciascuno di noi. Riguarda il medico di famiglia che gestisce le cartelle cliniche digitali, il piccolo imprenditore che deve proteggere i dati dei propri clienti, il Comune che eroga i sussidi, il genitore che usa lo smartphone per accedere allo sportello bancario. E riguarda le grandi infrastrutture su cui si regge la vita collettiva: quando un ospedale non riesce a garantire le cure dopo un attacco informatico, quando un Comune viene paralizzato da un ransomware e i cittadini non possono accedere ai servizi anagrafici, quando un'azienda perde dati sensibili e con essi posti di lavoro, non stiamo parlando di qualcosa di astratto. Stiamo parlando di famiglie, di lavoratori, di comunità colpite nel cuore dei loro diritti fondamentali. Chiunque oggi è esposto, e chiunque ha il diritto di essere protetto.

In questo scenario, la minaccia cyber evolve con una rapidità che impone alla politica, alle istituzioni e al mondo produttivo un salto di qualità. Assistiamo a campagne ransomware sempre più sofisticate, ad attacchi contro infrastrutture critiche, all'utilizzo delle vulnerabilità come leva sistemica di aggressione e a un ampliamento delle superfici di rischio legato alla trasformazione digitale e all'adozione di tecnologie emergenti.

Ho visto da vicino, nel mio lavoro parlamentare, quanto questa minaccia sia concreta e quanto ancora facciamo fatica a percepirla nella sua reale gravità. Gli attacchi cyber rappresentano oggi anche una nuova forma di

conflitto. Non sempre hanno il volto tradizionale dell'aggressione, ma possono produrre effetti concreti sulla sicurezza di uno Stato, sulla continuità dei servizi essenziali, sulla stabilità economica e sulla fiducia dei cittadini nelle istituzioni. Colpire una rete sanitaria, un'infrastruttura energetica, un sistema bancario o una piattaforma pubblica significa incidere direttamente sulla vita delle persone e sulla capacità di un Paese di funzionare. Per questo la cybersicurezza è ormai parte integrante della sicurezza nazionale: difendere lo spazio digitale significa difendere la sovranità, la democrazia e la libertà dei cittadini.

Ignorare questa realtà non è un'opzione: sarebbe una scelta politica irresponsabile. Abbiamo la responsabilità, come Parlamento e come istituzioni, di costruire risposte all'altezza della sfida, traducendo gli impegni normativi in regole chiare, in risorse adeguate e in tutele concrete per i cittadini.

Per questo è fondamentale promuovere una cultura della sicurezza informatica che non sia soltanto reattiva, ma preventiva, condivisa e diffusa. Non basta costruire difese tecnologiche: bisogna che i cittadini sappiano riconoscere un rischio, che i dipendenti pubblici siano formati, che le piccole e medie imprese abbiano strumenti adeguati. La consapevolezza è la prima linea di difesa, e investire nella formazione è un atto politico di civiltà.

Come Intergruppo Parlamentare per la Sicurezza Informatica e Tecnologica, riteniamo essenziale sostenere un dialogo stabile tra istituzioni, imprese, università, ricerca e operatori della cybersecurity. Le sfide che abbiamo davanti non possono essere affrontate da un solo soggetto, né possono essere delegate esclusivamente alla dimensione tecnica. Richiedono una visione politica, una responsabilità condivisa e una collaborazione strutturale tra pubblico e privato.

Allo stesso tempo, il quadro normativo europeo e nazionale ci richiama a una responsabilità crescente: costruire modelli di governance della sicurezza sempre più maturi, capaci di accompagnare l'innovazione tecnologica senza rinunciare alla protezione dei dati, dei servizi e delle infrastrutture strategiche. Innovare è necessario, ma innovare senza sicurezza significa esporre cittadini, imprese e istituzioni a nuove fragilità.

Questo Rapporto contribuisce in modo concreto a tale percorso. Non fotografa soltanto i principali fenomeni osservati, ma aiuta a leggere le tendenze evolutive della minaccia cyber, a comprendere dove si concentrano i rischi e a sviluppare una maggiore capacità di orientamento per chi ha responsabilità pubbliche, economiche e sociali. È uno strumento politico prima ancora che tecnico, perché vincere la sfida della sicurezza digitale richiede visione, coordinamento e la volontà di non lasciare indietro nessuno.

La sicurezza digitale è una sfida collettiva e, sempre di più, una questione di interesse nazionale. La capacità dell'Italia di affrontarla dipenderà dalla qualità della cooperazione tra istituzioni, imprese, comunità scientifica e cittadini. È su questa consapevolezza che dobbiamo continuare a lavorare insieme: perché proteggere lo spazio digitale significa proteggere la vita reale delle persone, la fiducia nelle istituzioni e il futuro del Paese.

Marco Gabriele Proietti

Presidente Cyber Security Foundation

Un progetto come questo nasce sempre da una responsabilità condivisa. La seconda edizione del Rapporto di Cyber Security porta con sé il valore di un percorso a più voci: istituzioni, esperti, partner e professionisti hanno intrecciato analisi, esperienze, dati e sensibilità diverse per restituire una lettura più chiara di una minaccia che cambia continuamente forma, intensità e capacità di impatto.

È il risultato di mesi di lavoro e del contributo di persone che hanno scelto di offrire il proprio sapere perché credono che la conoscenza, quando diventa patrimonio comune, sia già una prima forma di difesa collettiva.

Non si tratta soltanto di numeri, scenari o indicatori. Dietro ogni evidenza raccolta si riflette un pezzo della trasformazione che stiamo vivendo: il modo in cui proteggiamo le infrastrutture, custodiamo i dati, accompagniamo l'innovazione, rendiamo più sicuri i servizi e rafforziamo la fiducia nello spazio digitale.

Viviamo in un momento in cui la sicurezza digitale è entrata a pieno titolo nell'agenda della sicurezza globale. Gli attacchi informatici non sono più episodi isolati: sono strumenti di pressione geopolitica, leve di destabilizzazione economica, vettori di interferenza sui processi democratici. Ignorare questa dimensione significherebbe restituire un'analisi incompleta proprio nel momento in cui il Paese ha bisogno di strumenti più solidi per comprendere, prevenire e reagire.

È da questa consapevolezza che nasce il nostro impegno. Come Cyber Security Foundation, crediamo che la cybersecurity debba diventare sempre più una cultura diffusa: comprensibile senza essere banalizzata, rigorosa senza restare chiusa agli addetti ai lavori, capace di parlare alle istituzioni, alle imprese, alla pubblica amministrazione, alla ricerca e ai cittadini.

Il Cyber Security Report è proprio questo: uno strumento analitico, strutturato e accessibile per orientarsi tra i principali trend della minaccia cyber e le trasformazioni tecnologiche in corso. Una base di conoscenza utile non solo a descrivere ciò che accade, ma ad accrescere la capacità di prevenire, decidere e cooperare.

L'obiettivo a cui tendiamo non è soltanto documentare il presente, ma contribuire a costruire un'Italia digitalmente più sicura, più consapevole e più competitiva. Un Paese in cui la sicurezza non sia percepita come un vincolo all'innovazione, ma come la condizione che la rende possibile, credibile e sostenibile nel tempo.

La Fondazione continuerà a promuovere occasioni di studio, formazione, sensibilizzazione e dialogo tra tutti gli attori coinvolti, nella convinzione che la sicurezza digitale non si costruisca mai da soli. Richiede metodo, continuità, alleanze, responsabilità e una visione comune del futuro.

A tutti coloro che hanno reso possibile questa iniziativa, e a quanti ogni giorno lavorano per la sicurezza del nostro ecosistema digitale, va il nostro ringraziamento più sincero. Il loro contributo ci ricorda che proteggere lo spazio digitale significa rafforzare la resilienza del Paese e custodire quella fiducia senza la quale nessuna comunità moderna può davvero crescere.

Pietro Labriola

Amministratore Delegato TIM

TIM partecipa anche quest'anno alla realizzazione del Rapporto Cyber Security perché nessun soggetto può affrontare da solo la complessità della minaccia cyber. Servono collaborazione, condivisione delle informazioni e cooperazione operativa tra operatori infrastrutturali, istituzioni, ricerca e industria. Il Rapporto va esattamente in questa direzione: mette a sistema dati, esperienze e competenze diverse per offrire una lettura qualificata dei rischi e rafforzare la consapevolezza collettiva.

In questo lavoro TIM mette a disposizione un patrimonio distintivo: le proprie capacità di osservazione, analisi e monitoraggio delle minacce maturate ogni giorno sulle reti e nei sistemi digitali. Quello di TIM è un punto di osservazione fondamentale, perché consente di leggere l'evoluzione degli attacchi nel momento in cui si manifestano, individuare vulnerabilità emergenti e comprendere fenomeni che interessano imprese, Pubbliche Amministrazioni e cittadini.

Questa capacità è sempre più rilevante perché la minaccia cyber non resta confinata al perimetro tecnico da cui nasce. Un attacco può partire da un singolo dispositivo vulnerabile, propagarsi a una rete aziendale, bloccare servizi essenziali, compromettere dati sensibili e generare impatti economici, reputazionali e operativi rilevanti. È in questa escalation che la sicurezza digitale mostra tutta la sua centralità: non protegge solo sistemi e infrastrutture, ma la continuità dei servizi, la fiducia nei processi digitali e la capacità dell'Italia di crescere su basi solide.

La cybersicurezza è quindi la dimensione evoluta della sicurezza nell'economia digitale: protegge reti, dati, piattaforme, identità, servizi e processi che oggi rendono possibile il funzionamento di imprese, Pubbliche Amministrazioni e infrastrutture critiche. È un fattore abilitante dell'innovazione, dell'intelligenza artificiale, del cloud, dei servizi connessi e della continuità operativa. Senza cybersicurezza non può esserci pieno sviluppo digitale.

Per questo la sicurezza digitale è sempre più legata alla sovranità digitale. Rafforzare capacità nazionali di monitoraggio, prevenzione, risposta e protezione significa proteggere infrastrutture critiche, dati sensibili e servizi essenziali, riducendo dipendenze e aumentando l'autonomia strategica dell'Italia.

Da questa visione industriale nasce la strategia di TIM: accompagnare la trasformazione digitale dell'Italia con infrastrutture affidabili, servizi cloud sicuri, soluzioni di cybersecurity avanzata e competenze industriali italiane. Attraverso TIM Enterprise e Telsy, azienda del Gruppo dedicata alla cybersicurezza, TIM contribuisce a costruire un ecosistema digitale più sicuro, sostenibile e vicino ai bisogni reali di imprese e istituzioni.

TIM continuerà a investire nella cybersecurity e a sostenere iniziative che favoriscano la crescita di un ecosistema italiano della sicurezza digitale forte, innovativo e competitivo. Perché la resilienza cibernetica è oggi una componente essenziale della sicurezza, della sovranità e della crescita dell'Italia.

INDICE

Executive Summary

Nel 2025, con l'ampliarsi della digitalizzazione, il crescente uso dell'Intelligenza Artificiale e le evoluzioni del quadro geopolitico, aumentano le situazioni di rischio per cittadini, imprese ed istituzioni. Per questo diventa sempre più importante leggere il contesto in cui si opera, collegare i dati sulle minacce ai punti di vulnerabilità sistemici, anticipare i segnali di future tendenze.

Il **Cyber Security Report – Analisi delle minacce ed evoluzione dello scenario (anno 2025)** nasce proprio con l'intento di offrire delle chiavi di lettura accessibili sulla trasformazione del rischio cyber, combinando osservazione operativa, analisi di scenario e inquadramento regolatorio.

Il Rapporto, realizzato da **TIM** con la **Cyber Security Foundation** e il contributo del **Centro Studi TIM**, si basa sulle evidenze raccolte dai presìdi di difesa del Gruppo TIM nel corso del 2025 e si arricchisce, in questa edizione, di approfondimenti dedicati a cura di **Insikt Group**, unità di Threat Intelligence di **Recorded Future**, per rafforzare la lettura delle tendenze e delle tecniche osservate in alcuni ambiti specifici a livello internazionale.

L'analisi è organizzata in quattro parti: (i) principali attacchi (DDoS, ransomware, campagne malware e vulnerabilità), (ii) approfondimenti settoriali, (iii) elementi normativi e (iv) tecnologie emergenti.

i) Principali attacchi

DDoS: meno eventi, più pressione.

Sul fronte degli eventi DDoS (Distributed Denial of Service), si è registrata una riduzione del volume – circa 4.300 eventi, in calo del 36% rispetto al 2024 - in parte collegata anche ad azioni intraprese per aumentare la difesa complessiva del sistema. Tuttavia, le campagne sono risultate più concentrate, in particolare a marzo, giugno ed ottobre, con un aumento della pressione complessiva rispetto al passato. Cambiano anche le modalità con le quali si manifestano gli eventi DDoS: diminuiscono i casi ad elevata intensità (dal 39% al 29% quelli oltre la soglia dei 20 Gigabit/sec), aumenta il tempo medio di esposizione del 19%, anche se continuano a prevalere gli eventi che si concludono entro i 30 minuti. In aumento alcune tecniche di attacco che possono avvalersi dell'uso di sistemi di AI per aumentare il livello di minaccia complessivo in termini di rapidità ed efficacia. Per quanto riguarda i target, escludendo gli eventi verso famiglie e cittadini (circa 7 casi su 10 rilevati dal SOC TIM), il Government arriva al 46% del totale (quasi un attacco su due), seguito da Servizi professionali, Telecomunicazioni e Trasporti (in forte crescita rispetto al 2024).

Ransomware: in forte crescita in Europa e nel mondo, meno in Italia.

Nel 2025 sono stati registrate oltre 7.400 rivendicazioni di attacchi ransomware a livello globale

(+42% vs 2024), un'accelerazione che si inquadra nel più ampio processo di industrializzazione del cybercrime (in aumento del 40% il numero dei gruppi ransomware censiti), in cui l'impiego di tecniche di intelligenza artificiale automatizza la produzione di codice malevolo e migliora l'efficacia delle tecniche di adescamento. Quasi un evento su due riguarda gli USA, mentre l'UE è la seconda area più colpita con il 16% dei casi, seguita da Canada (5%) e Regno Unito (3%). Il fenomeno è in aumento anche in Italia (166 casi, +14% rispetto al 2024). Gli incrementi più marcati registrati in altri contesti ridisegnano la classifica dei Paesi europei più colpiti: la Germania supera il Regno Unito, mentre l'Italia scende al quarto posto. Circa 4 casi su 10 rilevati in Italia si concentrano nel Nord-Ovest (in Lombardia oltre il 30% dei casi), mentre la Manifattura e i Servizi professionali sono i settori più bersagliati, evidenziando che la maggiore densità industriale e la capacità di esercitare pressione, mettendo a rischio la continuità operativa, sono dei chiari fattori di esposizione a questa minaccia.

Campagne Malware: colpiti soggetti in circa 200 Paesi. Italia al sesto posto in Europa.

Secondo le evidenze raccolte da Insikt Group, nella prima metà del 2025, si è verificata un'intensa attività legata a campagne malware che hanno interessato oltre 200 Paesi. Quasi il 90% dei casi ha riguardato gli USA, mentre il Paese più colpito in Europa – UE ed extra-UE – è stato il Regno Unito. La diffusione del phishing in inglese contribuisce a spiegare la maggiore esposizione dei mercati dove questa lingua è più usata online. Tra le tipologie di minacce più diffuse, si evidenzia la crescita dei RAT (Remote Access Threats) sistemi che abilitano il controllo remoto e permettono azioni di esfiltrazione dati o attacchi più complessi. Aumentano le minacce ai dispositivi mobili (in particolare Android) che si indirizzano sempre più frequentemente verso sistemi di pagamento contactless (NFC).

Vulnerabilità e zero-day: la difesa corre, l'attacco accelera.

Una vulnerabilità è una falla in un software o in un dispositivo che può essere sfruttata per compromettere un sistema. Per ridurre il rischio, quando una vulnerabilità diventa nota è decisivo intervenire in tempi rapidi con patch e aggiornamenti. Nel 2025, il numero delle vulnerabilità note CVE (Common Vulnerabilities and Exposures) ha quasi raggiunto le 48.500 unità pubblicate (+20% rispetto al 2024, quasi il doppio rispetto a tre anni fa). In questa dinamica pesa anche l'uso crescente di strumenti di AI che accelerano l'individuazione delle falle (sia per correzione, sia per sfruttamento). Secondo i dati di Insikt Group, oltre il 50% delle attività di sfruttamento attribuite è state sponsored, segnale della crescente "strategicità" della dimensione offensiva e della capacità di trasformare rapidamente una vulnerabilità in strumento operativo ("weaponization").

Il Rapporto dedica un focus agli zero-day: falle non ancora conosciute dai produttori e quindi senza patch, che espongono sistemi e dispositivi a rischi immediati. In parallelo alla crescita delle CVE, non si osserva un aumento equivalente delle vulnerabilità di massima severità (CVSS ≥

9.8, in una scala 0-10) divulgate pubblicamente. Una parte di queste resta infatti fuori dai canali ordinari di "disclosure" perché può acquisire un valore di mercato elevato. Gli zero-day non interessano solo il cybercrime "da profitto": possono essere acquisiti e impiegati anche da governi, agenzie di intelligence e aziende della sorveglianza per attività di spionaggio, monitoraggio mirato o operazioni cibernetiche di natura strategica.

ii) Approfondimenti settoriali

Nella seconda parte il Rapporto sposta il punto di osservazione: dal livello operativo alla lettura del rischio. In una società sempre più dipendente dal digitale, un incidente non resta confinato al bersaglio: blocchi dell'attività, interruzioni di servizi, perdita di dati e danni reputazionali possono propagarsi rapidamente lungo servizi essenziali e filiere, generando effetti a catena su clienti, fornitori e controparti. Non a caso, **la minaccia cyber** ha mantenuto una presenza stabile dal 2012 ad oggi, tra i 10 fattori di preoccupazione più avvertiti a medio termine, nella classifica dei rischi globali del World Economic Forum, con la sola eccezione del 2016, caratterizzandosi come una presenza **persistente** nello scenario e di carattere **prioritario** nell'ottica delle imprese, in particolare europee. Allo stesso tempo, la dinamica degli attacchi – soprattutto nel ransomware – resta in larga misura **opportunistica**: non segue "direttrici" stabili, cambia spesso forma e obiettivi e diventa più efficace proprio quando le conseguenze aumentano la pressione, amplificandosi nei contesti economici e sociali.

Analisi condotte sull'ultimo triennio, combinando i dati di settori ed attaccanti mostrano che esiste un livello di specializzazione estremamente basso, sia a livello globale, sia nazionale. In particolare, per quanto riguarda l'Italia, dal punto di vista degli attaccanti emerge un quadro prevalentemente "generalista": solo 4 gruppi attivi nel nostro Paese mostrano una certa preferenza settoriale, mentre alcuni soggetti – in particolare LockBit, Rhysida, Hunters International e RansomHub – colpiscono indistintamente laddove emerga l'occasione. Anche guardando ai settori, l'evidenza è di bassa polarizzazione indicando che nella maggior parte dei comparti la pressione ransomware è distribuita fra più gruppi, senza una dominanza netta.

iii) Elementi normativi

Nella terza parte il Rapporto inquadra l'evoluzione normativa come risposta a un dato di fondo: quando gli effetti di un incidente si propagano lungo servizi e filiere, la cybersicurezza smette di essere un tema individuale e diventa un problema di tenuta del sistema. Proprio per questo non può essere governato solo con "più tecnologia" o con misure episodiche. Serve una cornice comune fatta di regole, processi e responsabilità, capace di rendere omogenea la capacità di prevenzione e risposta nei settori più esposti. Il **quadro normativo europeo** rappresenta il punto di riferimento per Paesi e operatori, ma occorre trovare il giusto equilibrio per permettere di governare il rischio Cyber Security in modo più efficiente.

Oggi, il baricentro europeo punta ad un sistema organizzato in cui la resilienza viene perseguita attraverso obblighi e processi per le organizzazioni che operano negli snodi più critici delle nostre società (NIS2, DORA), requisiti minimi per prodotti e componenti (CRA), e **gestione delle dipendenze di filiera.** Quest'ultimo aspetto, di grande rilievo attuale, è affrontato dalla Commissione europea attraverso proposte normative (CSA2 e – in via di pubblicazione - CAIDA) che trattano il tema delle dipendenze tecnologiche e dei vincoli giurisdizionali (in particolare relativi a cloud, dati e AI), fattori che possono interferire con la sovranità e l'autonomia strategica europea. In questo quadro, le agenzie di Cyber Security non svolgono soltanto una funzione di controllo, ma rappresentano un elemento essenziale della capacità europea di prevenire, coordinare e gestire il rischio cyber in modo sistemico.

iv) Tecnologie emergenti

Nella quarta ed ultima parte, il Rapporto sposta l'obiettivo dal 2025 al presente ed al futuro, con l'idea di fornire alcuni spunti su quanto sta avvenendo in termini di nuove minacce, nuove tecnologie e nuovi fronti di rischio. Il **principale catalizzatore di questo periodo è rappresentato dall'AI** che agisce da moltiplicatore accelerando alcune dinamiche offensive (phishing, frodi, abuso di servizi cloud/LLM, prompt injection e manipolazioni), ma anche come un valido supporto alla difesa (triage, SOC, analisi vulnerabilità).

Emergono nuove minacce che richiedono nuove denominazioni: **Promptware, Quishing, QRishing.** Si aprono nuove prospettive critiche nell'intersezione tra la dimensione fisica e quella digitale, laddove le minacce si spostano su nuovi dispositivi come **smart glasses** e sistemi di **realtà virtuale/avanzata** (VR/AR).

Un altro fronte di attenzione è rappresentato dalla discontinuità portata dalle tecnologie quantistiche: la grande capacità computazionale potrà mettere in crisi gli attuali sistemi di sicurezza crittografica. Questa discontinuità chiede soluzioni nuove, anch'esse basate sullo stesso sviluppo. Un esempio è quello delle **chiavi crittografiche quantum-safe**. Se questo sviluppo appare lontano, il rischio è già presente oggi, dal momento che alcuni attori ostili possono intercettare e conservare dati cifrati oggi, per decifrarli in futuro contando sugli sviluppi quantistici. Questa prospettiva, definita come "harvest now, decrypt later" richiede già oggi di mettere in campo delle soluzioni di protezione. Infine, la superficie di attacco potenziale si estende allo spazio, includendo nel perimetro le reti satellitari.

Man mano che lo **spazio** si consolida come infrastruttura abilitante per servizi critici, la sicurezza non può essere trattata come protezione puntuale del singolo satellite o della singola missione: diventa un tema di governance e resilienza che richiede una responsabilizzazione degli attori che operano in questo segmento.

Il punto di vista delle istituzioni

Servizio Polizia Postale e per la Sicurezza Cibernetica

Ivano Gabrielli
Direttore

Protezione del cittadino nell'era della manipolazione digitale

Negli ultimi due decenni la società ha subito una profonda trasformazione. La nascita delle nuove tecnologie, l'avvento dei social network e, in ultimo, l'affermarsi dei sistemi di intelligenza artificiale hanno modificato profondamente le nostre abitudini: è cambiato il nostro modo di concepire il lavoro, i rapporti umani, il nostro stile di vita, il nostro modo di informarci e, di conseguenza, anche il modo di percepire il mondo che ci circonda.

Se in passato, parlando di "cybersicurezza", si faceva quasi esclusivamente riferimento alla protezione di reti, server o infrastrutture informatiche, oggi "vittima privilegiata" della criminalità informatica è in primo luogo la persona: la sua identità, la riservatezza dei suoi dati personali e sensibili, la sua reputazione, le sue relazioni affettive ed economiche.

Il panorama della minaccia è quindi radicalmente cambiato: un audio apparentemente autentico, una videochiamata manipolata o un'identità social artificiale possono generare, in pochi minuti, danni personali, economici e reputazionali enormi. Ma la minaccia non si ferma a questo. Ad essere a rischio sono anche le nostre stesse capacità percettive: oggi è infatti molto facile creare contenuti falsi ma estremamente realistici, capaci di influenzare le opinioni, generare allarme sociale, persino orientare le scelte politiche di un Paese. La manipolazione dell'informazione è, quindi, uno dei rischi più rilevanti per la sicurezza digitale.

Come evidenziato, la risposta a questo tipo di minaccia deve fondarsi su **tre pilastri** fondamentali: prevenzione, educazione e cooperazione.

La **prevenzione** dovrà diventare sempre più proattiva, investendo in tecnologie avanzate, capaci di individuare tempestivamente le campagne fraudolente e i contenuti manipolati con l'intelligenza artificiale. In molti casi, infatti, il fattore tempo diventa decisivo per limitare il danno: molte frodi si consumano in tempi estremamente rapidi e la velocità dell'intervento è determinante per un positivo esito.

Alla prevenzione deve essere affiancata la **formazione**: le forze di polizia dovranno acquisire competenze specialistiche sempre più elevate. È necessario produrre uno sforzo per l'acquisizione e la formazione delle migliori competenze, una nuova generazione di esperti in sicurezza cibernetica che possano, una volta formati, essere

utili sin da subito all'esercizio di compiti istituzionali, per poi eventualmente esprimersi al di fuori delle istituzioni, concorrendo al presidio delle strutture informatiche del Paese, realizzando un efficiente sicurezza cibernetica partecipata.

Proprio in questa direzione va letta la recente assunzione di 200 ispettori cibernetici della Polizia di Stato, figura di nuova introduzione, che ultimeranno il corso di formazione nelle prossime settimane e che saranno impiegati all'interno degli Uffici territoriali della Polizia Postale, andando ad arricchire le fila degli operatori specializzati, impegnati nel contrasto dei crimini informatici.

Un secondo pilastro su cui investire è la **consapevolezza**. La cybersicurezza non può più essere considerata materia per soli esperti: deve diventare una competenza di cittadinanza, essa stessa "detentrice" di una parte del perimetro di sicurezza del Paese.

In questo contesto, non solo la scuola ma anche le famiglie, le istituzioni e i mezzi di informazione hanno un ruolo fondamentale nella diffusione di una cultura della sicurezza digitale.

In tal senso, da molti anni la Polizia Postale è impegnata con numerose campagne di informazione e sensibilizzazione dei cittadini sui rischi della rete, che coinvolgono tutte le fasce d'età, soprattutto quelle più vulnerabili, ossia minori ed anziani.

La terza dimensione strategica sarà la **collaborazione** tra istituzioni pubbliche, piattaforme digitali e operatori privati. È solo infatti attraverso la collaborazione, tra i diversi attori pubblici e privati coinvolti, che può realizzarsi una risposta adeguata alla minaccia. Sarà necessario rafforzare protocolli di cooperazione per la rimozione rapida di contenuti fraudolenti, il tracciamento delle attività criminali e la condivisione tempestiva delle informazioni di rischio.

Le grandi piattaforme social e i provider tecnologici dovranno assumere un ruolo sempre più responsabile nella verifica delle identità, nel contrasto alla diffusione di deepfake malevoli e nella tutela degli utenti vulnerabili.

In definitiva, la cybersicurezza è destinata a divenire una problematica non solo tecnica ma anche sociale, culturale e quindi democratica. La capacità di distinguere il vero dal falso, di proteggere la propria identità digitale e di fidarsi in modo consapevole degli strumenti tecnologici diventerà un elemento essenziale della convivenza civile.

Una delle *mission* della Polizia Postale è proprio quella di accompagnare questa trasformazione: contribuire a costruire un ecosistema di sicurezza partecipato, in cui cittadini, istituzioni e imprese collaborino per difendere uno spazio digitale che sia realmente sicuro, affidabile e umano.

Industrializzazione del cybercrime e AI criminale

Guardando ai dati operativi, nel raffronto tra 2024 e 2025, si registra **un innalzamento della minaccia**, in termini soprattutto qualitativi, più

che quantitativi. Assistiamo in molti casi, infatti, a una vera e propria selezione degli obiettivi ad alto valore strategico. Questa "chirurgia criminale" si manifesta in attacchi estremamente persistenti (APT) e studiati sulle specifiche vulnerabilità della vittima, spesso preceduti da lunghe fasi di ricognizione silente.

In relazione alle tecniche di attacco, dall'osservazione dei dati del **primo quadrimestre 2026**, le segnalazioni indicano le tecniche di **social engineering** come il principale vettore, seguono per frequenza gli attacchi di tipo **ransomware**, che mirano alla cifratura dei dati a scopo di estorsione, e gli episodi di accesso abusivo ai sistemi informatici.

Fatta questa premessa, va detto che l'**intelligenza artificiale** ha certamente portato a una **trasformazione strutturale del cybercrime**: da fenomeno spesso frammentato, individuale, si è **evoluto in un ecosistema industriale** altamente specializzato e globalizzato. Oggi molte organizzazioni criminali operano con logiche simili a quelle delle imprese tecnologiche: divisione del lavoro, outsourcing, servizi in abbonamento, customer support criminale, affiliazioni e monetizzazione dei dati.

La diffusione di attacchi su larga scala è rilevante, anche grazie alla disponibilità di modelli ***'crime as a service'*** che rendono facili da utilizzare strumenti complessi. Questo amplia la superficie d'attacco, specialmente per le infrastrutture medio-piccole, che si trovano ora vulnerabili a ransomware e altre minacce capaci di paralizzare le loro attività. Stiamo assistendo, inoltre, a un incremento nell'uso dei deepfake, usati non solo per disinformazione, ma anche per inganni più mirati come la simulazione vocale nelle frodi informatiche.

In tal senso, i sistemi di **IA generativa** rappresentano un'**arma a doppio taglio** nel panorama della sicurezza cibernetica. Anche se non sono stati progettati per rispondere a richieste dirette di supporto a crimini informatici, un utilizzo indiretto, o realizzato attraverso un dialogo più complesso potrebbe comunque far emergere **risposte utili per chi ha intenti malevoli**.

È pur vero, d'altro canto, che i Large Language Models (LLM) possono essere impiegati per potenziare le difese: è possibile, infatti, addestrare sistemi di sicurezza informatica usando come base i risultati e le ricerche condotte tramite questi modelli. In questo senso, l'impiego dell'IA generativa, o meglio ancora **agentica,** per migliorare le difese rappresenta una risorsa concreta per **anticipare le strategie di attacco e rendere i sistemi più resilienti**.

Servizio Operazioni e Gestione delle Crisi Cyber dell'ACN

Gianluca Galasso

Direttore

Nel corso dell'ultimo anno, il dominio della cybersicurezza ha mostrato con crescente evidenza i tratti di una minaccia strutturale, persistente e in continua evoluzione, caratterizzata da livelli sempre più elevati di sofisticazione e da una pressione costante sugli ecosistemi digitali. Per tale ragione si tratta di una dimensione strutturale della sicurezza del sistema Paese, che incide direttamente sulla continuità dei servizi essenziali, sulla competitività delle imprese, sulla sicurezza delle filiere produttive e sulla fiducia dei cittadini nelle istituzioni.

Il Rapporto Cyber Security 2026 offre, pertanto, uno strumento utile non solo per descrivere le principali fenomenologie osservate nel corso del 2025, ma anche per interpretarne il significato strategico. Dalla sua lettura emerge nettamente come il rischio cyber sia un fenomeno sistemico in grado di produrre impatti concreti sull'intero sistema.

In questo scenario l'intelligenza artificiale introduce una discontinuità di particolare rilievo, un vero e proprio cambiamento strutturale. L'AI non si limita più ad assistere gli analisti: può individuare catene di vulnerabilità complesse, ragionare sulle cause tecniche, costruire Proof of Concept (PoC) e proporre remediation. Questo riduce drasticamente il tempo tra scoperta di una vulnerabilità e disponibilità di un exploit funzionante. I nuovi modelli AI di frontiera hanno la capacità di trasformare catene di vulnerabilità complesse, che concatenano CVE a basso score, in exploit di alto profilo che superano le mitigazioni moderne e arrivano spesso a consentire l'accesso remoto con privilegi elevati ai sistemi attaccati. Questo abbassa la barriera tecnica dell'attacco e riduce la distanza tra gli attori avanzati e persistenti (APT) e gli operatori meno sofisticati e dotati di risorse, in termini di know-how e capacità tecnica, inferiori. Tutto ciò avrà verosimilmente un impatto sull'attuale sistema di tracciamento, condivisione e gestione delle vulnerabilità, ovvero il sistema delle CVE, il quale potrebbe collassare. Tale sistema, infatti, è stato progettato in un'epoca in cui le vulnerabilità pubblicate annualmente erano nell'ordine delle centinaia; si è passati dalle 321 CVE pubblicate nel 1999 alle quasi 29.000 del 2023 sino a giungere alle oltre 48.000 del 2025, con una previsione di superare le 150.000 nel 2030. Tale evoluzione modifica alcune assunzioni tradizionali della sicurezza informatica. Per lungo tempo, tra la scoperta di una vulnerabilità, la sua divulgazione, la disponibilità di una patch e l'effettivo sfruttamento da parte di un attaccante esisteva una finestra temporale che con-

sentiva alle organizzazioni di pianificare, testare e intervenire. Oggi quella finestra si riduce sensibilmente. La scoperta delle vulnerabilità diventa più industrializzata; la loro verifica può generare volumi crescenti di informazioni da analizzare; il rilascio di una patch può trasformarsi sempre più rapidamente anche in uno strumento utile per chi intende costruire rapidamente un exploit n-day. Ne deriva che il problema non è soltanto il proliferare delle vulnerabilità, in particolare critiche, ma la velocità con cui le stesse devono essere gestite all'interno delle organizzazioni necessitando processi di selezione più efficienti, la loro prioritizzazione e validazione più rapida ed accurata, funzionali a ridurre il rischio in tempi compatibili con la nuova velocità della minaccia.

Il problema non è solo quantitativo. Ogni CVE genera triage, scoring, mapping sugli asset, verifica di esposizione, decisione di patch, test di regressione, finestra di deployment e reportistica. In aggregato, questa diventa una tassa sulla vulnerabilità che consuma la capacità dei difensori prima ancora che venga applicata la remediation. Nell'era dell'AI, gestire ogni vulnerabilità come un caso isolato non sarà più sostenibile, aprire un ticket separato per ogni singolo bug può solo rallentare la difesa invece di migliorarla. Per tale ragione sarà indispensabile in un futuro molto prossimo ragionare per classi di vulnerabilità.

In tale contesto, i fondamentali della sicurezza non perdono valore: al contrario, diventano ancora più importanti. Inventario degli asset e delle interdipendenze spinto fino alle primitive di sistema richiamate dalle applicazioni utilizzate con particolare attenzione a quelle custom, conoscenza delle superfici esposte, gestione delle identità e dei privilegi, segmentazione, logging, monitoraggio, backup, aggiornamento dei sistemi, controllo delle configurazioni, sicurezza della supply chain e capacità di risposta agli incidenti restano elementi essenziali. La differenza è che devono funzionare in modo più integrato, continuo e misurabile. Quando i segnali sono frammentati tra strumenti diversi, quando i dati non vengono correlati, quando le procedure autorizzative sono troppo lente o quando il debito tecnologico limita la capacità di intervento, l'organizzazione perde il vantaggio temporale necessario per contenere l'attacco. In un ambiente caratterizzato da minacce a velocità macchina, la resilienza dipende dalla capacità di trasformare tempestivamente i dati in decisioni e le decisioni in azioni.

Per tale ragione, le priorità devono orientarsi verso capacità operative più robuste e interoperabili. Servono threat intelligence, detection ed early warning in grado di leggere tempestivamente segnali tecnici e segnali di contesto; servono processi di vulnerability management e patch management capaci di distinguere ciò che è realmente prioritario da ciò che è solo numericamente rilevante; servono capacità di incident management e crisis management in grado di sostenere scenari multi-incidente e picchi improvvisi di segnalazioni. Occorre ridurre il debito tecnologico, presidiare i sistemi legacy e quelli non più adeguatamente supportati, rafforzare la segmentazione, estendere i controlli sugli ambienti cloud e on-premise. L'automazione è indispensabile, ma deve essere governata: deve accelerare triage, correlazione e risposta, mantenendo controllo umano e responsabilità

nei passaggi decisionali più rilevanti.

Questo scenario impone una riflessione profonda sul significato stesso della sicurezza. Non si tratta di perseguire l'obiettivo, spesso illusorio, dell'impenetrabilità dei sistemi, quanto piuttosto di garantire la protezione dei dati e la continuità operativa delle organizzazioni. È in questa prospettiva che assume centralità un approccio integrato, fondato sulla capacità di coordinamento, sulla gestione del rischio e sullo sviluppo di adeguati piani di resilienza e di gestione delle crisi, accompagnati da solide capacità di rilevamento e risposta e da un elevato livello di prontezza operativa.

L'evoluzione del quadro normativo europeo si inserisce pienamente in questo contesto, configurandosi non come un mero rafforzamento degli obblighi, ma come una risposta necessaria alla vulnerabilità degli ecosistemi digitali. In particolare, la Direttiva NIS2 introduce un cambiamento sostanziale, spostando l'attenzione dall'adempimento tecnico alla responsabilità diretta del management e degli organi di vertice. Ne deriva una ridefinizione del ruolo della cybersicurezza, che viene progressivamente integrata nei processi di governance e nella gestione complessiva del rischio d'impresa, diventando elemento strutturale delle decisioni strategiche.

In questo percorso, la cybersicurezza assume sempre più una dimensione culturale. Essa non è più percepita esclusivamente come ambito tecnico o vincolo regolatorio, ma come componente essenziale della resilienza organizzativa e della capacità di operare in contesti complessi e dinamici. Questo cambiamento implica anche una revisione dei modelli di valutazione e implementazione delle misure di sicurezza, che devono essere sempre più orientati all'efficacia piuttosto che alla mera conformità.

Al centro di questa trasformazione si colloca il ruolo del management, chiamato a sviluppare una piena consapevolezza dei rischi cyber e a integrarli nei processi decisionali. Ciò implica la capacità di comprendere gli impatti potenziali, di valutare le priorità di intervento e, soprattutto, di accettare in modo informato il rischio residuo, superando l'idea di una sicurezza assoluta.

In definitiva, il passaggio dalla compliance ad un risk management e ad una readiness operativa efficace rappresenta un'evoluzione necessaria e irreversibile. Non si tratta soltanto di implementare controlli, ma di sviluppare capacità: capacità di prevenire, di rilevare, di rispondere e di adattarsi. In altri termini, si deve passare dal concetto "ho implementato queste misure di sicurezza e quindi sono sicuro che non mi accadrà nulla" al concetto "ho sviluppato e mantengo costantemente queste capacità di protezione e resilienza, quindi, sono in grado di affrontare la minaccia".

Questo cambiamento culturale farà davvero la differenza tra le organizzazioni che saranno pronte ad affrontare i rischi e a raccogliere i benefici della rapidissima evoluzione tecnologica e quelle che si troveranno a rincorrere affannosamente.

Cyber Crimes Center (C3), Dipartimento della Sicurezza Nazionale degli Stati Uniti (DHS)

Kimberly Long

Vicedirettore e Division Chief

A nome del Cyber Crimes Center (C3) del Dipartimento della Sicurezza Interna degli Stati Uniti (Department of Homeland Security), è un onore contribuire al rapporto annuale sulla Cyber Security della Fondazione Italiana per la Cybersicurezza. Questa pubblicazione segue un importante traguardo raggiunto nella nostra partnership.

Il rapporto di quest'anno affronta due questioni critiche che stanno plasmando il futuro della cybersicurezza:

Cyber Security e geopolitica

Il contesto internazionale dimostra sempre di più una continuità tra competizione geopolitica, pressioni sulle catene di approvvigionamento, attività cyber ostili e rischio di interruzione delle infrastrutture civili. La cooperazione tra alleati deve evolversi oltre il semplice scambio di informazioni. Dobbiamo perseguire una reale postura condivisa di preparazione, resilienza e risposta coordinata. Ciò significa sviluppare quadri comuni per la valutazione dei rischi, armonizzare i protocolli operativi e investire in formazione ed esercitazioni condivise che rafforzino fiducia e interoperabilità. Solo attraverso approcci così integrati possiamo contrastare efficacemente minacce che superano confini e settori.

