SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

Presentazione del Rapporto Clusit 2026

Introduzione
Anna Vaccarelli
Presidente Clusit

Apre i lavori **Anna Vaccarelli**, Presidente Clusit

Ospite d'onore **Nunzia Ciardi**, Vice Direttore Generale dell'ACN - Agenzia per la Cybersicurezza Nazionale

Saranno presentati i dati dell'ultimo Rapporto Clusit a cura di alcuni autori:

- **Alessio Pennasilico**, CS Clusit
- **Luca Bechelli**, CD Clusit
- **Sofia Scozzari**, CD Clusit
- **Silvio Ferrari,** Manager of Cyber Security Products, Fastweb + Vodafone
- **Giorgia Dragoni**, CS Clusit

Segue una tavola rotonda, moderata da **Alessio Pennasilico**, con gli esperti di security di alcuni dei principali fornitori di prodotti e servizi di sicurezza ICT, che arricchiranno il dibattito con le loro esperienze sul campo:

- **Nicola Dalla Vecchia**, Akamai
- **Luca Nilo Livrieri**, CrowdStrike
- **Umberto Pirovano**, Palo Alto Networks
- **Maurizio Taglioretti**, Netwrix

Nunzia Ciardi

Vice Direttore Generale

ACN

Rapporto Clusit 2026

14ª EDIZIONE

Intervento del Vice Direttore Generale dell’
Agenzia per la Cybersicurezza Nazionale

Nunzia Ciardi

Security Summit, Milano — 17 marzo 2026

L'Era degli Attacchi Estremi?

5.265

Incidenti globali 2025

+48,7%

Crescita vs 2024

Il più alto mai registrato

507

Incidenti in Italia

+42% — record nazionale

9,6%

Quota italiana globale

Paese più colpito d'Europa

I numeri sono reali — ma raccontarli senza distinguo genera allarme, non orientamento.

Il fenomeno Hacktivism

Un'anomalia statistica?

196 incidenti hacktivistici in Italia nel 2025 —
il **64% del totale mondiale**.

L'Italia pesa il 2,5% della popolazione globale. Questo dato non descrive una vulnerabilità reale: descrive un **bias del campione**.

Il Clusit stesso lo definisce *"perturbazione all'origine del campione"*.

Il Paradosso della Difesa

1

Attacco DDoS in corso

Traffico malevolo sommerge il sito

2

Geo-filtering attivato

Solo IP italiani ammessi — sito ripristinato in minuti

3

L'attaccante dall'estero vede errore

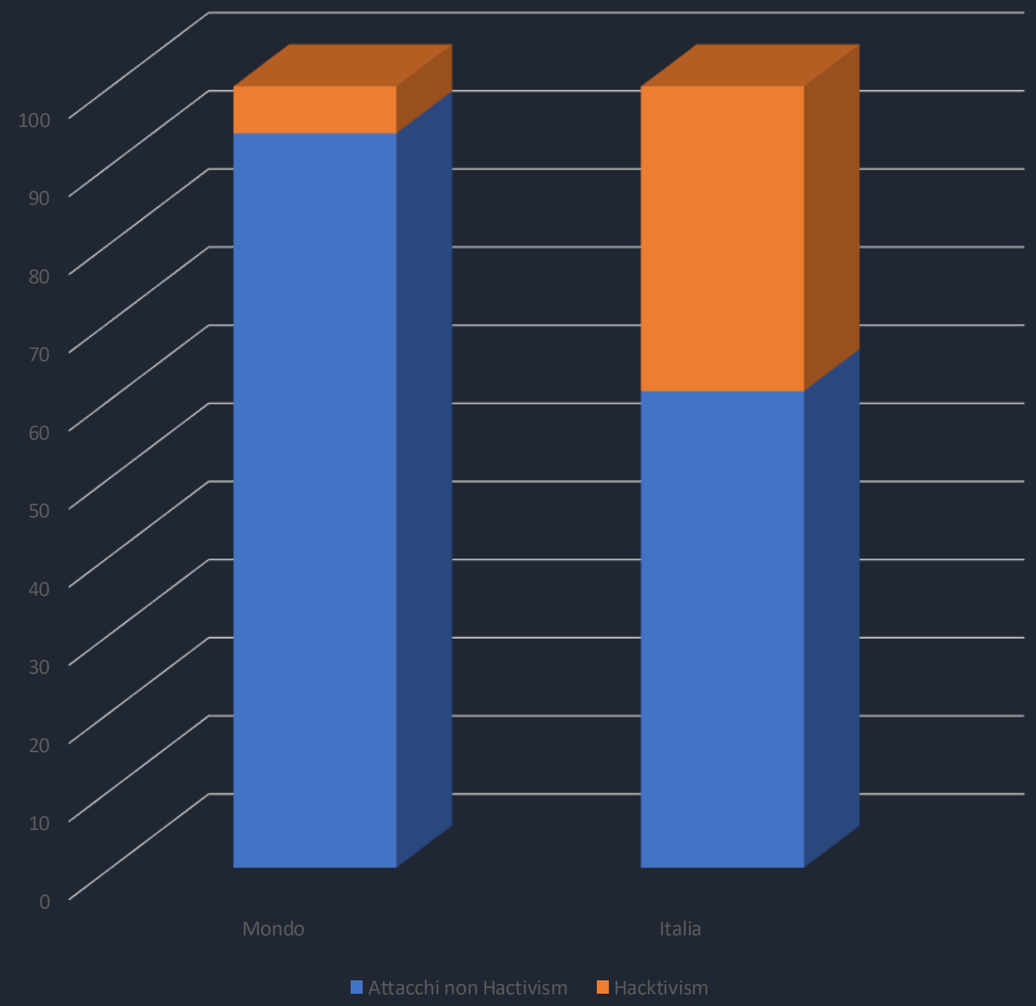
Pubblica screenshot: *"sito offline"* su Telegram

4

Entra nel campione Clusit

Fonte aperta confermata — conteggiato come incidente

Il Segnale Sotto il Rumore

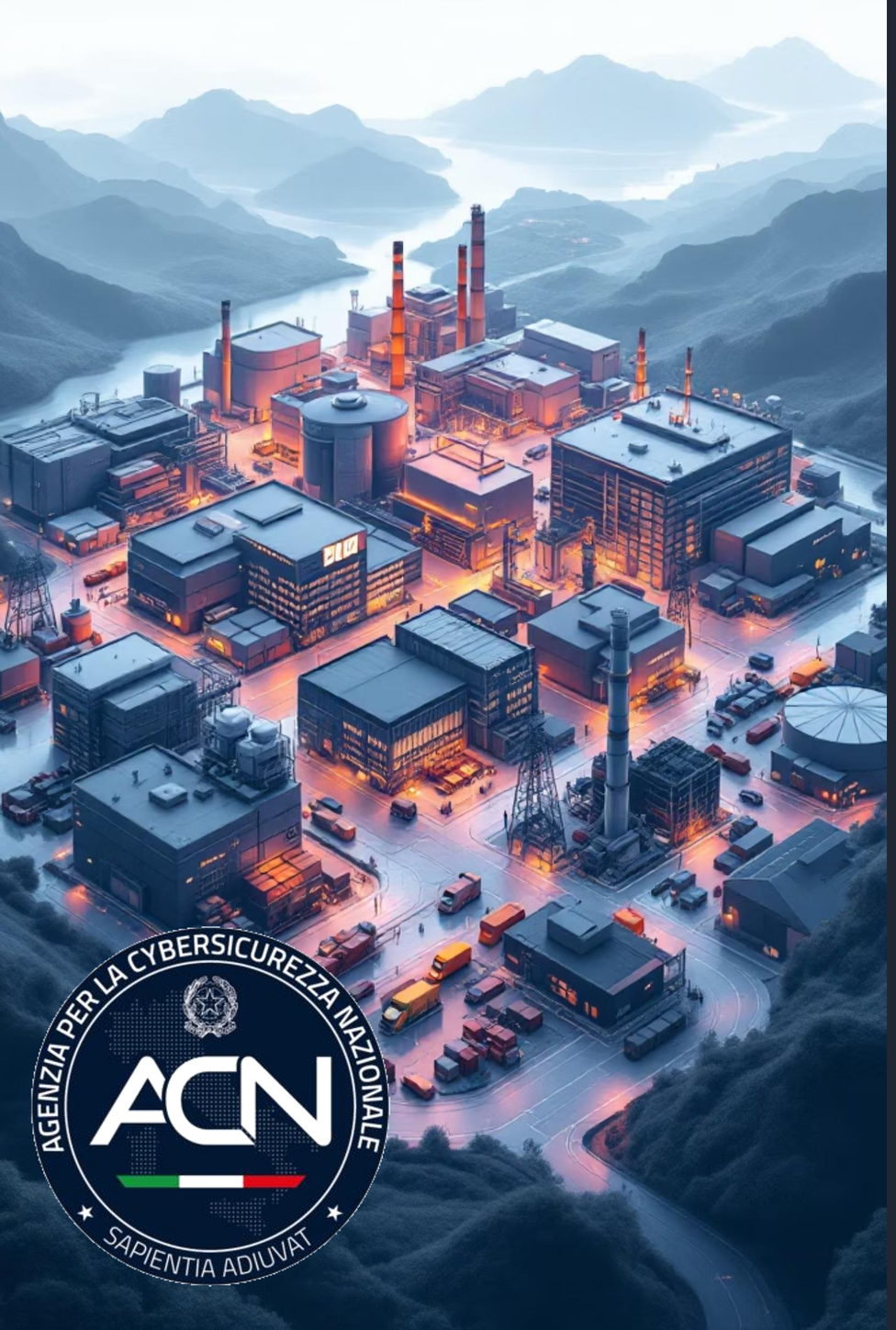


Una lettura diversa

Senza hacktivism, la crescita italiana è **+12%** — non +42%!

In un mondo dove gli attacchi crescono del 50%, fermarsi al 12% è un segnale.

C'è ancora da fare — ma qualcosa si muove.



Il Rischio Strutturale: il Manufacturing

16% globale

64 incidenti su 400 mondiali nel manifatturiero

PMI in rete

Distretti ad alta densità relazionale — vettore di propagazione del rischio

Digitalizzazione rapida

OT connesso, sistemi remoti — senza parallela maturazione della sicurezza

Know-how a rischio

File CAD, ricette di processo: patrimonio prezioso per attori malevoli

Non è colpa di nessuna singola azienda — è la struttura del sistema che genera vulnerabilità.

Segnali Positivi

Settore Finanziario

10° posto in Italia vs 6° globale — la regolazione cogente produce risultati misurabili.

Vulnerabilità -79%

Calo degli incidenti da vulnerabilità. CSIRT Italia: decine di migliaia di comunicazioni preventive nel 2025.

Gestione strutturata

Crescita degli incidenti "Undisclosed": comunicazione selettiva e consapevole — è governance.

Due Italie Digitali

Italia regolata

- Finanza, operatori essenziali, perimetro nazionale
- Segnali genuini di miglioramento
- Struttura organizzativa adeguata

Italia non regolata

- PMI manifatturiere, filiere di subfornitura
- Crescita degli incidenti reale e strutturale
- Sotto le soglie di compliance

Questa biforcazione è, per ACN, **il punto più utile** del Rapporto Clusit 2026.

La Sfida: Oltre il Perimetro

Regolazione NIS2

Perimetro obbligato e supply chain

Sicurezza diffusa

Cultura, competenze e protezione reale

Supporto PMI

Incentivi, standard condivisi

La regolazione costruisce il perimetro — la sfida è far sì che la sicurezza reale si diffonda **anche oltre**, attraverso incentivi, supporto tecnico e standard accessibili alle piccole imprese.

Conclusione: Dati con Coraggio Analitico

Distinguere il rumore dal rischio

Artefatti statistici ≠ vulnerabilità strutturali

Riconoscere i segnali di miglioramento

Non solo allarme — anche direzione

Costruire politiche che funzionano

Solo sulla distinzione — non sul numero aggregato

Il Rapporto Clusit è prezioso perché è trasparente. Il nostro compito è usarlo con tutta la sua potenza, senza rinunciare alla lettura critica.

I contenuti del Rapporto

Luca Bechelli
Comitato Direttivo
CLUSIT

Rapporto Clusit 2026 – Take Away e So What

- *Le normative generali e settoriali (GDPR, NIS2, DORA ecc.) iniziano a manifestare i loro effetti positivi, soprattutto in un tessuto di PMI che difficilmente investirebbe spontaneamente in sicurezza:*

  - I trend mostrano che gli attaccanti colpiscono progressivamente settori meno maturi digitalmente, evidenziando l'urgenza di un livello "igienico" minimo di difesa in tutti i comparti.

  - Le Autorità (ACN e Regolatori settoriali) stanno assumendo un ruolo di guida, più che solo «controllo», ma il gap rispetto ad altre geografie resta ancora significativo, con un tema di Digital Sovereignty che diventa ogni giorno più rilevante

  - ***Nel presente e nel prossimo futuro****: AI Act, Cyber Resilience Act e Direttiva CER non vanno letti ciascuno non come "l'ennesima compliance", ma come la cornice per coniugare innovazione (anche AI-based), etica digitale, protezione dei dati e sicurezza delle informazioni - inclusi gli ambiti OT/IoT – in ogni passo dello sviluppo di nuovi servizi tecnologici*

Rapporto Clusit 2026 – Take Away e So What

- *Delegare l'agenda cyber solo alla compliance rischia però di produrre investimenti poco aderenti al contesto e percepiti come oneri burocratici, invece che come leva di tutela del business: serve una governance della sicurezza strutturata, capace di gestire il rischio (prevenzione, mitigazione, trasferimento tramite assicurazioni o outsourcing qualificato, ad es. cloud) in modo sistematico*

    - NIS2 introduce una responsabilizzazione esplicita del top management sui rischi cyber, richiedendo un adattamento continuo della postura di sicurezza allo scenario in rapido cambiamento.

    - I numeri indicano che alcune misure funzionano (es: forte calo degli incidenti basati su vulnerabilità), ma la variabilità delle tecniche più utilizzate resta elevata anno su anno, rendendo il risk management un presidio centrale per fronteggiare l'evoluzione continua delle minacce

    - La vera leva abilitante è una gestione molto più stringente di sourcing e terze parti, con governo continuo dei servizi esternalizzati e collaborazione attiva dei fornitori, per evitare che adempimenti frammentati creino burocrazia, inefficienze e lacune di sicurezza.

Rapporto Clusit 2026 – Take Away e So What

- *La consapevolezza delle persone resta critica: l'aumento marcato degli incidenti da phishing è considerato inaccettabile e impone un'azione coordinata di scuole, università, media, soggetti pubblici e privati sulla cultura della cybersecurity, mentre la controversa percezione dell'entità del fenomeno di Hacktivism in Italia denota un sistema paese incapace di comprendere quali siano i pericoli reali da cui dobbiamo guardarci*

    - Deve aumentare la capacità di tutela della reputazione da parte delle vittime, tramite un'adeguata azione comunicativa delle situazioni di incidenti e crisi verso i diversi stakeholders

    - Allo stesso tempo, serve diffondere una visione più matura e consapevole dei rischi della digitalizzazione, per aiutare i decisori e i cittadini a contestualizzare e interpretare in modo più adeguato i diversi trend di (in)sicurezza che andiamo osservando anno su anno

Rapporto Clusit 2026 - Contenuti

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo

- Analisi dei principali incidenti cyber noti del 2025 a livello globale
- Analisi Fastweb + Vodafone della situazione italiana in materia di cyber-crime
- Attività e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica
- Attacchi DDos, ransomware, bot e violazioni delle API in Europa e a livello globale.

Rapporto Clusit 2026 - Contenuti

Speciale FINANCE

- Elementi sul cybercrime nel settore finanziario in Europa
- Come le banche aumentano il livello di sicurezza dei propri stakeholder

Speciale Intelligenza Artificiale

- Evoluzione dell'AI nella Cyber Security: dall'analisi statica al “ragionamento” dell'era GPT e verso sistemi AI autonomi
- Dall’Agentic SOC alla AI Detection & Response: come l’Intelligenza Artificiale sta ridefinendo la cybersecurity
- Il dilemma della fiducia: strategie di cyber resilience essenziali per l'Implementazione dell'Agentic AI
- L’intelligenza artificiale per sviluppare software aziendale: conoscerne i rischi
- OWASP AI Testing Guide: un nuovo standard per la Trustworthiness dei Sistemi di Intelligenza Artificiale.

Speciale Trasporti

- Cyber resilience nel trasporto ferroviario e nella mobilità urbana: stato dell'arte e sfide future
- Information security e aviazione civile, nuove frontiere

Rapporto Clusit 2026 - Contenuti

Survey

- Le tendenze della cybersecurity nel 2026

Focus On

- Cybersecurity IACS e Compliance Normativa - Valutazione della maturità dell'ecosistema industriale italiano
- La fragilità della sanità digitale: crescita degli attacchi, nuovi rischi dall'IA e un perimetro sempre più esteso
- La sicurezza guidata dall'identità nel contesto moderno
- Security by Design nei Digital Twin di Infrastrutture Critiche: un caso di studio nel settore idroelettrico
- Sicurezza nella supply chain ICT: obiettivo raggiungibile?
- Il cantiere che non si ferma: cybersecurity come nuovo vantaggio competitivo nelle costruzioni.
- Cyber Rebel: un progetto che valorizza la neurodivergenza nel settore della cybersecurity

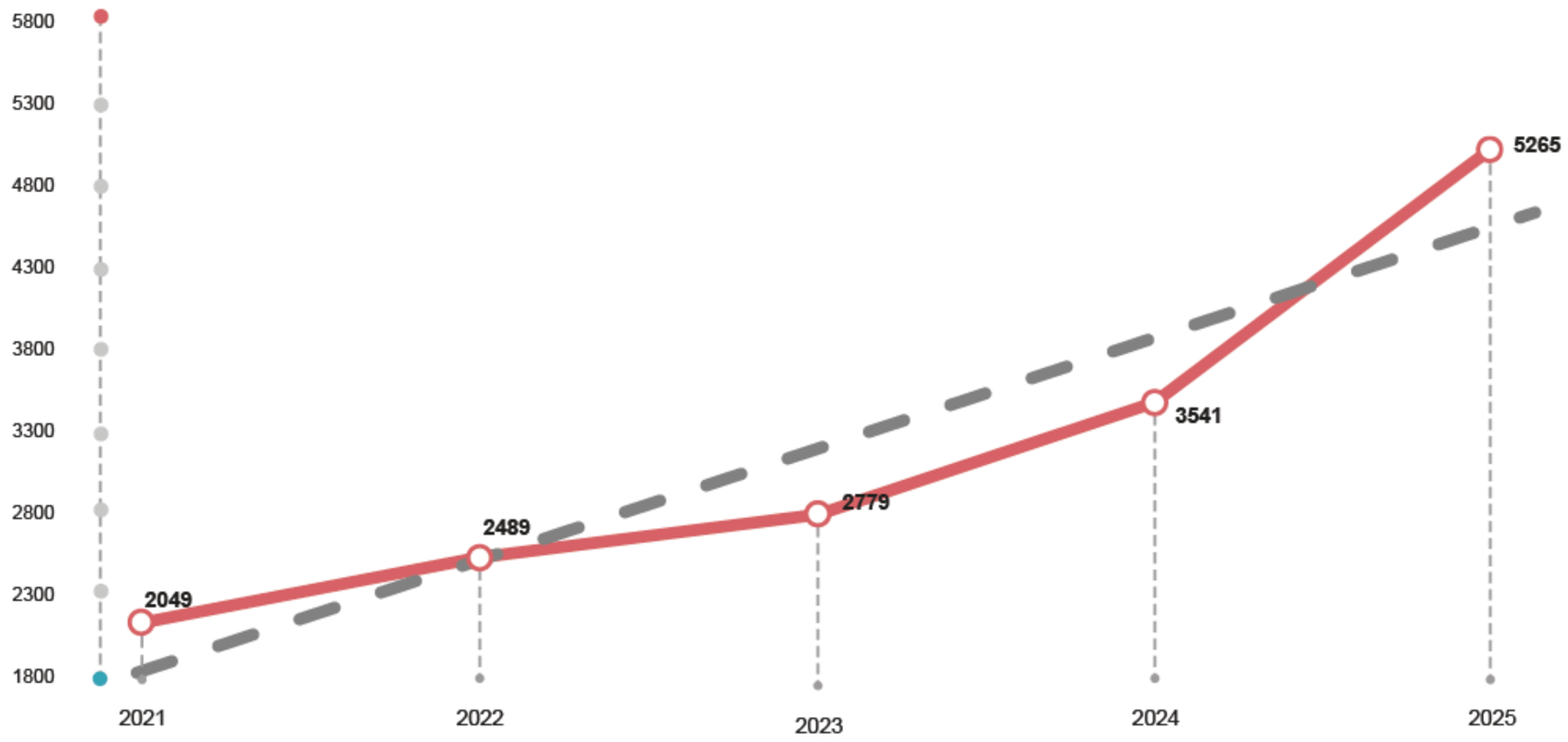
Analisi Clusit dei principali attacchi a livello globale