La firma e l'estensione del memorandum d'intesa tra la Cyber Security Foundation e il Cyber Crimes Center riflettono l'impegno condiviso nel rafforzare la cooperazione tra Italia e Stati Uniti nella comprensione, prevenzione e anticipazione delle minacce cyber globali.

AI, infrastrutture critiche e sicurezza nazionale

La convergenza tra intelligenza artificiale, minacce cyber e infrastrutture sempre più interconnesse rappresenta una sfida crescente per la sicurezza dei governi democratici. L'AI sta accelerando e ampliando le attività malevole – tra cui sviluppo di malware, phishing sofisticato, generazione di exploit, attività di ricognizione e inganni basati su deepfake – riducendo al contempo le barriere tecniche sia per i criminali informatici sia per gli attori statali. Allo stesso tempo, sistemi di infrastrutture critiche sempre più interconnessi aumentano il rischio che interruzioni in un settore possano generare effetti a cascata su altri.

Difendersi da queste minacce in evoluzione sta diventando sempre più complesso. La rapida innovazione tecnologica mette alla prova la capacità dei governi di armonizzare le normative,

mantenere la resilienza e garantire che anche gli enti più piccoli o con risorse limitate riescano a tenere il passo con le esigenze di cybersicurezza. La crescente dipendenza da strumenti difensivi basati sull'AI solleva inoltre preoccupazioni legate a un'eccessiva dipendenza da valutazioni generate dalle macchine e al possibile indebolimento delle competenze tecniche fondamentali tra i professionisti della cybersicurezza. Inoltre, deepfake e campagne di disinformazione generati dall'AI minacciano la fiducia pubblica, facilitano attacchi sofisticati di ingegneria sociale e indeboliscono le istituzioni democratiche e i servizi critici.

Per affrontare queste sfide, i governi democratici devono rafforzare le capacità tecniche e operative di cybersicurezza, al fine di rilevare, anticipare e contrastare meglio le minacce rivolte alle infrastrutture critiche. Ciò include il potenziamento della risposta agli incidenti, il supporto ai fornitori di servizi essenziali e il miglioramento della condivisione di informazioni in tempo reale tra settore pubblico e privato. Le pubbliche amministrazioni devono inoltre sfruttare tecnologie difensive abilitate dall'AI per il rilevamento di anomalie, la previsione delle minacce, la risposta automatizzata e l'identificazione delle vulnerabilità, mantenendo al contempo un approccio "human in the loop", cioè con supervisione umana, per garantire un adeguato controllo legale, etico e operativo. La formazione continua e il mantenimento delle competenze restano essenziali per preservare l'expertise tecnica e preparare i professionisti della Cyber Security a rispondere efficacemente a minacce sempre più sofisticate.

Come leggere il rapporto

Una struttura in 4 parti

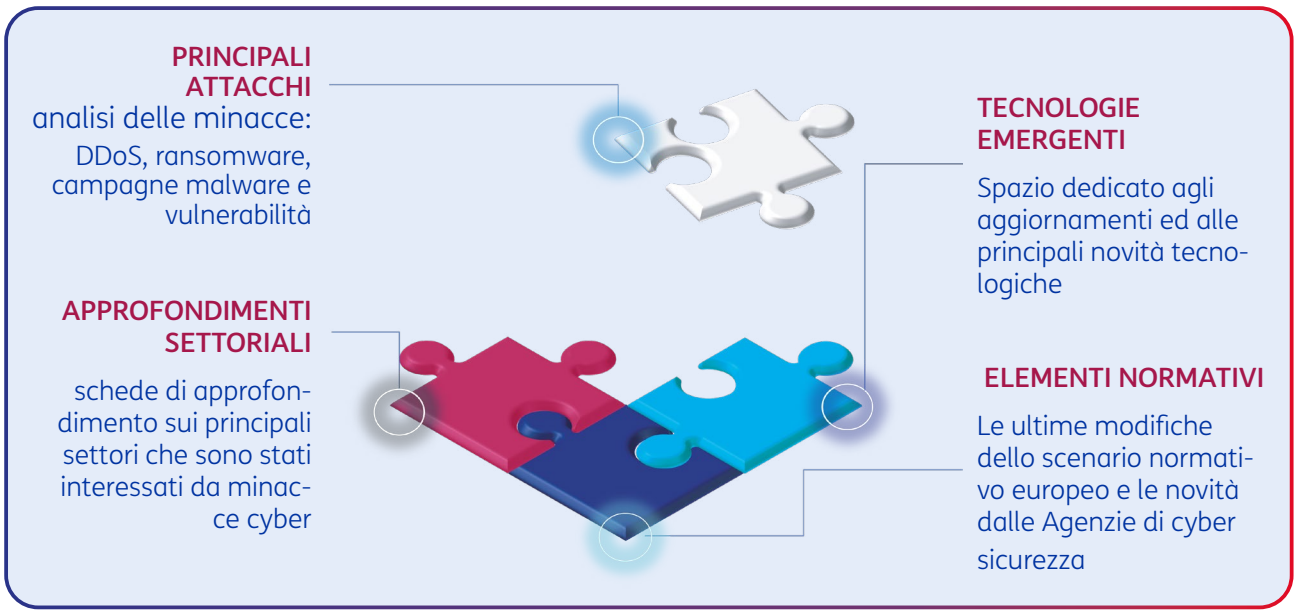
Il rapporto è organizzato su quattro principali aree di approfondimento e monitoraggio continuo:

PRINCIPALI ATTACCHI: in questa sezione vengono analizzate le principali evidenze raccolte nel corso dell'anno, basandosi sui dati provenienti in larga parte dall'attività svolta, con particolare riferimento a eventi DDoS (Distributed Denial of Service), ransomware e campagne malware. L'analisi tiene inoltre conto del tema delle vulnerabilità, sia come elemento che contribuisce ad ampliare la superficie esposta, sia come fattore abilitante nelle catene di attacco e nella diffusione di codice malevolo.

APPROFONDIMENTO SETTORIALE: la maggior parte degli attacchi informatici rilevati dai sistemi di monitoraggio del Gruppo TIM si rivolge al mondo consumer, costituito da famiglie e individui. Tuttavia, gli attacchi più dirompenti sono diretti verso il mondo delle aziende, dei settori produttivi e delle istituzioni, che rappresentano il fulcro della nostra attenzione. In questa sezione si fornisce un'analisi dei dati per ambiti di attacco, individuando i settori e gli attori istituzionali più colpiti, cercando di delineare le principali direttrici di attacco.

ELEMENTI NORMATIVI: il sistema di difesa cibernetico nazionale si basa sulle strategie e sulle normative definite a livello europeo. In questa sezione viene offerta una sintesi delle attività e delle iniziative in corso nell'Unione Europea.

TECNOLOGIE EMERGENTI: il contesto della Cyber Security è in continua evoluzione, influenzato soprattutto dalle innovazioni tecnologiche che possono rapidamente modificare le regole del settore. In questa sezione vengono aperti approfondimenti sulle novità dello scenario, sia in termini di difese sia di attacchi.



Principali attacchi

Con l'ampliarsi della digitalizzazione e la crescente adozione dell'Intelligenza Artificiale, cresce la superficie esposta alle minacce cyber e aumentano le modalità con cui queste possono essere perpetrate. Per questo, diventa sempre più importante ragionare in termini predittivi e proattivi ai fini della **resilienza**: capire cosa accade, anticipare i segnali e ridurre l'impatto quando un evento si trasforma in incidente.

È in questo quadro che si colloca la prima parte del rapporto, dedicata agli **eventi osservati nel 2025** dai presìdi di difesa del Gruppo TIM, ricordando che ogni anomalia o tentativo non si traduce automaticamente in un attacco riuscito. Nel corso dell'anno, le dinamiche risultano differenziate: sul fronte **DDoS** diminuiscono i casi registrati, ma le campagne tendono a concentrarsi e la pressione complessiva resta elevata. Il **ransomware** continua a rafforzare il proprio peso nello scenario, confermandosi una minaccia persistente e in accelerazione. Accanto a ciò, le **campagne malware** rimangono molto attive e in evoluzione, combinando tecniche consolidate e modalità operative emergenti. Cresce anche la rilevanza delle **vulnerabilità** e della rapidità con cui possono essere sfruttate, spesso come fattore abilitante lungo la catena d'attacco, anche grazie all'utilizzo dell'Intelligenza Artificiale.

In questo contesto, il lavoro di SOC (Security Operations Centers) e threat intelligence resta decisivo per interpretare correttamente i segnali, dare priorità alle evidenze più significative e contenere gli impatti.

PRIMA PARTE

Gli attacchi

Come li classifichiamo?

Avvicinarsi alla Cyber Security significa, prima di tutto, imparare a interpretare segnali ed eventi: capire se stiamo osservando un semplice indicatore, una tecnica in uso o un incidente vero e proprio. Questa lettura non è immediata perché lo stesso fenomeno può essere descritto con schemi e categorie differenti, a seconda della prospettiva adottata e dell'obiettivo dell'analisi.

Un riferimento molto diffuso è la tassonomia **MITRE ATT&CK®**, pensata per offrire una base comune di conoscenza sui comportamenti degli avversari. Il framework distingue il campo di osservazione in più domini - **Enterprise, Mobile** e **ICS** (Industrial Control System) - e organizza la descrizione degli attacchi attraverso **tattiche** (gli obiettivi), **tecniche** (le modalità operative) e, dove previsto, **sub-techniques**; l'impianto viene inoltre aggiornato nel tempo per riflettere l'evoluzione delle minacce.

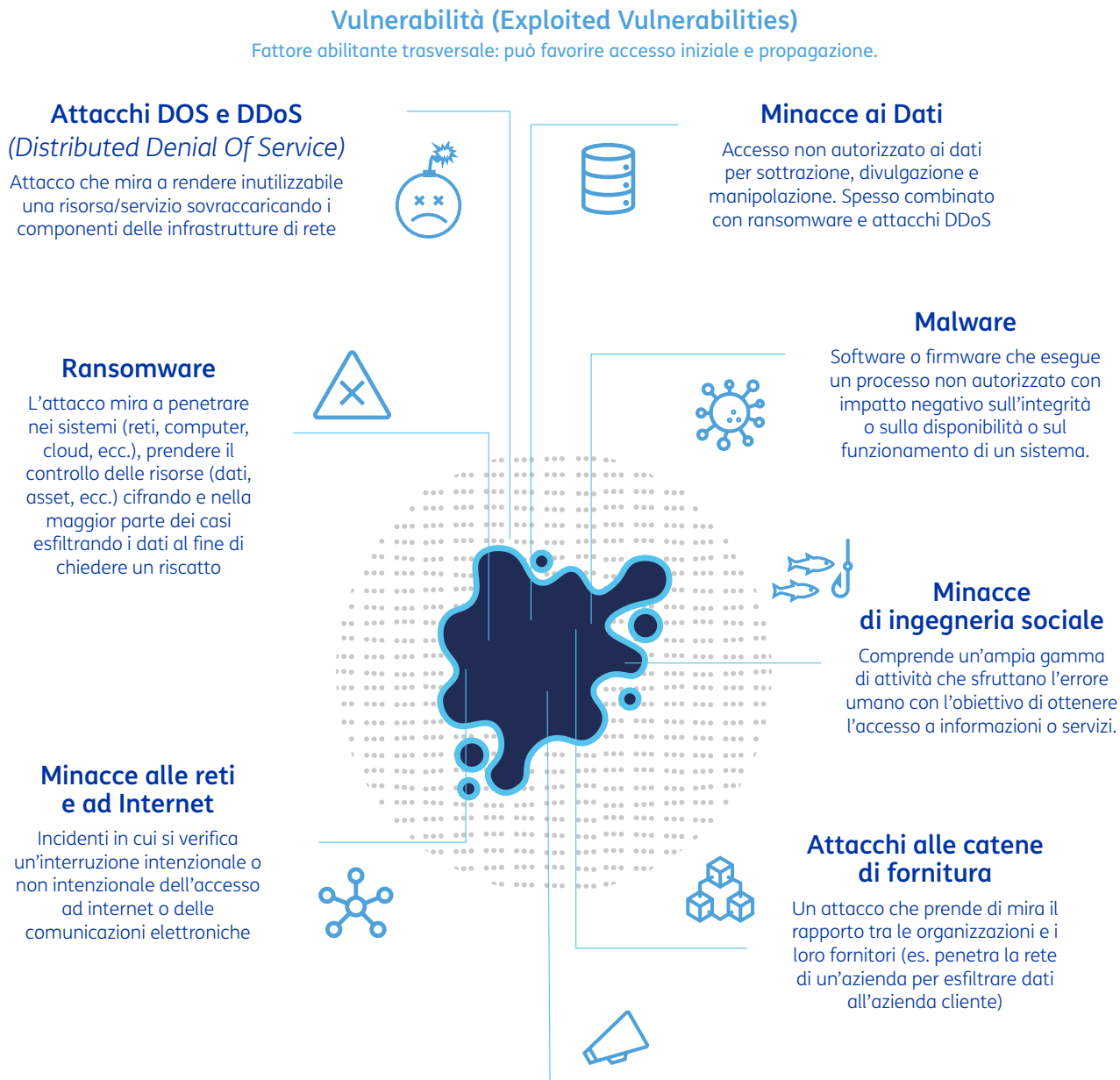
Un altro riferimento è **VERIS** (Vocabulary for Event Recording and Incident Sharing), che adotta un taglio diverso: non parte dalle tecniche, ma dalla descrizione strutturata degli incidenti. Il modello si fonda sulle "4A" - Actor, Action, Asset, Attributes - per rappresentare chi è coinvolto, cosa accade, quali risorse sono colpite e quali proprietà vengono impattate, offrendo un linguaggio coerente per classificare e confrontare eventi di sicurezza.

Questi schemi hanno un valore elevato per gli specialisti, ma possono risultare poco immediati per chi non lavora quotidianamente sul tema. Per questo, seguendo l'impostazione dello scorso anno, in questo rapporto adotteremo una chiave di lettura più accessibile, facendo riferimento alla classificazione che utilizza l'Agenzia dell'Unione Europea per la cybersicurezza (ENISA) nell'ENISA Threat Landscape (ETL), che declina lo stato e l'evoluzione delle minacce cyber, classificandole in otto principali tipologie e consentendo una lettura più diretta del fenomeno.

In particolare, ci concentreremo su due minacce più specifiche - come gli attacchi DDoS e il ransomware - e due dimensioni più trasversali, rappresentate dal malware e dalle vulnerabilità che abilitano o accompagnano diversi scenari di attacco.

Le principali minacce cyber

Nel quadro dell'**ENISA Threat Landscape**, l'ENISA individua **otto** tipologie principali di attacchi cyber, ossia eventi intenzionali volti a superare le difese di organizzazioni, imprese e cittadini con finalità diverse. Le **vulnerabilità** rappresentano un fattore abilitante trasversale: lo sfruttamento di falle note o emergenti può infatti costituire un vettore di intrusione e facilitare l'attivazione di più categorie di minaccia.



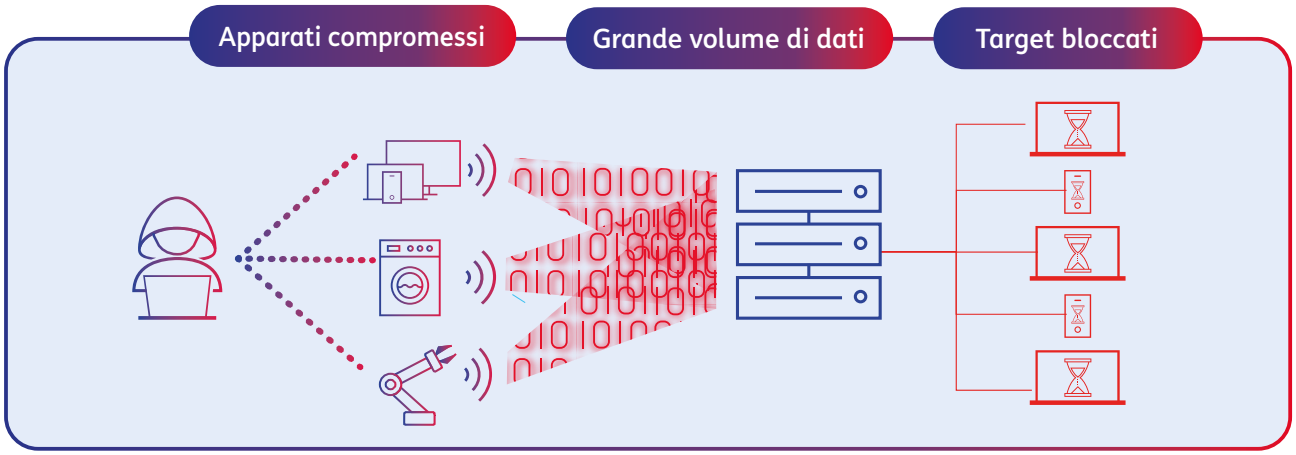
Attacchi **DDoS**

Un attacco **DoS/DDoS** (Denial of Service) si colloca tra le minacce alla **disponibilità** di un servizio o di una risorsa digitale. In questo rapporto l'attenzione è rivolta soprattutto ai DDoS **volumetrici**, nei quali l'avversario genera un forte afflusso di traffico verso un sito, un server o un'infrastruttura di rete, fino a saturarne le capacità e a degradare (o interrompere) l'erogazione del servizio. Spesso l'azione viene amplificata sfruttando reti di dispositivi compromessi o utenti ignari: il traffico arriva da molte sorgenti e da più direzioni, ed è proprio questa natura distribuita che caratterizza i DDoS.

Dal punto di vista dell'utente, l'effetto è immediato: i servizi digitali si interrompono, le pagine web non si caricano, le applicazioni non rispondono, l'accesso a dati e funzionalità diventa difficoltoso o impossibile. È una dinamica simile a quella dei picchi di affluenza su piattaforme molto richieste, quando il sistema non riesce a gestire l'aumento improvviso di richieste e va in saturazione.

Pur essendo chiaro il meccanismo generale, la rilevazione non è sempre lineare. Gli attacchi possono infatti **presentarsi in modo graduale o "a ondate"**, rendendo meno netta la distinzione tra fasi diverse; possono **partire da origini geografiche molteplici** e, in alcuni casi, **prendere di mira anche componenti di monitoraggio.** Inoltre, nel tempo cambiano tecniche e bersagli: si osservano sempre più spesso attacchi rivolti a interfacce web e API, difficili da identificare anche per la presenza di **traffico cifrato**, insieme a **strategie di elusione** (ad esempio IP dinamici o header HTTP manipolati) che mirano a mascherare il traffico malevolo.

I **SOC** del Gruppo TIM, operando sul presidio di rete, sono in grado di intercettare queste dinamiche e attivare misure di prevenzione e mitigazione; nelle pagine successive vengono presentate le principali evidenze tratte dall'attività di monitoraggio, contrasto e analisi.



Attacchi DDoS
Sintesi 2025

meno eventi,
più pressione

~4.300

Eventi DDoS 2025
(**-36%** vs 2024)

A fronte di meno eventi osservati, **nel 2025 le campagne sono più concentrate e la pressione resta elevata.** Gli attacchi più gravi - elevata potenza con lunga durata - **diminuiscono** rispetto al 2024.

ISTITUZIONI SOTTO ATTACCO

Quasi **1 attacco su 2**

colpisce il Government
nel segmento non domestico

3 eventi al giorno
superano 20 Gbps

I settori più colpiti da eventi DDoS

Istituzioni / Government
Servizi professionali
Telecomunicazioni
Trasporti
Istruzione

il 17% degli eventi è di
massima severità
(alta potenza, lunga durata: -9 p.p. vs 2024)

meno potenza, più durata:

~46 minuti
(durata media: **+19%** vs. 2024)
86% degli attacchi si esaurisce **entro 30 minuti**

Attacchi DDOS nel 2025: meno eventi, più pressione

Nel 2025 sono stati osservati circa 4.300 eventi DDoS dai SOC del Gruppo TIM. Il confronto rispetto al 2024, in cui erano stati registrati quasi 6.700 eventi, va valutato con attenzione dal momento che la netta diminuzione osservata (-36%) può essere collegata ad azioni intraprese per aumentare la difesa complessiva del sistema (ad esempio, mitigazioni a monte) che potrebbero aver influito sull'ampiezza del perimetro di osservazione.

Andamento degli attacchi DDoS: una panoramica

Esaminando diverse fonti sul tema, si osserva una certa variabilità dei volumi annuali dei DDoS nel confronto al periodo precedente. In effetti, le fonti non misurano lo stesso oggetto. Alcuni report contano attacchi osservati e mitigati all'interno di una specifica piattaforma di protezione, altri contano incidenti raccolti tramite segnalazioni e fonti istituzionali, altri ancora descrivono eventi nel perimetro di una o più organizzazioni, che può cambiare nel tempo anche per effetto delle strategie di difesa e di "mitigazione a monte".
Ad esempio, nell'osservazione degli eventi DDoS a livello globale, Cloudflare e Digicert presentano evidenze non sempre allineate che potrebbero dipendere dal diverso perimetro di osservazione e dalle diverse soluzioni di mitigazione adottate.

A fronte della riduzione dei volumi annui, si registra un aumento della pressione degli eventi DDoS perché gli attacchi risultano più concentrati nel tempo: campagne più mirate e "raffiche" ad alta intensità si addensano in poche finestre determinando un aumento degli indici di concentrazione (es. Gini). Il mutamento del profilo di attacco è comune ad altri lavori di analisi che, seppure non direttamente confrontabili per perimetro e metrica rispetto a questo, convergono nel descrivere dinamiche DDoS "a ondate" nel corso dell'anno.

Potenza dell'evento

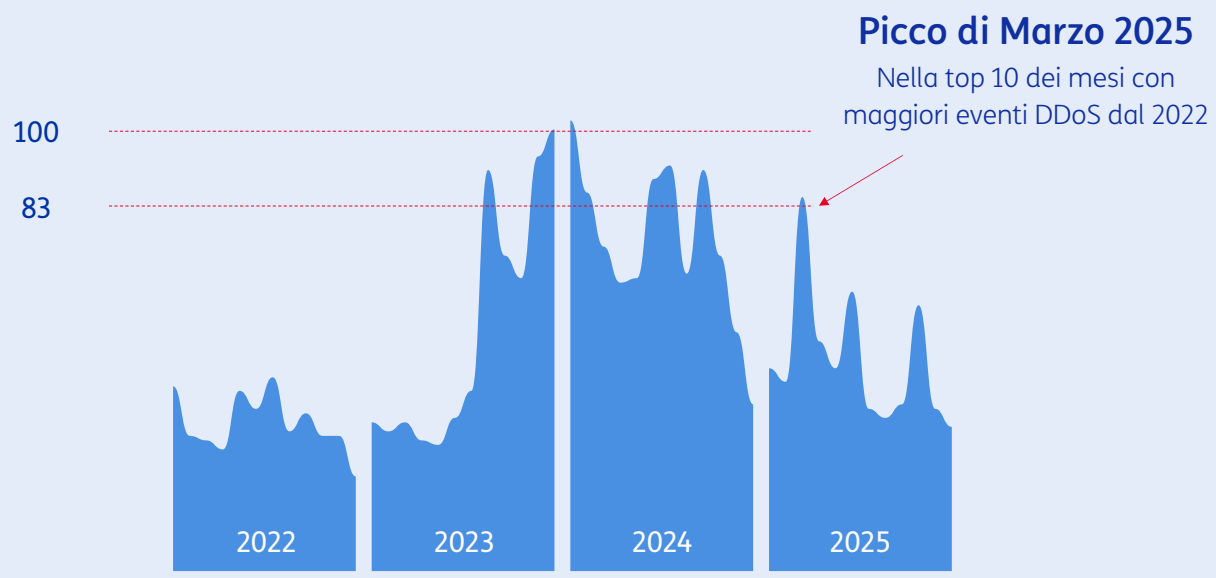
3 attacchi al giorno oltre i 20 Gbps

Marzo 2025 nella Top 10 dei mesi più caldi dal 2022 ad oggi.

In particolare, rimanendo nel nostro perimetro di osservazione, si registra una forte concentrazione in tre momenti ben individuabili nel tracciato dell'andamento degli eventi e precisamente a marzo, giugno ed ottobre 2025. Di questi, il più rilevante si manifesta a marzo 2025, con una densità di eventi talmente elevata che lo porta ad entrare nella "Top 10" dei mesi con maggiori casi DDoS dal 2022 ad oggi.

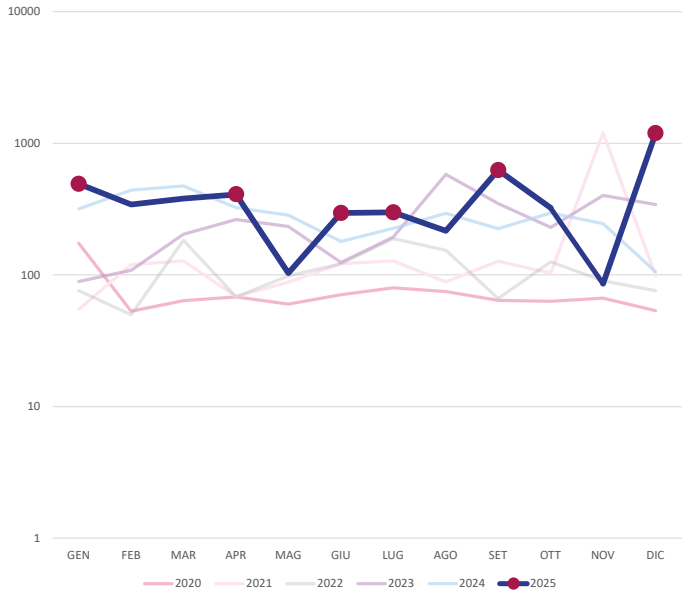
Andamento degli eventi DDoS

Numero indice: 100 = mese con maggior numero di eventi (gennaio 2024)



Dimensione massima di banda occupata da un singolo attacco nell'arco di un mese

Numero indice: media del periodo = 100. Asse verticale su scala logaritmica



L'aumento della pressione si evidenzia anche da un'altra prospettiva. Se consideriamo la dimensione massima di banda occupata da un singolo attacco nell'arco di un mese e confrontiamo tra di loro le dinamiche di ciascun anno dal 2020 ad oggi, si rileva che il 2025 raggiunge il picco in ben 6 mesi su 12, con un evento a dicembre che rappresenta il secondo in assoluto per intensità, inferiore solo ad un evento registrato a novembre 2021.

Attacchi DDoS e contesto geopolitico

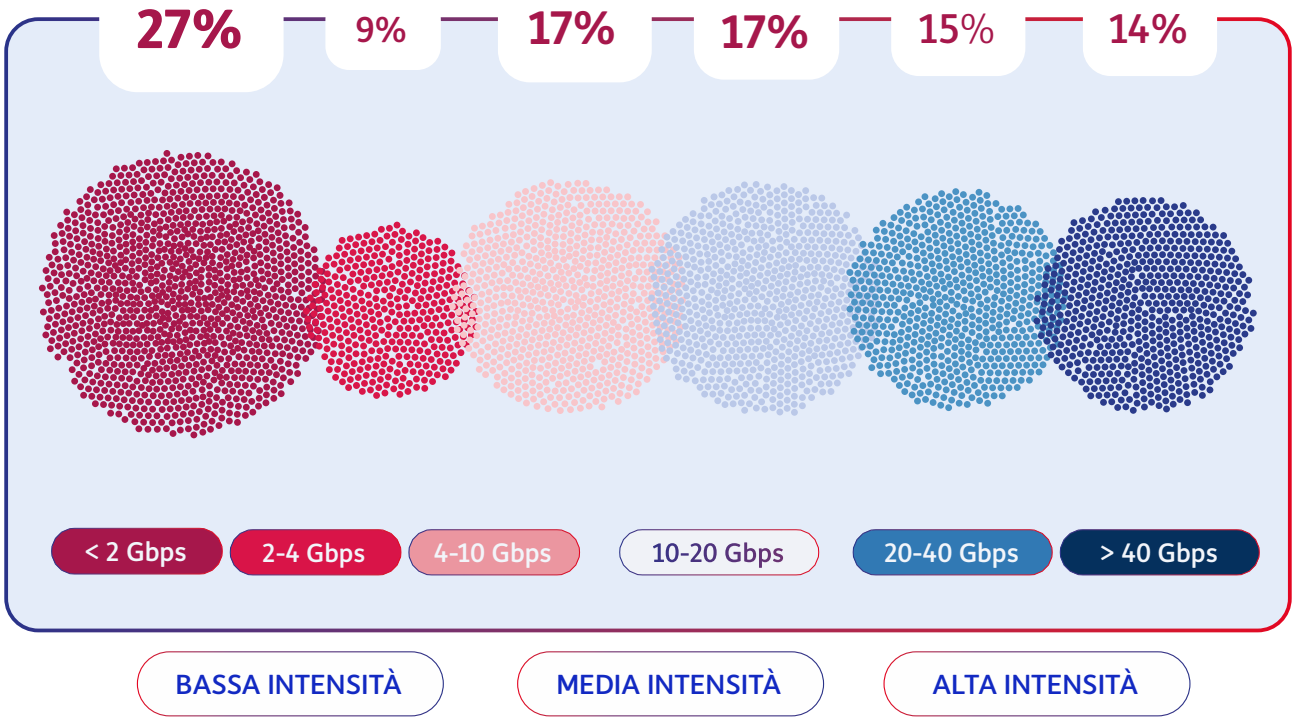
Fonti nazionali ed internazionali evidenziano una forte intensificazione di eventi – non necessariamente DDoS – a marzo 2025, mese nel quale il contesto geopolitico si presenta particolarmente acceso, culminando nella ripresa delle operazioni militari a Gaza (metà mese). Anche l'hacktivismo filo-russo presenta una intensa dinamica nel primo trimestre (in particolare, il gruppo NoName057(16) è stato particolarmente attivo a febbraio 2025), mentre nel mese di giugno si verifica la guerra dei 12 giorni tra Israele ed Iran, evento che può aver dato luogo ad una maggiore attività, pur senza un coinvolgimento diretto del nostro Paese. Nonostante il contesto geopolitico possa essere considerato un potenziale fattore di accelerazione, è bene precisare che non ci sono evidenze certe che possa aver influito sull'aumentata pressione verso l'Italia in queste specifiche finestre temporali.

Nel 2025, gli eventi DDoS osservati presentano un profilo in cui la componente ad alta intensità – tipicamente superiore a 20 Gbps – resta significativa, pur in presenza di una maggioranza di casi con potenza più ridotta. In particolare,

- **gli attacchi con potenza superiore a 20 Gbps rappresentano circa il 29%** del totale (a fronte del 39% nel 2024), ossia circa 3 eventi su 10;
- **il 54% degli eventi ricade sotto i 10 Gbps**, ossia nelle classi di potenza inferiore.

In media, ciò equivale a circa 12 attacchi al giorno, di cui circa 3 sopra i 20 Gbps e circa 1,5 a elevatissima intensità (oltre 40 Gbps).

Eventi DDoS 2025 per classe di intensità
La distribuzione nel 2025



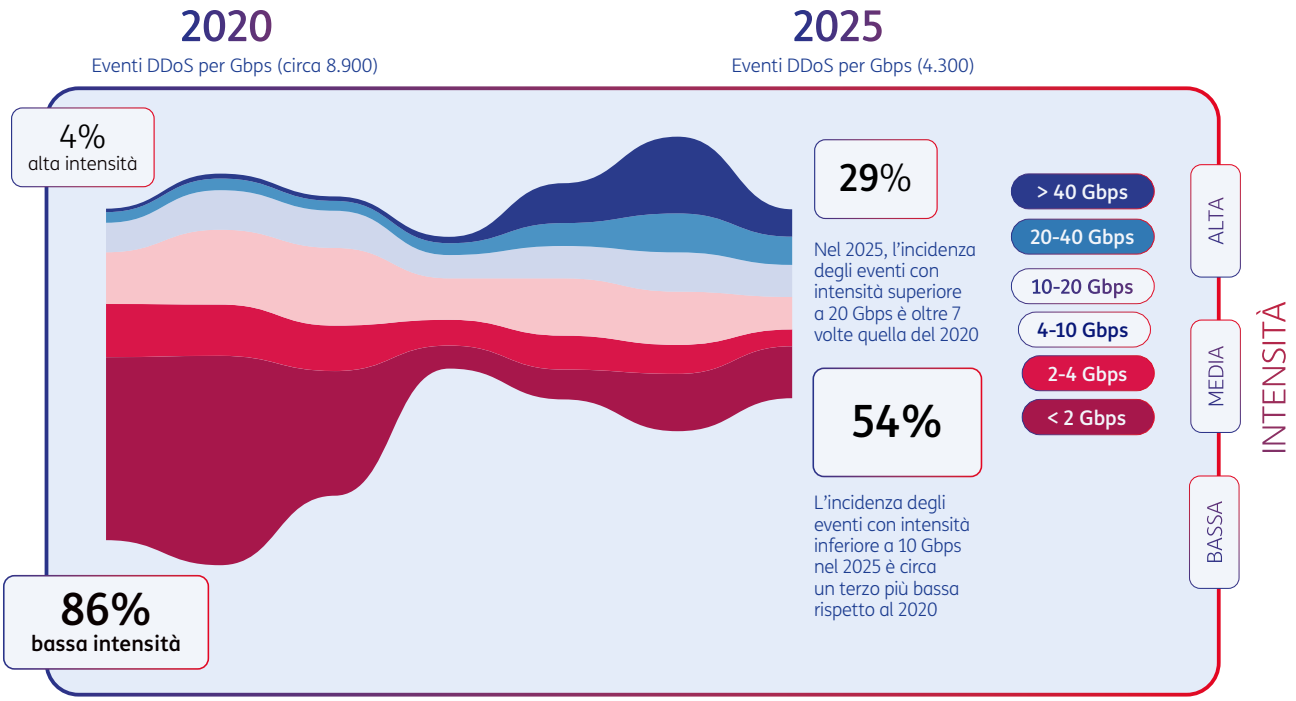
Distribuzione degli eventi DDoS: evoluzione e tendenze recenti

L'analisi della distribuzione per potenza degli eventi DDoS nel tempo evidenzia un cambiamento significativo nei profili di intensità.

Nel 2019 la stragrande maggioranza degli attacchi era caratterizzata da bassa intensità (circa l'87% del totale). Negli anni successivi, si è osservato un incremento progressivo degli attacchi ad alta intensità, che nel 2024 hanno raggiunto circa il 40% degli eventi registrati, di cui una larga parte superiore ai 40 Gbps (Gigabit al secondo). Questa crescita è attribuibile a diversi fattori, tra cui la riduzione dei costi dei servizi di DDoS a pagamento e l'accentuazione degli attacchi in relazione al deterioramento del quadro geopolitico internazionale.

Nel corso dell'ultimo anno, tuttavia, si è verificato un ritorno predominante degli eventi a bassa e bassissima intensità, che tornano a costituire la principale classe di potenza rilevata tra gli attacchi osservati.

Eventi DDoS 2025 per classe di intensità
Evoluzione nel corso del tempo

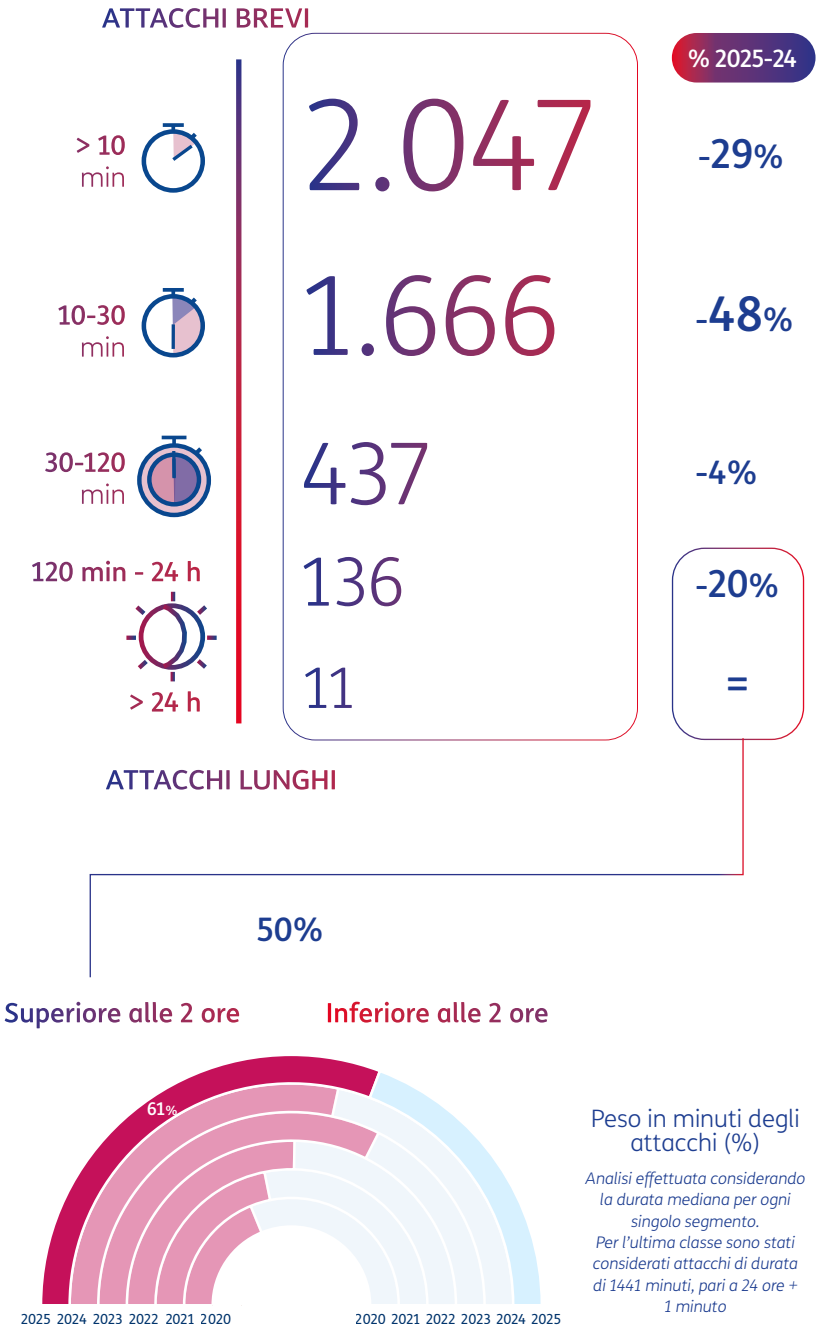


Durata dell'evento

quasi 9 eventi su 10 si conclude in 30 minuti

Sul piano temporale, si evidenzia una prevalenza di eventi di breve durata: i casi che si concludono entro 30 minuti rappresentano l'86% del totale, mentre gli attacchi con durata superiore alle 2 ore restano una quota marginale dell'attività complessiva (3,4% nel 2025, in aumento rispetto al 2,7% dell'anno precedente). Tra questi ultimi, gli eventi molto lunghi, con durata superiore al giorno, risultano sostanzialmente stabili (0,3%).

Se però si passa dalla semplice conta degli episodi alla misura dell'esposizione complessiva (cioè "eventi trasformati in minuti"), la lettura cambia: i 147 eventi con durata superiore alle 2 ore concentrano circa il 61% della durata annuale complessiva (in aumento rispetto al 57% dell'anno precedente, erano il 38% nel 2020). In questo quadro, la durata media di un evento DDoS nel 2025 è pari a circa 46 minuti, con un incremento del 19% rispetto al 2024.