Sofia Scozzari
Comitato Direttivo
CLUSIT

Incidenti Cyber per anno 2021 - 2025

+49%

è l'aumento degli incidenti cyber nel 2025 rispetto al 2024



© Clusit - Rapporto 2026 sulla Cybersecurity

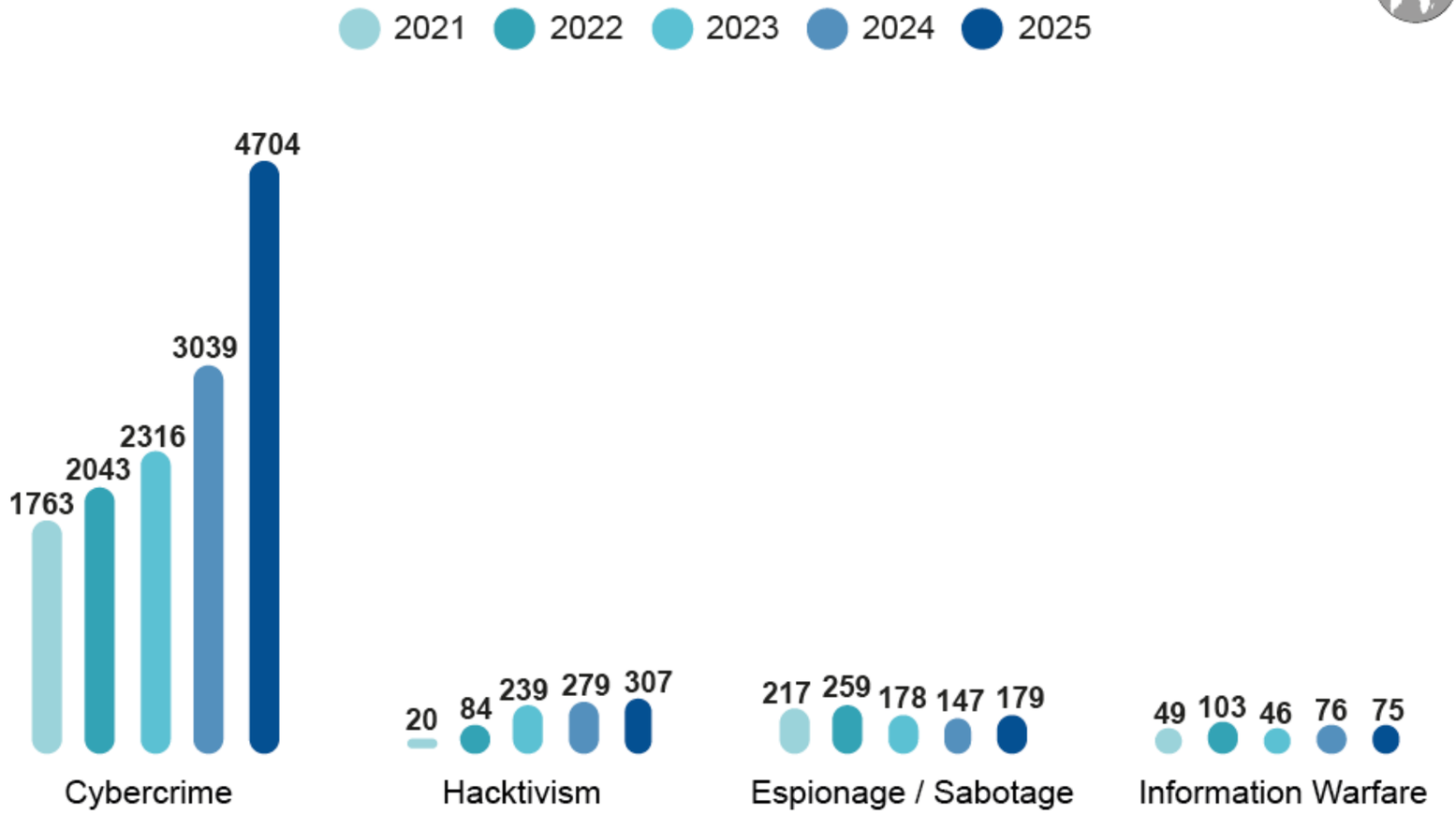
9 su 10

sono incidenti di matrice Cybercrime rispetto alle altre tipologie

+55%

È la crescita degli incidenti Cybercrime dal 2024 al 2025

Attaccanti 2021 - 2025



© Clusit - Rapporto 2026 sulla Cybersecurity

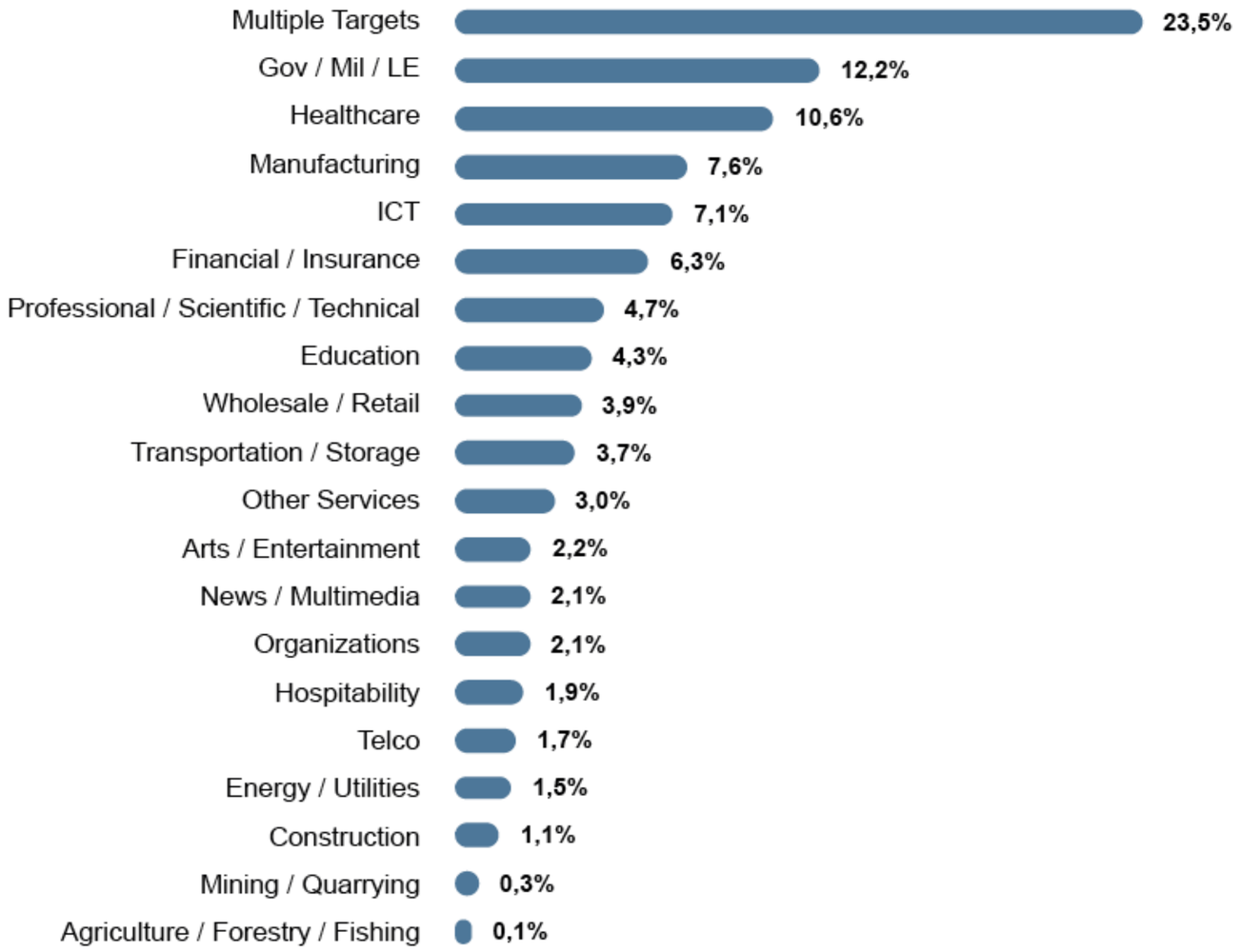
Distribuzione delle vittime 2025

+37%

È la crescita del numero degli incidenti a danno dei settori GOV / Mil / LE

1 su 5

è un incidente derivante da una campagna generalizzata su più settori



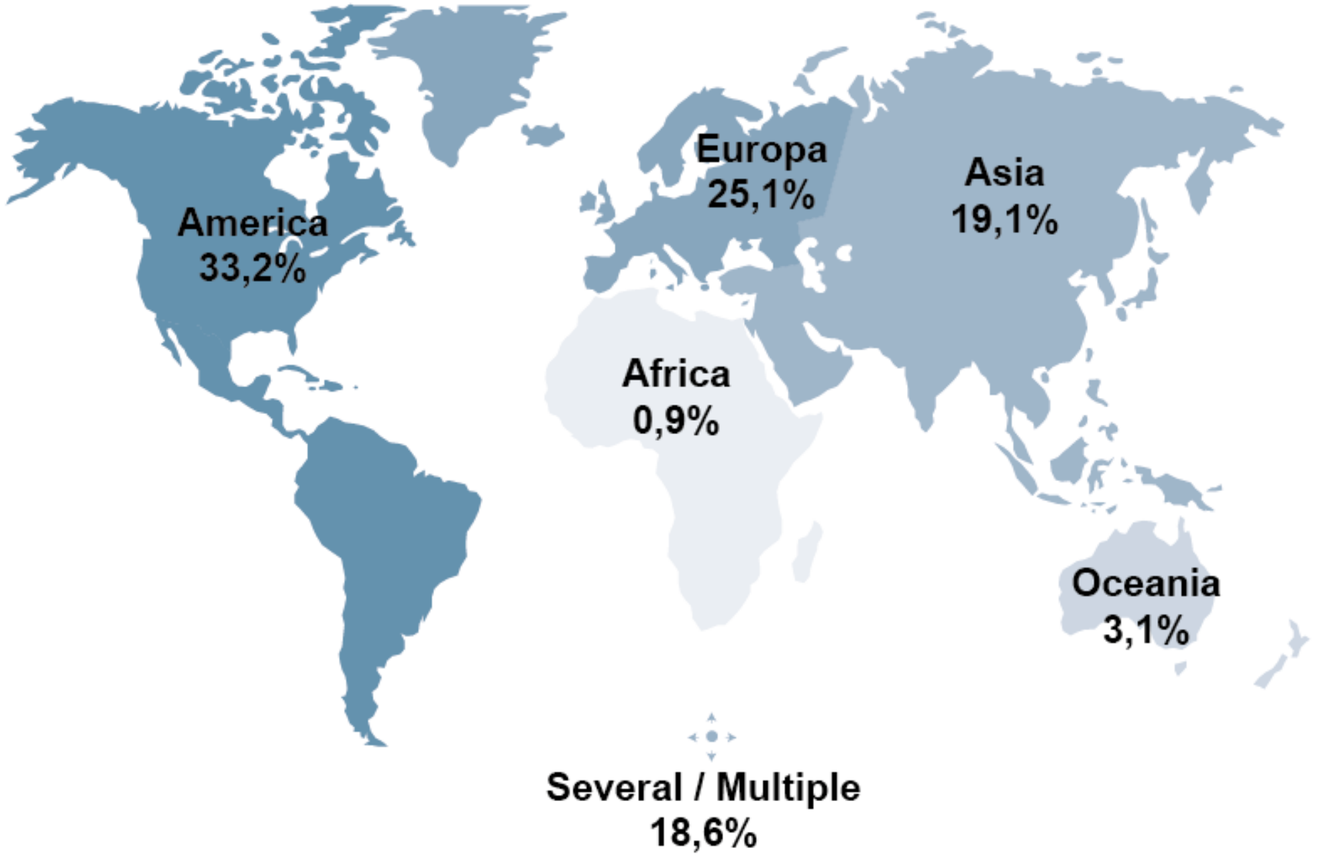
Geografia delle vittime 2025

+21%

è la crescita degli incidenti avvenuti nel continente Europeo

+131%

è la crescita degli incidenti avvenuti nel continente Asiatico



© Clusit - Rapporto 2026 sulla Cybersecurity

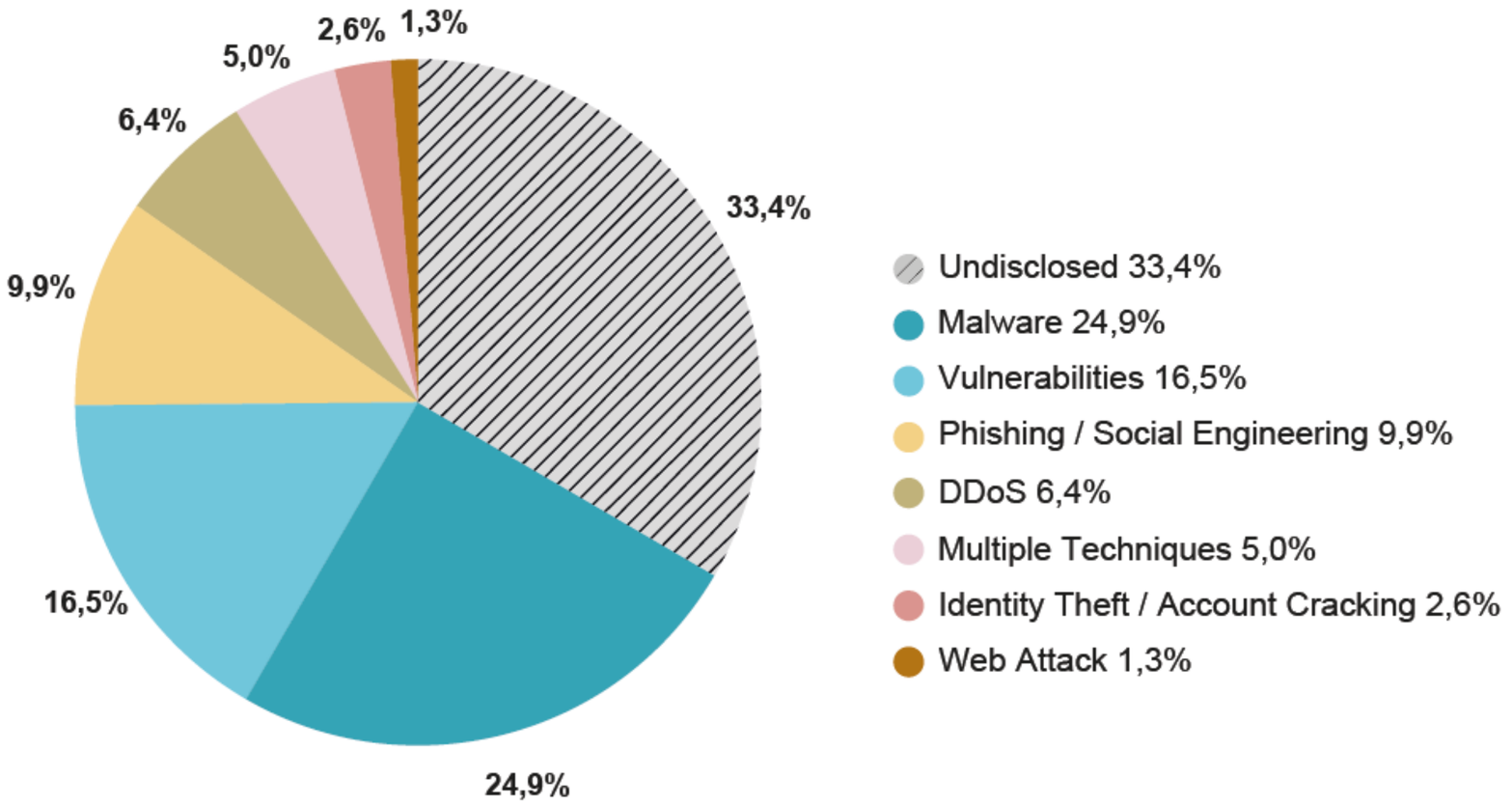
Distribuzione delle tecniche di attacco 2025