Relazione tra potenza e durata dell'evento

I dati evidenziano una relazione inversa tra potenza e durata. Osservando la distribuzione degli eventi, le classi estreme mostrano in modo molto evidente questa relazione. Se consideriamo i casi ad elevatissima potenza, oltre i 40 Gbps, circa il 96% si conclude entro 30 minuti e solo lo 0,8% supera le 2 ore. Invece, per i casi con potenza d'attacco inferiore ai 2 Gbps, la quota degli eventi oltre le 2 ore sale al 9,2%, mentre quella degli eventi con durata fino a 30 minuti, pur rimanendo preponderante, come peraltro in tutti gli altri gruppi, scende al 66%.

Attacchi oltre 30 minuti: un esito raro sopra 10 Gbps, molto più frequente sotto questa soglia

Anche dal punto di vista statistico, usando una semplice comparazione tra gruppi, emerge una relazione tra potenza e durata dell'attacco. Una metrica particolarmente adatta quando si vogliono confrontare probabilità (e non solo conteggi) è il Risk Ratio (RR) o rapporto di probabilità: misura quanto è più (o meno) probabile che si verifichi un evento in un gruppo rispetto a un altro. In questo caso definiamo:

- Esposizione: attacco con potenza >10 Gbps (vs ≤10 Gbps);
- Evento: attacco con durata >30 minuti (vs ≤30 minuti).

Tra gli eventi con potenza ≤10 Gbps, quelli che superano i 30 minuti sono 517 su 2.304 (il 22,4% del totale) mentre 1.787 (il 77,6%) si esauriscono entro la mezz'ora. Tra gli eventi con potenza >10 Gbps, quelli che superano i 30 minuti sono 67 su 1.993 (3,4%), mentre 1.926 (96,6%) terminano entro la mezz'ora. Il RR si calcola come rapporto tra le due probabilità di "attacco lungo" (>30 min):

$$RR = \frac{P(>30 \mid >10\ \text{Gbps})}{P(>30 \mid \leq 10\ \text{Gbps})} = \frac{3{,}4\%}{22{,}4\%} \approx 0{,}15$$

Ciò significa che, sulla base delle occorrenze, gli "attacchi lunghi" sono circa 1 su 30 nel gruppo >10 Gbps, contro circa 1 su 4,5 nel gruppo ≤10 Gbps, con un RR≈0,15.

In definitiva, un attacco con potenza >10 Gbps ha una probabilità di durare oltre 30 minuti circa 85% più bassa rispetto a un attacco ≤10 Gbps.

Se consideriamo che, nel 2024 la probabilità di superare i 30 minuti era pari al 15,9% per gli eventi ≤10 Gbps e al 3,6% per quelli >10 Gbps, con un RR≈0,23, ne deriva che nel 2025 l'associazione tra bassa potenza e durate più lunghe risulta più marcata. Questo è coerente con l'interpretazione secondo cui gli attacchi "pesanti" e ad alto impatto siano più frequentemente rapidi, mentre la componente degli eventi con durata >30 minuti tende a concentrarsi maggiormente negli attacchi di bassa intensità.

Severità degli eventi

in diminuzione gli eventi gravi

Per quanto ogni evento presenti le sue specificità in termini di impatto, finalità, obiettivi e risorse colpite, nonché una grande varietà di tecniche e modalità messe in atto, nel nostro sistema di analisi tendiamo a concentrarci sulle variabili di intensità e durata. L'incrocio di questi due aspetti ci consentono di definire uno spazio – la matrice della severità degli eventi – dove possiamo osservare nel tempo come cambiano le caratteristiche degli attacchi DDoS, individuando diverse aree di riferimento (attacchi lievi, bassi, medi e gravi). Questo ci consente anche di visualizzare la tendenza e la direzione in cui si stanno orientando gli attacchi.

Abbiamo osservato che gli eventi DDoS stanno mostrando un'importante trasformazione con una crescita dell'incidenza dei casi di intensità bassa e di durata breve, un cambiamento molto significativo rispetto allo scorso anno. Questo nella mappa si traduce in un cambiamento del baricentro degli attacchi registrati.

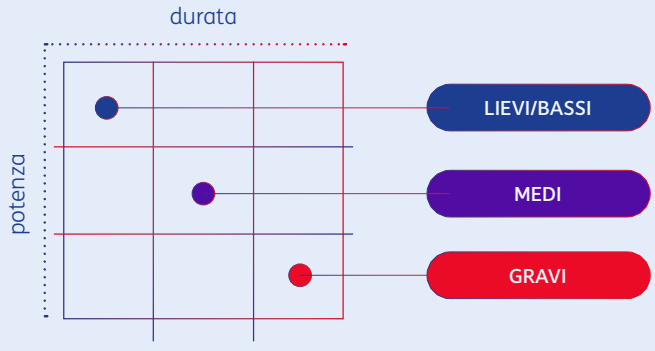
L'analisi storica dei dati raccolti a partire dal 2019 mostra che inizialmente il baricentro degli attacchi si colloca in un'area di severità bassa. A partire dal 2022 si registra un progressivo aumento della potenza, accompagnato da oscillazioni nella durata, che determina uno spostamento del baricentro verso un'area di severità intermedia.

Il baricentro degli attacchi si riporta ai livelli del 2022-2023

Nel 2025, pur mantenendosi l'intensità su valori comparabili a quelli registrati nel periodo 2022-2023, la durata media torna ad aumentare. Questo comporta un lieve cambiamento nella dinamica del baricentro che era stata registrata negli ultimi anni, pur rimanendo complessivamente all'interno di una zona di severità intermedia.

LA MAPPA DELLA SEVERITÀ

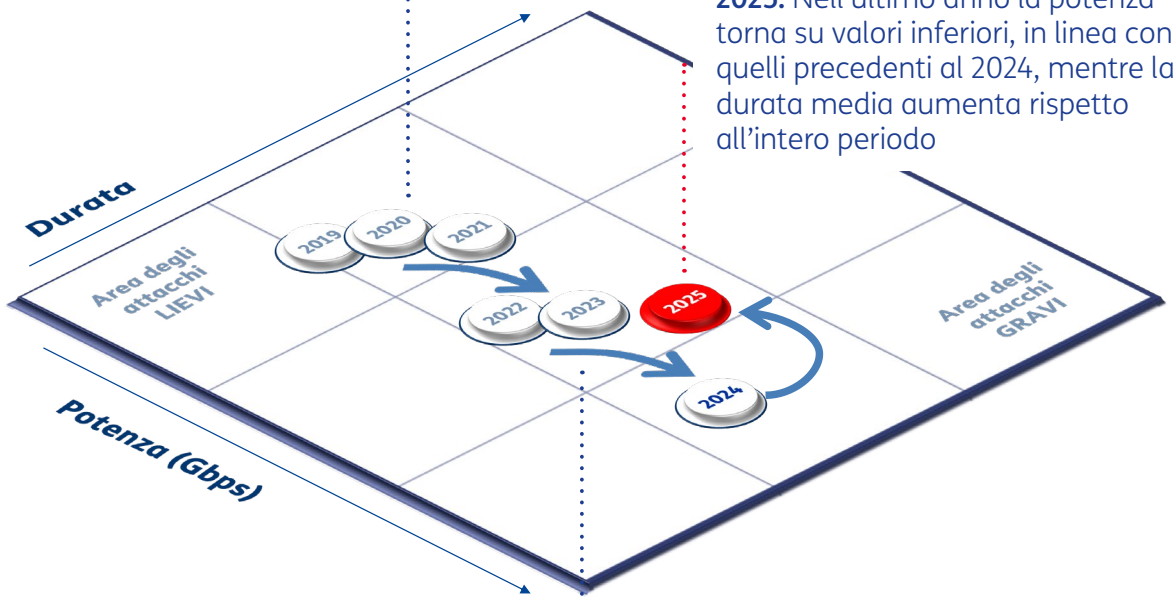
L'incrocio delle due variabili definisce uno spazio in cui è possibile collocare ogni attacco in funzione della durata e della potenza, consentendo anche di analizzare l'evoluzione degli eventi nel tempo.



LA MAPPA DELLE SEVERITÀ
2024 vs 2025

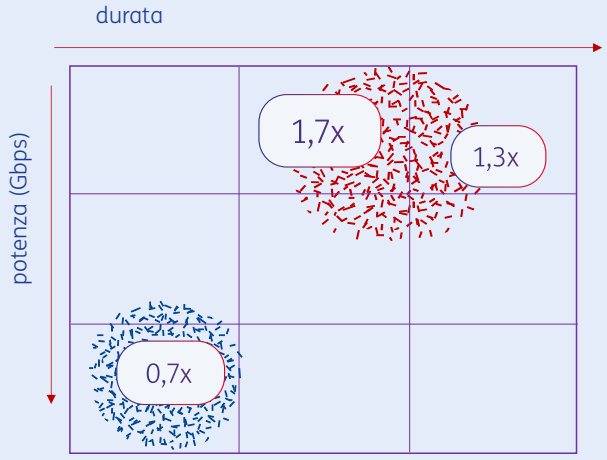
2019-2021. Dal 2019 al 2021 la maggior parte degli attacchi DDoS presentano una bassa intensità (tra 2 e 4 Gbps) ed una durata inferiore ai 30 minuti

2025. Nell'ultimo anno la potenza torna su valori inferiori, in linea con quelli precedenti al 2024, mentre la durata media aumenta rispetto all'intero periodo



2022-24. Il triennio 2022-2024 mostra una progressiva crescita della potenza, con oscillazioni nella durata

2024 VS 2025



La mappa permette di evidenziare le aree in cui si registrano i cambiamenti più significativi tra il 2024 ed il 2025.

Mitigazione

adattamento a scenari in rapida evoluzione

Gli eventi della massima severità si riducono nell'ultimo anno, ma restano su livelli elevati

Lo spostamento del baricentro verso un'area intermedia è una naturale conseguenza dei trend osservati negli ultimi anni e diventa ancora più evidente quando si analizza l'andamento degli attacchi di severità maggiore.

Nel 2020 gli eventi classificati come "gravi" rappresentavano il 6% del totale. Nel 2022 la loro incidenza era salita al 12%, raddoppiando in due anni. Il 2024 ha segnato il punto di massima espansione, con una quota che ha raggiunto il 26%, più che quadruplicando il valore iniziale.

Nel 2025 si osserva un cambiamento significativo: gli attacchi di massima severità scendono al 17%, interrompendo la crescita costante degli anni precedenti. Pur rimanendo su livelli superiori rispetto al periodo precedente al 2022, la riduzione riflette il generale calo della potenza media degli eventi, accompagnato però da un aumento della durata, che sposta parte degli attacchi verso profili meno intensi ma più persistenti.

Gli eventi di severità media, che tra il 2020 e il 2024 erano più che raddoppiati fino a raggiungere il 22%, nel 2025 registrano un'ulteriore crescita, arrivando al 24% del totale. Nel complesso, gli attacchi di severità media e alta rappresentano oggi il 41% del totale, una crescita significativa rispetto al 16% registrato nel 2020, pur con una diversa distribuzione interna dovuta al ridimensionamento degli attacchi più intensi e alla contestuale espansione della fascia intermedia.

Un contesto che richiede un impegno costante e dinamico in termini di prevenzione e mitigazione

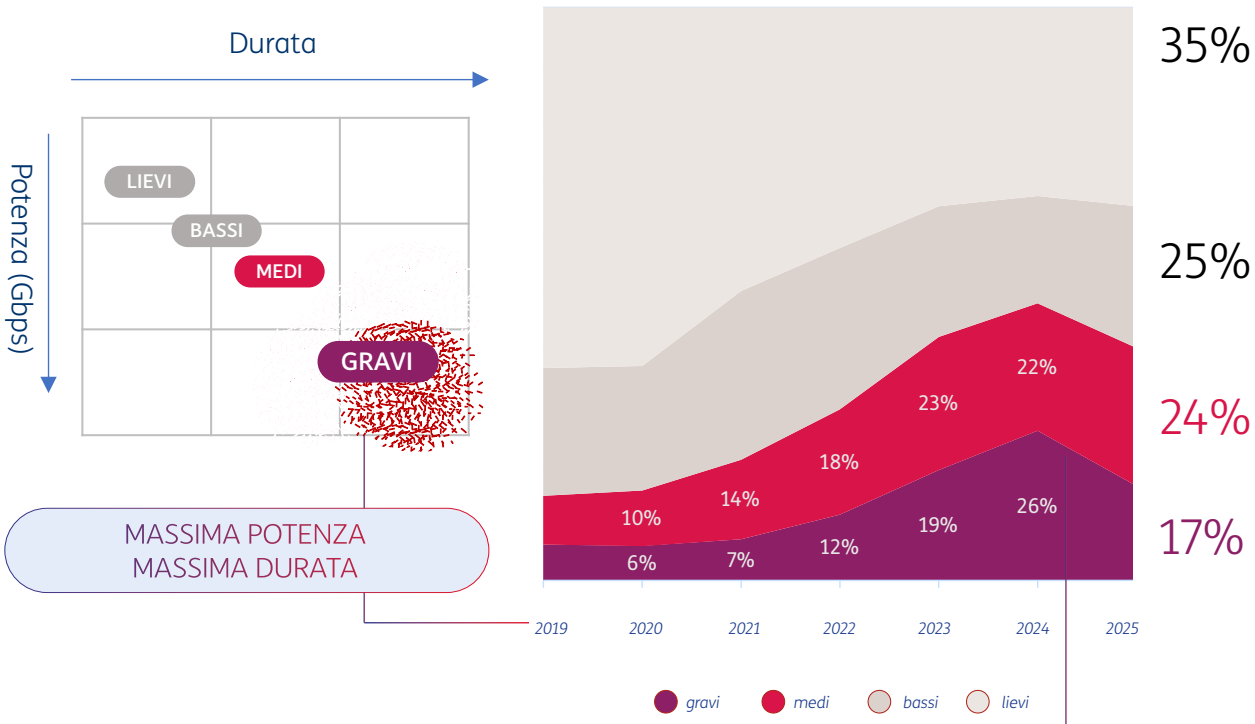
L 'aumento delle capacità di attacco registrato negli ultimi anni ha imposto un rafforzamento continuo delle capacità difensive. La trasformazione costante delle tecniche di attacco, inclusi gli attacchi DDoS, richiede un aggiornamento permanente delle tecnologie e dei sistemi di prevenzione, identificazione, mitigazione e contrasto, per garantire la protezione e la continuità operativa di imprese, PA e cittadini.

L'analisi delle attività di mitigazione conferma con chiarezza questa dinamica. Nel 2024 il volume degli interventi ha raggiunto il livello più elevato dell'intero periodo, risultando oltre tre volte superiore rispetto al 2019 e più che raddoppiato rispetto al 2020. Si tratta del punto di massimo impegno operativo, coerente con l'aumento della potenza e della frequenza degli attacchi osservato nello stesso anno.

Anche in questo caso, il 2025 segna un punto di svolta: il numero di mitigazioni diminuisce rispetto al picco del 2024, pur mantenendosi su valori nettamente superiori al periodo precedente al 2022. La riduzione è in linea con il calo della potenza media degli attacchi, ma non implica un alleggerimento del rischio complessivo. La maggiore durata degli eventi e la crescente variabilità dei profili osservati hanno continuato a richiedere un livello elevato di attenzione operativa, confermando la necessità di un approccio difensivo dinamico e adattivo, capace di rispondere a scenari in rapida evoluzione.

ANDAMENTO DEGLI ATTACCHI PER SEVERITÀ

Attacchi per livello di severità %



UN IMPEGNO COSTANTE E DINAMICO

-9 p.p.

nel 2025, riduzione in linea con il calo della potenza media

ma questo non implica un alleggerimento del rischio complessivo

Tecniche di attacco

Una maggiore gamma di tecniche utilizzate

Un attacco DDoS (Distributed Denial of Service) mira a rendere indisponibile un servizio (sito, applicazione, rete) generando molto traffico o molte richieste fino a superare la capacità del sistema di gestirle. È "distribuito" perché spesso il traffico proviene da molte sorgenti (ad esempio dispositivi compromessi) e arriva da più direzioni, rendendo più difficile bloccarlo. Questo può avvenire seguendo tecniche differenti:

- **Volumetrici**: puntano a saturare la banda (es. UDP/DNS/SSDP/Memcached/Chargen reflection).
- **Di protocollo** (rete/trasporto): mirano a esaurire risorse di rete o a spezzare/confondere il traffico (es. TCP flood, IP/UDP fragmentation).
- **Applicativi** (L7): imitano utenti veri verso un sito/app (es. HTTP flood).
- "**Reflection/Amplification**": usano server aperti su Internet come specchi: inviano richieste con mittente falsificato (l'indirizzo della vittima); lo "specchio" risponde con dati molto più grandi, moltiplicando la potenza dell'attacco.

Nel 2025 la composizione degli attacchi DDoS osservati mostra una forte concentrazione su pochi vettori "classici":

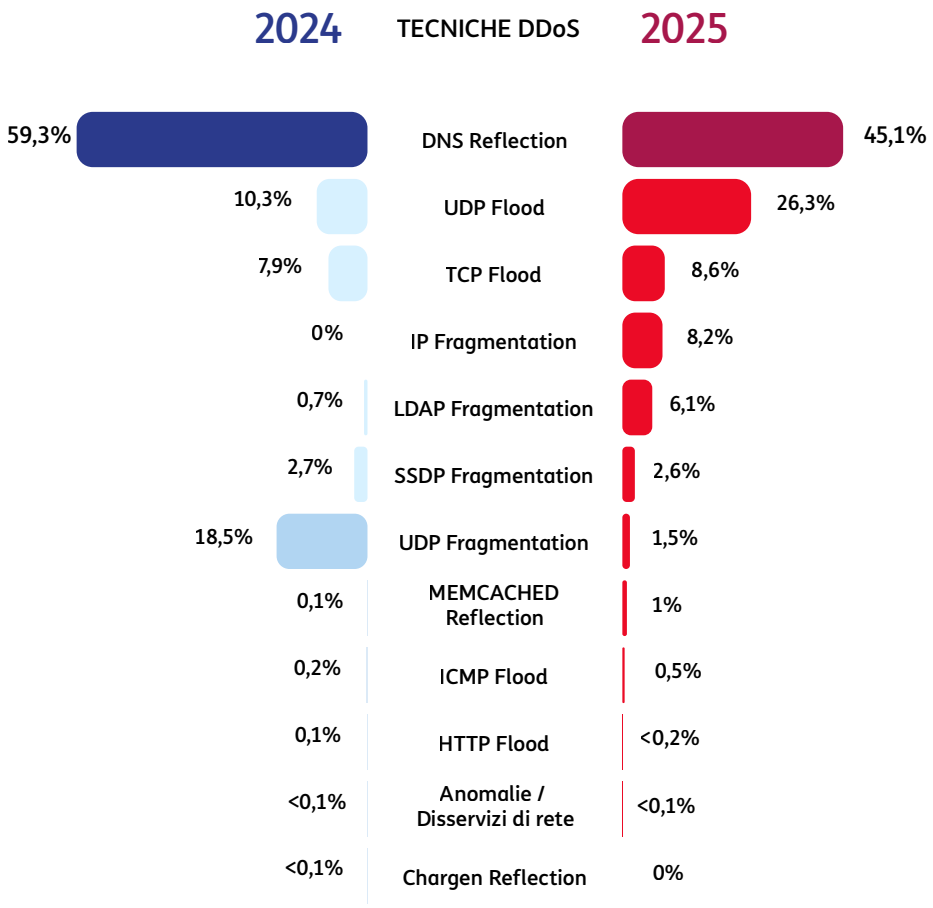
- la DNS Reflection è il vettore più utilizzato e interessa circa il 45,1% degli attacchi
- l'UDP Flood è la seconda tecnica più frequente e pesa circa il 26,3%.

Considerate insieme, queste due tecniche superano il 70% del totale, indicando che una quota rilevante dell'attività si basa su modalità di attacco relativamente standardizzate e ad alta scalabilità. Le altre tecniche di attacco mostrano un peso complessivamente più contenuto, spesso caratterizzate da impieghi episodici o da picchi localizzati in specifici periodi dell'anno.

Il confronto con il 2024 evidenzia alcuni spostamenti rilevanti nella "cassetta degli attrezzi" degli attaccanti. Pur restando il vettore principale, la DNS Reflection registra una contrazione marcata rispetto al 2024 (-51%) mentre cresce in modo significativo l'UDP Flood (+63%). Tra le tecniche più marginali, emergono l'IP Fragmentation (assente nel 2024, aumenta all'8,2% nel 2025) e la LDAP Reflection (da 62 attacchi nel 2024 a 262 nel 2025), mentre si contrae (-95%) la UDP fragmentation, che era il terzo vettore di attacco nel 2024.

Gli attacchi DDoS basati su tecniche di DNS Reflection/Amplification non sono, in sé, una manifestazione nuova né direttamente riconducibile all'impiego dell'intelligenza artificiale. Tuttavia, la crescente disponibilità di strumenti AI può contribuire ad accrescerne l'efficacia e la scalabilità, supportando gli attaccanti nell'individuazione dei sistemi esposti, nell'ottimizzazione dei vettori di amplificazione e nell'orchestrazione di campagne più rapide, adattive e multi-vettore. Pur non emergendo, allo stato, casi pubblicamente documentati che attestino in modo univoco l'uso dell'AI in specifici attacchi DNS Reflection, il fenomeno si inserisce in una più ampia evoluzione delle minacce DDoS verso modelli operativi sempre più automatizzati e industrializzati.

Eventi DDoS per tecnica di attacco
Confronto tra i principali vettori utilizzati nel 2024 e 2025



Oltre alla composizione complessiva, è utile guardare quando i diversi vettori risultano più attivi, perché questa lettura aiuta a distinguere tra "rumore di fondo" e possibili campagne o cambi di tecnica:

- La DNS reflection, il vettore più utilizzato, risulta intensamente sfruttata fino a giugno (concentrazione di circa l'81% del totale del vettore nel primo semestre)
- l'UDP flood è concentrato nella seconda metà dell'anno (circa il 75% degli eventi).
- La crescita della IP fragmentation si manifesta solo nella seconda parte dell'anno.
- Il TCP flood è particolarmente rilevante nei mesi di picco, con un segnale evidente a marzo
- Altre tecniche (LDAP reflection, SSDP reflection) presentano dei picchi in alcune finestre temporali.

Questa distribuzione temporale suggerisce una dinamica "a ondate": alcuni vettori costituiscono lo zoccolo duro dell'attività, mentre altri compaiono in finestre specifiche, compatibili con campagne più circoscritte o con sperimentazioni/rotazioni dei vettori per aggirare difese e filtri.

Guida alle principali tecniche di attacchi DDoS

DNS Reflection: tecnica di riflessione che sfrutta server DNS come "specchi": l'attaccante invia richieste in modo che le risposte DNS vengano dirette verso la vittima, aumentando il traffico in ingresso.

UDP Flood: "alluvione" di pacchetti UDP verso il bersaglio. È un vettore tipicamente volumetrico: punta a saturare banda e capacità di rete, spesso con traffico relativamente semplice da generare.

TCP Flood (es. SYN Flood, ecc.): traffico TCP progettato per stressare la gestione delle connessioni e/o le risorse di stato dei sistemi perimetrali (firewall, bilanciatori). In varie analisi è associato a un tentativo di saturare tabelle e capacità di gestione delle sessioni.

IP Fragmentation: vettore basato sulla frammentazione IP: punta a bloccare o degradare il destinatario rendendo oneroso (o problematico) il riassemblaggio dei pacchetti frammentati.

UDP Fragmentation: variante in cui i pacchetti UDP vengono frammentati; l'effetto è aumentare l'overhead di gestione del traffico e rendere più complessa l'analisi/filtraggio, con impatti potenziali su apparati e sistemi di difesa.

LDAP Reflection (CLDAP): tecnica di riflessione che sfrutta server LDAP/CLDAP esposti come "specchi", analogamente alla DNS reflection: l'attaccante stimola risposte che vengono indirizzate alla vittima.

SSDP Reflection: tecnica di riflessione che sfrutta SSDP/UPnP (spesso su dispositivi/servizi esposti): in alcune analisi è riportata come ormai molto ridotta anche grazie alla progressiva messa in sicurezza dei dispositivi IoT.

Memcached Reflection: tecnica di riflessione che sfrutta server memcached esposti: può generare risposte molto ampie rispetto alla richiesta, con forte effetto volumetrico (quando esistono server "aperti" sfruttabili).

ICMP Flood: flood basato su ICMP (es. "ping" massivo): punta a saturare banda o capacità di elaborazione; spesso è un vettore di contorno rispetto a DNS/UDP.

HTTP Flood (livello applicativo): molte richieste HTTP verso un sito o una API: può consumare risorse applicative (CPU, thread, backend) anche senza volumi di banda eccezionali.

Anomalie / disservizi di rete: categoria residuale che indica eventi "simili a DDoS" ma potenzialmente dovuti anche a malfunzionamenti o condizioni di rete.

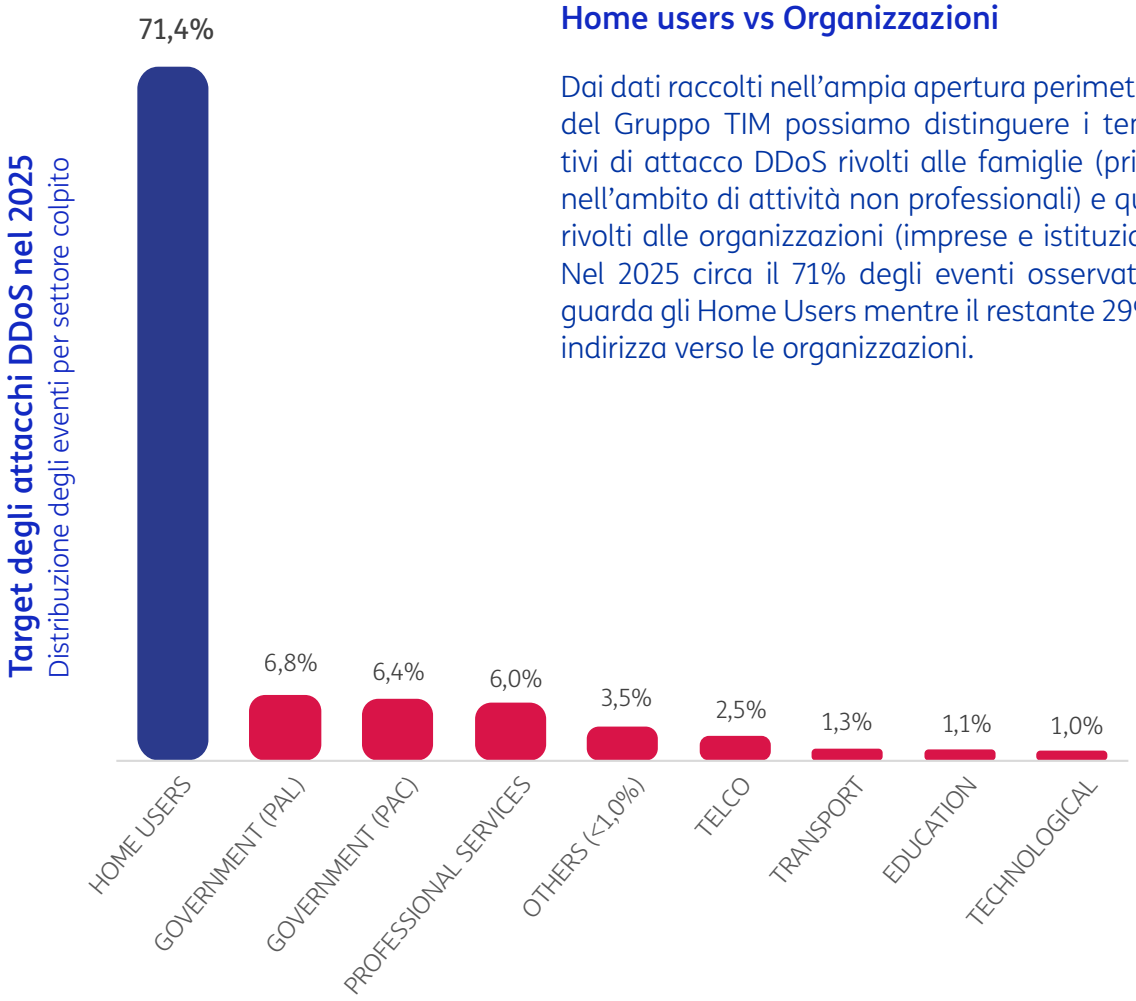
L'AI può rendere le operazioni DDoS più accessibili, automatizzate e adattive, soprattutto nelle piattaforme DDoS-for-hire. Il suo impatto è più evidente negli attacchi applicativi HTTP/HTTPS Flood, dove può aiutare a individuare endpoint più vulnerabili o costosi da servire. Per i vettori volumetrici e infrastrutturali – UDP flood, TCP flood, reflection/amplification e fragmentation – non emergono ancora evidenze pubbliche di un uso AI specifico, ma queste tecniche sono compatibili con campagne multi-vettore sempre più automatizzate[1].

1 Fonte: Netscout, https://www.netscout.com/threatreport/wp-content/uploads/2026/03/NETSCOUT-2H-2025-Threat-Report.pdf

Target degli attacchi DDoS

Istituzioni sotto attacco

Gli attacchi DDoS mirano a rendere indisponibili risorse e servizi digitali attraverso un sovraccarico di traffico o di richieste. Quando non sono guidati da finalità estorsive, l'obiettivo principale è spesso la discontinuità del servizio: creare disservizi, rumore e incertezza, colpendo ciò che risulta più esposto o più vulnerabile in un dato momento. In questo senso, la strategia può essere opportunistica perché l'attaccante tende a privilegiare quei punti del sistema che possono essere messi sotto pressione con maggiore facilità o con un impatto percepito più alto e dunque la composizione dei target può variare nel tempo, seguendo l'evoluzione del contesto tecnico (superficie esposta, difese, disponibilità di botnet/servizi DDoS-for-hire) e l'emergere di nuove opportunità operative. Proprio per questo, monitorare nel tempo l'evoluzione dei target è essenziale a comprendere dove si possono individuare nuove opportunità di attacco e dove, di conseguenza, serve rafforzare resilienza e priorità di difesa.



Home users vs Organizzazioni

Dai dati raccolti nell'ampia apertura perimetrale del Gruppo TIM possiamo distinguere i tentativi di attacco DDoS rivolti alle famiglie (privati nell'ambito di attività non professionali) e quelli rivolti alle organizzazioni (imprese e istituzioni). Nel 2025 circa il 71% degli eventi osservati riguarda gli Home Users mentre il restante 29% si indirizza verso le organizzazioni.

Il confronto 2023-2025 aiuta però a leggere questo dato in prospettiva: gli home users restano la porzione più importante degli eventi registrati, ma il loro peso relativo tende a ridursi nel tempo, dall'80,6% del 2023 al 76,8% del 2024 fino al 71,4% del 2025. Questa dinamica suggerisce una lettura "a due livelli": da un lato, la pressione verso il segmento domestico resta la base quantitativa del fenomeno (la "massa" degli eventi), dall'altro, cresce la quota di attacchi che si indirizza verso target non domestici. Questo appare ancora più significativo dal momento che il confronto nel tempo risente delle diverse strategie di difesa del perimetro che influiscono sul volume complessivo dei casi rilevati: nonostante il forte calo degli eventi registrati nel corso del 2025 aumenta l'incidenza della componente "non domestica", a significare che l'interesse a colpire organizzazioni e istituzioni aumenta nel corso degli ultimi tre anni.

Gli attacchi verso imprese/istituzioni

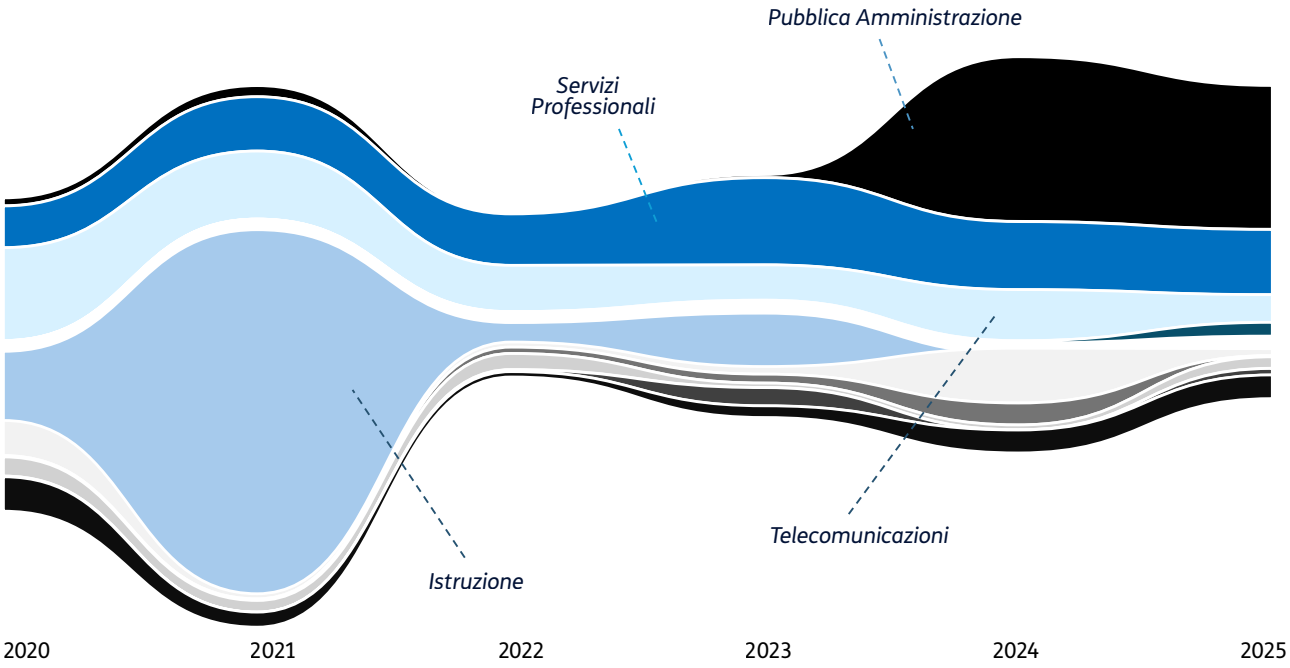
Depurando gli eventi dalla componente Home Users, il 2025 restituisce una mappa di settori colpiti che rende bene l'idea della selezione compiuta dagli attaccanti:

1. Government (PAL e PAC)
2. Servizi professionali
3. Telecomunicazioni
4. Trasporti (in forte crescita rispetto al 2024)
5. Istruzione

La presenza di "Government" al primo posto, insieme a Trasporti e Istruzione, suggerisce una pressione verso ambiti in cui un DDoS può generare un impatto immediatamente percepibile (portali, servizi digitali, accessi, continuità operativa), con possibili effetti a catena su cittadini e imprese.

In particolare, la componente istituzionale è quella che registra la maggiore crescita e diventa un bersaglio privilegiato. In una prospettiva storica, il 2024 rappresenta uno spartiacque. Fino a quell'anno, l'incidenza degli attacchi al segmento Government oscillava tra l'1 e il 2,5% sul totale degli eventi indirizzati al segmento non domestico (ovvero tra lo 0,2 e l'1% del totale degli eventi registrati). Nel 2024 l'incidenza salta al 42% del segmento non domestico per poi aumentare nel 2025 al 46%. Ciò significa che quasi un attacco su due, escludendo quelli rivolti agli Home Users, si indirizza verso questo target. Solo nel 2021 si era registrata una maggiore concentrazione su un settore – quello dell'Education – anche a causa della maggiore esposizione dovuta allo svolgimento delle lezioni a distanza nel periodo in cui erano in vigore le misure di confinamento anti-Covid.

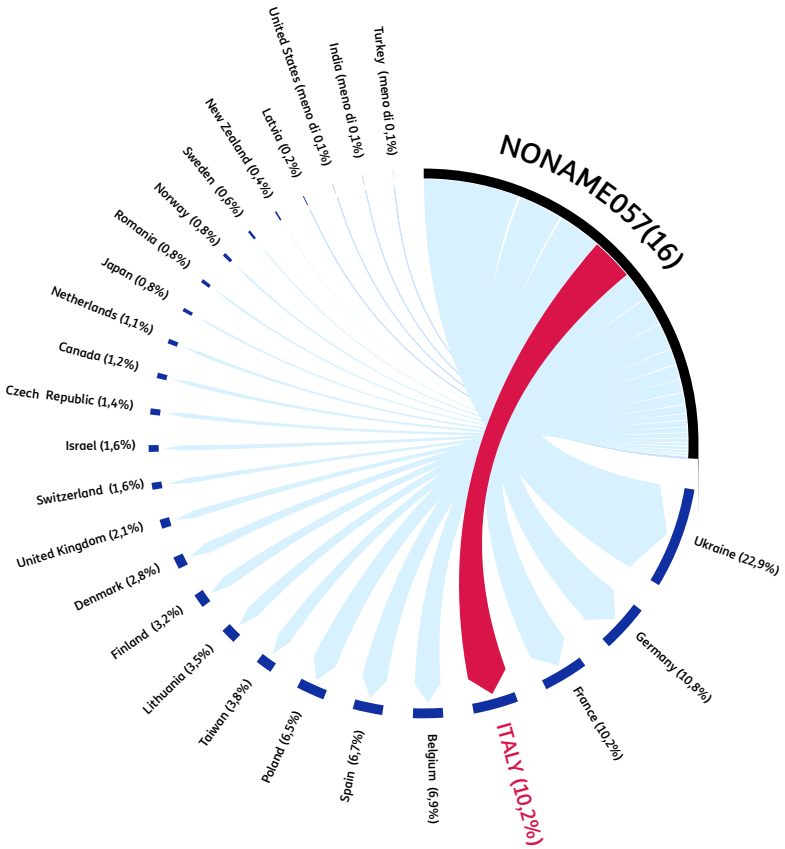
Attacchi DDoS verso target non Home: settori maggiormente colpiti nel 2025



Attacchi collettivo NoName057(16)

NoName057(16) è un gruppo di hacktivisti filo-russi emerso nel marzo 2022, poco dopo l'invasione su vasta scala dell'Ucraina da parte della Russia. Nel panorama degli attacchi DDoS di matrice hacktivista e geopolitica legati al conflitto russo-ucraino, il collettivo filorusso NoName057(16) emerge come uno dei driver più attivi e persistenti con migliaia di target/host unici colpiti in poco più di un anno e una focalizzazione ricorrente su enti governativi e settore pubblico in Paesi europei/NATO percepiti come avversari. Anche ENISA lo cita tra i gruppi più attivi nel contesto DDoS.

L'allineamento di NoName057(16) con gli interessi strategici della Russia è costantemente ribadito attraverso le comunicazioni pubbliche del gruppo su Telegram, dove i suoi attacchi vengono presentati come una rappresaglia diretta per le azioni intraprese dagli avversari della Russia. L'arma principale del gruppo è uno strumento DDoS personalizzato chiamato "DDoSia" ed il framework operativo che circonda questo strumento è noto come "DDoSia Project", che comprende strumenti ed infrastrutture tali da permettere a persone con scarse o nulle competenze tecniche di partecipare alle operazioni del gruppo di minaccia.



Nel corso del 2025, l'Italia ha rappresentato il quarto Paese più colpito dalle azioni di questo collettivo dopo Ucraina, Germania e Francia.

Dai dati raccolti, si conferma che NoName rappresenta una quota significativa dei DDoS "hacktivisti" rivendicati/attribuiti in ambito geopolitico e in Italia la sua azione ha rappresentato una quota che oscilla tra il 20 ed il 35% degli attacchi indirizzati ai settori Energy, Telco, Finance, Media, Technology e quasi 1 attacco su 2 indirizzato al settore Government.