1 su 4

È un incidente causato da Malware, al 1° posto nel 2025

+65%

È la crescita del numero degli incidenti basati su Vulnerabilità

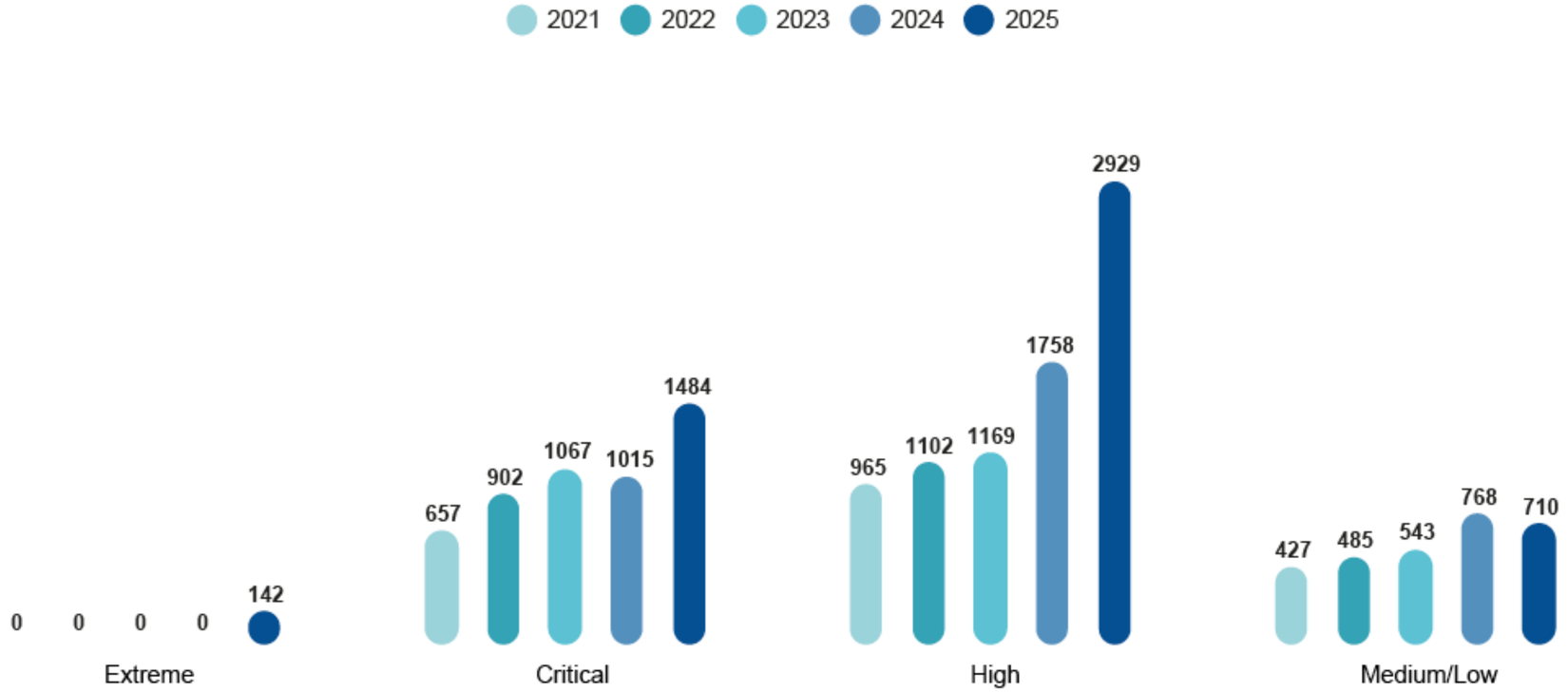


© Clusit - Rapporto 2026 sulla Cybersecurity

Severity 2021 - 2025

1 su 3

incidenti hanno una severity Critical o Extreme



Approfondimento Fastweb + Vodafone

Silvio Ferrari
Manager of Cyber Security Products
Fastweb + Vodafone

I TREND DEL CYBER CRIME

nel 2025

87 milioni
di eventi di
sicurezza in Italia

+26%

Ancora **in crescita** gli attacchi **DDoS**

5.930 **+26%**

I settori più colpiti

1° posto Pubblica Amministrazione **36%**

2° posto Servizi **14,7%**

Cambia il profilo degli attacchi: i **cyber criminali** scelgono **strumenti mirati** per attacchi sempre più **efficaci**.

Infezioni malware **+116%**

IoT Consumer **+1171%**

Servizi telnet esposti in internet **+51%**

L'aumentata **consapevolezza** dei rischi informatici, l'adozione di **sistemi difensivi rafforzati dall'AI** ed alcuni **interventi normativi**, rafforzano le capacità difensive delle organizzazioni.

AI sempre più utilizzata dai cybercriminali, **per aumentare l'efficacia degli attacchi**.

+16% Attacchi **DDoS combinati** in forte crescita.

73,1% I messaggi e-mail malevoli che risultano **verticali** e **mirati**.

+47% In forte crescita il traffico di **Bot Crawler** collegati all'AI.

-6% attacchi **SQL Injection**.

-5,4% Attacchi di **social engineering**.

-12% Sfruttamento di piattaforme **malware-aaS**.

Analisi Fastweb + Vodafone per il Rapporto Clusit su rilevazione dati del 2025 da rete Fastweb e 7Layers e confrontati con il 2024.

FASTWEB + vodafone

Malware e Botnet | Tipologie

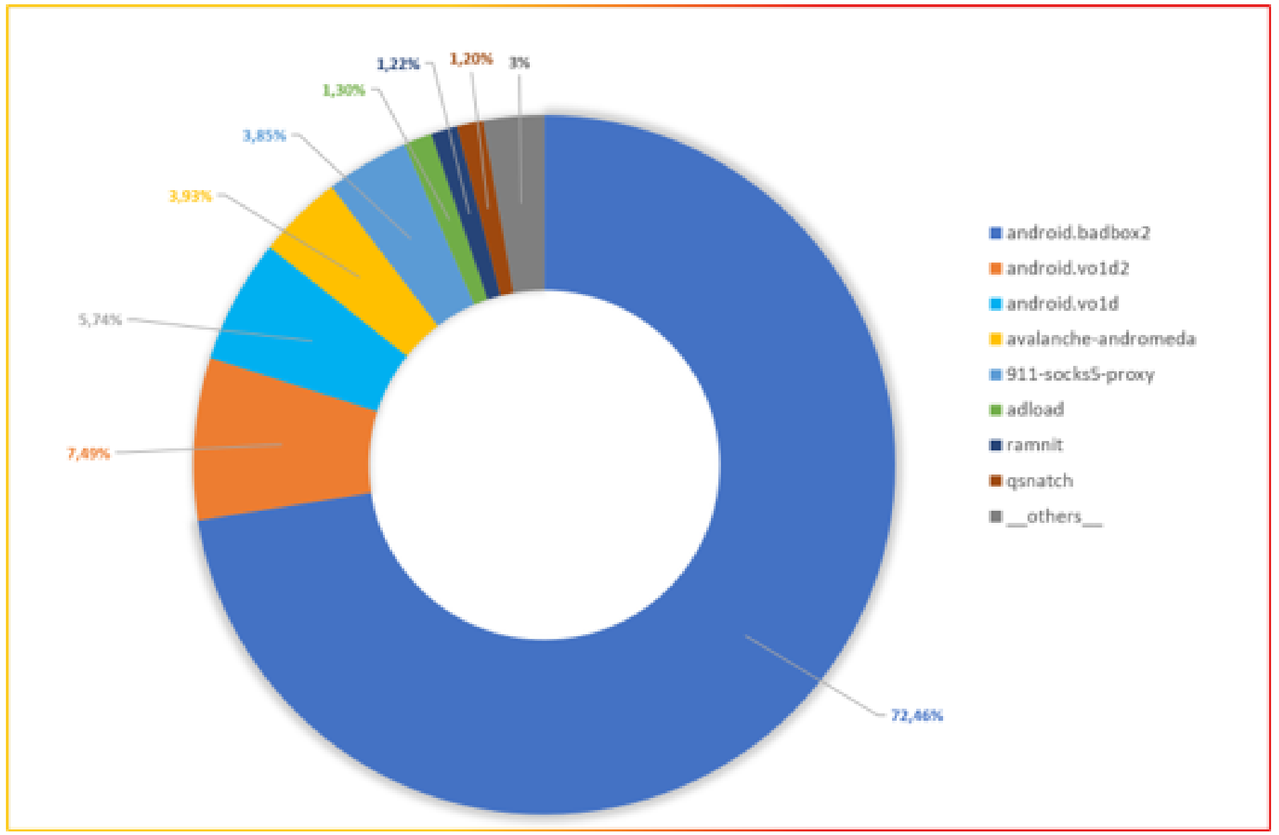
85,69%

I prodotti **IoT Consumer** Android-based sono stati target preferenziali

Avalanche-Andromeda, piattaforma **malware-aaS**, **in calo** di 12 p.p. rispetto al 2024

Diminuisce la varietà di **minacce**, ma aumentano **pervasività ed efficacia**.

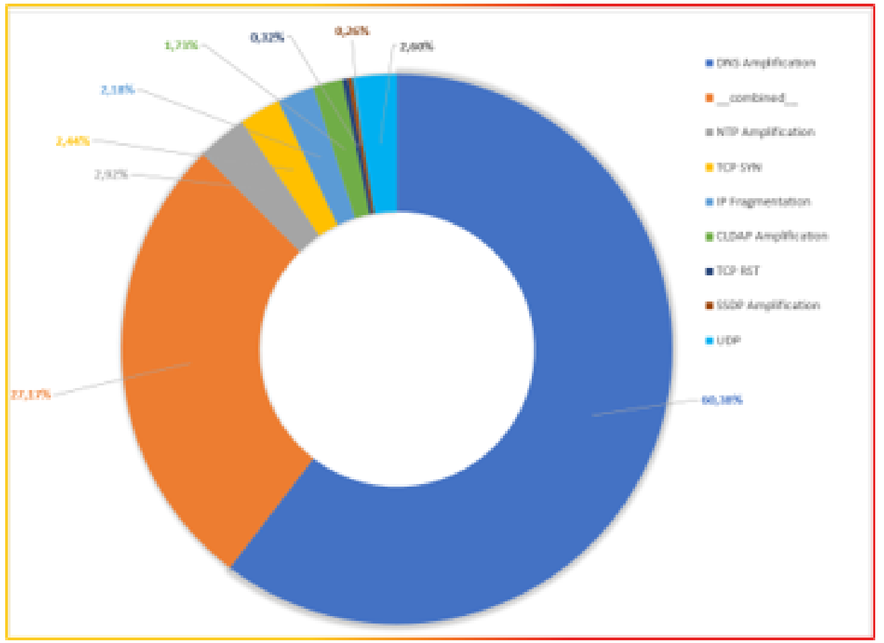
Sempre più importante l'implementazione della **security-by-design**, per ridurre esposizione e impatto.



Famiglie di botnet identificate nel 2025

ATTACCHI DDoS

Distribuzione mensile delle anomalie DDoS



Tipologie di attacco DDoS

+26%

5.930 attacchi DDoS, in crescita rispetto al 2024.

La **Pubblica Amministrazione** guida ancora la classifica delle vittime (36%)

+16,21%

Aumentano gli **attacchi ibridi o multi-vettore** e salgono al 27,17%.

Attacchi meno intensi ma **più frequenti** e distribuiti (carpet bombing).

Sicurezza dei sistemi e delle web application

+31%

31.500 i sistemi con servizi esposti, in forte aumento rispetto allo scorso anno.