La rilevanza operativa del gruppo è confermata dal fatto che è stato oggetto di un'azione coordinata internazionale (Operazione Eastwood) che ha mirato a interromperne l'infrastruttura di attacco. L'operazione, condotta tra il 14 e il 17 luglio 2025, ha coinvolto azioni internazionali delle forze dell'ordine che hanno portato a due arresti (un arresto preliminare in Francia e uno in Spagna), sette mandati di arresto emessi (sei dalla Germania e uno dalla Spagna) e 24 perquisizioni domiciliari in Repubblica Ceca, Francia, Germania, Italia, Polonia e Spagna.

Attacchi **Ransomware**

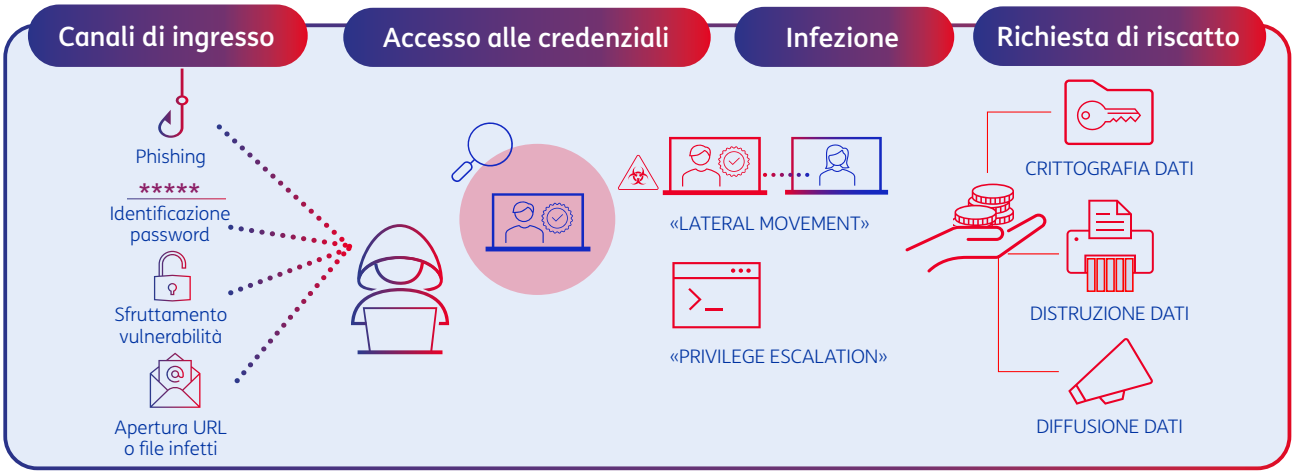
Il **ransomware** è oggi una delle minacce più pervasive perché combina impatto tecnico e leva economica: gli attaccanti mirano a prendere il controllo di risorse e dati di un'organizzazione e a trasformare l'interruzione del servizio (o la perdita di confidenzialità) in una richiesta di riscatto.

Nel tempo il modello si è evoluto: accanto alla cifratura o al blocco dei sistemi, molti gruppi adottano schemi a **doppia estorsione**, in cui l'esfiltrazione preventiva di informazioni diventa un ulteriore elemento di pressione, con possibili ricadute reputazionali, legali e regolatorie. Un fattore che contribuisce alla diffusione del fenomeno è la "industrializzazione" dell'offerta criminale, in particolare attraverso il modello **Ransomware-as-a-Service (RaaS),** che rende disponibili strumenti e infrastrutture anche ad attori meno specializzati e favorisce un ecosistema dinamico e frammentato, in cui l'AI inizia a diventare un fattore che amplifica la minaccia.

Dal punto di vista operativo, un attacco ransomware si inserisce quasi sempre in una catena di fasi: dall'**accesso iniziale** (ad esempio tramite social engineering, credenziali, servizi esposti o vulnerabilità) alla **propagazione nell'ambiente** e alla **ricerca dei sistemi più critici**, fino alla fase di **impatto ed estorsione.**

Osservare e misurare il ransomware, tuttavia, non è semplice: una parte rilevante delle evidenze disponibili deriva da contenuti resi pubblici dagli stessi gruppi (ad esempio tramite rivendicazioni), mentre un'altra parte può non emergere; inoltre, nel monitoraggio dei canali di pubblicazione può accadere che alcune rivendicazioni vengano rimosse o modificate nel tempo, influenzando la lettura complessiva.

Per questo, l'analisi del fenomeno ransomware presentata nel Rapporto si fonda sulle evidenze raccolte attraverso i sistemi di monitoraggio e analisi adottati, nonché sulle informazioni disponibili e verificabili nel perimetro osservato. I dati illustrati restituiscono pertanto una rappresentazione qualificata della componente rilevabile del fenomeno, idonea a coglierne l'evoluzione, i principali trend e le dinamiche operative, senza pretendere di esaurirne l'intera dimensione. Come per molte manifestazioni della minaccia cyber, una parte degli eventi può infatti rimanere al di fuori dei circuiti di osservazione pubblica o istituzionale, in ragione delle modalità di emersione, comunicazione e rilevazione degli incidenti.



Attacchi Ransomware
Sintesi 2025

Nel 2025 sono stati tracciate oltre 7.400 attacchi ransomware

a livello globale (+**42**% vs 2024).

Un attacco su due colpisce imprese negli **Stati Uniti**; l'UE è la seconda area più colpita (16%).

166

Attacchi ransomware rilevati verso l'Italia nel 2025
(+14% vs 2024)

I settori più colpiti da attacchi ransomware

Manifatturiero
Servizi professionali
Commercio/Retail
Settore tecnologico

L'Italia passa dal 2° al 4° posto in Europa per attacchi ransomware,

tra Francia (3°) e la Spagna (5°). La Germania raggiunge la vetta della classifica in UE e in Europa, sorpassando il Regno Unito.

123 **gruppi ransomware censiti nel 2025 a livello globale**

In Italia guidano **Qilin** e **Akira**, seguiti da **Everest**, **Sarcoma** e **LockBit** (tra gli altri).

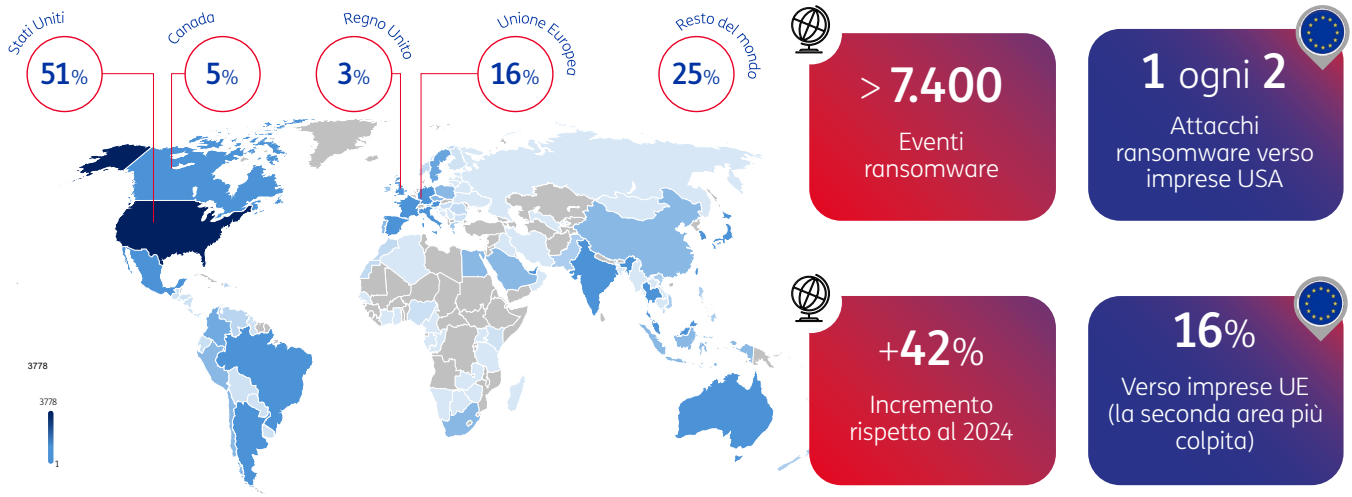
Le regioni più interessate dal ransomware nel 2025 sono **Lombardia, Emilia Romagna, Lazio e Veneto.**

Evoluzione del ransomware nel 2025

Nel 2025 il ransomware si è confermato come uno dei fenomeni più rilevanti e persistenti nel panorama della sicurezza informatica globale. Il monitoraggio e l'analisi delle minacce digitali effettuati dai sistemi di threat intelligence del Gruppo TIM sono stati in grado di registrare oltre 7.400 attacchi ransomware a livello globale, in crescita del 42% rispetto all'anno precedente.

Questo incremento segnala una forte accelerazione del fenomeno, dovuta a una molteplicità di fattori. Da un lato, la diffusione dei modelli di Ransomware as a service (RaaS) permette anche ad attori con minori competenze specialistiche di lanciare attacchi appoggiandosi ad infrastrutture e servizi già pronti. Un abbassamento della soglia di ingresso al cybercrime che troverebbe riscontro nel deciso aumento del numero di attaccanti. D'altro canto, è indubbio che il contesto digitale in cui opera un'azienda è sempre più complesso e questo rende più difficile proteggere i sistemi con la stessa rapidità con cui evolvono le minacce. Una parte dell'incremento osservato potrebbe essere messa in relazione a un effetto di maggiore visibilità del fenomeno. Tuttavia, è plausibile che una parte del fenomeno resti ancora in ombra, dal momento che i dati raccolti riflettono le rivendicazioni rese intenzionalmente visibili e non includono casi in cui l'attacco non sfocia in una pubblicazione o in una rivendicazione esplicita. Inoltre, nel monitoraggio dei Data Leak Site (DLS), può accadere talvolta che alcune rivendicazioni vengano successivamente rimosse o modificate, influenzando il conteggio degli eventi osservati.

Intensità degli attacchi Ransomware nel mondo – anno 2025



Le aree più colpite

Dal punto di vista geografico, il 2025 mostra una forte concentrazione degli attacchi verso le economie più digitalizzate.

Un attacco su due ha colpito imprese statunitensi, confermando gli Stati Uniti come il principale bersaglio dei gruppi ransomware. L'Unione Europea rappresenta il 16% degli attacchi complessivi e si colloca come la seconda area più colpita, in un contesto caratterizzato da un ampio e articolato tessuto imprenditoriale.

Per relativizzare i volumi rispetto alla dimensione del tessuto produttivo, rapportiamo gli eventi al numero di imprese attive. Questa normalizzazione va letta con cautela, perché presuppone una comparabilità della visibilità/attribuzione degli eventi tra contesti che potrebbe non essere pienamente omogenea. In questa lettura, il quadro mostra una situazione differente: per ogni milione di aziende, negli USA si registrano circa 109 attacchi ransomware, mentre in Canada 78, nel Regno Unito 46 e nell'Unione Europea 35. Ciò continua ad evidenziare la forte rilevanza degli Stati Uniti, che si confermano un target privilegiato, mentre Regno Unito ed UE mostrano incidenze più basse e questo potrebbe essere interpretato anche come un segnale di diversa capacità difensiva e resilienza.

Italia ed Europa

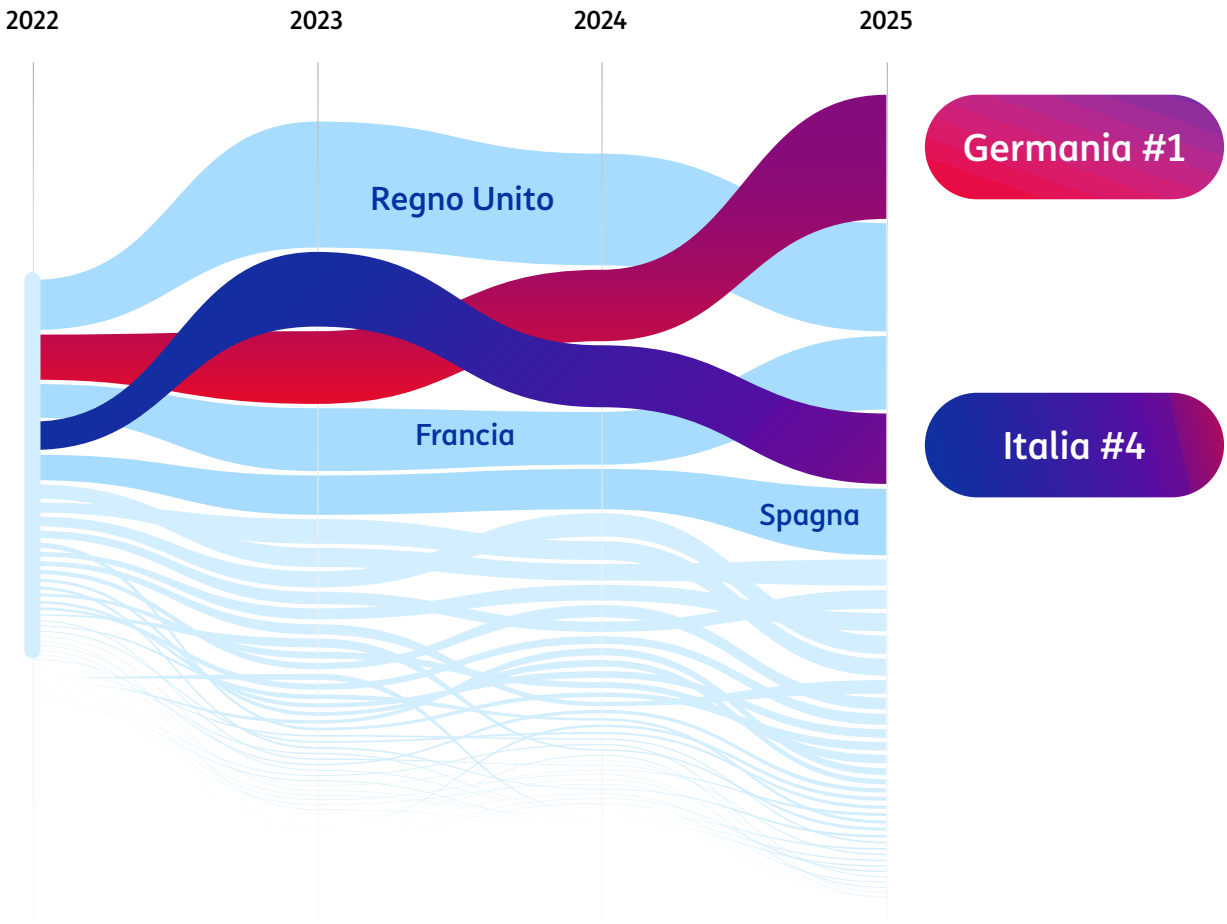
Nel 2025 gli attacchi rilevati in Italia aumentano del 14%, passando da 146 a 166, un segnale che il Ransomware continua ad essere una minaccia per il sistema produttivo nazionale. Guardando al contesto europeo ci si rende conto che il Ransomware registra quasi ovunque incrementi ancora più importanti: Germania +74%, Spagna +65%, Francia +40%. A livello UE la crescita complessiva è stata del +40%. Allargando l'orizzonte ai paesi europei che non fanno parte dell'Unione, si evidenzia una situazione differente per il Regno Unito, che mostra una lieve diminuzione (-3%).

Queste dinamiche influiscono sul posizionamento dei singoli Paesi nella classifica delle aree più colpite in Europa, considerando i Paesi UE e non UE. In particolare:

- l'Italia scende progressivamente dal secondo posto del 2023 al quarto del 2025.
- La Germania, nello stesso arco temporale, compie il percorso inverso diventando il primo Paese in UE e in Europa per attacchi Ransomware subiti.
- La Francia supera l'Italia portandosi al terzo posto, mentre la Spagna risulta stabile al quinto.
- Il Regno Unito, che guidava la classifica dal 2022, scende in seconda posizione dietro la Germania.

La perdita di posizioni dell'Italia, in questa particolare classifica, non va valutata necessariamente come un segnale positivo, visto che il Ransomware continua a crescere anche nel nostro Paese, ma solo come un'evoluzione del fenomeno meno marcata rispetto ad altri contesti comparabili, una situazione che può essere dettata anche da scelte opportunistiche degli attaccanti.

Ranking dei Paesi europei più colpiti nel corso del tempo



In Italia gli attacchi Ransomware aumentano del 14%, ma tutti gli altri grandi Paesi europei fanno registrare crescite superiori (+74% in Germania, +65% in Spagna, +40% in Francia). Il Regno Unito vede un trend in lieve diminuzione (-3%).

In termini di ranking, l'Italia continua a scendere: era al secondo posto tra i Paesi europei più colpiti da Ransomware nel 2023, è ora al quarto posto. La Germania è diventata nel 2025 il Paese europeo più colpito

Il ransomware in Italia

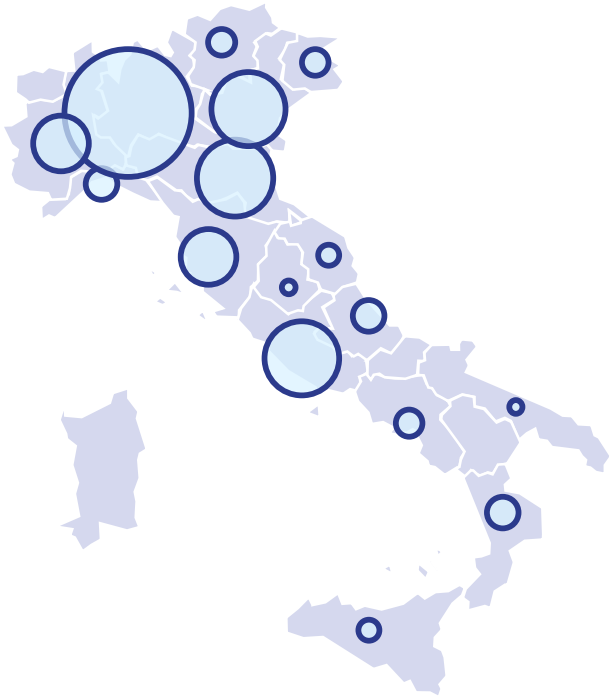
Distribuzione territoriale

L'analisi territoriale degli attacchi Ransomware mostra che, nel 2025, il fenomeno tende a polarizzarsi in alcune aree, con una dinamica complessivamente più intensa nel Centro-Nord rispetto al Mezzogiorno.

La **Lombardia** si conferma come principale epicentro nazionale con 53 attacchi, pari al 31,9% del totale. Rispetto al 2024, si registra una crescita sia in termini assoluti che relativi (+4,5 punti percentuali). Altre regioni in cui il Ransomware si concentra in modo significativo nel 2025 sono l'**Emilia-Romagna** (20 casi, pari al 12% del totale), il **Lazio** ed il **Veneto** (entrambe con 19 casi). In particolare, in Veneto, i casi di Ransomware quasi raddoppiano rispetto al 2024, anche se – dati i volumi limitati – una variazione di pochi casi può generare oscillazioni molto elevate. Complessivamente, nelle quattro prime regioni per numero di casi Ransomware, si concentrano i due terzi degli attacchi.

Il **Mezzogiorno**, nel complesso, pesa meno sul totale, anche se non mancano eccezioni puntuali (Calabria e Sicilia). Il dato non implica che il Mezzogiorno "migliori" in senso strutturale, ma segnala che la crescita degli episodi rilevati è stata più intensa nel Nord e più debole altrove. Da una parte, questa polarizzazione è coerente con la situazione economica del Paese: il Ransomware punta a colpire laddove c'è una maggiore densità industriale e di servizi avanzati e dove è più alta la probabilità di ottenere "leva" (continuità operativa, dati sensibili, supply chain) perché anche una singola interruzione può produrre degli effetti negativi nelle filiere e nelle catene di fornitura.

Va considerato, in ogni caso, che la distribuzione territoriale è osservata attraverso eventi rivendicati o comunque resi pubblicamente visibili e dunque una parte del fenomeno può rimanere non osservabile e la probabilità di emersione potrebbe non essere omogenea tra regioni.



Circa 4 ransomware su 10 colpiscono nelle regioni del nord-ovest

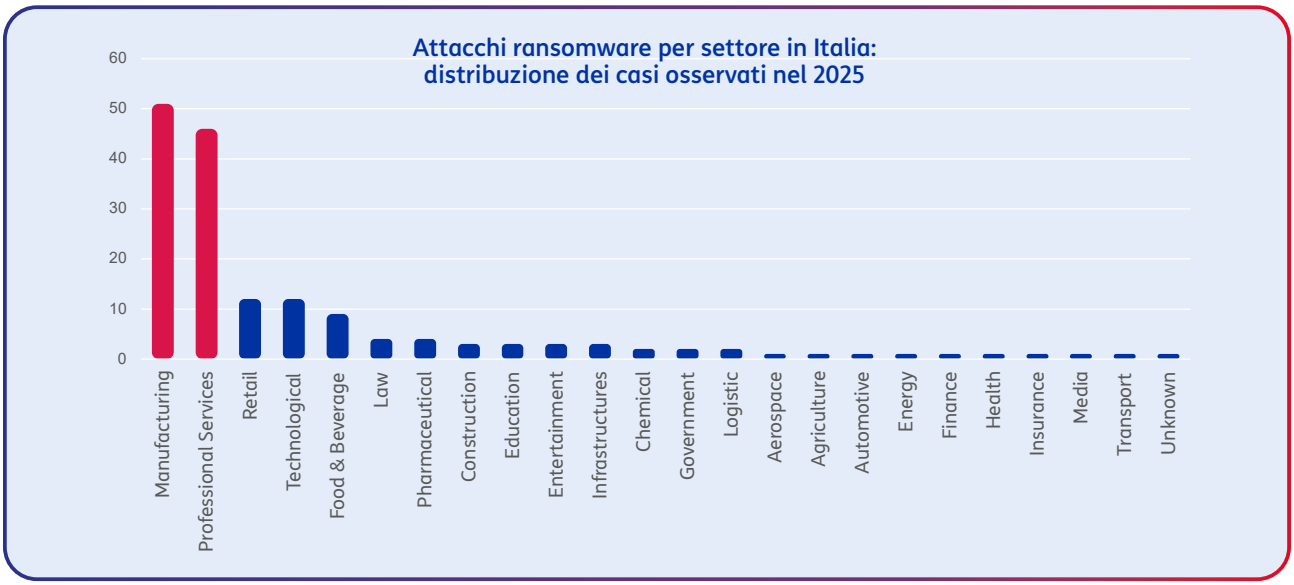
I settori italiani più colpiti

Nel 2025, come osservato anche nel 2024, la distribuzione settoriale degli attacchi Ransomware mostra una forte concentrazione in alcuni ambiti specifici ed una lunga "coda" di settori colpiti in modo episodico.

La Manifattura resta il principale bersaglio con 51 casi (30,7% del totale), seguita dai Servizi professionali con 46 casi (27,7%). Da soli, questi due settori rappresentano oltre la metà degli episodi osservati. Segue un secondo gruppo di comparti con volumi intermedi: Retail e Tecnologico (entrambi con 12 casi, 7,2% ciascuno) e Food & Beverage (9 casi, 5,4%). Nel complesso, i primi quattro settori (Manifattura, Servizi professionali, Retail, Tecnologico) concentrano circa tre quarti degli attacchi, mentre gli altri comparti si distribuiscono su valori ridotti (spesso 1-4 episodi). Questo profilo suggerisce un rischio non "diffuso in modo uniforme", ma aggregato in aree produttive e di servizio ad alta intensità di processi, filiere e dati. Anche in questo caso, ribadiamo la cautela con la quale vanno valutati questi dati, basati esclusivamente su rivendicazioni.

Il confronto con il 2024 segnala alcune variazioni rilevanti, soprattutto nei settori a maggior peso. I Servizi professionali aumentano in modo netto, passando da 32 a 46 casi (+14): la loro incidenza sul totale cresce di circa +5,8 punti percentuali (dal 21,9% al 27,7%). La Manifattura cresce da 44 a 51 casi (+7), ma la sua quota rimane sostanzialmente stabile (+0,6 punti), a indicare che resta un bersaglio strutturale più che un settore "in accelerazione" relativa.

Il comparto Tecnologico cresce leggermente (da 10 a 12 casi), mentre Food & Beverage aumenta (da 6 a 9). Di segno opposto il Retail, che scende da 14 a 12 casi e riduce la propria incidenza (da 9,6% a 7,2%; circa -2,4 punti).



Questa concentrazione di attacchi su alcuni segmenti specifici suggerisce alcune considerazioni.

- Gli attacchi ransomware diretti prevalentemente verso Manifattura e Servizi professionali possono essere indice di azioni finalizzate a **massimizzare l'impatto dell'attacco**: sistemi produttivi e supply chain possono amplificare gli effetti di una singola interruzione, mentre i servizi professionali tendono a operare su dati sensibili e relazioni fiduciarie (clienti, fornitori, controparti), aumentando i costi indiretti di un incidente.
- Il **livello di digitalizzazione** del settore influisce sulla potenziale esposizione verso possibili attacchi. Allo stesso tempo, è anche verosimile che le aziende che operano in settori ad alta intensità digitale abbiano anche una maggiore consapevolezza rispetto a questo rischio.
- È da tenere in debito conto che alcuni settori siano soggetti a un **livello di regolamentazione** più elevato rispetto ad altri e questo richiede una capacità più strutturata in termini di investimenti, governance e capacità di risposta. Ciò può influire sulla probabilità che un attacco si trasformi in un evento rivendicato o in una pubblicazione di dati.

Se espandiamo il perimetro dell'osservazione a livello globale ed europeo, emergono delle conferme e delle differenze rispetto alla situazione osservata in Italia. Per facilitare il confronto, abbiamo raggruppato i settori in filiere, in modo da ridurre la frammentazione, aggregando attività di settori contigui lungo la catena del valore e/o accomunate da profili simili di operatività, dipendenza digitale e potenziale propagazione dell'impatto[2].

La lettura trasversale conferma che:

- la **filiera Servizi Finanziari & Professionali** è la prima per peso a livello globale e in UE, al secondo posto in Italia. Mediamente quasi 1 evento su 3 si indirizza verso questo target: 30,8% globale, 29,6% UE, 31,3% Italia. Il fatto che le quote siano così vicine suggerisce un pattern relativamente stabile, non legato a una specificità nazionale.
- Altre filiere che presentano profili simili sono **ICT & Media** e **Consumer/Retail/Hospitality**. In questi due ambiti, l'Italia è leggermente sotto la media UE ma relativamente vicina al profilo globale (ICT & Media: 9,6% Italia vs 11,3% UE e 9,9% Globale; Consumer: 12,7% Italia vs 15,9% UE e 13,8% Globale).

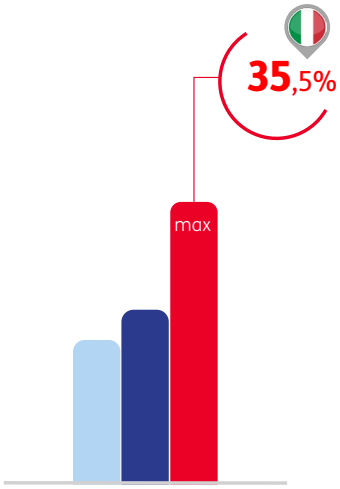
Si individuano invece alcune specificità del nostro contesto rispetto alla situazione europea e globale:

- Poco più di un evento Ransomware su tre in Italia è diretto verso la **filiera Manifattura Avanzata** (35,5%), mentre in altri contesti questa incidenza è più bassa (22% in UE, 18,2% Globale). È invece molto simile, in tutti e tre i contesti, la ripartizione degli attacchi tra i comparti della filiera, con il Manufacturing che è ovunque al di sopra dell'80% dei colpi Ransomware del raggruppamento. In parte, questo è dovuto all'ampio perimetro del comparto, ma vanno considerati anche aspetti tecnico-economici (il fermo ha un costo immediato) e l'elevata esposizione rispetto ad altri settori del raggruppamento, sia in termini di catene di fornitura molto lunghe, sia per la contemporanea presenza di sistemi IT e OT.

2 In questo modo si minimizza anche il rischio che minime differenze tassonomiche tra i diversi contesti possano alterare il confronto.

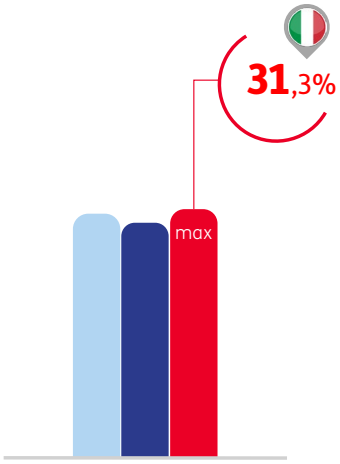
- La **filiera Istituzionale & Sociale** pesa di più nel contesto globale (13,6%) che in UE (9,9%) e in Italia (3,6%). In particolare, a livello globale, è molto più forte l'incidenza del settore Sanità, che invece in UE e in Italia è molto più bassa. È comunque da considerare che in questo raggruppamento, in UE e in Italia, una parte rilevante degli attori è potenzialmente in-scope NIS2. Questo amplia e struttura gli obblighi di gestione del rischio e di segnalazione per entità essenziali e importanti e ciò può tradursi in un innalzamento del livello di prevenzione e incident response.

Ransomware nelle filiere produttive
Confronto Italia, UE, Mondo



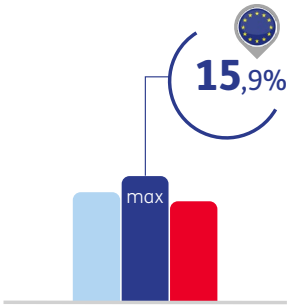
Manifatturiera Avanzata

A livello globale 18% degli eventi ransomware verso questa fileira in Italia 35%, sopra media UE (22%).



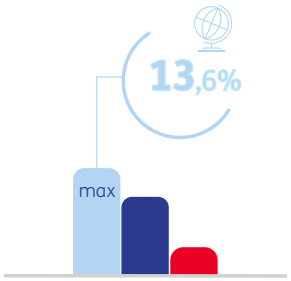
Servizi Finanziari & Professionali

Prima per peso a livello globale e UE (In Italia al 2° posto). Circa 1 evento su 3 verso questo target.



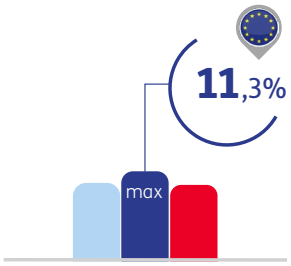
Consumer, Retail & Hospitality

Italia (12,7%) sotto la media UE (15,9%), ma in linea col profilo globale (13,8%).



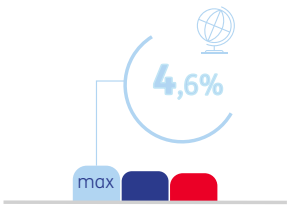
Istituzioni & Sociale

In Italia quota più bassa (3,6%) vs UE (9,9%) e globale (13,6%). A livello globale molto significativo il peso dei ransomware alla sanità



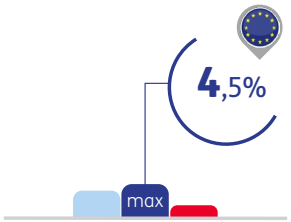
ICT & Media

Profilo molto omogeneo nei tre contesti. Italia 9,6%, sotto la media UE (11,3%) ma in linea con il profilo globale (9,9%),



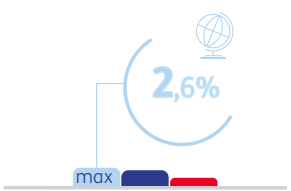
Costruzioni & Infrastrutture

Italia sotto la UE, ma in linea col profilo globale (12,7% Italia vs 15,9% UE e 13,8% Globale).



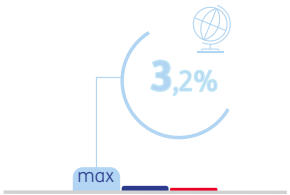
Mobilità, Trasporti & Logistica

In Italia 1,8% dei casi, mentre in UE (4,5%) e a livello globale (3,7%) l'incidenza è più che doppia



Energia & Risorse

Incidenze molto contenute per questa filiera di importanza critica (Italia 1,2%; UE: 2,1%; Globale 2,5%)



Non classificate

Casi ransomware residuali, con rivendicazioni non classificabili in modo certo

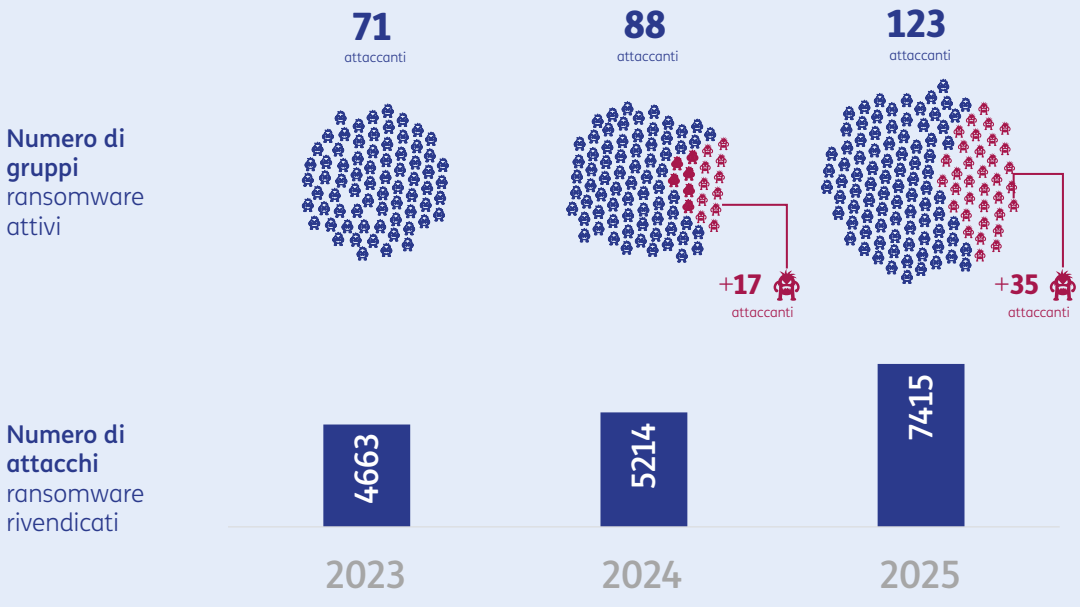
Gli attaccanti

I 7.415 eventi ransomware rivendicati a livello globale sono stati attribuiti a 123 gruppi distinti. In particolare, i più attivi nel corso dell'anno sono stati Qilin (1.034) e Akira (753), seguiti da Cl0p (429), Play (391), SAFEPAY (378) e INC RANSOM (374). Nel triennio 2023 - 2025, i dati mostrano un fenomeno in crescita non solo per numero di eventi, ma anche per numero di attori censiti:

- 2023: 4.663 eventi, 71 attaccanti
- 2024: 5.214 eventi, 88 attaccanti (+12% volumi; +24% attaccanti)
- 2025: 7.415 eventi, 123 attaccanti (+42% volumi; +40% attaccanti)

In altri termini, nel tempo aumenta la platea di gruppi osservati e non solo l'intensità dei gruppi leader. Una possibile interpretazione è la progressiva diffusione del modello RaaS che può abbassare la soglia di ingresso nel cybercrime, contribuendo all'aumento del numero di attaccanti osservati e alla frammentazione dell'ecosistema.

Evoluzione degli attori ransomware
Crescono volumi e numero di gruppi attivi nel triennio 2023-2025



Gli attaccanti più attivi in Italia rispecchiano solo in parte la classifica mondiale per numero di attacchi osservati. I primi due gruppi sono Qilin (30) e Akira (22), seguono Everest (9) e Sarcoma (9), poi LockBit (8) e DragonForce (7) ed infine completano la classifica dei primi dieci gruppi INC RANSOM (6), Lynx (6), Fog (5) e RansomHub (4).

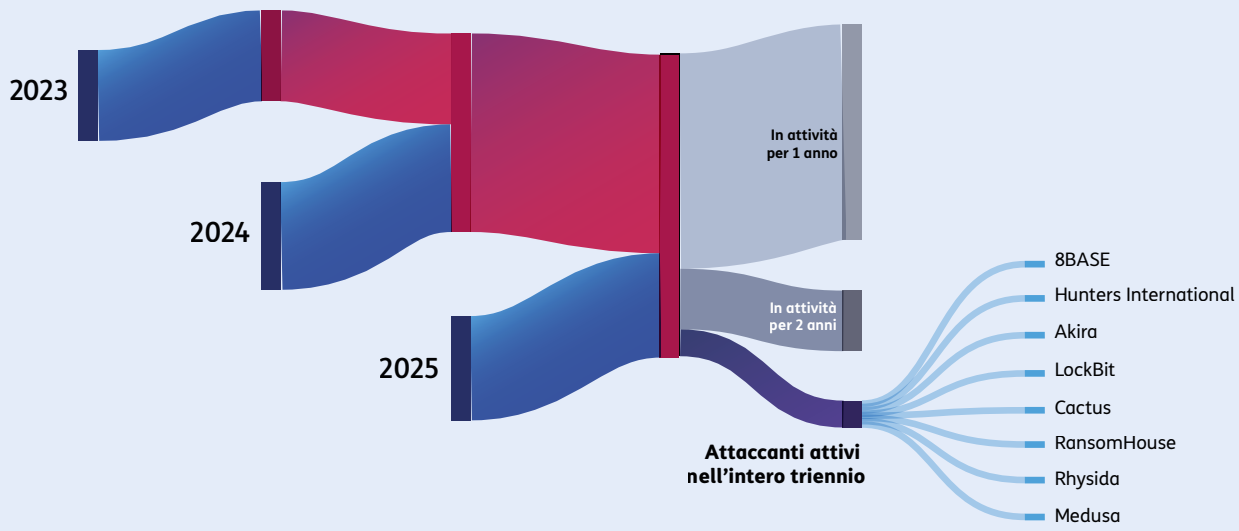
Dei gruppi attivi nel periodo 2023-2025, solo 8 presentano una continuità in tutto il triennio, anche se solo Akira e LockBit entrano nella top 10 del 2025.

In effetti, si assiste a un forte ricambio e questo è coerente con un ecosistema dinamico, in cui l'emergere o il declino di un brand può essere influenzato da rebranding, migrazioni di affiliati e variabilità delle campagne osservate.

Nel più ampio processo di industrializzazione del cybercrime, il ransomware mostra segnali crescenti di convergenza con l'impiego di tecniche di intelligenza artificiale che possono automatizzare la produzione di codice malevolo, le tecniche di adescamento e la costruzione di campagne. Pur non essendo sempre possibile attribuire in modo univoco tali capacità ai singoli gruppi più attivi, il fenomeno segnala una crescente industrializzazione del ransomware, in cui l'AI agisce come moltiplicatore di scala, velocità e accessibilità delle campagne criminali[3].

3 Fonte: AKAMAI, Ransomware Report 2025

Distribuzione degli attaccanti in base all'anno di prima osservazione e alla durata dell'attività



Campagne **Malware**

Una campagna malware è un'azione coordinata finalizzata a **diffondere e attivare software malevolo** su sistemi, reti e dispositivi, sfruttando più canali di distribuzione e famiglie diverse di codice intrusivo (trojan, worm, spyware, ecc.), ciascuna con logiche operative specifiche. Nel 2025 emerge con maggiore evidenza il carattere **trasversale** del malware: non rappresenta solo "l'esito" di un attacco, ma spesso si colloca lungo l'intera catena, abilitando compromissione iniziale, persistenza, controllo remoto e sottrazione di dati.