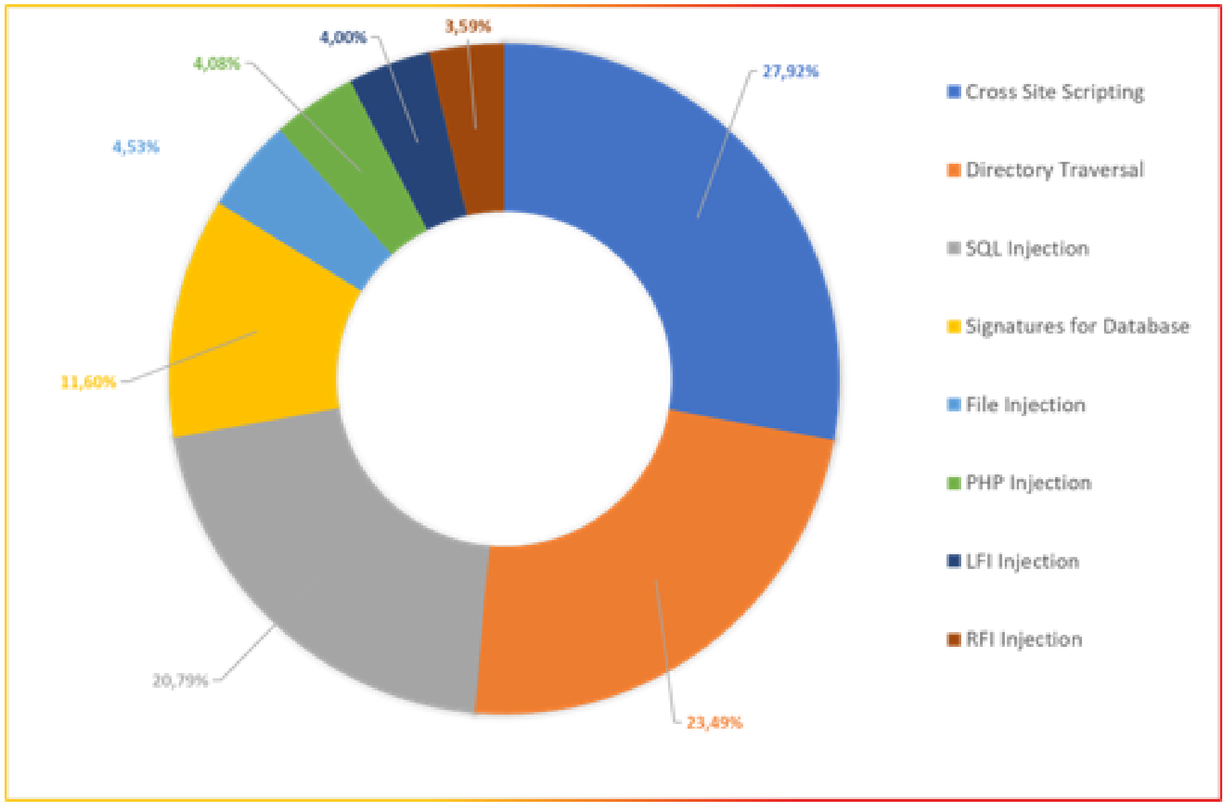
Telnet è ancora il servizio maggiormente esposto, in crescita del 51% rispetto al 2024.

Crescono gli attacchi Cross Site Scripting (+12,11%), a discapito di SQL Injection (-6 p.p.).

11,6%

Novità rispetto al 2024: gli attacchi specifici verso i Database (**Signatures for Database**)

Importante aumento di **Bot Crawler** collegati a sistemi **intelligenza artificiale**.



12%

Aumentano gli **attacchi originati in Italia,** che si posiziona seconda, dopo gli USA e prima di UK

MAIL SECURITY | Trend e minacce

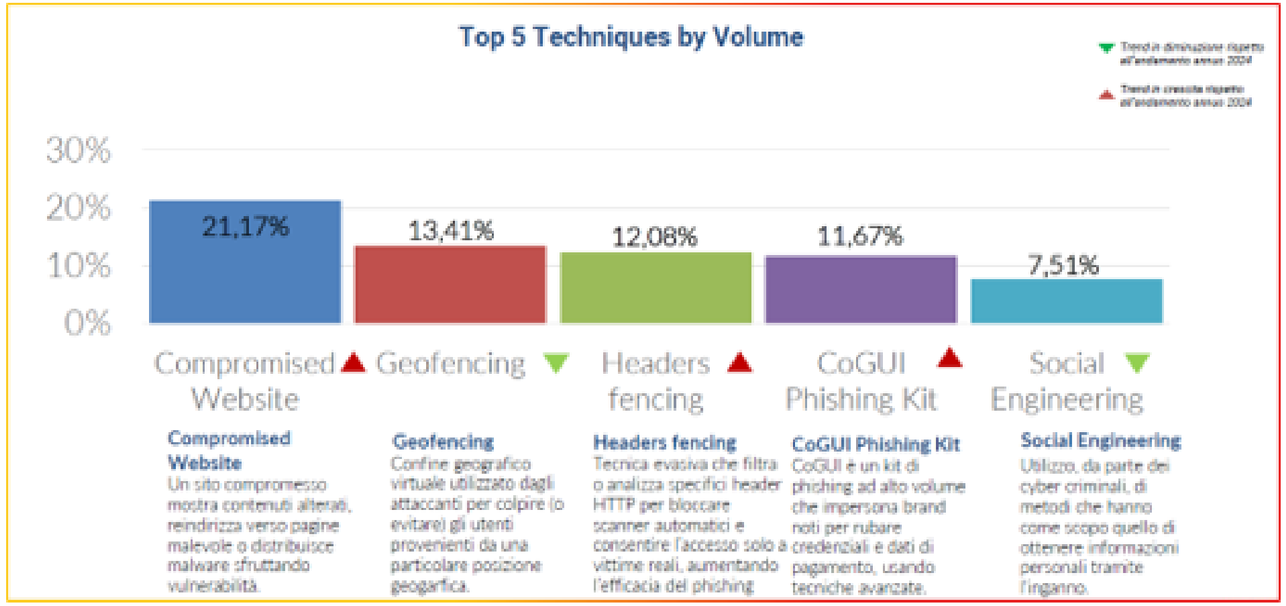
89,5%

Il **click-through** è ancora la tecnica di attacco preferenziale

73,1%

Individual threats: gli invii si fanno sempre più personali e **mirati** supportati dall'uso di **AI**.

Tra le threat categories prevale ancora il **phishing**, che si sta sempre più specializzando nella sottrazione di credenziali (sia business che consumer)



Analisi delle principali tecniche di attacco

7Layers | Analisi delle tecniche di attacco

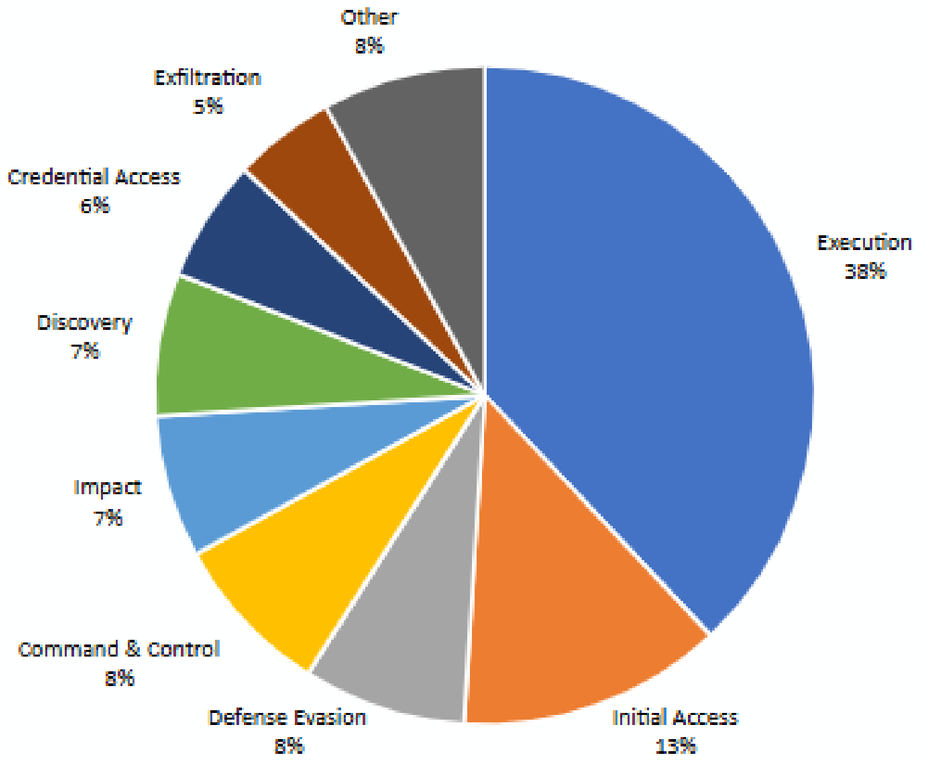
Dall'analisi di 7Layers delle tecniche di attacco, classificate secondo il MITRE, la **distribuzione** risulta sostanzialmente **immutata** rispetto allo scorso anno.

Prevalgono ancora le tattiche di **Execution** (stabilmente al 38%).

Crescente sofisticazione nelle tecniche di **phishing** ed un **aumento** in frequenza e **complessità** dello sfruttamento degli **zero-day**.

-4%

Rispetto al 2024 lo sfruttamento di tecniche di **Exfiltration** è **diminuito** di 4 p.p.



ANALISI FASTWEB | Key Findings

L'AI continua ad accelerare il miglioramento delle tecniche e degli strumenti. Gli attacchi sono sempre più sofisticati, multi-vettore e persistenti.