Nella pratica, queste campagne combinano **vettori tecnici** e **vettori sociali**. Da un lato, continuano a sfruttare vulnerabilità e servizi esposti (in particolare quando riguardano componenti di accesso o perimetro), dall'altro ricorrono a tecniche di ingegneria sociale sempre più efficaci, che possono indurre l'utente a eseguire azioni apparentemente legittime (allegati, link, pagine compromesse o istruzioni ingannevoli). Allo stesso tempo, le osservazioni più recenti confermano che una parte rilevante dell'operatività malware ruota attorno alle infrastrutture di **Command & Control**, necessarie per mantenere comunicazione e controllo sui sistemi compromessi, e all'abuso di credenziali e servizi remoti esposti come leva di accesso e monetizzazione.

Gli obiettivi delle campagne malware possono essere diversi e spesso coesistono nella stessa operazione:

- **acquisire accesso non autorizzato** ai dispositivi e mantenerne il controllo (anche in forma persistente);
- **sottrarre informazioni sensibili** (credenziali, dati finanziari, accessi a servizi);
- **utilizzare i dispositivi compromessi** come piattaforme operative (spam, frodi, ulteriore distribuzione di payload, infrastrutture di supporto);
- **danneggiare o rendere indisponibili dati e file**, fino a scenari estorsivi quando l'infezione si collega a catene di attacco che includono cifratura e richiesta di riscatto.

Queste campagne possono avere una diffusione ampia oppure concentrarsi su specifici target (settori, Paesi, tipologie di utenti). In particolare, nel quadro 2025, si osserva una evoluzione che combina tecniche consolidate e modalità emergenti.

Campagne Malware
Sintesi 2025

194mila

Rilevazioni C2
(Command & Control)

nelle osservazioni malware (H1 2025)

Nel 2025 prevalgono gli attacchi basati sul controllo remoto dei sistemi, definiti Command & Control (framework MITRE ATT&CK). Seguono lo sfruttamento di password rubate e di accessi remoti non protetti, con l'obiettivo di fare profitto.

In crescita nel 2025 i malware di tipo RAT (Remote Access Threat)

Sistemi che abilitano **controllo remoto** e possono fungere da punto di partenza per attività di **esfiltrazione** e per attacchi più complessi.

Il mobile si conferma uno degli ambiti a maggiore crescita per il malware

SpyNote rappresenta

~50%

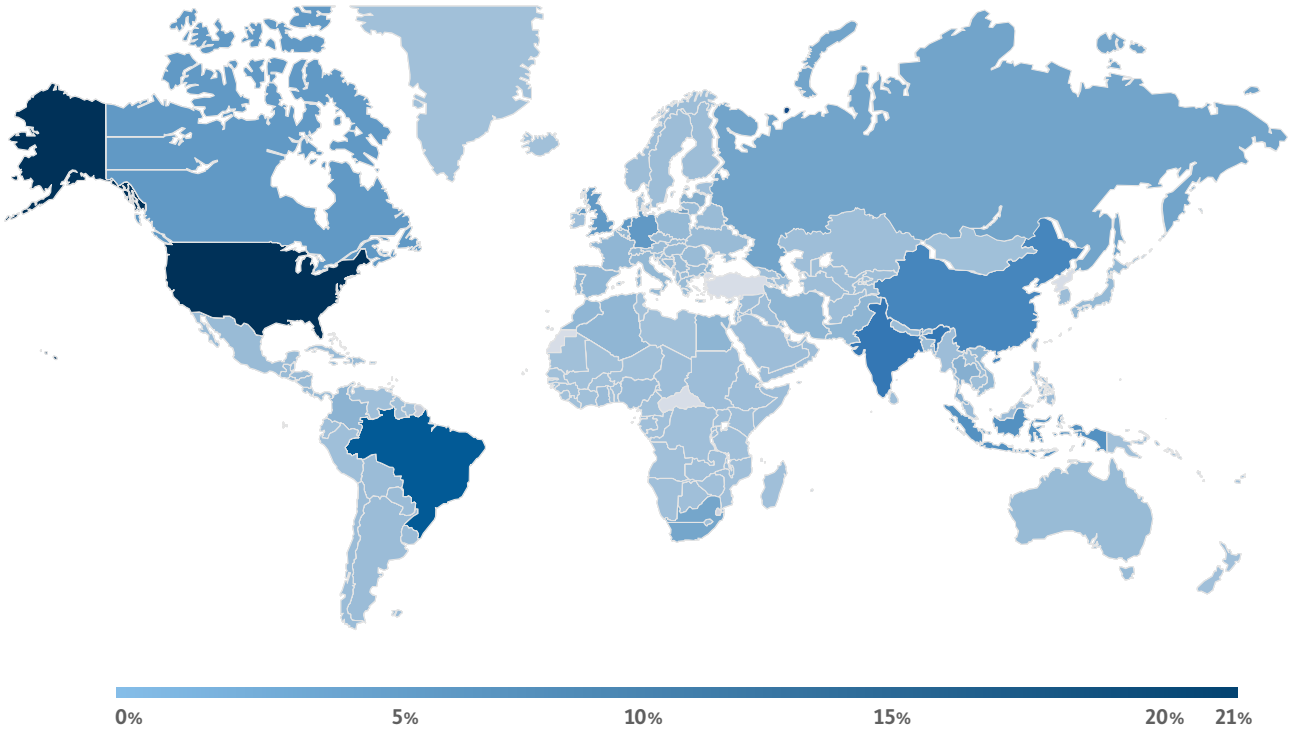
delle evidenze dai principali server C2 mobile

Evoluzione del panorama malware

Le analisi condotte dal team di Threat Intelligence Insikt Group di Recorded Future, utilizzate per sviluppare questa sezione, mostrano che nel 2025 si è verificata un'intensa attività legata a campagne malware.

In particolare, sono stati documentati attacchi malware che hanno coinvolto vittime in circa 200 Paesi, di cui circa l'88% localizzate negli Stati Uniti che rappresentano l'area più colpita.

L'elevato numero di soggetti colpiti negli USA è probabilmente legato all'ampia presenza di strumenti digitali, ma anche all'uso della lingua inglese che è generalmente utilizzata nelle campagne di phishing. A ciò si aggiunge il ruolo del paese come hub infrastrutturale, che fornisce servizi di hosting e digitali a livello globale e lo rende particolarmente esposto.

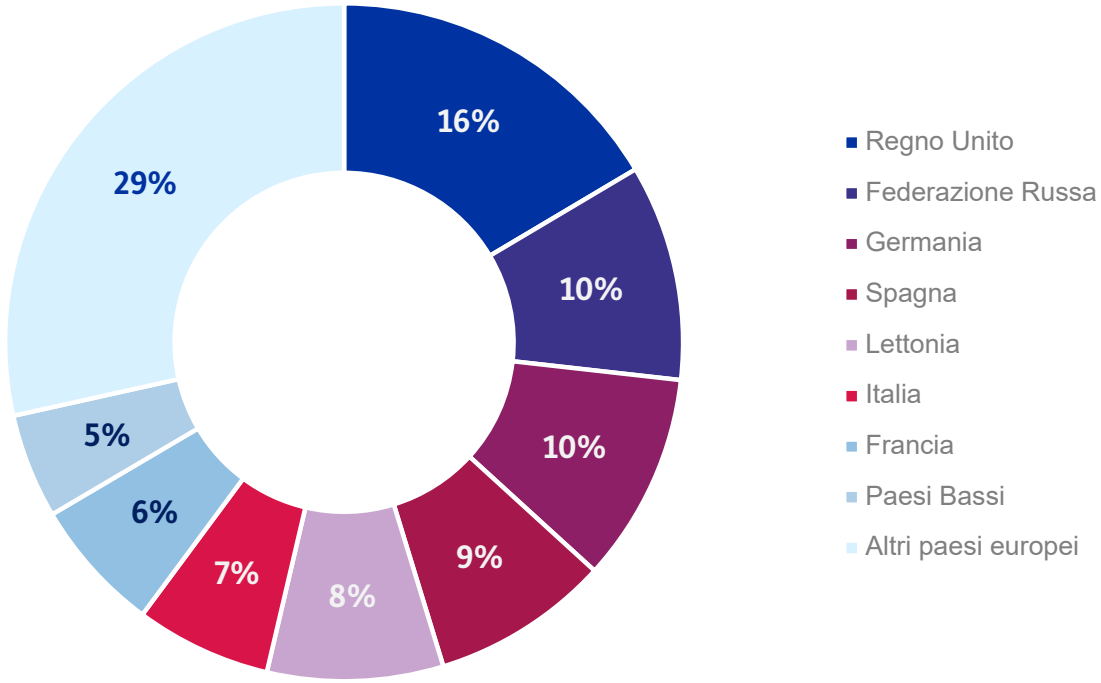


Fonte: Recorded Future - 2025 Year in Review: Malicious Infrastructure

Malware: Italia al 6° posto in Europa (UE ed extra-UE) per numero di casi

Per quanto riguarda i Paesi europei – UE ed extra-UE – la maggior parte delle vittime uniche di campagne malware si concentra nel Regno Unito (16% dei casi totali registrati a livello europeo), seguito da Russia, Germania, Spagna e Lettonia. Segue l'Italia con il 7% dei casi.

Impatto malware nei Paesi europei
% sul totale degli eventi registrati in Europa (UE e extra-UE)

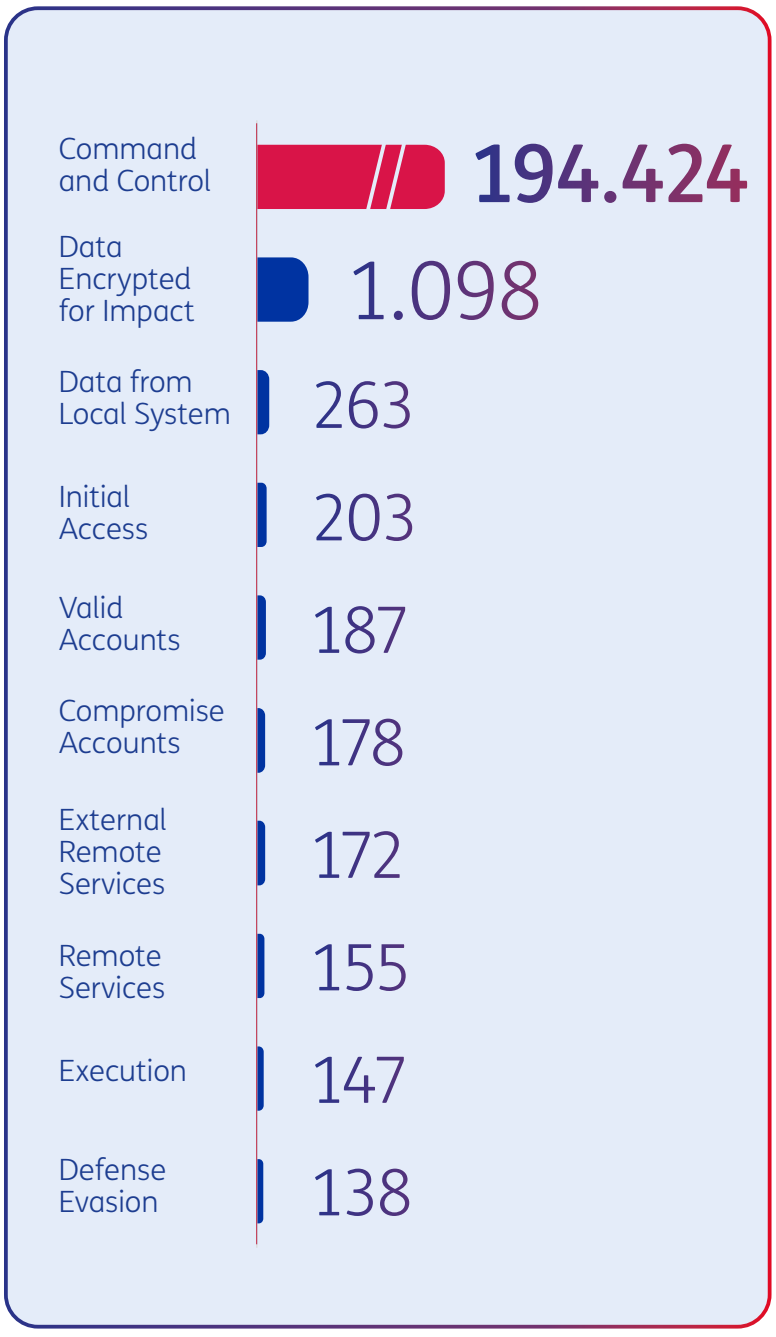


Tecniche di Attacco (TTPs)

L'analisi delle tecniche, tattiche e procedure (TTPs) utilizzate nelle campagne malware della prima metà del 2025 evidenzia un'evoluzione caratterizzata da una combinazione di innovazione tecnica e riutilizzo di strumenti consolidati.

Le osservazioni, analizzate secondo il framework MITRE ATT&CK, mostrano una forte concentrazione su un insieme ristretto di tecniche chiave, utilizzate in modo ricorrente e combinato. Restano centrali le tecniche di Command & Control (C2) con oltre 194 mila rilevazioni osservate. A queste seguono tecniche basate sull'abuso di credenziali valide e sull'utilizzo di servizi remoti esposti, direttamente collegate alla monetizzazione e allo sfruttamento degli accessi.

Top 10 TTP osservate nel primo semestre 2025



La “regia” esterna che permette di controllare i dispositivi compromessi

Il Command and Control (C2) rappresenta l’infrastruttura attraverso cui un attaccante mantiene la comunicazione con i sistemi compromessi. Dopo la compromissione, un dispositivo infetto non agisce come un meccanismo “a programma fisso”, ma rappresenta un punto avanzato nel sistema dal quale è possibile attivare una serie di operazioni. In altri termini, nella maggior parte dei casi, l’operazione richiede un coordinamento dall’esterno poiché l’attaccante deve poter mantenere una comunicazione con il sistema compromesso per inviare comandi, scaricare ulteriori payload, esfiltrare dati e coordinare attività malevole su larga scala. È quindi un indicatore chiave di compromissione attiva ed evidenzia una minaccia persistente.

Focus su ClickFix, una nuova modalità di attacco

Accanto alle tecniche consolidate, si diffondono rapidamente nuove modalità di attacco basate sull’interazione diretta con l’utente. Tra queste, si distingue la tecnica nota come ClickFix, identificata come uno dei principali vettori di accesso iniziale. Si tratta di una tecnica di ingegneria sociale che induce gli utenti a eseguire manualmente comandi malevoli, presentati come operazioni necessarie per risolvere errori o completare verifiche di sicurezza. A differenza degli attacchi tradizionali, non sfrutta vulnerabilità tecniche ma il comportamento dell’utente, rendendo più difficile il rilevamento da parte dei sistemi di sicurezza. ClickFix può operare attraverso due modalità principali:

- inducendo l’utente a copiare ed eseguire manualmente comandi,
- oppure sfruttando meccanismi di clipboard hijacking per automatizzare il processo.

Una volta eseguito il comando, il sistema può essere reindirizzato verso siti legittimi come copertura, mentre in background viene scaricato e installato il malware.

Principali famiglie di malware

Le evidenze basate sulle infrastrutture di Command & Control consentono di identificare le famiglie che mantengono una presenza più stabile e continuativa, poiché legate all'infrastruttura utilizzata dagli attaccanti per "gestire" sistemi compromessi. Queste evidenze non rappresentano necessariamente l'intero spettro delle minacce in circolazione, ma offrono un'indicazione delle infrastrutture più attive nel periodo analizzato.

A questa panoramica si può aggiungere una vista più dinamica, basata sui dati che originano dalla "public sandbox" di Recorded Future, in cui è possibile caricare file o link sospetti per analizzarli in un ambiente separato e sicuro. Chiaramente, i dati costituiscono campioni non rappresentativi in quanto basati solo su quanto viene caricato dalla community, ma esprimono comunque una vista privilegiata sulle evoluzioni quotidiane, molto utile per identificare immediatamente i primi segnali di minacce circolanti.

Le famiglie di Malware più diffuse nelle infrastrutture C2

Il confronto con il 2024 evidenzia cambiamenti significativi nella composizione delle famiglie prevalenti. Sebbene gli infostealer rimangano una componente centrale del panorama delle minacce, in linea con le finalità economiche degli attori malevoli, le specifiche famiglie dominanti risultano mutate.

Alcuni malware precedentemente diffusi, come Vidar, RedLine Stealer e LokiBot, hanno registrato un forte calo, anche a seguito di operazioni di contrasto.

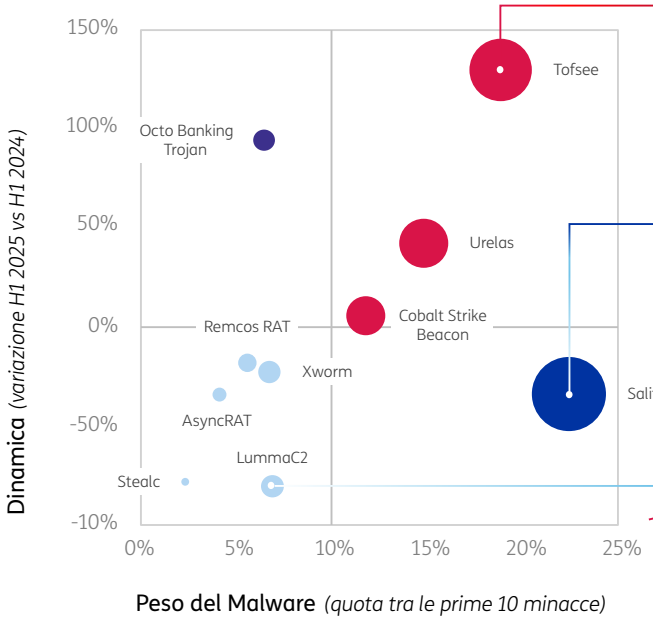
Sality, una botnet polimorfica identificata per la prima volta nel 2003, continua a essere tra le famiglie più rilevate dopo una significativa riemersione nel 2024.

Analogamente, avviene per **Tofsee**, trojan modulare attivo, ossia un malware che si presenta come software legittimo o innocuo – inducendo l'utente a eseguirlo e attivando così il codice malevolo – e che può integrare diversi moduli funzionali per svolgere attività malevole differenti.

Si osserva anche un ridimensionamento di alcune piattaforme malware-as-a-service. In particolare, **LummaC2** ha registrato un calo marcato a seguito di operazioni coordinate che hanno portato al sequestro di oltre 2.300 domini e alla compromissione della sua infrastruttura principale.

I Remote Access Trojan (RAT) stanno diventando sempre più rilevanti. Famiglie come **Remcos**, **AsyncRAT** e **XWorm** rientrano tra le più diffuse, riflettendo l'utilizzo di strumenti accessibili e versatili che consentono il controllo diretto dei sistemi compromessi. Questi malware vengono impiegati sia per attività di esfiltrazione di dati sia come punto di partenza per attacchi più complessi, inclusi quelli ransomware.

Le prime 10 minacce nelle piattaforme C2 (H1 2025)



TOFSEE minaccia in forte crescita (+130%), al secondo posto tra le più diffuse

Trojan modulare attivo
Prima identificazione 2013

SALITY
la più diffusa, in calo (-34%) rispetto al H1 2024

Botnet Polimorfico
Prima identificazione 2003

LUMMAC2
in calo dopo importanti operazioni di contrasto

Infostealer
Prima identificazione 2022

La matrice è una rappresentazione riferita alla sole prime 10 minacce. La rappresentazione coglie solo una parte del totale delle minacce malware

Le prime 10 minacce nella public sandbox di Recorded Future (H1 2025)

Cryptominer	RAT	Stealware	Offensive Security Tool	Botnet
XMRig	njRAT DCRat XWorm AsyncRAT	RedLine LummaC2 Stealc	Cobalt Strike	Mirai

TROJAN BANCARI
Progettato specificatamente per sottrarre credenziali di accesso ed informazioni sensibili relative all'online banking e comprometterne gli account

INFO STEALER
Malware che infettano computer ed apparati per rubare dati o informazioni

LOADER
Progettati per scaricare ed installare software malevoli. Aprono la strada ad altri Malware

RAT
Remote Access Trojan
I Remote Access Trojan o RAT si installano in un computer, in un dispositivo mobile o in un apparato ed aprono un varco che permette a degli attaccanti di poter controllare la macchina infetta a distanza

BOTNET POLIMORFICA
Una botnet è una rete di dispositivi compromessi, controllati da remoto. Si definisce polimorfica quando il malware è in grado di modificarsi rendendo più difficile il rilevamento da parte dei sistemi di sicurezza.

Le famiglie di Malware più diffuse nella public sandbox di Recorded Future

La classifica basata sui file analizzati pubblicamente, più sensibile alle dinamiche di breve periodo, evidenzia una distribuzione differente.

Da gennaio a giugno 2025, **XMRig Miner** è stata la famiglia di malware più segnalata. XMRig Miner è uno strumento di cryptojacking a più fasi, tipicamente distribuito tramite loader o exploit dannosi, che dirotta segretamente le risorse della CPU infetta per creare criptovaluta Monero (XMR) e impiega meccanismi di elusione e persistenza per evitare il rilevamento e massimizzare il tempo di attività.

Nel corso del primo semestre del 2025, **Cobalt Strike**, **njRAT**, **DCRat** e **XWorm** si sono classificati tra i primi cinque per numero di progetti presentati al pubblico di Recorded Future Triage.

Espansione delle minacce su dispositivi mobili

È possibile effettuare un approfondimento specifico sul dominio mobile, che si conferma come uno degli ambiti di maggiore crescita all'interno del panorama malware, a causa della crescente dipendenza dai dispositivi mobili in tutti gli aspetti della vita quotidiana, in particolare per l'uso dei dispositivi per attività in ambito finanziario e aziendale.

Secondo Insikt Group, per quanto riguarda le evidenze che derivano dai principali server C2 di malware per dispositivi mobili, nel 2025 le principali minacce sono:

- **SpyNote**, che è diventato il principale vettore malware, rappresentando circa la metà del volume rilevato a livello di server C2;
- Il trojan bancario **Octo**, che ha registrato un aumento significativo, passando dal 6% nel 2024 al 18% nel 2025, seguito da MoqHao che ha registrato un'impennata simile.

La quota di **Hook** è diminuita drasticamente, passando da oltre il 40% al 14% dei server C2 associati al malware mobile.

Come nel 2024, tutte le prime dieci famiglie di malware mobile per volume C2, ad eccezione di LightSpy, hanno preso di mira dispositivi Android, sottolineando la maggiore esposizione di Android al malware mobile per diversi motivi (quota globale di mercato dominante, un ecosistema di dispositivi più frammentato tra diverse piattaforme hardware e versioni software non sempre aggiornate, la natura open-source del sistema operativo). Questo aumenta la superficie di attacco e facilita la distribuzione di software malevolo.

Tecniche di compromissione e controllo del dispositivo

La diffusione del malware mobile avviene principalmente attraverso tecniche già consolidate, tra cui phishing, download fraudolenti e impersonificazione di applicazioni legittime, come servizi finanziari, browser o piattaforme di streaming. In alcuni casi, le campagne risultano alta-

mente mirate, con malware progettati per colpire specifiche categorie di utenti, come nel caso di campagne che hanno preso di mira personale militare o giornalisti attraverso applicazioni apparentemente legittime.

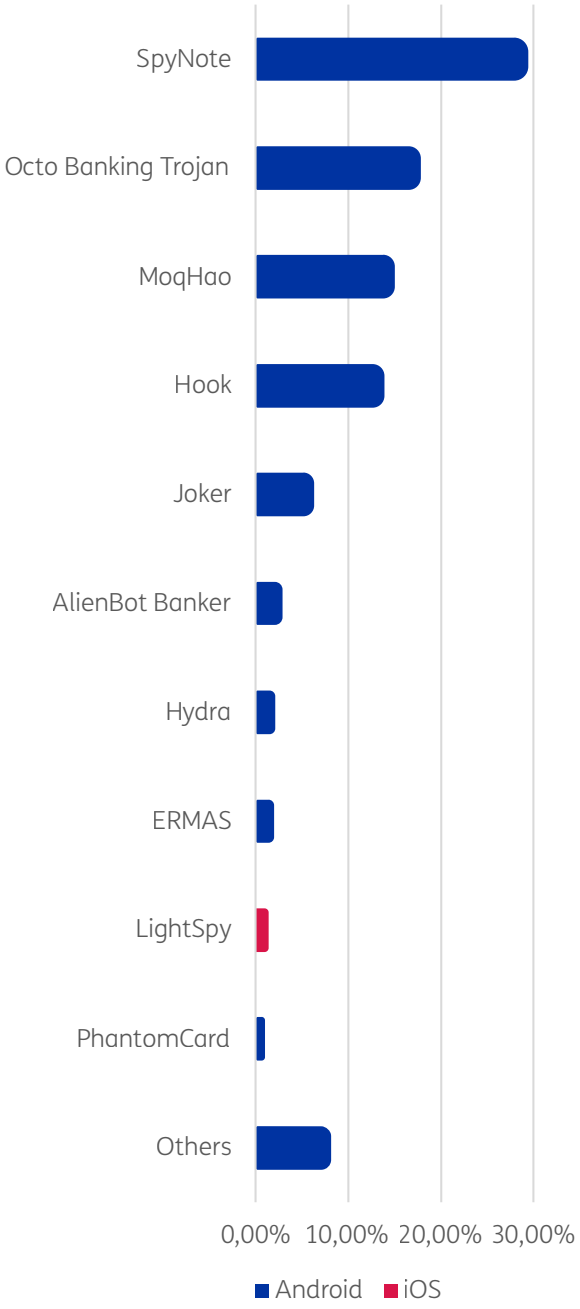
Una volta installato, il malware sfrutta frequentemente funzionalità legittime del sistema operativo per ottenere privilegi elevati. In particolare, l'abuso dei servizi di accessibilità rappresenta una tecnica ricorrente, consentendo agli attaccanti di intercettare notifiche e messaggi, acquisire credenziali tramite overlay e automatizzare operazioni sul dispositivo.

Si osserva inoltre l'uso di tecniche più sofisticate, tra cui l'utilizzo di ambienti virtualizzati, che consentono di eseguire applicazioni clonate, come quelle bancarie, aggirando i meccanismi di rilevamento tradizionali.

Attacchi ai sistemi di pagamento

Gli attacchi ai sistemi di pagamento sono in aumento, in particolare quelli basati su tecnologia contactless. In questo contesto si inserisce SuperCard X, una piattaforma malware-as-a-service progettata per abilitare attacchi basati su NFC. Gli attori

Top 10 malware mobile per attività C2



malevoli rilanciano in tempo reale la comunicazione NFC tra dispositivo della vittima e un terminale sotto il loro controllo, consentendo transazioni fraudolente o altre operazioni non autorizzate. Questo tipo di minacce è in crescita, con casi concreti di frode e perdite economiche, a conferma della loro maturità operativa e del potenziale impatto su larga scala.

Questo scenario richiede un approccio alla difesa multilivello, in grado di rispondere a un panorama malware caratterizzato da tecniche ricorrenti, forte adattabilità e integrazione tra componenti tecniche e ingegneria sociale.

Mitigazioni

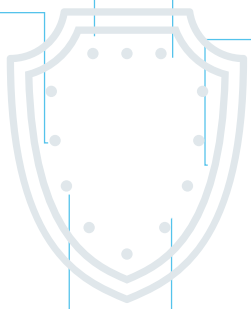
Questo scenario richiede un approccio alla difesa multilivello, in grado di rispondere a un panorama malware caratterizzato da tecniche ricorrenti, forte adattabilità e integrazione tra componenti tecniche e ingegneria sociale.

Rilevamento avanzato
Superare il modello a firme, con **Endpoint Detection Response**, **analisi comportamentale** e **monitoraggio delle comunicazioni C2**

Riduzione superficie d'attacco
Rafforzare l'**autenticazione**, limitare servizi esposti su Internet, **aggiornare** i sistemi e controllare l'esecuzione di **applicazioni e script**

Formazione utenti
Ridurre l'efficacia del **social engineering** e di tecniche come **ClickFix** tramite formazione su messaggi, download e istruzioni sospette

Sicurezza mobile
Proteggere dispositivi aziendali e BYOD: app solo da **fonti affidabili**, controllo dei **permessi sensibili**, update costanti e attenzione ai **servizi di accessibilità**



Protezione e -commerce
Contrastare **Magecart** con **Content Security Policy**, controllo script di terze parti, monitoraggio pagine di pagamento e verifica integrità del codice

Threat intelligence
Integrare feed di threat intelligence per monitorare **IoC** e tecniche emergenti, migliorarando **prevenzione e risposta**

Che cos'è Magecart?

- Le campagne Magecart sono operazioni criminali che prendono di mira i siti di e-commerce per intercettare i dati di pagamento (ad esempio i dati della carta) nel momento in cui l'utente li inserisce durante il checkout.
- Si tratta di attacchi modulari e a più fasi in cui prima il codice malevolo viene introdotto nelle pagine di pagamento per poi intercettare i dati delle carte di pagamento, eludendo i controlli di sicurezza attraverso l'offuscamento e l'abuso di servizi legittimi.

Vulnerabilità

Tutti i componenti hardware o software di un prodotto digitale contengono dei codici, delle istruzioni che ne definiscono il funzionamento e ogni codice può contenere degli errori, dei "bug" di programmazione che – in un contesto di Cyber Security – rappresentano delle falle di sicurezza che un malintenzionato può sfruttare per ottenere accessi non autorizzati o compromettere un sistema. Per far fronte a questo rischio, i produttori rilasciano sistematicamente delle "patch", ossia delle correzioni, da scaricare e installare per risolvere la criticità e mettere in sicurezza il sistema. Questo processo implica che il produttore si accorga del bug, individui il correttivo e pubblichi la patch nella propria pagina ufficiale di sicurezza oppure programmi la correzione negli aggiornamenti periodici del software.

Le vulnerabilità di sicurezza non ancora conosciute dal produttore e dunque neanche pubblicamente, per le quali non esistono ancora patch disponibili, vengono definite vulnerabilità "zero-day" (0day). Il nome fa riferimento al fatto che il produttore ha "zero giorni" per individuare una soluzione nel momento in cui la vulnerabilità diventa nota e sfruttabile anche ai fini di cyber attack.

Campagne vulnerabilità
Sintesi 2025

+20%

aumento delle CVE identificate nel corso del 2025

(CVE: Common Vulnerabilities and Exposures)

Il numero delle CVE note ha raggiunto le 48.448 unità nel 2025. Erano all'incirca 40.300 a fine 2024.
Dal 2022 il numero è pressoché raddoppiato.

Microsoft tra i vendor più colpiti: quasi 3 volte quello degli altri produttori (Apple, ecc.).

Secondo i dati analizzati da Insikt Group, **oltre il 50%** delle attività di sfruttamento attribuite **è state sponsored**

Evoluzione delle vulnerabilità nel 2025

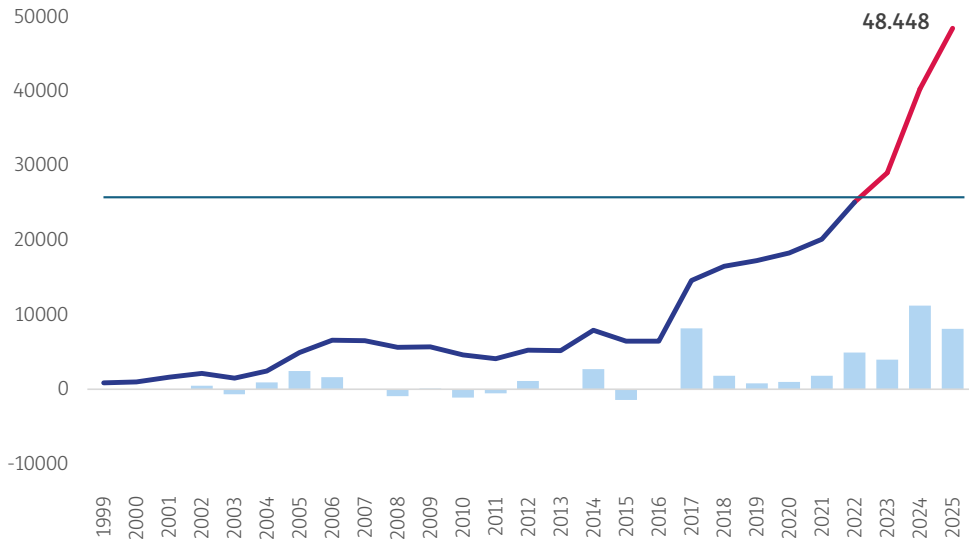
Nel 2025, il quadro delle vulnerabilità note mostra una crescita molto intensa.

A livello complessivo, aumenta la "superficie" di rischio, con quasi 48.500 CVE (Common Vulnerabilities and Exposures) pubblicate, in aumento del 20% rispetto alle circa 40.300 del 2024. Valutando l'incremento delle CVE in semestri, si mette in evidenza un'accelerazione ancora più significativa della dinamica osservata nel 2025. Nel primo semestre 2025 sono state pubblicate 23.667 CVE, con una crescita del 16% rispetto allo stesso periodo dell'anno precedente[4], mentre nella seconda metà del 2025 sono state rilasciate circa 24.780 CVE in aumento del 24% rispetto alle circa 19.920 del secondo semestre 2024. Ne deriva anche che, nel 2025, il fenomeno ha continuato ad espandersi progressivamente per tutto il corso dell'anno a differenza del 2024.

La serie storica delle vulnerabilità mette in evidenza un deciso salto in avanti nell'ultimo triennio, in cui le CVE sono pressoché raddoppiate (erano circa 25.000 nel 2022). L'incremento registrato nel 2025 (+8.140 CVE) segue in ordine di importanza quello del 2024 (+11.242) e si avvicina a quello del 2017 (+8.194) per lungo tempo il record assoluto registrato dal 1999.

4 Recorded Future - CYBER THREAT ANALYSIS: H1 2025 Malware and Vulnerability Trends

Attacchi ransomware per settore in Italia
Distribuzione dei casi osservati nel 2025



Fonte: cvedetails.com

Nella scala di severità delle CVE – che classifica la gravità delle vulnerabilità da un minimo di 0 ad un massimo di 10 - la crescita in valore assoluto dell'ultimo triennio è trainata soprattutto dalle vulnerabilità di criticità media (tra 5 e 7) che incidono per circa il 45% dell'incremento complessivo, mentre quelle ad alto impatto, nella classe 9-10, rappresentano solo il 10% della crescita totale.

Questo andamento suggerisce che l'incremento del numero complessivo di CVE non si traduce automaticamente in un aumento delle vulnerabilità a più alto impatto, ma riflette piuttosto un ampliamento della superficie di attacco all'interno della quale le vulnerabilità più critiche risultano meno rappresentate nella disclosure pubblica.

CVE e concetto di vulnerabilità

Il programma CVE (Common Vulnerabilities and Exposures) nasce per dare un'identità univoca alle vulnerabilità e collegarle a versioni specifiche di software e componenti (ad esempio software e librerie condivise), così che più soggetti possano riferirsi alla stessa falla in modo coerente tramite un CVE ID.

Non tutte le vulnerabilità ottengono un identificativo CVE. Affinché una vulnerabilità venga registrata come CVE, è necessario che sia divulgata pubblicamente e che venga assegnato un identificativo da parte di una CNA (CVE Numbering Authority), secondo le regole previste per la gestione delle CVE. Inoltre, il prodotto vulnerabile deve essere "customer-installable" o pubblico (ad esempio open source). Servizi online proprietari o infrastrutture SaaS generalmente non ottengono CVE perché il cliente non installa il codice.

Nel perimetro CVE, una vulnerabilità è una debolezza nella logica computazionale (codice) presente in componenti software o hardware che, se sfruttata, produce un impatto negativo su confidenzialità, integrità o disponibilità; la mitigazione avviene di norma con modifiche al codice, ma può includere anche cambiamenti o deprecazioni di specifiche e funzionalità (fino alla rimozione di protocolli/funzioni coinvolte).

Per descrivere la "gravità" delle vulnerabilità si usa il CVSS (Common Vulnerability Scoring System), che fornisce una misura qualitativa della severità e non una misura diretta del rischio.

CVSS v2.0 e v3.x si basano su tre gruppi di metriche (Base, Temporal, Environmental), mentre CVSS v4.0 adotta una struttura diversa (Base, Threat, Environmental, Supplemental).

Le metriche producono un punteggio numerico da 0 a 10 e una cosiddetta "vector string" che sintetizza i valori utilizzati per derivare lo score.

Questo rende CVSS adatto come standard comune per industrie, organizzazioni e governi che necessitano di valutazioni coerenti, anche per calcolare la severità delle vulnerabilità sui propri sistemi e supportare la priorità degli interventi di remediation.

Sfruttamento delle vulnerabilità: principali tendenze

Per questa sezione vengono utilizzate le informazioni e le analisi elaborate dal team di Threat Intelligence Insikt Group della società Recorded Future.

Le famiglie di Vulnerabilità più diffuse

Nel panorama delle vulnerabilità analizzate, ricorre con maggiore frequenza una famiglia di debolezze tipiche delle applicazioni web: in particolare risultano prevalenti problemi legati a Cross-Site Scripting (CWE-79) e SQL Injection (CWE-89), seguiti da Cross-Site Request Forgery (CWE-352), da categorie più generiche di injection (CWE-74) e da casi di controlli di autorizzazione mancanti o incompleti (Missing Authorization, CWE-862). In altri termini, una parte rilevante delle falle continua a concentrarsi nelle interfacce web, che restano un punto d'ingresso relativamente semplice quando esposte o poco protette.

CWE	Debolezza (famiglia)	Descrizione	Dove colpisce	Effetti tipici
CWE79	**CrossSite Scripting (XSS)**	Vulnerabilità di tipo "injection" nelle applicazioni web.	È una debolezza "classica" delle interfacce web che può trasformare input non fidato in codice eseguibile nel browser dell'utente, permettendo furto di sessione e azioni non autorizzate nel contesto del sito	Furto di sessione, azioni eseguite a nome della vittima, manipolazione contenuti, pivot verso altre frodi.
CWE89	**SQL Injection (SQLi)**	Vulnerabilità di tipo "injection" nelle applicazioni che interrogano n database	Colpisce in particolare le interfacce web/API e i punti in cui l'applicazione passa parametri a query SQL (login, ricerca, filtri, form, funzioni amministrative): il database è spesso un obiettivo privilegiato perché concentra dati sensibili o critici.	Lettura/esfiltrazione dati, bypass autenticazione, modifica/cancellazione informazioni; in alcuni scenari può contribuire a escalation più gravi.

CWE352	**CrossSite Request Forgery (CSRF)**	Vulnerabilità nelle web application in cui il sistema non riesce a verificare se una richiesta è stata voluta davvero dall'utente che la invia. Rientra nella categoria di Richieste "forzate" con sessione attiva.	Colpisce soprattutto le funzioni che modificano lo stato (state-changing) su siti e applicazioni web: cambio email/password, modifiche profilo, autorizzazioni, operazioni dispositive o workflow applicativi. È tipicamente rilevante quando l'app si basa su sessioni/cookie e non distingue tra richiesta legittima e richiesta "forzata" dall'esterno.	Esecuzione di azioni non autorizzate nel contesto dell'utente (es. modifiche impostazioni, operazioni dispositive); se l'utente colpito ha privilegi elevati, l'impatto può estendersi fino alla compromissione di funzionalità amministrative dell'applicazione.
CWE74	**Injection (categoria generica)**	Famiglia "ombrello": input non validato finisce in un interprete/linguaggio (non solo SQL), alterandone l'esecuzione.	Colpisce tutte le situazioni in cui dati provenienti dall'esterno finiscono dentro un interprete o un componente che "parsa" comandi: non solo database SQL, ma anche shell/OS, directory service, parser, template engine, ecc. In altre parole, è rilevante ogni volta che l'app "mescola" dati e comandi e li passa a un componente che li esegue o li interpreta.	Lettura non autorizzata di dati, aggiramento di controlli (bypass), alterazione della logica di esecuzione (fino a modifiche non previste o esecuzione indesiderata), perdita di integrità dei dati; in alcuni casi può aiutare a nascondere attività (azioni poco tracciate).
CWE862	**Missing Authorization**	Debolezza di controllo accessi: l'applicazione non esegue (o non applica) un controllo di autorizzazione quando un attore tenta di accedere a una risorsa o compiere un'azione.	È una debolezza "strutturale": non dipende solo dall'input, ma dal modello di controllo accessi. In pratica, anche se l'utente è autenticato, il sistema non verifica se ha davvero i permessi per quella specifica operazione o per quei dati. Colpisce soprattutto API, endpoint e funzioni applicative che espongono dati o operazioni sensibili (aree amministrative, download di documenti, profili, pratiche/ordini, funzioni di modifica/cancellazione).	Accesso non autorizzato a dati (lettura), modifica/cancellazione di dati, bypass di meccanismi di protezione e, nei casi peggiori, escalation di privilegi (assumere identità/ruoli più elevati) tramite accesso a funzioni riservate.

La persistenza di queste vulnerabilità, in particolare legate a injection e scripting, indica che gli attaccanti cercano opportunità in servizi e applicazioni esposte o poco protette, in cui le interfacce web possono diventare un punto d'ingresso relativamente semplice.

Le Vulnerabilità “in the wild”

Generalmente, la maggior parte delle vulnerabilità viene divulgata senza evidenze pubbliche di sfruttamento. Solo un sottoinsieme più ristretto presenta evidenze di utilizzo in attacchi reali, cioè al di fuori di test e dimostrazioni. Questo tipo di vulnerabilità viene definito in gergo “in the wild” e naturalmente il rischio è estremamente elevato perché l’attacco è già entrato nelle pratiche operative degli attaccanti.

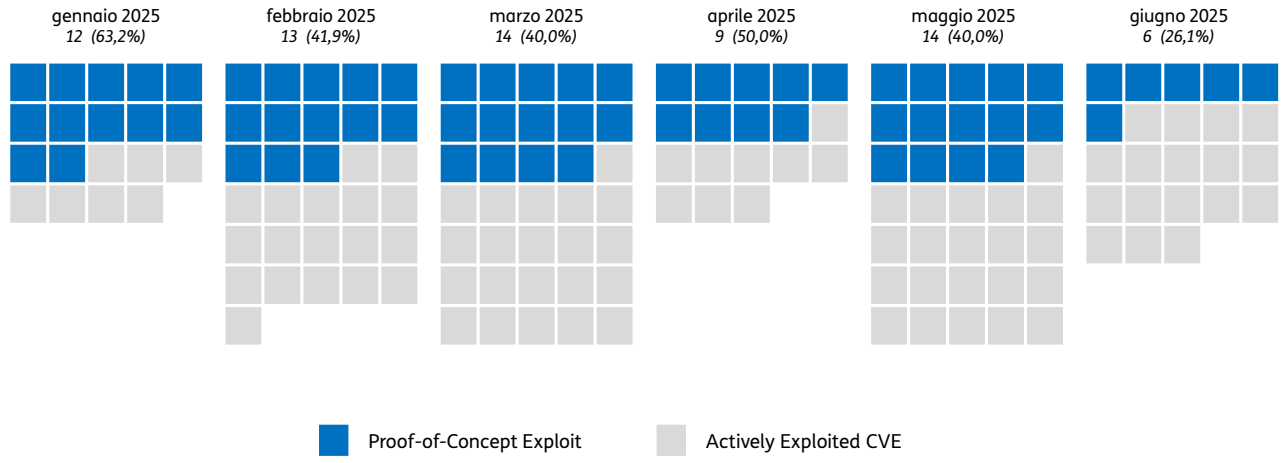
Secondo i dati raccolti dal team di intelligence Insikt Group di Recorded Future[5], nella prima metà del 2025 sono 161 vulnerabilità con CVE utilizzate “in the wild”, superando quanto riportato nei cataloghi ufficiali (secondo CISA KEV[6], nello stesso periodo se ne registrano 136).

Di queste, il 42% presentava una PoC pubblica (Proof of Concept), cioè una dimostrazione pratica che mostra come la vulnerabilità possa essere sfruttata. Nel restante 58% dei casi potrebbe trattarsi di exploit non pubblici, vulnerabilità non ancora divulgate o altre casistiche.

Un elemento di rischio è rappresentato dalla possibilità per gli attaccanti di analizzare la correzione una volta pubblicata, adottando tecniche di reverse engineering per individuare rapidamente il difetto e colpire i sistemi non ancora aggiornati. La tempestività, nella produzione delle patch correttive ma soprattutto nell’installazione, assume quindi un ruolo sempre più cruciale.[7]

5 Recorded Future - CYBER THREAT ANALYSIS: H1 2025 Malware and Vulnerability Trends
6 Catalogo Known Exploited Vulnerabilities dell’agenzia governativa statunitense Cyber Security and Infrastructure Security Agency.
7 KB4830: Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2.4465

Proof-of-Concept exploit e CVE attivamente sfruttate
Distribuzione degli eventi osservati nel primo semestre 2025



Fonte: Recorded Future – Cyber Threat Analysis: H1 2025 Malware and Vulnerability Trends nel primo semestre 2025

Tra le vulnerabilità sfruttate, 111 su 161 (69%) non richiedevano autenticazione, mentre 78 (48%) potevano essere sfruttate da remoto attraverso la rete. Molte di queste vulnerabilità potevano dunque essere sfruttate direttamente da Internet, senza credenziali e senza accesso interno preliminare.

Inoltre, 48 casi (30%) consentivano Remote Code Execution (RCE), cioè l'esecuzione di codice da remoto sul sistema bersaglio, mentre 11 casi (7%) permettevano l'elevazione dei privilegi. I dati mostrano quindi una preferenza per vulnerabilità a basso attrito operativo, che non richiedono autenticazione e consentono l'esecuzione di codice remoto, riducendo tempi e complessità dell'attacco.

Rispetto alla finalità, si osserva che le vulnerabilità sfruttate sono spesso usate per distribuire malware (151 casi) e in un sottoinsieme rilevante risultano collegate a ransomware (73 casi). Il contenuto malevolo distribuito attraverso le vulnerabilità con maggiore frequenza è rappresentato dalle backdoor, cioè meccanismi di accesso nascosto che consentono all'attaccante di mantenere una presenza persistente e tornare successivamente sul sistema compromesso.

I trend globali

A livello globale si evidenzia un trend di crescita: i CVE divulgati aumentano (+16% rispetto a H1 2024) e lo sfruttamento di vulnerabilità con CVE assegnato si conferma una pratica consolidata. I 161 casi osservati nella prima metà del 2025 indicano che la disponibilità di una CVE non rappresenta più una barriera allo sfruttamento, ma spesso ne accelera lo sfruttamento, con un impatto rilevante in termini di malware e ransomware.

Tra i vendor più colpiti, Microsoft rappresenta il caso più evidente: i suoi prodotti spiegano il 17% delle vulnerabilità sfruttate osservate. La sua esposizione è superiore di oltre tre volte rispetto ai successivi vendor più bersagliati (Apple, Ivanti e Linux), un dato che – con ogni probabilità – riflette la diffusione capillare delle piattaforme Microsoft negli ambienti enterprise. Gli attaccanti tendono infatti a privilegiare tecnologie molto diffuse, perché massimizzano il numero potenziale di vittime.

Un'ulteriore tendenza rilevante è la crescente attenzione verso gli strumenti progettati per proteggere le reti. Il 17% delle CVE sfruttate riguardava soluzioni di sicurezza per il perimetro di rete e i punti di accesso, come le VPN SSL, i firewall di nuova generazione (nextgeneration firewall), i gateway di sicurezza (secure gateway) e gli strumenti di gestione remota. La loro posizione lungo il perimetro di rete li rende particolarmente attraenti come punto di ingresso iniziale, perché una loro compromissione può favorire la propagazione successiva verso altri segmenti interni della rete o verso sistemi e servizi collegati a valle, come server applicativi, sistemi di autenticazione e risorse condivise.

Secondo i dati analizzati da Insikt Group, **oltre il 50% delle attività di sfruttamento attribuite è state-sponsored**, con capacità di sfruttamento (o "weaponization") **entro giorni o addirittura ore** dalla disclosure – a conferma del peso strategico che la dimensione offensiva delle vulnerabilità sta assumendo.

Questo elemento segnala non solo motivazioni più ampie rispetto al cybercrime opportunistico, ma anche una capacità elevata di trasformare rapidamente una vulnerabilità nota in strumento operativo.

Il fenomeno delle vulnerabilità “zero-day”

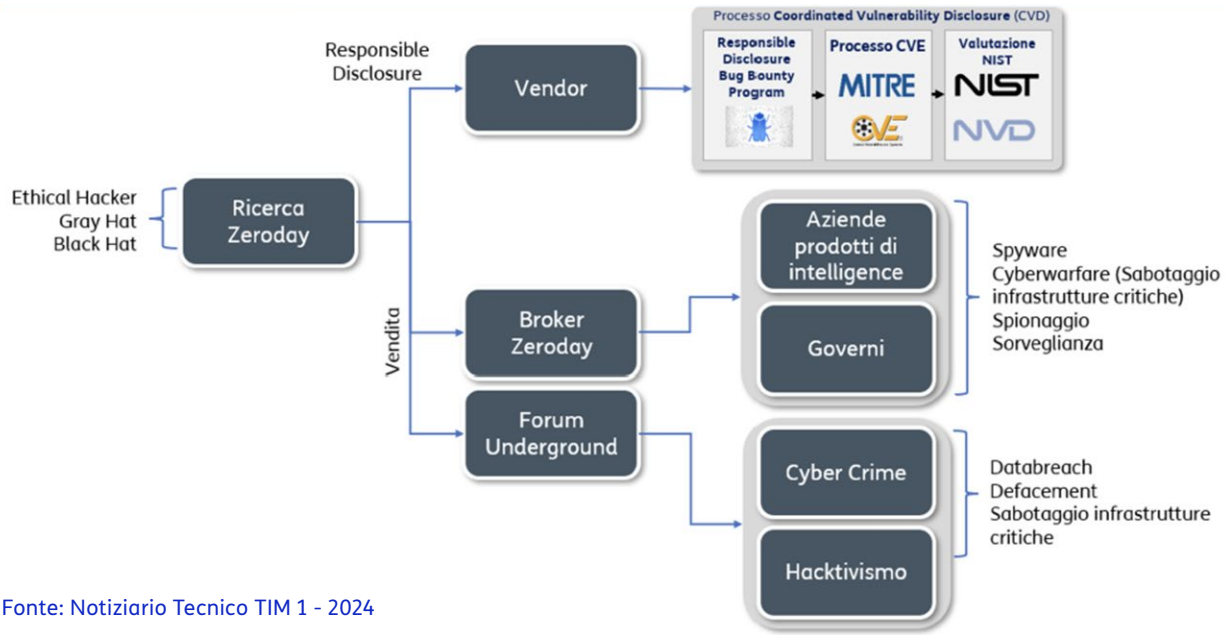
Gli zero-day sono vulnerabilità di sicurezza non ancora conosciute dal vendor e prive di una patch correttiva, che espongono sistemi e dispositivi a rischi immediati. In effetti, finché questa debolezza rimane nell’ombra qualunque sistema che si basa sul software o sull’hardware vulnerabile si trova esposto a chiunque ne scopra l’esistenza.

Se da un lato gli zero-day dovrebbero essere gestiti attraverso processi di divulgazione responsabile, finalizzati alla correzione delle vulnerabilità e alla riduzione del rischio complessivo, nella pratica possono spesso alimentare **canali non pubblici**, nei quali vulnerabilità ed exploit – ossia codici specifici che servono a sfruttare queste debolezze - vengono trattati come risorse strategiche e utilizzati per finalità offensive. In effetti, dal momento che le difese non sono attrezzate per riconoscere un attacco basato su una vulnerabilità non nota, i sistemi sono più esposti ad azioni malevole.

La figura seguente[8] illustra i principali percorsi che uno zero-day può seguire, dalla ricerca iniziale fino agli esiti difensivi o, in alternativa, allo sfruttamento in contesti di cybercrime, sorveglianza e operazioni mirate.

8 Brolli, Massimiliano; Cianfarani, Elenia; Dattola, Andrea Carlo Maria. Il panorama degli zero-day e la ricerca svolta in TIM. Notiziario Tecnico TIM, n. 1–2024 (Cyber Security), 2024. https://www.gruppotim.it/content/dam/gt/notiziario-tecnico/articoli/2024-1/pdf-nt-1-2024/Notiziario-Tecnico-TIM-1-2024-Panorama-Zero-day.pdf

Flusso di gestione di uno zeroday, dalla d divulgazione responsabile alla vendita



Fonte: Notiziario Tecnico TIM 1 - 2024

Esiste un mercato strutturato degli zero-day, nel quale vulnerabilità ed exploit non ancora noti ai vendor vengono trattati come risorse di elevato valore. In effetti, la possibilità di sfruttare le vulnerabilità non ancora note permette ad un malintenzionato di penetrare in sistemi o dispositivi per poi accedere ad informazioni sensibili o pregiate – anche a scopo di spionaggio industriale – nonché di attivarsi per interrompere, ad esempio, un servizio fornito da un'infrastruttura critica.

In questo contesto operano broker specializzati, che agiscono da intermediari tra i ricercatori di sicurezza (bug hunter) e i soggetti interessati all'acquisizione degli exploit. Tali intermediari acquistano vulnerabilità zero-day ed exploit associati, con valutazioni che possono raggiungere anche milioni di dollari, soprattutto nel caso di falle particolarmente critiche o difficili da individuare, come gli zero-day zero-click. Si tratta di attacchi che non richiedono alcuna azione dell'utente (niente click, download, apertura di link o allegati) e che consentono a un attaccante di compromettere un dispositivo o un sistema automaticamente, sfruttando la vulnerabilità senza che la vittima se ne accorga.

Un tema critico: vulnerabilità ad elevata severità (CVSS v3 ≥ 9.8)

Negli ultimi cinque anni, le attività di ricerca interne condotte tramite strumenti e tecniche differenti, hanno portato all'emissione di circa 200 CVE, un segnale della grande capacità del gruppo di intercettare, individuare e portare a evidenza vulnerabilità zero-day. Da questo osservatorio privilegiato emergono delle evidenze di grande interesse sulle dinamiche che stanno caratterizzando questo segmento.

Da un lato, si rileva una **forte crescita degli zero-day**, anche in relazione all'adozione di tecniche di analisi del software supportate da **AI generativa**, che contribuiscono a ridurre i tempi necessari per individuare vulnerabilità e accelerano la finestra utile di sfruttamento prima della disponibilità di una patch.

Allo stesso tempo, il panorama mostra un'evoluzione nella distribuzione della severità: mentre aumentano gli zero-day a **basso impatto**, negli ultimi tempi si osserva una diminuzione delle disclosure pubbliche delle CVE ad **altissimo impatto**. Tale riduzione non è attribuibile a un miglioramento della qualità del software, ma piuttosto a fattori di contesto, tra cui una **minore divulgazione pubblica delle vulnerabilità più critiche** (ad esempio con **CVSS v3 ≥ 9.8**), a fronte di una crescita complessiva del numero di vulnerabilità registrate.[9]

È proprio questa seconda dinamica, la riduzione delle vulnerabilità a più alta criticità, che lascia supporre una **crescente strategicità degli zero-day** nell'ambito dello sviluppo di un **mercato dedicato** a sfruttare queste situazioni ancora non note, in cui vulnerabilità ed exploit vengono trattati come risorse di elevato valore economico. A titolo di esempio, uno zero-day in grado di consentire la compromissione completa di un iPhone può raggiungere un valore di circa 3 milioni di euro, mentre exploit particolarmente rari o potenti, come quelli zero-click, possono arrivare a decine di milioni di dollari.

9 CVE security vulnerability database. Security vulnerabilities, exploits, references and more

Un fattore chiave, nella diminuzione delle disclosure pubbliche degli zero-day ad alto impatto, è rappresentato dall'attività dei broker e dalla diffusione di programmi di "bug bounty" privati, che incentivano la segnalazione riservata delle vulnerabilità attraverso ricompense economiche. Broker pubblici come Crowdfense e Zerodium riportano esempi di "taglie" particolarmente elevate (iOS ~ 5–7 milioni $, Android ~ 5 milioni $, Chrome oneclick full chain ~ 2–3 milioni $), a conferma della crescente competizione su questo mercato.

L'aumento significativo delle ricompense associate agli exploit zero-day riflette una trasformazione profonda del mercato delle vulnerabilità, nel quale il valore delle falle non ancora note ai produttori è cresciuto in modo rilevante nel tempo, attirando l'interesse di una platea sempre più ampia di soggetti.

Attori, Rischi e Implicazioni Strategiche del mercato degli Zero-day

Gli exploit zero-day non vengono acquisiti esclusivamente da attori criminali orientati al profitto, ma anche da governi, agenzie di intelligence e aziende attive nel settore della sorveglianza, per attività di spionaggio, monitoraggio mirato o operazioni cibernetiche di natura strategica. In questi scenari, gli zero-day vengono generalmente sfruttati in modo selettivo, contro target specifici, riducendo la probabilità di intercettazione e di divulgazione pubblica della vulnerabilità. Questo contribuisce a mantenere una parte delle vulnerabilità più critiche al di fuori dei normali circuiti di disclosure, con implicazioni rilevanti per la sicurezza di organizzazioni, infrastrutture e Stati.

L'acquisizione di uno zero-day comporta tuttavia anche un rischio elevato per gli stessi acquirenti, poiché il rilascio di una patch correttiva può avvenire anche a distanza di poche ore, rendendo l'investimento improvvisamente inutile. Questo aspetto spiega perché tali exploit vengano spesso impiegati rapidamente e in modo mirato, prima che la vulnerabilità perda valore operativo.

In questo contesto si inseriscono anche iniziative di operatori emergenti che dichiarano compensi estremamente elevati per strumenti di compromissione avanzata; tuttavia, in alcuni casi permangono incertezze sull'identità degli attori coinvolti e sulla natura dei clienti, rendendo necessaria una valutazione prudente di tali affermazioni.

Possibili evoluzioni

L'evoluzione delle capability AI orientate all'adozione di strumenti nel lavoro quotidiano incide in modo significativo sulla velocità, riducendo i tempi di esecuzione nelle attività ripetitive e multistep. Questa dinamica rafforza il carattere di dual-use delle tecnologie: le stesse capacità che possono migliorare l'efficacia difensiva possono anche facilitare l'automazione di attività malevole. In parallelo, la crescente valenza strategica degli zero-day ne conferma il ruolo di risorse ad alto valore, contese tra difesa, intelligence e mercato, mentre l'ethical hacking resta un elemento chiave per fornire un'analisi concreta che non sempre l'AI è in grado di fornire.

In questo scenario, la gestione delle vulnerabilità si conferma sempre meno come un esercizio puramente tecnico e sempre più come un problema di **tempestività, contesto e governo del rischio.**

Approfondimenti settoriali

Una quota rilevante degli attacchi osservati riguarda il mondo consumer, ma gli episodi più critici e che creano maggiori disagi colpiscono imprese e istituzioni, con impatti operativi, economici e reputazionali. Quando il bersaglio è un ente pubblico o un operatore di servizi essenziali, l'indisponibilità dei sistemi può riflettersi sulla vita quotidiana dei cittadini e, nei casi più critici, coinvolgere profili di interesse per la sicurezza nazionale.

Per questo, in questa sezione, non ci limitiamo a descrivere le minacce, ma proponiamo un'analisi dei dati disponibili nello scenario di osservazione, per comprendere la loro natura e il modo in cui queste possono trasformarsi in impatti concreti sui nostri sistemi economici e sociali.

In altri termini, l'obiettivo delle pagine che seguono è quello di spostare l'ottica dall'osservazione delle minacce alla lettura del rischio.

SECONDA PARTE

Dalle minacce alla lettura del rischio

Nella prima parte di questo rapporto abbiamo ricostruito il "campo di battaglia", osservando quanto e come si sono manifestate le principali minacce cyber nel 2025.

In questa seconda parte ci concentriamo sui settori, partendo da un'evidenza di fondo: la dimensione cyber non è più una variabile tecnica, ma una condizione con cui i contesti economici e sociali devono fare i conti.

Blocchi dell'attività, interruzioni nell'offerta di servizi, perdita di dati, danni reputazionali. Attacchi e intrusioni portano conseguenze operative e organizzative che, in una società sempre più dipendente dal digitale, si propagano rapidamente. Per questo diventa essenziale integrare l'osservazione delle minacce con una "lettura del rischio", individuando i settori che risultano più esposti e sotto pressione. Solo affrontando il rischio in modo consapevole è possibile costruire sistemi sempre più resilienti.

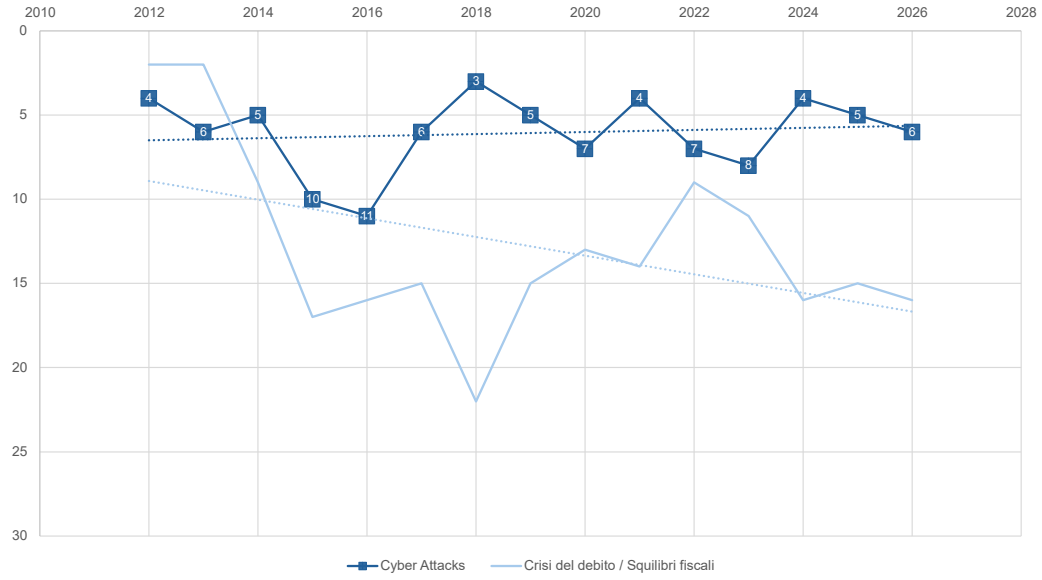
Evidenza #1. Il rischio cyber è sempre più persistente, ma va migliorata la consapevolezza complessiva della società

Da ormai oltre vent'anni il World Economic Forum (WEF) esamina l'evoluzione dei principali rischi globali attraverso il Global Risks Report. L'obiettivo di questo lavoro è quello di esplorare in chiave prospettica i rischi globali che possono manifestarsi in un orizzonte temporale futuro, attraverso un'indagine estesa a esperti e figure influenti di diversi ambiti: dalle istituzioni alle organizzazioni, dall'accademia alla società civile. Nonostante i cambiamenti di struttura e di modalità di lettura del rischio che sono avvenuti nel corso di questo lungo periodo, la serie dei rapporti mantiene un'importanza anche in chiave retrospettiva, permettendo di ricostruire l'evoluzione della percezione dei rischi sistemici e di identificare le minacce che ricorrono tra le priorità dell'agenda globale. Da questa panoramica, **emerge con forza la persistenza del rischio cyber.**

All'inizio degli anni 2010, con gli effetti della crisi del 2008 ancora presenti, gli attacchi informatici erano considerati un rischio emergente. Tuttavia, già allora, per chi osservava con maggiore attenzione, la crescente integrazione tra mondo fisico e digitale iniziava a far emergere i primi segnali di un rischio in consolidamento, con un progressivo aumento dell'esposizione di imprese, istituzioni e infrastrutture alle minacce cyber.

Nel tempo, il rischio cyber ha mantenuto una presenza stabile tra i 10 rischi più avvertiti a medio termine, con la sola eccezione del 2016. Anche nell'ultimo rapporto, in un anno dominato da confronti geoeconomici e conflitti, il rischio cyber si trova al 6° posto nella prospettiva a breve termine (2 anni) e comunque tra i primi 10 sia nella classifica di quelli a impatto immediato (al 9° posto), sia in quella a 10 anni (8° posto).

Gravità relativa dei rischi - Posizione nel ranking



Fonte: World Economic Forum – The Global Risks Report

Uno spunto utile ci proviene dalla classifica per "stakeholders group". Se per il settore privato e per i governi il rischio cyber si posiziona rispettivamente al 4° ed al 5° posto, tra accademia e organizzazioni internazionali scende di qualche posizione (8°) mentre esce dalle prime dieci per la società civile, a conferma del fatto che può risultare meno "visibile", nella percezione quotidiana, da chi non si occupa direttamente della gestione operativa di servizi, infrastrutture e continuità. Questa distanza è rilevante anche sul piano operativo, perché capacità di risposta e resilienza dipendono sempre più dal livello di consapevolezza dei rischi legati all'uso di strumenti e servizi digitali, e non soltanto dall'adozione di norme e misure tecniche.

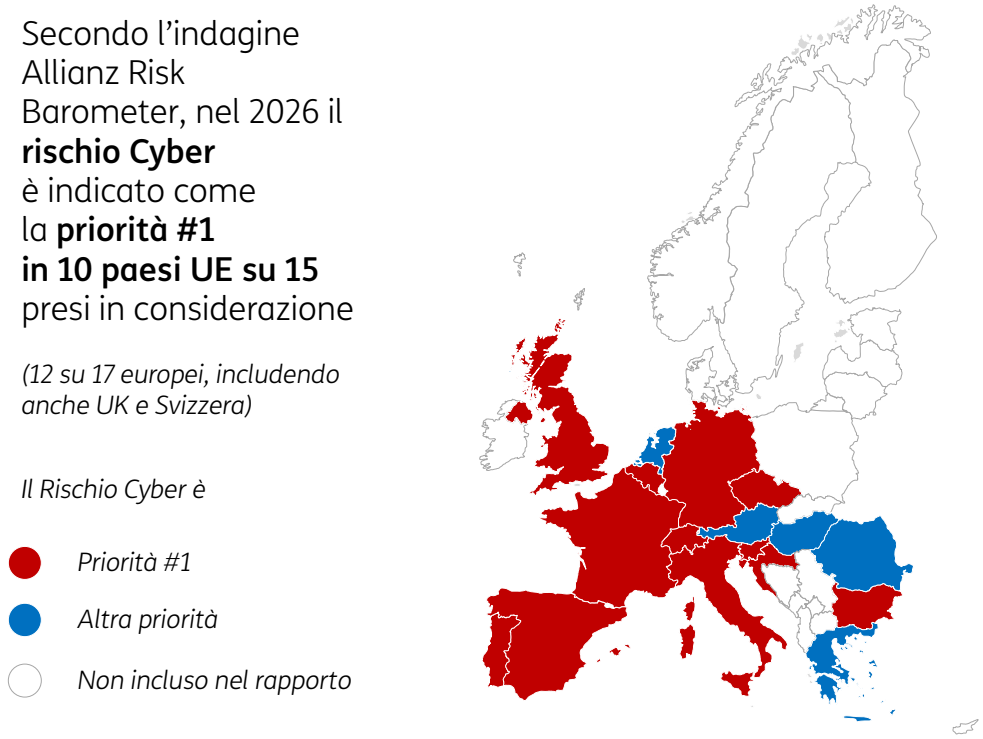
Evidenza#2. Il rischio cyber è sempre più prioritario, soprattutto in UE

Se il Global Risks Report del WEF offre una prospettiva "macro" dei rischi globali, le imprese restituiscono spesso una lettura ancora più netta, perché misurano il rischio su una variabile molto concreta: la continuità operativa. In effetti, gli effetti di un attacco cyber ad un'azienda vengono "misurati" in fermi dell'attività, indisponibilità dei sistemi, perdita di dati e conseguenze legali o reputazionali, aspetti che si impongono rapidamente nella scala delle priorità.

Secondo i dati che possono essere ricavati dall'Allianz Risk Barometer, la percezione dei rischi legati ad attacchi cyber in Italia si è affermata in maniera rilevante e con intensità crescente. Dopo una fase di rapida emersione (dal 23% nel 2017 al 49% nel 2020), dal 2021 il cyber si stabilizza al 1° posto nel ranking nazionale, mantenendo la leadership anche a fronte di oscillazioni nell'intensità percentuale, dovute anche al proliferare delle situazioni che possono mettere a rischio la continuità operativa delle imprese in questo periodo storico. Nonostante tutto, il rischio cyber resta la priorità numero 1 e non solo in Italia. La raccolta di dati mostra che la quota di economie in cui gli incidenti cyber, nel 2026, sono al 1° posto include 10 Paesi UE su 15 (12 su 17 considerando anche UK e Svizzera), mentre erano "solo" la metà nel 2025 (5 Paesi UE su 15). Lo stesso rapporto evidenzia che il cyber è il top global risk per il quinto anno di fila e che è al primo posto in tutte le classi dimensionali (grandi, medie e piccole imprese).

Secondo l'indagine Allianz Risk Barometer, nel 2026 il **rischio Cyber** è indicato come la **priorità #1 in 10 paesi UE su 15** presi in considerazione

(12 su 17 europei, includendo anche UK e Svizzera)



Fonte: elaborazione grafica su dati Allianz Risk Barometer 2026

Evidenza#3. Gli attacchi (ransomware) sono guidati da ragioni di opportunità

Dentro questo quadro, il ransomware rappresenta la minaccia che più di altre rende immediata la visibilità dell'effetto, perché genera un'interruzione dell'attività e impedisce di lavorare, produrre, erogare un servizio, propagandosi sulla filiera. Nel caso delle minacce a doppia o tripla estorsione, con esfiltrazione dei dati e minaccia di diffusione, si accompagna ad un effetto moltiplicatore che aumenta la pressione sul soggetto colpito e amplifica il danno potenziale.

Come abbiamo avuto modo di osservare nella sezione dedicata agli attacchi, anche nel 2025 il ransomware si conferma una minaccia persistente e in accelerazione. I modelli di Ransomware-as-a-Service (RaaS), abbassando la soglia d'ingresso e favorendo la proliferazione di gruppi e varianti, contribuiscono in modo molto significativo a questa crescita osservata, con gruppi che si manifestano in modo episodico e che si affiancano ad altri che restano delle minacce consolidate nel tempo.

Per trovare conferme di questa estrema variabilità, è stata effettuata un'analisi finalizzata a verificare se i gruppi ransomware mostrino pattern di specializzazione settoriale, cioè una tendenza a colpire con maggiore frequenza alcuni ambiti (industrie o istituzioni).

Per farlo, abbiamo costruito una matrice di specializzazione che incrocia *attori ransomware* e settori colpiti e rende confrontabili le relazioni "chi attacca / chi viene colpito". La matrice non si limita a contare gli eventi, ma evidenzia le sovra-rappresentazioni: per ciascuna coppia attore-settore misura quanto l'incidenza osservata si discosti dall'incidenza media di riferimento (baseline) del dataset.

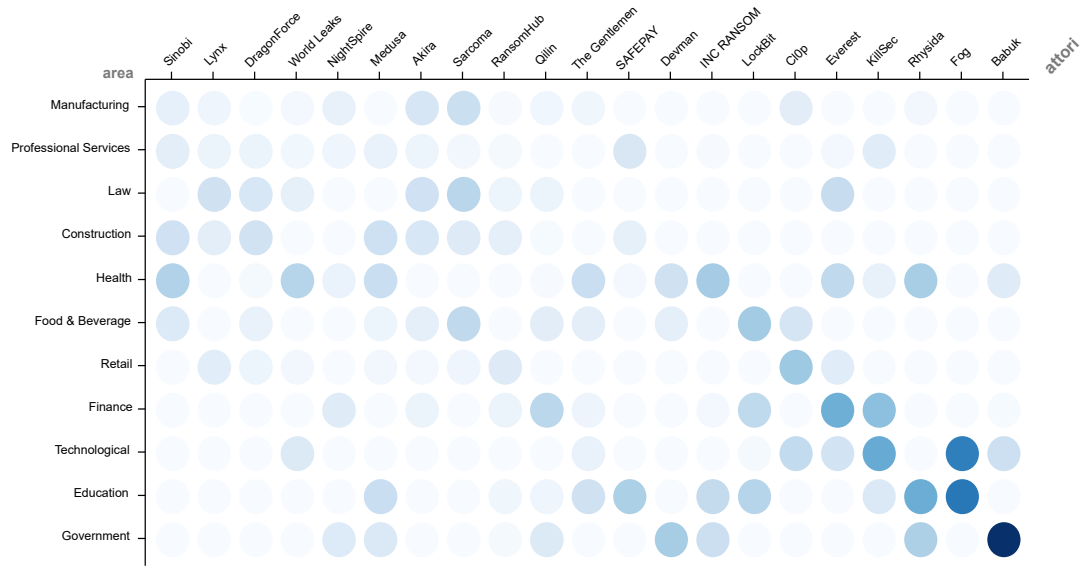
Chiarire se esistano pattern di specializzazione non è un semplice esercizio. Se alcuni gruppi mostrassero una propensione sistematica verso determinati settori, questa ricorrenza diventerebbe un'informazione utile per orientare in anticipo prevenzione e risposta, mentre in assenza di indicazioni la difesa deve puntare su resilienza diffusa e rapidità di risposta[10].

Purtroppo, il quadro che si evidenzia a livello globale mostra che le azioni rivendicate colpiscono ad ampio spettro, senza una specializzazione netta da parte degli attaccanti. Prendendo in esame solo gli attacchi rivendicati nel 2025 dai gruppi più attivi verso i settori più colpiti, il quadro mostra un'elevata dispersione, con solo 2-3 specializzazioni:

- l'accoppiamento tra Government-Babuk, che presenta di gran lunga la maggiore prevalenza nell'insieme osservato;
- la preferenza di Fog verso i settori dell'Istruzione e delle imprese tecnologiche.

10 Va comunque considerato che queste evidenze rappresentano delle semplici indicazioni statistiche, non come attribuzioni deterministiche, poiché nel ransomware strumenti e denominazioni possono essere riutilizzati e cambiare nel tempo.

Matrice Globale degli attori ransomware per settore



I valori esprimono una misura relativa di concentrazione. Colori più scuri esprimono valori > 1 ed indicano che, per quell'attore, il settore è colpito più della media attesa; Colori progressivamente più chiari indicano un comportamento in linea con la media (valori ≈ 1) o sotto-rappresentazione (valori < 1).

Per l'Italia, la verifica di pattern stabili di specializzazione tra gruppi ransomware e settori appare un esercizio delicato perché la numerosità dei casi osservati non consente, né su base annua né sull'intero periodo 2022–2025, di distinguere con sicurezza abbinamenti robusti. Per questo l'analisi è stata ricondotta a una lettura di concentrazione tramite indice HHI, applicata ai soli gruppi con un numero minimo di rivendicazioni e ai settori con un livello sufficiente di rappresentatività[11].

- Sul **lato degli attaccanti, la distribuzione dei valori indica un quadro prevalentemente "generalista":** il 60% dei gruppi presenta un HHI inferiore a 0,3 (in una scala che varia tra 0, comportamento più generalista (bassa concentrazione) e 1, maggiore concentrazione e specializzazione), segnale di un'attività tendenzialmente trasversale più che focalizzata su pochi comparti. Tra i gruppi con comportamento più generalista si collocano LockBit (0,160), Rhysida (0,180), Hunters International (0,184) e RansomHub (0,185). All'estremo opposto, emergono invece casi di maggiore specializzazione settoriale per quattro gruppi che superano la soglia di 0,5: 8BASE (0,680), Everest (0,630), Argonauts Group (0,556) e DragonForce (0,514).

- **Anche guardando ai settori, l'evidenza è di bassa polarizzazione**: i valori oscillano tra 0,08 (Manufacturing) e 0,32 (Construction) e nove settori su dieci restano sotto 0,25. In termini interpretativi, ciò indica che nella maggior parte dei comparti la pressione ransomware è distribuita fra più gruppi, senza una dominanza netta. L'unica eccezione è il settore Construction, dove la concentrazione risulta più elevata.

11 Escludendo attaccanti attivi sporadicamente e settori con un numero di attacchi inferiori alla soglia, sono stati censiti e analizzati il 57% del totale degli eventi ransomware rivendicati nel periodo di osservazione 2022-2025.

L’esposizione dei settori

Una vista d’insieme

Le tre evidenze convergono su un punto: il rischio cyber è strutturale e prioritario, ma la dinamica degli attacchi – soprattutto ransomware – resta in larga misura opportunistica, quindi non sempre prevedibile per “traiettorie” stabili. Per questo, dopo la cornice generale, il rapporto concentra l’analisi su un numero limitato di settori chiave, selezionati in base alla pressione osservata e al potenziale di impatto (continuità operativa, dati, effetti di filiera). Monitorare un settore e confrontarlo con altri aiuta a individuare l’andamento degli attacchi nel tempo. Si può rilevare una differenza tra dati nazionali e internazionali, che nei settori più esposti indica debolezza o, al contrario, un livello maggiore di protezione rispetto alla media globale.

Nella scheda di sintesi riportiamo le informazioni rilevanti per ciascuno dei settori esaminati in merito alle tipologie di attacco DDoS e Ransomware osservate nella prima parte del rapporto.