Cresce la superficie d'attacco, anche nel perimetro domestico (Consumer IoT), mentre ancora troppi sistemi espongono in Internet applicativi e servizi vulnerabili.

Le minacce informatiche impattano significativamente la Pubblica Amministrazione, ma si stanno estendendo anche ad altri settori vitali per l'economia, come l'Energia ed i Servizi.

Le aziende si difendono sempre più efficacemente e intensificano l'adozione di programmi di awareness. Security by design e sicurezza della «supply-chain» devono diventare sempre più centrali nella strategia di sicurezza.

La cyber security rappresenta una priorità strategica: è più efficace se sostenuta da interventi normativi e da meccanismi pubblici di sostegno agli investimenti delle aziende.

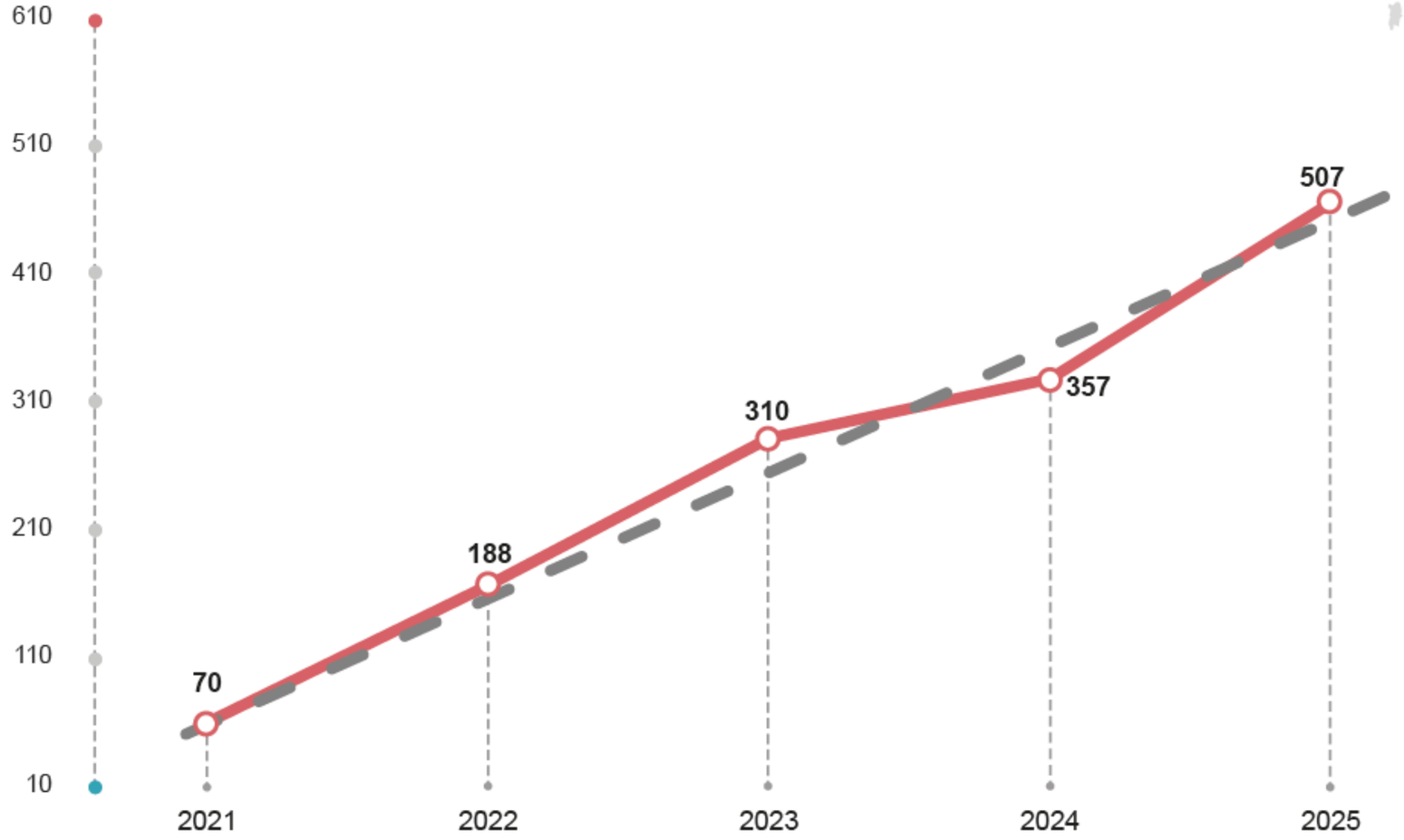
Approfondimento Dati Italia

Giorgia Dragoni
Osservatorio Cybersecurity & Data Protection
Politecnico di Milano