LE SCHEDE SETTORE

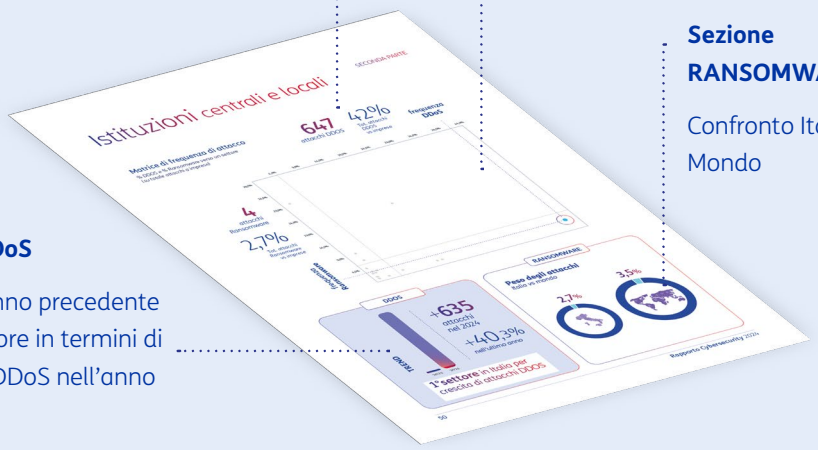
Le schede settore sono ripartite in quattro sezioni: una più generale di sintesi, una dedicata al DDoS, una al Ransomware e una vista d’insieme sulle frequenza d’attacco

VOLUMI TOTALI

Numero di attacchi di tipo DDoS e Ransomware

MATRICE frequenza d’attacco

Posizionamento del settore rispetto alle minacce DDoS e Ransomware



Sezione RANSOMWARE

Confronto Italia vs Mondo

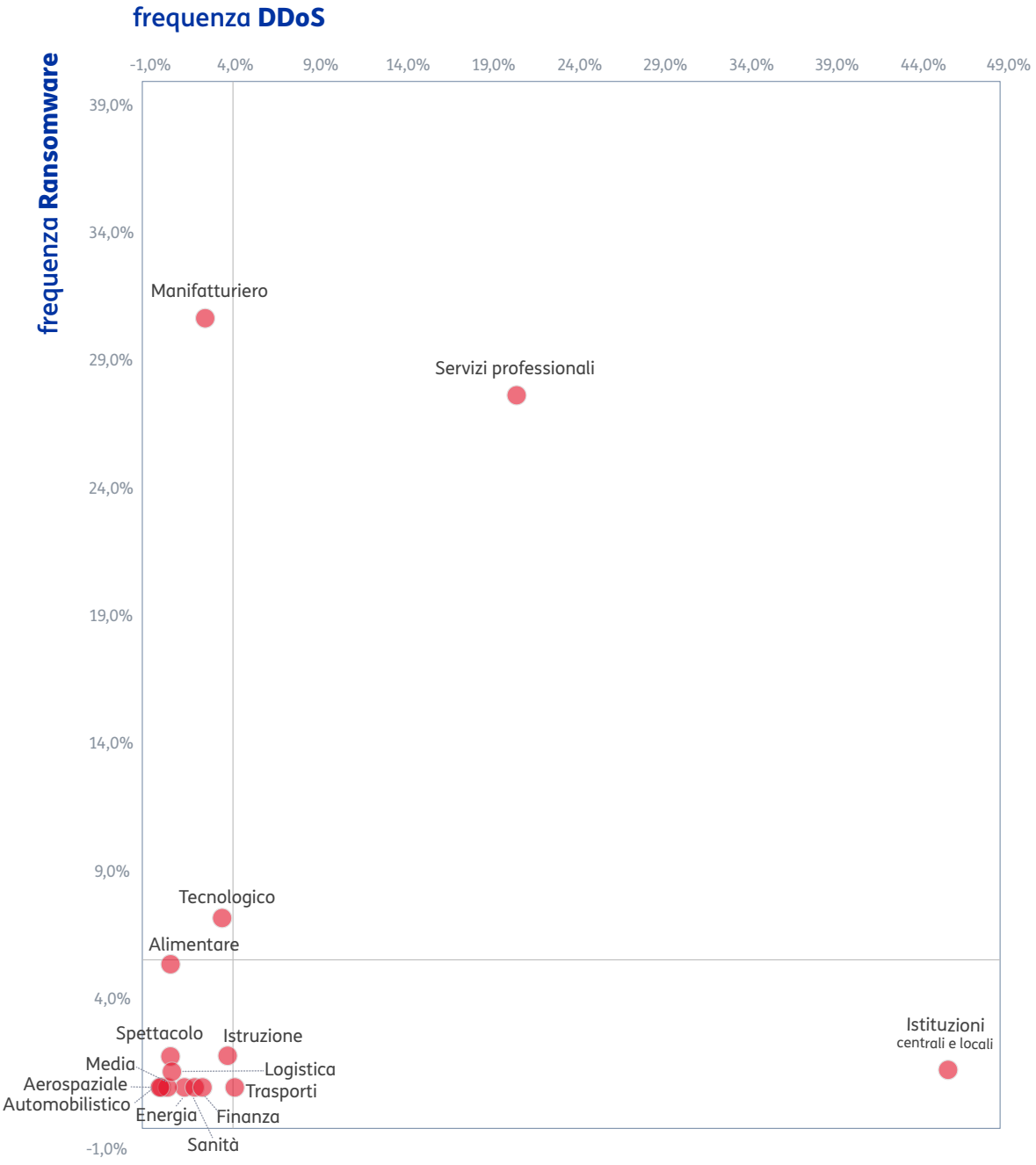
Sezione ATTACCHI DDoS

Andamento attacchi vs anno precedente e posizionamento del settore in termini di variazione degli attacchi DDoS nell’anno

Il peso degli attacchi in **tutti i settori** monitorati

Matrice di frequenza di attacco

DDoS e Ransomware verso un settore
(quota % su totale attacchi a imprese)



Istituzioni centrali e locali

Matrice di frequenza di attacco

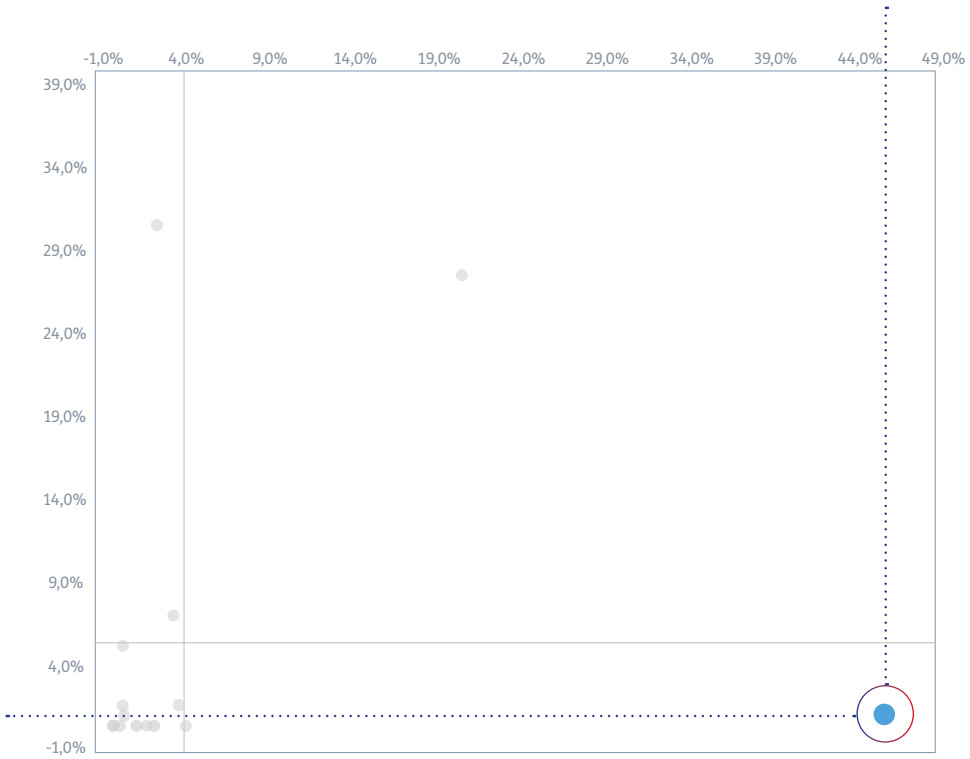
DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

565 *eventi DDoS*

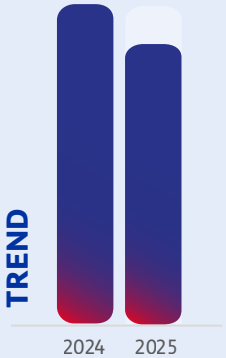
46% *degli eventi DDoS vs imprese*

2 *attacchi Ransomware*

1,3% *degli attacchi Ransomware vs imprese*



DDOS



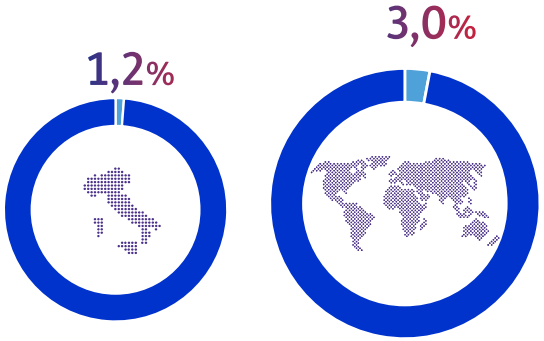
-82 *eventi nel 2025*

-12,7% *nell'ultimo anno*

1°settore in Italia in valore assoluto, ma con un'importante **riduzione degli eventi DDoS registrati**

RANSOMWARE

Peso degli attacchi
Italia vs mondo



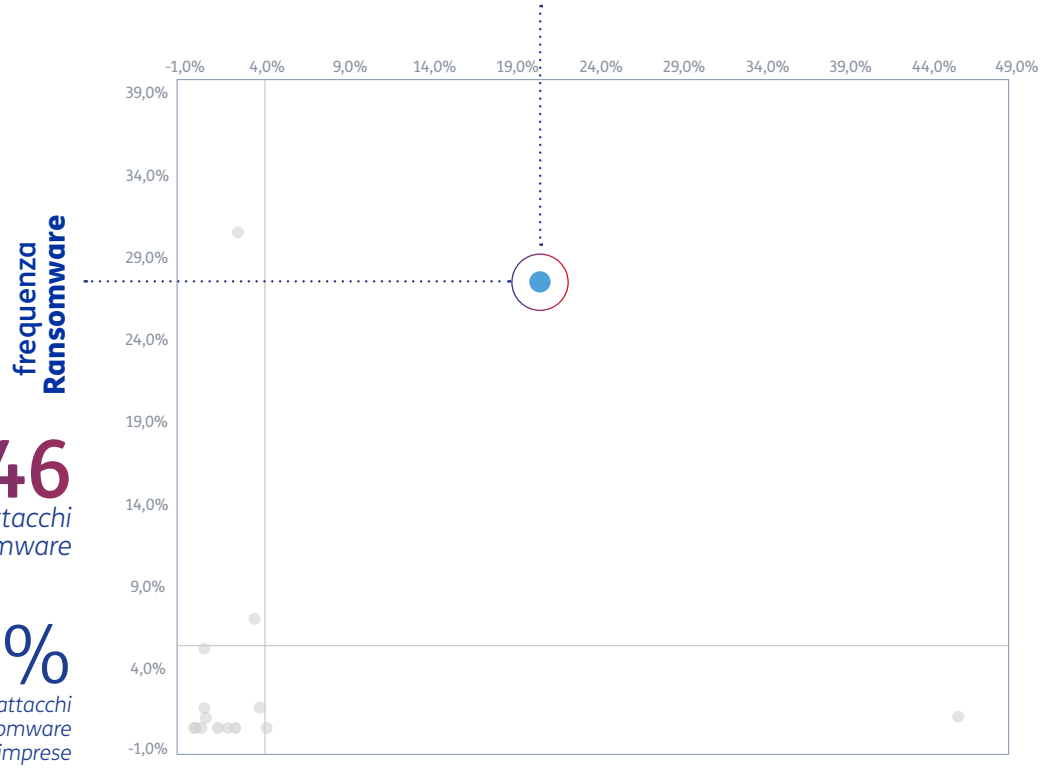
Servizi professionali

Matrice di frequenza di attacco

DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

256 *eventi DDoS*

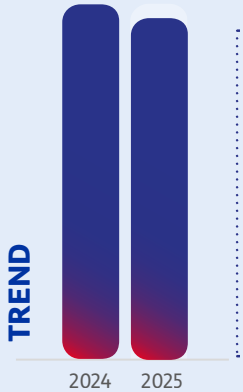
21% *degli eventi DDoS vs imprese*



46 *attacchi Ransomware*

30,5% *degli attacchi Ransomware vs imprese*

DDOS



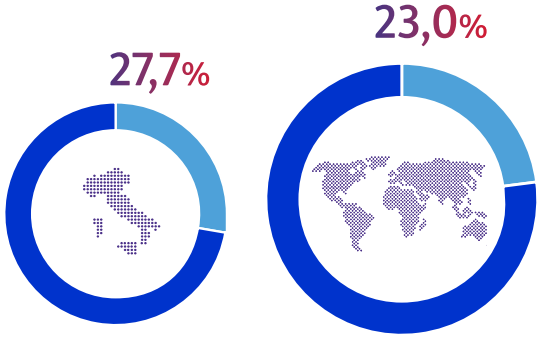
-11 *eventi nel 2025*

-4,1% *nell'ultimo anno*

Eventi DDoS **in linea** con quelli tracciati nell'anno precedente

RANSOMWARE

Peso degli attacchi
Italia vs mondo



Settore tecnologico

Matrice di frequenza di attacco

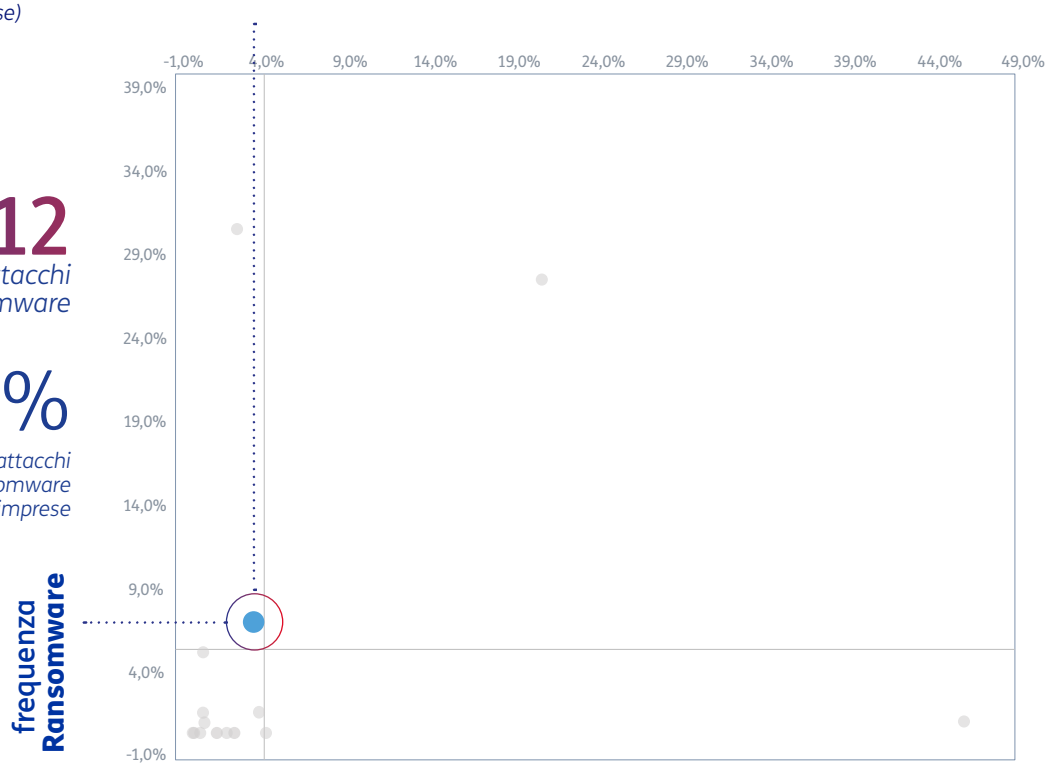
DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

45 *eventi DDoS*

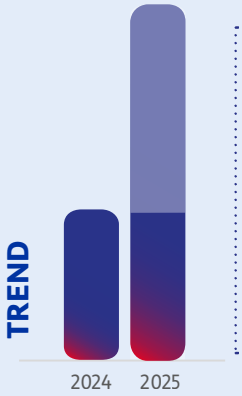
3,7% *degli eventi DDoS vs imprese*

12 *attacchi Ransomware*

8% *degli attacchi Ransomware vs imprese*



DDOS



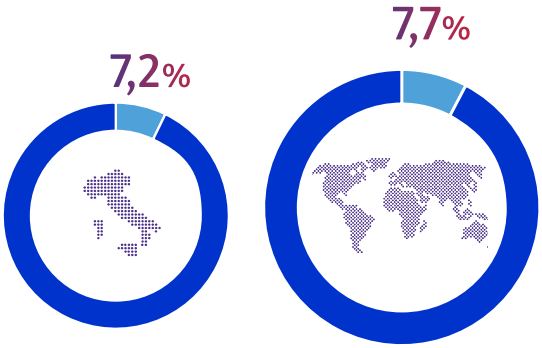
+26 *eventi nel 2025*

+137% *nell'ultimo anno*

Nella **TOP 5** in Italia per crescita di eventi DDoS

RANSOMWARE

Peso degli attacchi
Italia vs mondo



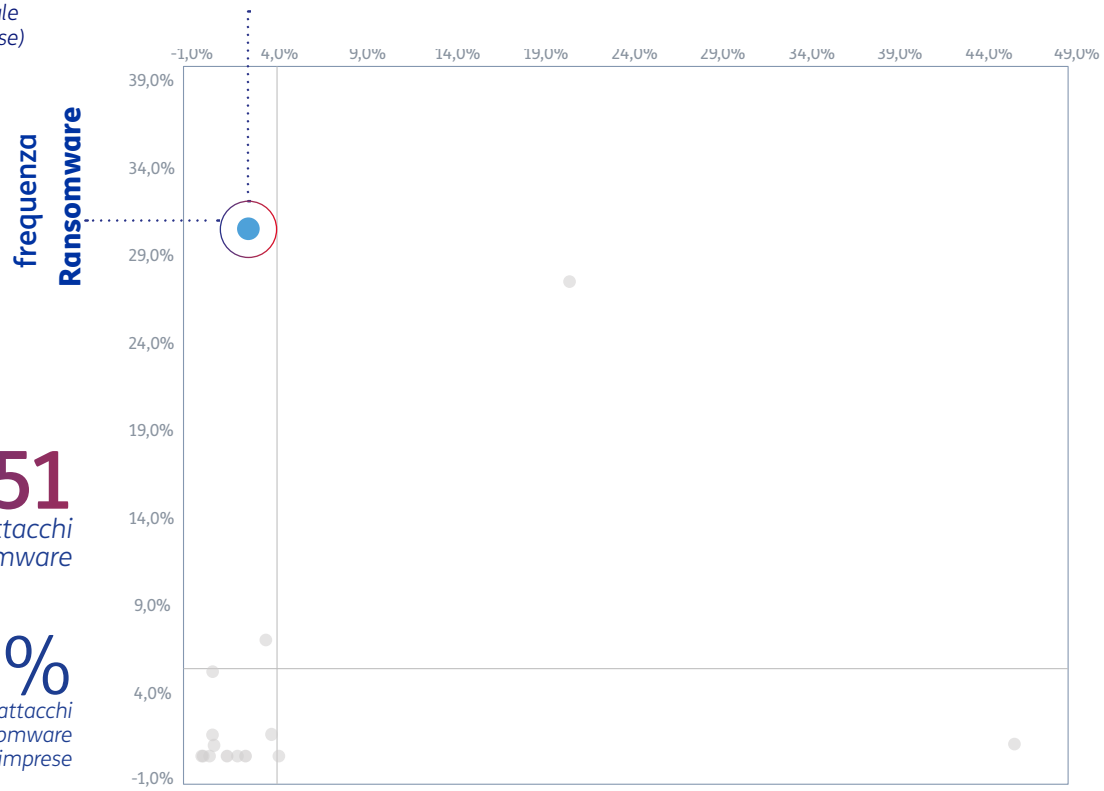
Manifatturiero

Matrice di frequenza di attacco

DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

33 *eventi DDoS*

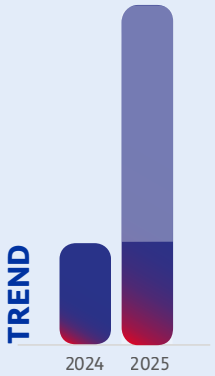
2,7% *degli eventi DDoS vs imprese*



51 *attacchi Ransomware*

34% *degli attacchi Ransomware vs imprese*

DDOS



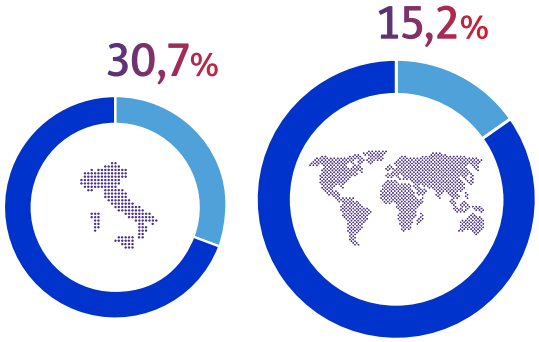
+23 *eventi nel 2025*

+230% *nell'ultimo anno*

3° settore in Italia per crescita di eventi DDoS nell'ultimo anno

RANSOMWARE

Peso degli attacchi
Italia vs mondo



Sanità

Matrice di frequenza di attacco

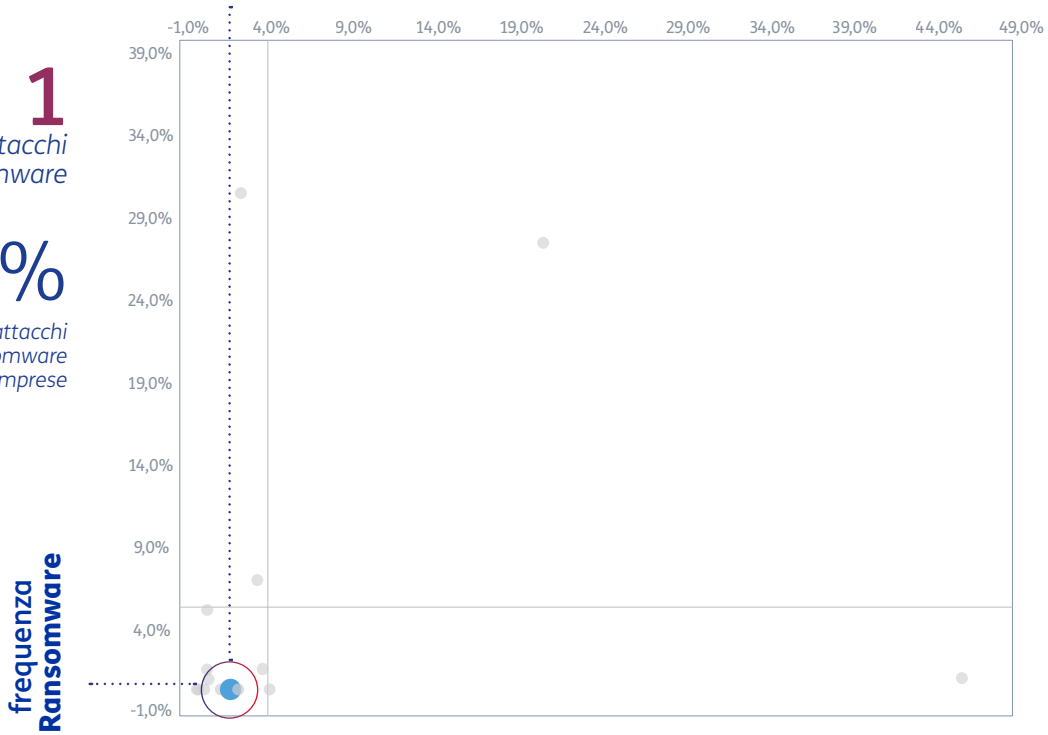
DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

26 *eventi DDoS*

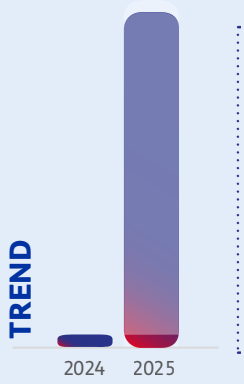
2,1% *degli eventi DDoS vs imprese*

1 *attacchi Ransomware*

0,7% *degli attacchi Ransomware vs imprese*



DDOS

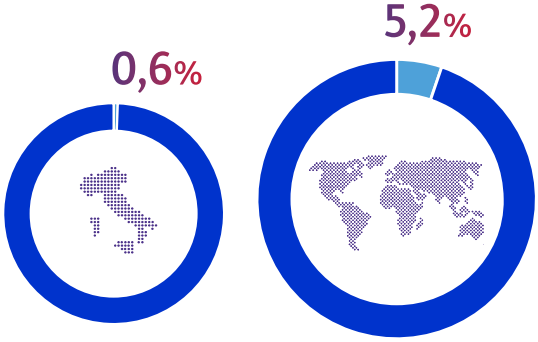


x26 *rispetto al 2024*

1°settore in Italia per crescita di eventi DDoS nell'ultimo anno

RANSOMWARE

Peso degli attacchi
Italia vs mondo



Elementi normativi

In una società sempre più dipendente dal digitale, gli effetti di incidenti cyber non restano confinati al bersaglio, ma si propagano rapidamente lungo servizi e filiere. Il tema cessa quindi di essere individuale, legato alla singola impresa o ambito produttivo, e diventa sistemico. Un fattore che – come osservato – è persistente, prioritario e poco prevedibile. Colpisce senza direttrici prestabilite, cambiando spesso forma, modalità ed obiettivi, e diventa più efficace proprio quando le conseguenze aumentano la pressione, amplificandosi nei contesti economici e sociali.

Se il rischio è sistemico non si può governare solo con più tecnologia o con misure episodiche. Si governa con regole, processi e responsabilità. È esattamente qui che si innesta la logica delle normative europee, che non sono pensate per sostituire le strategie delle singole organizzazioni, ma per costruire un livello comune di resilienza, definendo standard e obblighi che rendono più omogenea la capacità di prevenzione e risposta nei settori più esposti e, più in generale, lungo l'infrastruttura digitale su cui poggia la vita economica e istituzionale.

Dopo aver spostato il punto di osservazione dalle minacce alla lettura del rischio, il passo successivo che viene proposto in questa terza parte è quello di capire quali strumenti di governance vengono messi in campo per ridurre la fragilità del sistema nel suo complesso e qual è lo stato di evoluzione delle normative.

TERZA PARTE

Il governo di un rischio sistemico

Negli ultimi anni, l'Unione europea ha progressivamente esteso l'attenzione alla Cyber Security, adottando una prospettiva più ampia. Procedure e requisiti per assicurare una maggiore tenuta del tessuto produttivo e la continuità dei servizi, l'affidabilità delle infrastrutture critiche, la progressiva riduzione delle dipendenze critiche sono diventati elementi centrali nella visione strategica dell'Unione europea.

L'obiettivo principale di questa visione è quello di rafforzare sia la capacità di prevenzione, sia la resilienza nel lungo periodo attraverso una copertura "end-to-end", che possa individuare e intervenire preventivamente sui punti critici del sistema: dispositivi, infrastrutture critiche, servizi essenziali, catene di fornitura, cloud e gestione dei dati.

Il controllo di tutti questi ambiti, così differenti tra di loro, richiede però:

- Una **distribuzione chiara delle responsabilità**. La resilienza non può essere assicurata con un approccio centralizzato, ma occorre il coinvolgimento coordinato di tutti gli attori interessati. Questo implica una definizione chiara dei compiti, degli oneri, delle capacità di risposta e dei tempi in cui bisogna agire.
- Una **lettura olistica del rischio**. La copertura end-to-end funziona solo se, seguendo l'intero percorso del rischio, si riduce gradualmente la superficie esposta e si costruiscono capacità operative di rilevazione preventiva, mitigazione e recupero rapido dopo un incidente in tutti gli ambiti interessati.
- Un **quadro coerente e comparabile tra tutti i Paesi europei**. Se settori e Paesi adottano criteri non allineati tra loro, il sistema di protezione si indebolisce e diventa difficile "fare sistema". La frammentazione, infatti, moltiplica i punti deboli e aumenta l'esposizione complessiva.

La vasta produzione normativa collegata a questo processo e la stratificazione di atti e provvedimenti su questo tema rischia di aumentare l'entropia del sistema.

Un aspetto particolarmente delicato in un contesto che invece richiede un'architettura completa e articolata che dia la possibilità di governare il rischio Cyber Security a livello europeo attraverso standard e obblighi comuni. Solo in questo modo è infatti possibile allineare e omogeneizzare gli assetti di prevenzione, difesa e risposta dei diversi Paesi Membri, nonché di costruire infrastrutture di gestione capaci di interagire e cooperare in modo efficace. Questo sta spingendo le istituzioni europee a individuare degli assi di intervento che possano portare ad una semplificazione ed una responsabilizzazione di tutti gli attori.

Da un punto di vista estremamente schematico, semplificando le numerose interrelazioni tra i diversi atti e disposizioni adottati nel tempo, il quadro regolamentare europeo della Cyber Security può essere letto come una mappa a più livelli.

Un primo blocco riguarda le regole che disciplinano organizzazioni e servizi, ossia i soggetti chiamati a garantire la resilienza operativa nei settori esposti. In questo ambito, la normativa di riferimento è la NIS2 (Network and Information Systems Directive), che punta a costruire un quadro di riferimento comune per i settori critici. Accanto a questa si collocano normative settoriali verticali con criteri e disposizioni ancora più stringenti, come DORA (Digital Operational Resilience Act), che si applica all'ambito finanziario per aumentarne la sicurezza digitale e la resilienza operativa, introducendo anche requisiti specifici per i fornitori ICT critici.

Un secondo blocco presidia prodotti e componenti digitali, definendo i requisiti minimi affinché hardware e software possano essere immessi e mantenuti nel mercato unico in condizioni di sicurezza. In questa cornice si inserisce il CRA – Cyber Resilience Act - che stabilisce requisiti orizzontali "by design" e obblighi di gestione delle vulnerabilità lungo l'intero ciclo di vita, con logiche di conformità differenziate per classe di rischio e un raccordo esplicito con il sistema europeo di certificazione Cyber Security. Nello stesso perimetro rientrano anche aspetti legati alla protezione dei sistemi IoT e l'interazione con l'AI Act, quando un prodotto digitale include soluzioni di intelligenza artificiale ad alto rischio.

Un terzo filone, in fase di consolidamento, riguarda le dipendenze di filiera. L'obiettivo è rafforzare la fiducia nella supply chain e affrontare fattori di rischio non sono solo tecnici, ma anche strategici (ad esempio, confini giurisdizionali, interferenze e vincoli) che incidono direttamente sulla robustezza complessiva del sistema. In questo ambito, assumono rilievo i processi di due diligence su componenti e fornitori, insieme alla gestione dei fornitori considerati ad alto rischio. La proposta di CSA2 (Cyber Security Act), presentata a gennaio 2026 dalla Commissione europea e ora all'inizio dell'iter di valutazione, potrebbe diventare uno dei riferimenti principali di questo filone, integrandosi con strumenti già esistenti, ad esempio in materia di Toolbox, strumenti non vincolanti ma che hanno comunque indicato delle prospettive in materia di sicurezza.

Impianto normativo UE Cyber Security

evoluzione 2025 e novità 2026

Direttiva NIS2: dal recepimento alla fase attuativa

La Direttiva NIS2 rappresenta uno dei principali strumenti dell'Unione europea per innalzare il livello comune di cybersicurezza nei settori critici. Dopo l'entrata in vigore della Direttiva (UE) 2022/2555 nel gennaio 2023, il 2024 ha segnato il passaggio alla fase di recepimento nazionale (da completare entro il 17 ottobre 2024). In Italia, tale recepimento è avvenuto con il D.Lgs. 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024. Da tale data, l'Agenzia per la Cybersicurezza Nazionale (ACN) opera come Autorità nazionale competente NIS e punto di contatto unico.

Rispetto alla precedente Direttiva NIS, la NIS2 amplia in modo significativo il perimetro dei soggetti e dei settori presi in esame. Viene superata la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali che aveva caratterizzato il precedente impianto, sostituita dalla classificazione tra soggetti essenziali e soggetti importanti. La nuova disposizione coinvolge non solo settori tradizionalmente critici, come energia, trasporti, sanità, finanza, infrastrutture digitali e Pubblica Amministrazione, ma anche ambiti ulteriori, tra cui gestione dei rifiuti, alimentare, chimica, manifatturiero, servizi postali, servizi ICT, fornitori digitali e organizzazioni di ricerca.

Nel 2025 la NIS2 è entrata nella fase propriamente attuativa. I soggetti pubblici e privati rientranti nel campo di applicazione sono stati chiamati a registrarsi sul portale ACN in una prima finestra compresa tra il 1° dicembre 2024 e il 28 febbraio 2025. A regime, la registrazione o l'aggiornamento della registrazione si svolge dal 1° gennaio al 28 febbraio di ogni anno, mentre gli ulteriori aggiornamenti informativi annuali seguono le scadenze previste da ACN. La fase attuativa prevede inoltre l'adozione dell'elenco dei soggetti NIS, la notifica ai soggetti interessati e la progressiva definizione degli obblighi di base.

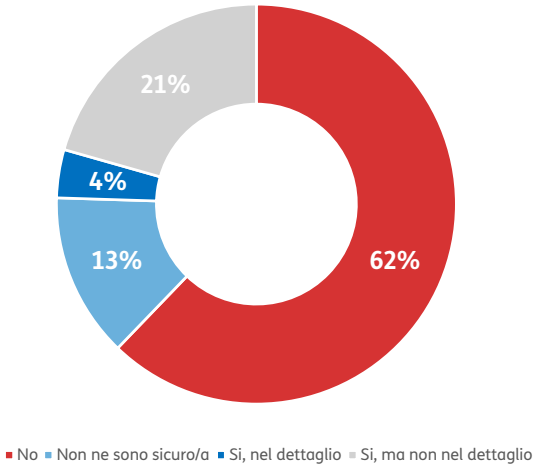
Il cambiamento introdotto dalla NIS2 non è soltanto quantitativo, legato all'ampliamento del numero di soggetti coinvolti, ma anche qualitativo. Le organizzazioni devono adottare misure tecniche, operative e organizzative proporzionate al rischio, rafforzare la gestione degli incidenti, presidiare la sicurezza della catena di fornitura, garantire la continuità operativa e documentare la propria capacità di prevenire, rilevare, rispondere e recuperare da eventi cyber.

Particolare rilievo assume il sistema di notifica degli incidenti significativi, articolato in più fasi: una prima segnalazione tempestiva, una notifica più strutturata entro 72 ore e una analisi dettagliata dell'incidente entro un mese. Questo meccanismo rende la gestione degli incidenti un processo organizzativo formalizzato, verificabile e integrato con le responsabilità degli organi direttivi.

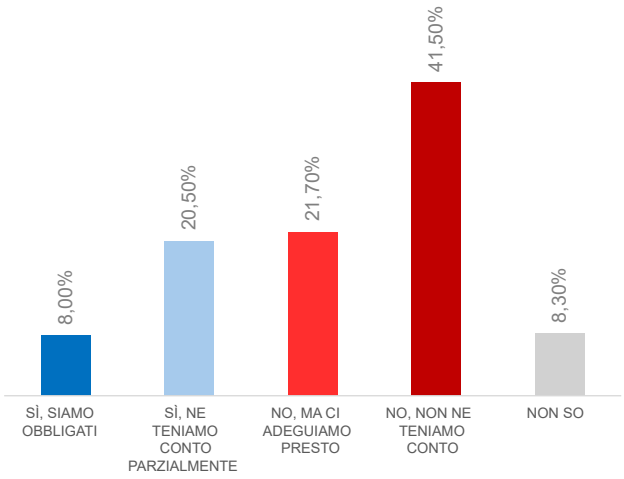
NIS2: consapevolezza delle imprese

La fase attuativa della NIS2 si inserisce in un mercato in cui la consapevolezza della normativa è ancora limitata. Secondo una recente indagine condotta dalla società Format Research[12] – finalizzata a comprendere la conoscenza dei rischi cyber delle aziende italiane – alla domanda di conoscenza spontanea, il 62,2% delle imprese dichiara di non conoscere la NIS2 e il 13,3% non è sicuro di conoscerla. Solo il 24,5% afferma di conoscerla almeno parzialmente, con appena il 3,9% che dichiara una conoscenza "nel dettaglio". La conoscenza della NIS2 aumenta tra le imprese più vicine al perimetro della normativa, in particolare tra le realtà di maggiori dimensioni e appartenenti a settori più direttamente interessati dagli obblighi.

"Conosce la normativa NIS2?"



"La sua impresa nell'ambito di processi IT tiene conto di quanto prevede la normativa NIS2?"



Dopo un breve richiamo ai contenuti della normativa, aumenta l'attenzione dichiarata: l'8,0% delle imprese afferma di applicare la NIS2 per obbligo, il 20,5% ne tiene conto parzialmente e il 21,7% prevede di adeguarsi a breve. Tuttavia, il 41,5% continua a dichiarare di non tenerne conto. Anche le misure di protezione adottate mostrano una maturità disomogenea. Prevalgono presidi di base, come antivirus, firewall e backup, mentre risultano meno diffusi controlli più evoluti e attività di formazione dei dipendenti. L'adeguamento alla NIS2 richiede, tuttavia, non solo tecnologie, ma anche processi, responsabilità e maggiore consapevolezza interna.

12 Cyber Security. Polizze Cyber Risk: conoscenza, utilizzo e prospettive. Roma, 24 aprile 2026. https://formatresearch.com/2025/09/03/Cyber Security-indagine-multiclient-format-research/

Un esercizio: attacchi ransomware verso soggetti potenzialmente in ambito NIS2

In Italia, il processo di individuazione dei soggetti NIS è gestito dall'ACN attraverso il meccanismo di registrazione e valutazione previsto dal D.Lgs. 138/2024. Tuttavia, l'elenco dei soggetti essenziali e importanti non è pubblico. Di conseguenza, non è possibile verificare direttamente per ciascuna impresa se essa sia formalmente inclusa nel perimetro NIS2.

A solo titolo di ricerca empirica, è stato effettuato un approfondimento sull'elenco delle rivendicazioni ransomware registrate nell'ultimo biennio al fine di valutare un eventuale impatto della normativa. Per superare parzialmente il limite informativo, è stato adottato un approccio di classificazione probabilistica. A tale proposito è stato costruito un modello che non attribuisce una qualifica giuridica definitiva, ma stima la probabilità che un'impresa rientri nello "scope NIS2" sulla base di tre elementi principali: il settore di attività, la dimensione dell'impresa e l'eventuale presenza di condizioni particolari o deroghe note o possibili. La metodologia utilizza quindi una logica "a regole + probabilità", dove le regole normative forniscono il giudizio principale, mentre la componente probabilistica misura il livello di confidenza in presenza di dati incompleti o ambigui.

Applicando questa procedura ai dati sugli attacchi ransomware emergono alcune evidenze da verificare ulteriormente. Nel 2024 sono state osservate 143 aziende italiane colpite da ransomware, di cui 39 classificate dal modello come probabilmente rientranti in "scope NIS2". Nel 2025 le aziende colpite salgono a 160, di cui 52 in probabile "scope NIS2". In termini percentuali, la quota di aziende colpite potenzialmente soggette alla NIS2 passa quindi dal 27,3% nel 2024 al 32,5% nel 2025. Chiaramente, il modello si basa su classificazioni probabilistiche e non su conferme ufficiali ACN e due sole annualità non sono sufficienti per individuare trend stabili. Nei prossimi anni sarà quindi importante continuare a verificare come varia la quota di aziende potenzialmente in "scope NIS2" colpite. Un eventuale aumento persistente potrebbe indicare che gli attori ransomware continuano a colpire imprese rilevanti per settori critici; al contrario, una riduzione potrebbe segnalare un primo effetto positivo delle novità introdotte dalla NIS2.

Altre norme

Cyber Resilience Act

Il Cyber Resilience Act (Regolamento (UE) 2024/2847), che definisce requisiti orizzontali di Cyber Security per i prodotti con elementi digitali, è entrato in vigore il 10 dicembre 2024. Il quadro principale degli obblighi si applicherà dall'11 dicembre 2027, mentre gli obblighi di segnalazione decorreranno dall'11 settembre 2026. A partire da tale data, i fabbricanti dovranno trasmettere le segnalazioni tramite la CRA Single Reporting Platform, istituita e mantenuta da ENISA, con un early warning entro 24 ore dalla consapevolezza e una notifica completa entro 72 ore, secondo le ulteriori scadenze previste.

Il CRA è un regolamento orizzontale: mira a garantire un livello minimo di sicurezza per hardware e software immessi sul mercato UE come "prodotti con elementi digitali", inclusi i componenti e, nei casi previsti, le relative solu-

zioni di elaborazione remota. In quanto norma di sistema, si coordina con altri atti dell'Unione e con regole settoriali che, in presenza di requisiti equivalenti o superiori, possono incidere sul perimetro applicativo. Nel merito, il CRA rafforza l'approccio "secure by design" e disciplina requisiti essenziali e processi di gestione delle vulnerabilità lungo il ciclo di vita, con una classificazione dei prodotti in categorie legate a criticità e rischio.

Il regolamento prevede inoltre un coordinamento con l'AI Act per i prodotti con elementi digitali che risultino classificati come sistemi di IA ad alto rischio, definendo le modalità con cui dimostrare la conformità ai requisiti di Cyber Security nei due quadri normativi.

La Commissione presenterà una relazione di valutazione e revisione entro il 10 dicembre 2030.

Dal Cyber Security Act al CSA2

Il Cyber Security Act (CSA), cioè il Regolamento (UE) 2019/881, ha rafforzato il ruolo dell'ENISA e introdotto un quadro europeo di certificazione della cibersicurezza per prodotti, servizi e processi ICT. Su questa base si inserisce la proposta di CSA2, presentata dalla Commissione europea il 20 gennaio 2026, che punta ad aggiornare e rafforzare l'impianto esistente, estendendo l'attenzione ai rischi emergenti, in particolare quelli legati alla catena di fornitura ICT.

La proposta prevede un meccanismo che consentirebbe alla Commissione di designare fornitori ad alto rischio e di limitare l'utilizzo dei relativi componenti ICT in settori chiave, (ad esempio, energia, trasporti, infrastrutture digitali e telecomunicazioni, ecc).

Rispetto all'attuale CSA, la proposta amplia inoltre l'ambito della certificazione introducendo uno schema di "postura di sicurezza cibernetica", volto a valutare la sicurezza organizzativa complessiva e la capacità delle entità di gestire in modo continuativo il rischio cyber. Questo strumento è concepito per facilitare la conformità agli obblighi NIS2 per le organizzazioni che operano in più Stati membri.

La proposta rafforza infine il ruolo dell'ENISA nello sviluppo di orientamenti europei in materia di Cyber Security e dei sistemi di certificazione, prevedendo anche un termine massimo di 12 mesi per la preparazione di uno schema candidato alla certificazione dopo una richiesta della Commissione.

HRV: High Risk Vendors

Per fornitori ICT ad alto rischio si intendono operatori la cui presenza nella catena di fornitura può rappresentare un fattore di vulnerabilità per infrastrutture e servizi critici, non solo sotto il profilo tecnico, ma anche per aspetti legati a dipendenze strategiche, vincoli giurisdizionali o possibili interferenze esterne. Sono per questo delle aziende extra-UE, con forti legami governativi del Paese di origine. Nel quadro della proposta CSA2, il tema assume rilievo perché la Commissione potrebbe designare tali fornitori e limitare l'uso dei relativi componenti ICT in settori considerati essenziali.

Sovranità digitale e infrastrutture strategiche

schemi cloud e sovranità

Quadro europeo

La sovranità tecnologica e digitale è una delle priorità strategiche dell'Unione Europea. In questo ambito, la Commissione punta a rafforzare la capacità dell'UE di decidere in modo autonomo, diversificare le catene di approvvigionamento, cooperare con paesi e entità terzi di fiducia, e promuovere apertura e interoperabilità. Il tema riguarda in particolare i servizi cloud, soprattutto quando trattano dati sensibili o supportano funzioni critiche.

Il rapporto Draghi del 2024 ha evidenziato come i paesi dell'UE si trovino particolarmente esposti sul fronte cloud, dipendendo in modo significativo dall'offerta di soluzioni gestite da attori che rispondono a giurisdizioni esterne all'Unione, in particolare hyperscaler statunitensi. Per questo indica ai Paesi Membri di presidiare l'ambito delle soluzioni di sovereign cloud (sicurezza e crittografia) che possono permettere di mantenere il controllo sui dati.

In questa direzione si colloca anche l'attesa proposta di un EU Cloud and AI Development Act (CAIDA o CADA), volta a definire regole comuni per i servizi cloud destinati ad ambiti particolarmente critici, inclusi requisiti sulla residenza dei dati e politiche europee per la gestione dei dati sensibili, integrando principi e logiche di disposizioni e schemi di certificazione precedenti che non si sono rivelati finora sufficienti.

Classificazione dei dati e cloud nella PA italiana

Anche l'Italia ha sviluppato un quadro regolatorio specifico per guidare la migrazione della Pubblica Amministrazione verso un modello di cloud sicuro e sovrano[13]. Tale impianto, avviato con la Strategia Cloud Italia e con le successive determinazioni dell'ACN, è oggi ricondotto al Regolamento ACN n. 21007/24 del 27 giugno 2024, applicabile dal 1° agosto 2024. In questo quadro, il sistema distingue dati e servizi in tre categorie: ordinari[14], critici[15] e strategici[16].

Per dati e servizi ordinari o critici, le PA possono utilizzare provider cloud qualificati da ACN, inclusi fornitori extra-UE, nel rispetto dei requisiti tecnici e di sicurezza previsti per ciascun livello di classificazione. Gli aggiornamenti normativi più recenti hanno inoltre introdotto la possibilità di trasferire dati ordinari e critici al di fuori dell'UE, senza autorizzazione preventiva formale dell'amministrazione proprietaria del dato e senza notifica all'ACN.

Per dati e servizi strategici, invece, resta previsto un livello di controllo sovrano più elevato. In questi casi, la gestione e il controllo delle chiavi crittografiche devono rimanere sotto giurisdizione italiana. L'autorizzazione della PA titolare dei dati rimane obbligatoria per qualsiasi trasferimento dei dati strategici al di fuori del territorio nazionale.

13 https://www.acn.gov.it/portale/cloud/regolamento-cloud-per-la-pa

14 Dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

15 Dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese.

16 Dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale.

Il ruolo delle agenzie di Cyber Security

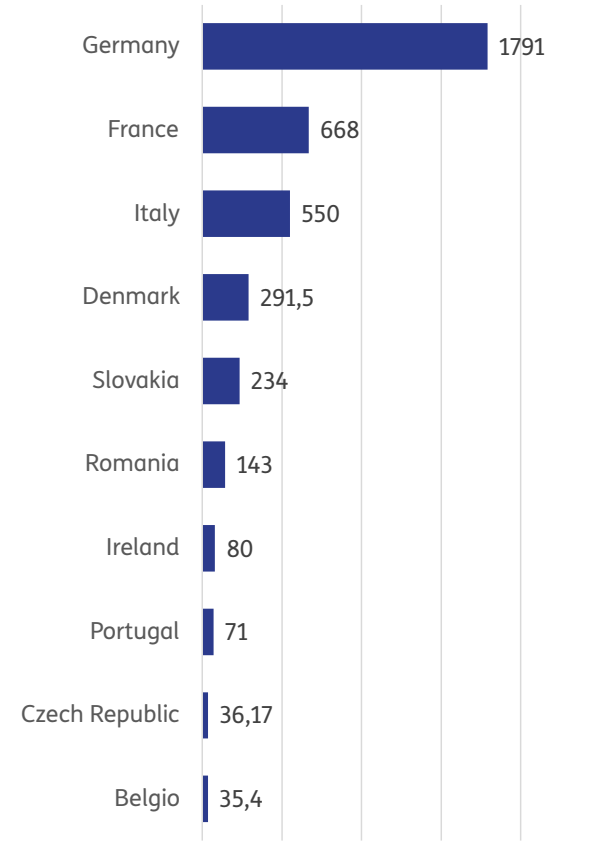
“Regia” e coordinamento

L’efficacia del quadro europeo di Cyber Security non dipende soltanto dalle norme, ma anche dalla capacità delle istituzioni di renderle operative attraverso coordinamento, supervisione e risposta agli incidenti.

A livello europeo, il coordinamento avviene attraverso organismi e strumenti che mettono in rete Stati membri, Commissione europea ed ENISA, con l’obiettivo di favorire lo scambio informativo, sviluppare linee guida comuni e rafforzare la capacità di risposta a incidenti con impatti transfrontalieri, anche attraverso le reti operative europee a supporto della gestione degli incidenti e delle crisi. In questa logica rientra il ruolo del NIS Cooperation Group, come perno di cooperazione strategica, anche nei dossier relativi alla sicurezza delle reti 5G e delle catene di fornitura ICT.

Sul piano nazionale, le agenzie di cybersicurezza operano come autorità competenti e punto di riferimento regolatorio per i soggetti coinvolti, talvolta in collaborazione con altri attori istituzionali o operativi, traducendo gli obblighi normativi in adempimenti e presìdi verificabili. Nel caso italiano, il recepimento della NIS2 attribuisce all’ACN il ruolo di Autorità nazionale competente NIS e punto di contatto unico, con responsabilità legate alla registrazione dei soggetti, agli aggiornamenti informativi e alla progressiva definizione degli obblighi attuativi.

Numero di addetti nelle agenzie di cyber security in UE



Fonte: Cullen International

Accanto alla funzione di vigilanza, il sistema include una componente operativa rappresentata dai CSIRT nazionali, che facilitano la gestione delle notifiche di incidente, supportano la risposta tecnica e il coordinamento durante le crisi cyber. A livello delle singole organizzazioni, ciò si traduce anche nell'individuazione di referenti dedicati verso autorità competenti e CSIRT, così da garantire continuità nelle comunicazioni e nella gestione delle notifiche.

Infine, le autorità svolgono un ruolo crescente nella gestione dei rischi legati alla supply chain ICT. Le più recenti iniziative europee sottolineano infatti la necessità di individuare, mappare e aggregare le dipendenze critiche e supportare, ove necessario, misure di diversificazione e de-risking rispetto a fornitori considerati ad alto rischio.

In questo quadro, le agenzie di Cyber Security non svolgono soltanto una funzione di controllo, ma rappresentano un elemento essenziale della capacità europea di prevenire, coordinare e gestire il rischio cyber in modo sistemico.

Tecnologie emergenti

L'attuale panorama della sicurezza cyber è in profonda e rapida trasformazione, guidato da un'accelerazione senza precedenti dalle innovazioni tecnologiche.

L'Intelligenza Artificiale sta modificando profondamente sia il fronte degli attacchi, sia quello della difesa. Questa tecnologia permette di sviluppare nuove soluzioni e tecniche oltre a potenziare quelle già esistenti.

L'aumento della potenza computazionale che potrà arrivare dallo sviluppo delle tecnologie quantistiche rappresenta una minaccia sempre più concreta, che spinge già oggi attaccanti e difensori ad operare prevedendo l'adozione futura di queste traiettorie.

A questi sviluppi si aggiungono elementi di accelerazione che derivano dal confronto geopolitico, che apre nuovi fronti di attenzione.

QUARTA PARTE

Le nuove frontiere

Mentre le regole cercano di stabilizzare il sistema, il rischio si trasforma in modo continuo. L'evoluzione tecnologica porta nuove soluzioni, sviluppate con l'obiettivo di aumentare la produttività dei sistemi e favorire l'innovazione ed il progresso. Ma allo stesso tempo, queste possono diventare strumenti che si applicano anche come soluzioni offensive e difensive sul piano cyber, cambiando rapidamente il campo di battaglia, ridefinendo il profilo del rischio, aprendo nuovi ambiti da tenere sotto controllo con nuove norme, procedure e regole che rimodulano costantemente le scelte di resilienza.

La quarta parte ha l'obiettivo di aprire un breve approfondimento sulle novità tecnologiche che sono emerse tra il 2025 e i primi mesi del 2026 e stanno trasformando lo scenario:

- nuove minacce, in particolare derivanti dal progressivo uso dell'AI nel dominio cyber
- nuovi sviluppi, rappresentati dalla discontinuità tecnologica che portano le tecnologie quantistiche
- nuovi fronti che si aprono anche a seguito delle dinamiche geopolitiche.

L'AI sta entrando in maniera sempre più decisa nella gamma di soluzioni utilizzate dai cybercriminali, rendendo il phishing e le frodi più scalabili e convincenti, anche tramite deepfake e identità sintetiche che rendono l'inganno più rapido, economico e difficile da contrastare. Nella prospettiva che assumiamo in questa sezione, l'AI viene soprattutto identificata come un acceleratore del cybercrime, una "lente" per leggere come cambiano velocità, dimensioni e qualità dell'attacco, e quali conseguenze operative ne derivano. Tuttavia, la versatilità dell'AI consente anche di potenziare gli strumenti in mano alle difese, migliorando e rendendo più tempestiva la capacità di rilevazione e analisi di malware e phishing e rafforzando la capacità preventiva di controllo delle superfici esposte.

La discontinuità portata dalle tecnologie quantistiche in termini di capacità computazionale incide sulle soluzioni di sicurezza crittografica e individua delle nuove prospettive di attenzione per imprese ed istituzioni. La *quantum readiness*, ossia il livello di preparazione delle organizzazioni a realizzare la migrazione dalla crittografia attuale a soluzioni resistenti ai computer quantistici, si trasforma da pianificazione a investimento strategico concreto, al fine di mitigare il rischio che dati - oggi cifrati - vengano raccolti e conservati, per essere decifrati in futuro quando la tecnologia quantistica sarà matura. Questo impone la migrazione proattiva verso la Post-Quantum Cryptography (PQC) e la *crypto-agility*, la capacità di aggiornare o sostituire rapidamente algoritmi, configurazioni e componenti crittografiche (chiavi/protocolli) senza interrompere i servizi.

Lo spazio emerge come un livello cyber-fisico critico di contesa geopolitica, poiché i sistemi robotici e le infrastrutture spaziali passano dalla sperimentazione al dispiegamento operativo, diventando fondamentali per connettività e sicurezza. Ciò espande la superficie d'attacco con nuove vulnerabilità, rendendo la Cyber Security spaziale un tema di resilienza sistemica in un contesto di crescente competizione.

Per ciascuna di queste tre prospettive, questo capitolo propone una rassegna di esempi più interessanti delle novità che stanno emergendo, con l'obiettivo di mostrare concretamente come questo ambito sia interessato da cambiamenti continui.

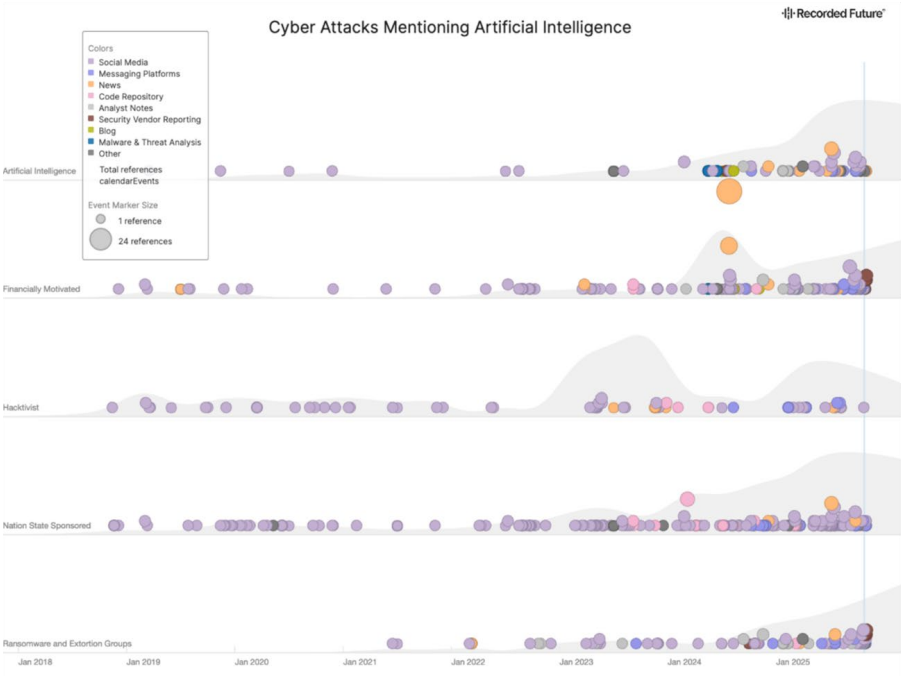
L’AI nel dominio Cyber

AI in chiave cyber offensiva

Negli ultimi anni l’AI, in particolare l’AI generativa sta incidendo sul dominio cyber in modo sempre più evidente. Le analisi dell’unità di Threat Intelligence Insikt Group[17] di Recorded Future evidenziano che l’impatto più concreto dell’AI non è (ancora) l’attacco totalmente autonomo, ma soprattutto l’integrazione dell’AI nei processi, che accelera decisioni, automazioni e interazioni uomo-macchina.

Gli sviluppi offensivi più significativi sono stati osservati in ambiti come phishing, frodi, malware e “weaponization” della supply chain software18, aumentando la complessità operativa ed estendendo la superficie esposta.

Questo processo sta accelerando sempre di più a partire dal 2022, a seguito del rilascio di ChatGPT-3.5 nel novembre 2022 che ha rappresentato un punto di svolta per l’accessibilità della GenAI.



17 Recorded Future - Insikt Group: 2026 State of Security - How global fragmentation is redefining conflict across cyber, crime, and influence; FOCUSED INTELLIGENCE REPORT: 2025 - Artificial Intelligence (AI) and Large Language Models (LLMs); Annual Payment Fraud Intelligence Report 2025

18 Quest’ultimo sviluppo rappresenta una minaccia sottile ma estremamente pericolosa, trasformando la catena di fornitura del software in un’arma operativa: invece di colpire direttamente la vittima finale, l’attaccante compromette la filiera “a monte”, nella distribuzione di aggiornamenti legittimi attraverso canali ufficiali o anche nelle librerie e negli strumenti che gli sviluppatori includono naturalmente nel progetto.

Osservando la mappa degli attacchi cyber che fanno riferimento all'uso dell'AI per attori di minaccia, si individua ovunque un trend di crescita, più pronunciato per i Nation-state sponsored e i Ransomware group.

Per comprendere l'impatto concreto di questa traiettoria, può essere utile spostare l'attenzione dal "trend" alle modalità operative, osservando alcuni esempi del modo in cui l'AI viene effettivamente incorporata nei flussi di lavoro e nelle catene decisionali che sostengono l'attività degli attori di minaccia.

AI usata dagli attaccanti per migliorare tecniche già note

L'uso dell'AI generativa sta rendendo più semplice ed economico mettere in campo attività criminali tradizionali, perché abbassa la barriera d'ingresso nella produzione di contenuti convincenti: messaggi, pagine e materiali di supporto possono essere generati rapidamente e adattati su larga scala, facilitando campagne di phishing e truffe più efficaci e industrializzate. In parallelo, cresce l'impiego di contenuti audio e video sintetici per frodi basate su deepfake e identità non autentiche: la possibilità di imitare volti e voci aumenta la credibilità delle impersonificazioni e rende più complessi i processi di verifica, attribuzione e contestazione, con un impatto diretto anche su indagini e gestione degli incidenti.

Monetizzazione illecita dei servizi AI nel cloud

Il LLMjacking è una forma emergente di abuso delle risorse cloud in cui gli attaccanti, dopo aver sottratto credenziali o chiavi di accesso ai servizi (API) in ambienti cloud, riescono a utilizzare come utenti legittimi i servizi LLM a pagamento e ne sfruttano i consumi a carico della vittima. In questo schema, l'obiettivo non è solo l'accesso ai dati, ma la monetizzazione della capacità computazionale: l'uso illecito delle API viene "scaricato" sul conto della vittima, mentre l'attaccante rivende o impiega tale capacità per attività fraudolente su larga scala. Le campagne osservate seguono uno schema ricorrente di abuso di credenziali cloud: gli attori malevoli sfruttano vulnerabilità applicative per sottrarre le credenziali, poi verificano in modo sistematico quali servizi di intelligenza artificiale sono disponibili e instradano le richieste verso provider LLM commerciali (tra cui Anthropic, OpenAI e AWS Bedrock), puntando a un vantaggio economico con la massima discrezione operativa. In un caso documentato[19], sono state impiegate tecniche di evasione "a basso rumore": gli attaccanti hanno cercato di passare inosservati facendo alcune richieste "di prova" alle API con parametri errati per capire se il servizio fosse utilizzabile e se il monitoraggio fosse attivo (log abilitati). Questo indica campagne più mature, pensate per durare e massimizzare il guadagno riducendo i rischi.

19 Recorded Future - Cloud Threat Hunting and Defense Landscape - Pag. 13

L'effetto può essere economicamente rilevante: in alcuni scenari, l'uso non autorizzato di servizi LLM ad alto costo può generare spese anomale molto rapidamente, con stime che raggiungono i 46.000 dollari al giorno, rendendo il LLMjacking un vettore concreto di danno finanziario oltre che un indicatore di compromissione delle identità cloud.

AI "agentica" nei servizi e nei pagamenti.

Un ambito in rapida evoluzione è l'"agentic commerce": soluzioni in cui un agente AI può eseguire operazioni al posto dell'utente, ad esempio effettuare acquisti o completare transazioni. Questo modello introduce un elemento di rischio nuovo: oltre a verificare l'identità di chi opera, diventa necessario valutare e proteggere anche l'intent, cioè l'intenzione con cui l'azione viene avviata, dall'utente o dall'agente. In pratica, la stessa sequenza di azioni può rappresentare un'operazione legittima oppure una frode automatizzata; di conseguenza, l'intent diventa una nuova superficie d'attacco e aumenta anche la complessità delle verifiche e delle dispute in caso di incidenti. Anche quando le responsabilità sono definite, capire se si tratta di una frode esterna, di un abuso da parte dell'utente o di un comportamento anomalo dell'agente può richiedere infatti più tempo e risorse.

Attacchi "contro" l'AI

Con la diffusione dei LLM (Large Language Model) e assistenti collegati a dati aziendali e strumenti operativi, cresce una classe di minacce che non punta tanto a "rompere" i sistemi tradizionali, quanto a manipolare il comportamento del modello.

Una prima direttrice è la prompt injection, anche indiretta: istruzioni malevole possono essere annidate in contenuti apparentemente innocui - come testo, immagini o file - e, quando il sistema li recupera come elementi di contesto, possono influenzare l'output o spingere l'assistente a compiere azioni non desiderate.

In parallelo, si osserva il rischio di data poisoning e manipolazione delle fonti: contaminando dataset, documenti o basi conoscitive, un attaccante può distorcere risposte e decisioni in modo persistente, con un impatto particolarmente rilevante nei sistemi RAG e nelle knowledge base interne[20], dove l'affidabilità delle informazioni è parte integrante del controllo di sicurezza e del processo decisionale.

20 I sistemi RAG (RetrievalAugmented Generation) sono soluzioni che recuperano informazioni da una base dati o knowledge base configurata e le usano come contesto per generare risposte. Per "knowledge base interne" si intendono repository di conoscenza/documenti dell'organizzazione, centralizzati e accessibili a persone autorizzate, utilizzati come fonte informativa di riferimento.

Nuove minacce, nuove denominazioni. Promptware, Quishing, QRishing e non solo.

Nel lessico della Cyber Security stanno emergendo aree in cui la novità non è solo tecnica, ma anche linguistica: servono parole per descrivere vettori che stanno diventando ricorrenti e che non si lasciano ridurre ai soli schemi "classici". Un esempio è il **Promptware**. La rapida diffusione di sistemi basati su LLM e agenti "collegati" a strumenti e dati (browser, documenti, servizi) sta aprendo una classe di minacce più complesse che vanno oltre al "semplice" prompt injection, inteso come una anomalia isolata, e che possono innescare una sequenza multi-step. Il punto critico è che, man mano che gli LLM si trasformano in "agenti" collegati a fonti e strumenti operativi, il confine tra dato e comando tende a sfumare: contenuti web apparentemente innocui (testo nascosto, commenti HTML, istruzioni non visibili) possono essere ingeriti dal sistema come contesto e indirizzarne il comportamento, soprattutto quando l'assistente ha permessi per navigare, recuperare informazioni o agire su servizi esterni.
Altre minacce che appaiono a seguito degli sviluppi tecnologici e che richiedono delle nuove concettualizzazioni sono quei vettori che si collocano tra dimensione fisica e digitale. Esempi di queste tipologie sono i phishing che avvengono utilizzando i QR code come vettore d'inganno, invitando l'utente a scansionarlo per "verifiche" o "sblocco account", e portandolo poi su pagine che raccolgono credenziali. Una "nuova" forma di phishing denominata **Quishing** o **QRishing**.
Infine, si affaccia un fronte meno discusso ma destinato a crescere: VR/AR e smart glasses, cioè dispositivi indossabili più leggeri che integrano sensori e assistenti AI e che, secondo alcune analisi di scenario, potrebbero favorire un'adozione più ampia proprio grazie a form factor più "portabili", minacce future per le quali non esiste ancora una denominazione accreditata.

AI in chiave cyber difensiva

AI nella difesa: efficienza operativa e individuazione di vulnerabilità

Sul versante difensivo, l'AI generativa sta mostrando un valore operativo sempre più concreto lungo alcune funzioni chiave della sicurezza, pur senza eliminare la necessità di supervisione umana. Ambiti di applicazione sempre più importanti si rilevano nell'analisi delle vulnerabilità, nelle attività di triage e analisi dei SOC e, in parte, anche nel penetration testing, con benefici di efficienza che richiedono comunque controllo e validazione da parte di analisti per garantire affidabilità e ridurre i rischi di errori o interpretazioni fuorvianti.

Uno degli ambiti più interessanti è quello dell'individuazione delle vulnerabilità, su cui appare promettente la soluzione proposta dalla società Anthropic, specializzata nella ricerca e sviluppo sull'intelligenza artificiale. Nel 2025, Anthropic ha compiuto un balzo in avanti nella catena evolutiva dei suoi modelli linguistici, con il rilascio di nuove versioni di Claude utilizzati prevalentemente in ambiti di produttività e sviluppo software. Nella primavera del 2026, Anthropic ha presentato Claude Mythos Preview e l'iniziativa Project Glasswing, descrivendoli come un tentativo di usare capacità avanzate di lettura del codice per rafforzare la sicurezza del software "critico" prima che competenze simili diventino più diffuse. Secondo quanto riportato da Anthropic, Mythos Preview avrebbe raggiunto un livello di efficacia tale da individuare e aiutare a correggere vulnerabilità su sistemi e componenti ampiamente utilizzati. Per questo la società ha scelto un rilascio a accesso controllato, rivolto a un gruppo di partner e a organizzazioni che mantengono infrastrutture software rilevanti – tra cui, tra le altre AWS, Microsoft, Apple, Google e Linux Foundation – riunite nel consorzio Project Glasswing[21]. L'elemento che rende il caso interessante non è tanto la singola promessa tecnologica quanto la direzione che punta su una capacità di "leggere" codice e individuare debolezze che accorcia la distanza tra scoperta del difetto e necessità di mitigazione.

Sviluppi di questo tipo possono contribuire ad accrescere la consapevolezza nel settore e favorire un'evoluzione verso un approccio più orientato alla sicurezza fin dalla progettazione. Allo stesso tempo, come visto in occasioni passate, capacità non governate possono tramutarsi in soluzioni che entrano nella gamma di strumenti degli attaccanti.

Governare l'AI nei processi: dati, permessi e responsabilità

Allo stesso tempo, l'AI è anche uno strumento che permette alle organizzazioni di migliorare la propria postura di sicurezza, integrandola all'interno dei workflow, dei dati e degli strumenti aziendali e individuando situazioni anomale che necessitano di controllo o potenziali falle di sicurezza sulle quali attivare preventivamente azioni di protezione. In questo ambito vanno naturalmente bilanciati opportunità e rischi.

Se da un lato questo fornisce alle organizzazioni nuove soluzioni, dall'altro espande anche la superficie di attacco potenziale utilizzando l'AI come vettore.

21 https://www.anthropic.com/glasswing

Per contrastare questo rischio, la difesa non riguarda più soltanto “cosa” il modello è in grado di riconoscere, ma anche i dati e le autorizzazioni che l’AI usa per operare e la tracciabilità delle azioni che può compiere, soprattutto quando è collegata a strumenti operativi, dal momento che decisioni e automazioni possono propagare rapidamente effetti indesiderati lungo l’intera catena di processo. Una cosiddetta “fallibilità della verifica su larga scala” può portare la minaccia nei processi decisionali e rendere più difficile distinguere segnali legittimi da manipolazioni o contenuti sintetici.

Di fronte a questo rischio, serve uno stretto governo dell’AI che rappresenta una sfida non solo tecnica ma organizzativa, con controlli più complessi, triage, e analisi delle responsabilità decisionali ed operative.

La discontinuità del Quantum

Le Quantum Technologies sfruttano alcune proprietà della fisica quantistica per trattare l'informazione in modo diverso rispetto ai computer e alle comunicazioni tradizionali. Per comprendere come la quantistica entra nel mondo della Cyber Security conviene distinguere due ambiti:

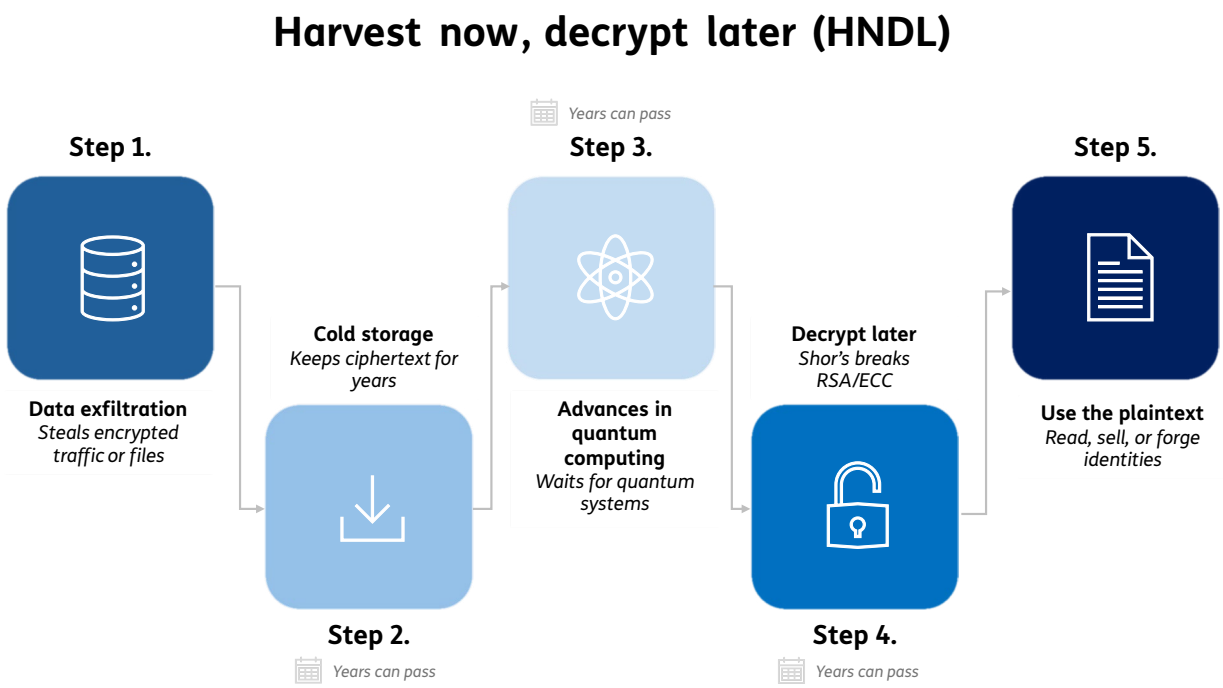
- Lo sviluppo di processori basati su tecnologie quantistiche rappresenta un salto in avanti per capacità computazionale. Questo comporta che – attraverso le tecnologie quantistiche – è possibile risolvere più velocemente alcuni problemi rispetto ai computer classici. In ambito sicurezza, la conseguenza centrale è che un quantum computer sufficientemente potente potrebbe rendere vulnerabili molte forme di crittografia a chiave pubblica oggi usate ovunque per scambiare chiavi, autenticare identità e firmare software e documenti.
- Questa discontinuità chiede soluzioni nuove, anch'esse basate sullo stesso sviluppo. Un esempio è quello delle chiavi crittografiche quantum-safe. In ambito comunicazioni, ad esempio, utilizzando le leggi della fisica quantistica è possibile distribuire chiavi crittografiche in modo tale che un'eventuale intercettazione sia rilevabile.
- Attraverso questo sviluppo si punta a realizzare infrastrutture e approcci quantum safe combinando ed integrando soluzioni diverse, prevalentemente Post Quantum Cryptography (PQC) e Quantum Key Distribution (QKD).

In altri termini, se da un lato il quantum abilita nuove capacità, dall'altro introduce una discontinuità di sicurezza, perché questo sviluppo mette a rischio e può compromettere gran parte della crittografia a chiave pubblica su cui si basano le comunicazioni digitali odierne. Per questo si lavora sullo sviluppo di soluzioni quantum-safe, in grado di contrastare questa minaccia. Per quanto questo sviluppo appaia futuribile, già oggi esistono degli aspetti critici.

Il rischio "harvest now, decrypt later"

La migrazione dagli attuali strumenti crittografici verso soluzioni resistenti alle minacce quantistiche, definito *quantum readiness*, richiede oggi un deciso avanzamento anche a causa del rischio "*harvest now, decrypt later*" (HNDL)[22]: attori ostili possono intercettare e conservare dati cifrati oggi, confidando nella possibilità di decifrarli in futuro quando le capacità quantistiche saranno mature.

22 Mascelli, Jillian, and Megan Rodden (2025). Harvest Now Decrypt Later : Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks, Finance and Economics Discussion Series 2025-093. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.093.



Fonte: Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat - Palo Alto Networks

In altri termini, la minaccia quantistica non è solo futura ma anche retrospettiva, agendo già oggi, soprattutto per dati con requisiti di riservatezza di lungo periodo, e questo richiede azioni immediate che facilitino la migrazione verso soluzioni di sicurezza basate sulla **Post-Quantum Cryptography (PQC)** che integrano anche inventari crittografici, gestione delle dipendenze e roadmap dei fornitori - perché la migrazione alla PQC diventa un tema di continuità e fiducia nel tempo, non solo un aggiornamento tecnico.

La crypto-agility

Affinché la *quantum readiness* sia effettiva nel tempo, diventa necessario affiancare alla migrazione verso la PQC una capacità strutturale di adattamento. La crypto-agility va intesa come una capacità organizzativa, non solo tecnologica: significa essere in grado di aggiornare e sostituire nel tempo algoritmi e componenti crittografiche in modo ordinato, tenendo conto sia dei tempi necessari alla migrazione sia della durata di riservatezza richiesta dai dati. In questo senso, è un elemento chiave per proteggere informazioni lungo l'intero ciclo di vita.

Un fronte emergente: lo spazio

Il sistema spaziale può essere letto come un ecosistema articolato in segmenti – orbitale, terrestre, di collegamento (uplink/downlink) e utente (terminali e dispositivi) – ciascuno con funzioni specifiche e con rischi che possono propagarsi tra le componenti. Non una singola risorsa, ma un'infrastruttura complessa, in cui vulnerabilità e minacce possono originare in un segmento e generare effetti a cascata sugli altri.

Con l'integrazione crescente dei servizi spaziali nella vita quotidiana e nelle applicazioni critiche, la Cyber Security diventa una priorità trasversale per soggetti titolari, gestori, utenti e produttori.

Le raccomandazioni istituzionali[23] sottolineano infatti la necessità di trattare la sicurezza cibernetica come requisito primario lungo l'intero ciclo di vita e la filiera, poiché vulnerabilità in sistemi spaziali interconnessi possono incidere sulla continuità e sull'affidabilità dei servizi abilitati dallo spazio.

Ma non solo. L'espansione delle costellazioni satellitari e l'intensificarsi delle attività spaziali rendono questa infrastruttura un ambito sempre più rilevante per connettività, servizi e sicurezza, alimentando una competizione crescente su resilienza, accesso e controllo di queste capacità. In questo scenario, risorse spaziali e componenti di terra interconnesse ampliano – in prospettiva - la superficie d'attacco.

La minaccia più probabile non è tanto un guasto sistemico su larga scala, quanto un'interruzione mirata e ripristinabile, in grado di produrre impatti immediati (su sicurezza, economia o continuità dei servizi) restando al di sotto delle tradizionali soglie di escalation.

I principali vettori richiamati in questo ambito includono:

- **Jamming/spoofing GNSS (PNT disruption/ manipulation)**[24]: interferenze e falsificazioni del segnale possono compromettere l'affidabilità dei servizi che dipendono da comunicazioni e segnali satellitari, con ricadute operative su continuità e sicurezza dei sistemi utilizzatori.
- **Attacchi al segmento terrestre**[25] (centri di controllo e infrastrutture operative): la componente di terra è indicata come la più accessibile e vulnerabile, spesso perché fortemente interconnessa e "ITlike", diventando un punto di ingresso privilegiato per compromissioni con effetti sul resto del sistema.

23 CISA, Cyber Security and Infrastructure Security Agency - Recommendations to Space System Operators for Improving Cyber Security

24 Federal Aviation Administration - GNSS Interference Resource Guide - Jamming & Spoofing

25 CISA – Recommendations to Space System Operators for Improving Cyber Security;
NDSS Symposium 2024 – Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks

- **Supply chain e tecniche lungo il ciclo d'attacco**: la filiera – che include componenti, software/firmware e fornitori - costituisce una fonte rilevante di rischio; di conseguenza, le raccomandazioni richiamano misure di supply chain risk management (inclusi controlli e verifiche) e un approccio difensivo che consideri la possibile propagazione delle minacce tra segmenti[26].

In questo quadro sta maturando un insieme di indirizzi e raccomandazioni per rafforzare la Cyber Security dei sistemi spaziali. Il documento *Recommendations to Space System Operators for Improving Cyber Security* della CISA sintetizza le principali fonti di rischio e propone opzioni di mitigazione, invitando a utilizzarle in coerenza con il NIST Cyber Security Framework (CSF) per informare profili, piani di mitigazione e strategie di sicurezza[27].

La stessa impostazione "a segmenti" consente inoltre di declinare linee guida e pratiche in modo mirato, con indicazioni specifiche per gli ambiti più esposti.

In sintesi, man mano che lo spazio si consolida come infrastruttura abilitante per servizi critici, la sicurezza non può essere trattata come protezione puntuale del singolo satellite o della singola missione: diventa un tema di governance e resilienza endtoend, guidato da riferimenti condivisi e da raccomandazioni istituzionali lungo l'intera catena, dai segmenti alle interconnessioni e agli stakeholder coinvolti.

26 SoK: Evaluating the Security of Satellite Systems

27 Il NIST CSF è un quadro di riferimento volontario per la gestione del rischio cyber: offre un linguaggio comune per valutare, prioritizzare e comunicare gli obiettivi di sicurezza e le azioni necessarie. È organizzato in funzioni (ad esempio Identify, Protect, Detect, Respond, Recover; Govern) e può essere adattato alla singola organizzazione tramite profili che descrivono lo stato attuale e lo scenario target, supportando l'impostazione di una roadmap di miglioramento coerente con priorità e livello di rischio.

QUESTO VOLUME è STATO REALIZZATO CON IL CONTRIBUTO DI:

Matteo **MACINA**

Cybersecurity Foundation
Vice-Presidente Operativo

Antonio DI RONZA

Cybersecurity Foundation
Comitato Tecnico Scientifico

Enrico **BARELLA**

Emanuela **VELLA**

Samuele **BALLETTA**
Max **BRUGNOLI**
Claudia **GERBINO**
Matteo **PETRANGELI**
Cristina **UBALDINI**

Laura **BODO**
Elenia **CIANFARANI**
Stefano Gaspare **LAMBORGHINI**
Riccardo **RASPONI**
Flavia **VENDITTELLI**

Massimiliano **BROLLI**
Chiara **COLTELLACCI**
Maria Rosaria **MURATORE**
Gian Luigi **SAVIOLI**

Si ringraziano per i dati forniti Cullen International e Format Research

CYBER SECURITY FOUNDATION

TIM

Cyber Security Report

Analisi delle minacce ed evoluzione dello scenario

anno 2025

www.gruppotim.it

www.cybersecurityfoundation.it