Incidenti Cyber in Italia 2021 - 2025

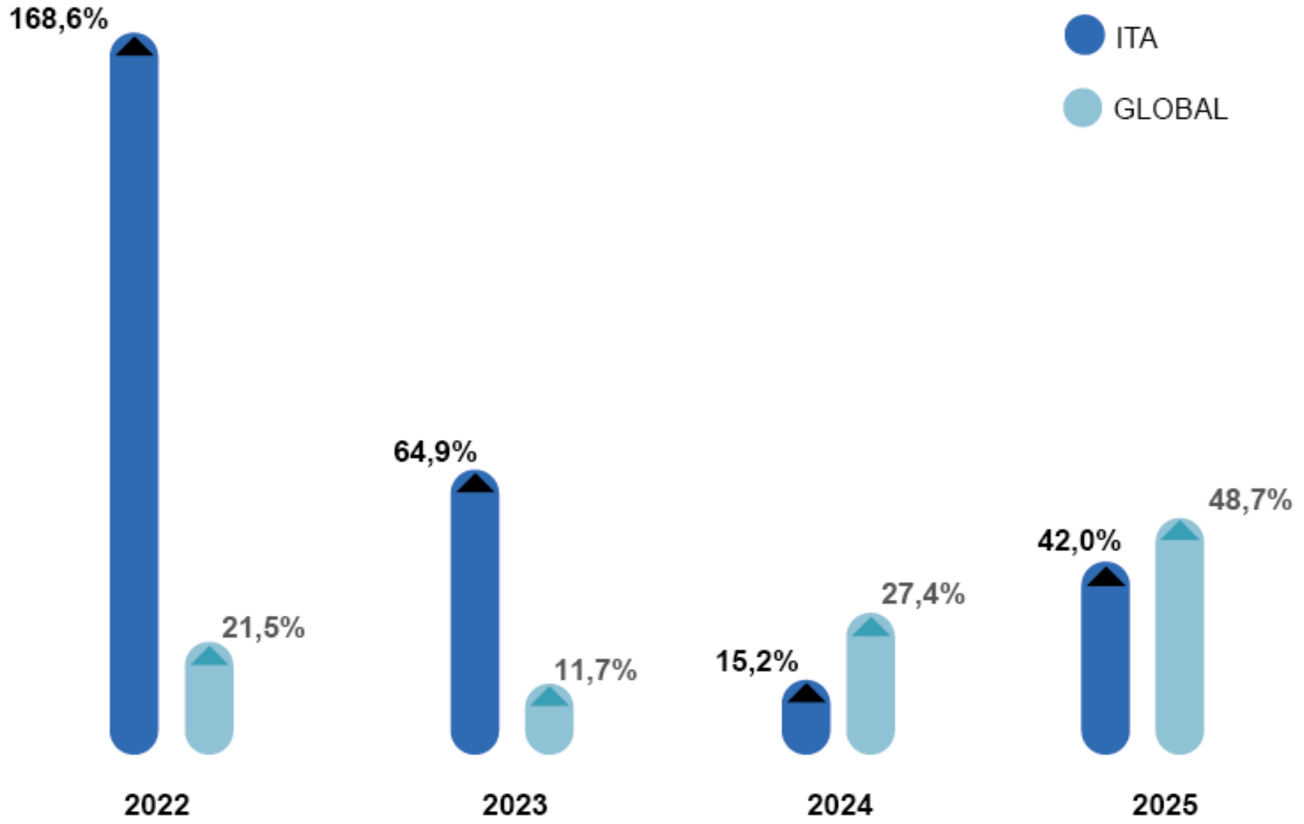
+42%

è l'aumento degli incidenti cyber nel 2025 rispetto al 2024 in Italia



© Clusit - Rapporto 2026 sulla Cybersecurity

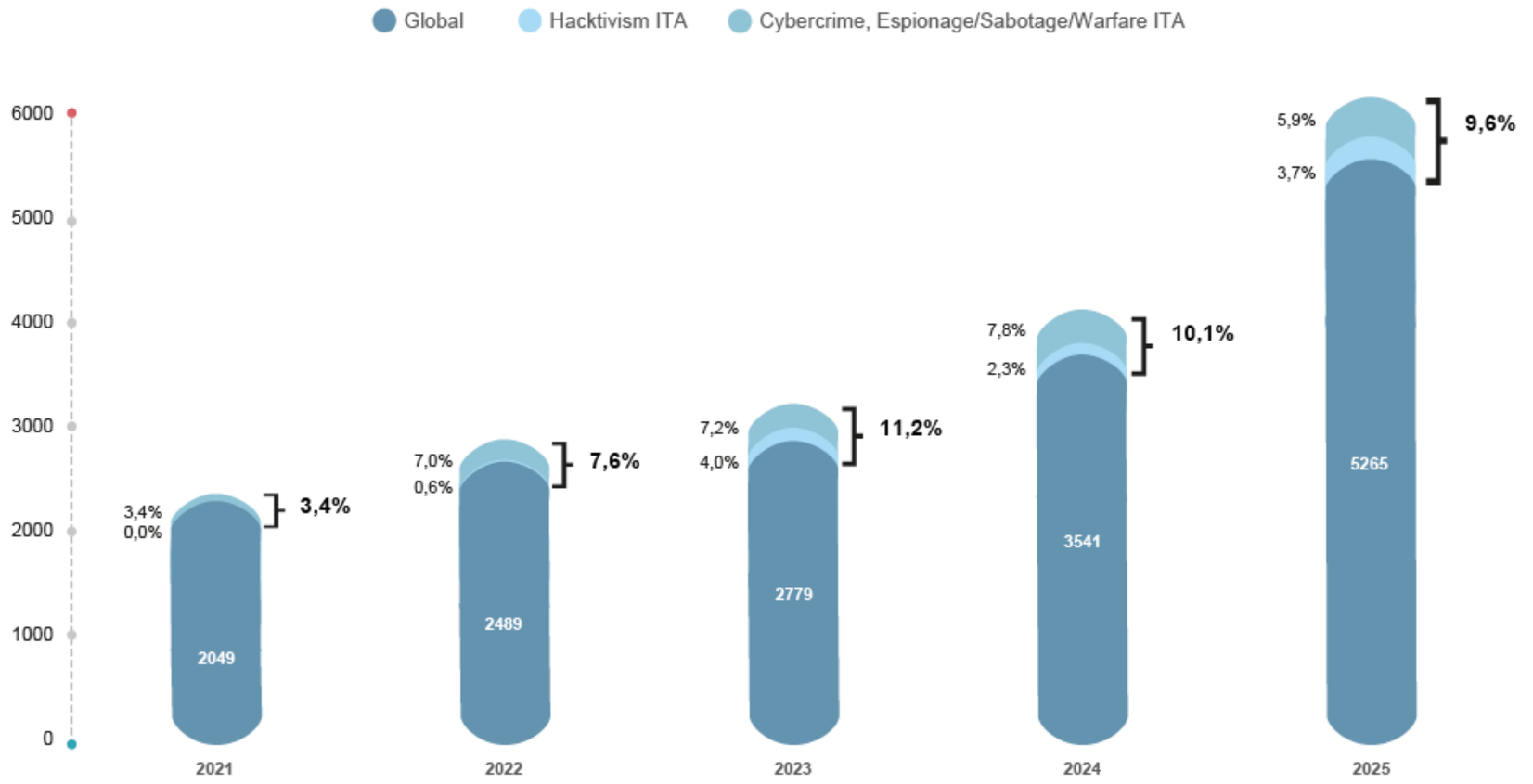
Confronto crescita % Italia vs Global



Confronto Italia vs. Global 2021 - 2025

9,6%

è la percentuale di incidenti cyber avvenuti in Italia rispetto al resto del mondo



© Clusit - Rapporto 2026 sulla Cybersecurity

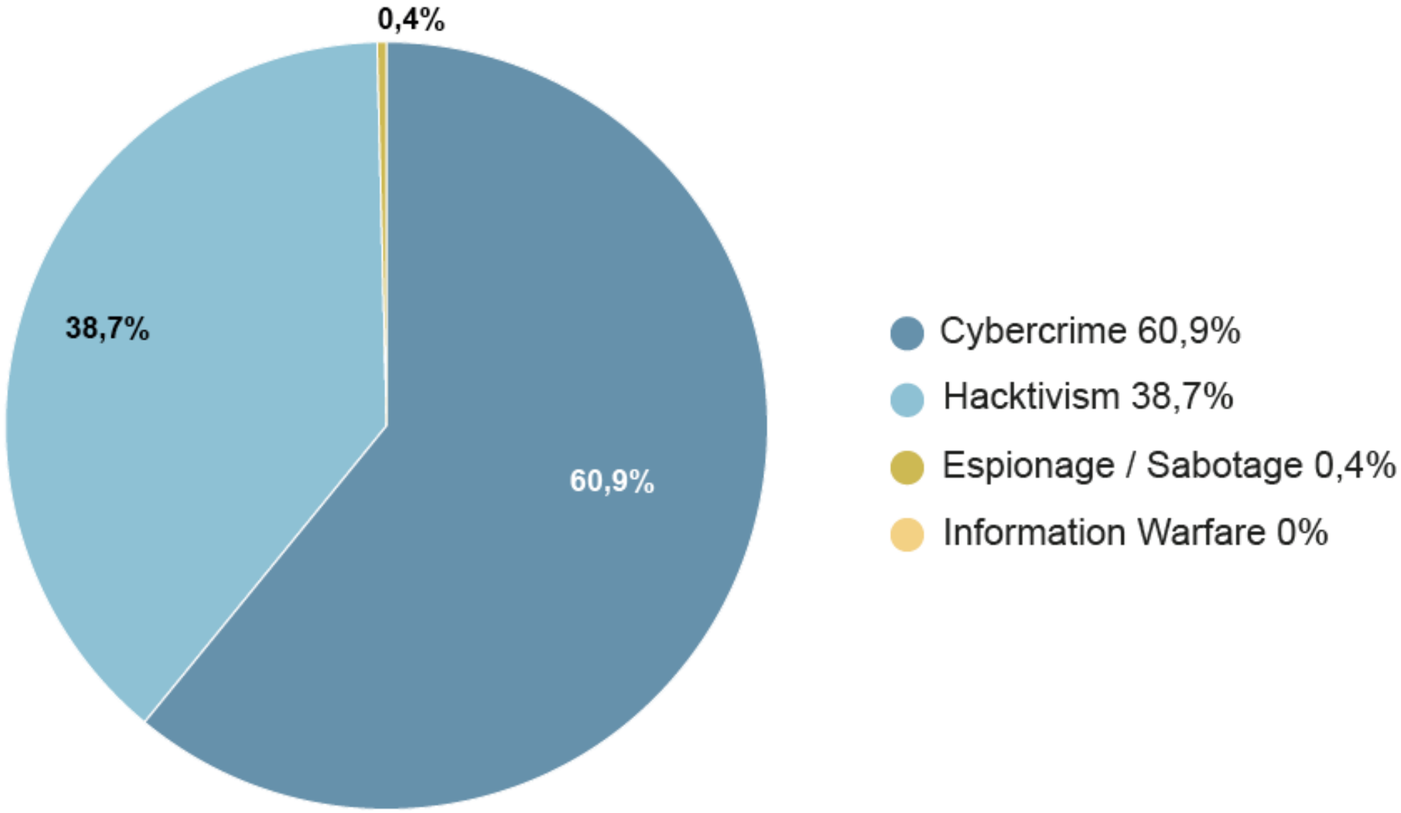
Attaccanti in Italia 2025

61%

è la percentuale di incidenti di matrice Cybercrime in Italia

+145%

è la crescita degli incidenti di Hacktivism in Italia rispetto al 2024



© Clusit - Rapporto 2026 sulla Cybersecurity

Vittime in Italia 2025

16%

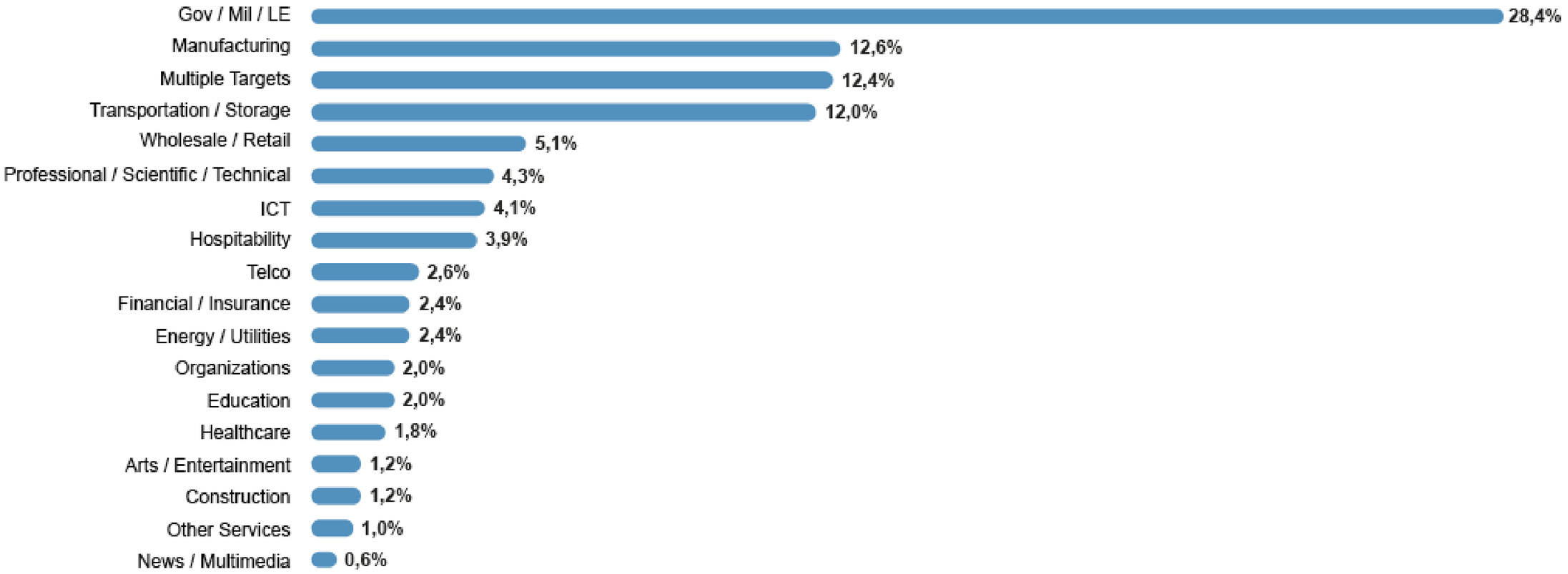
degli incidenti al settore Manifacturing nel mondo avviene in Italia

+290%

è la crescita degli attacchi al settore GOV/MIL/LE in Italia

+134%

è la crescita degli attacchi al settore Transportation / Storage in Italia



Tecniche di attacco in Italia 2025

DDOS

è la principale tecnica di attacco in Italia

+66%

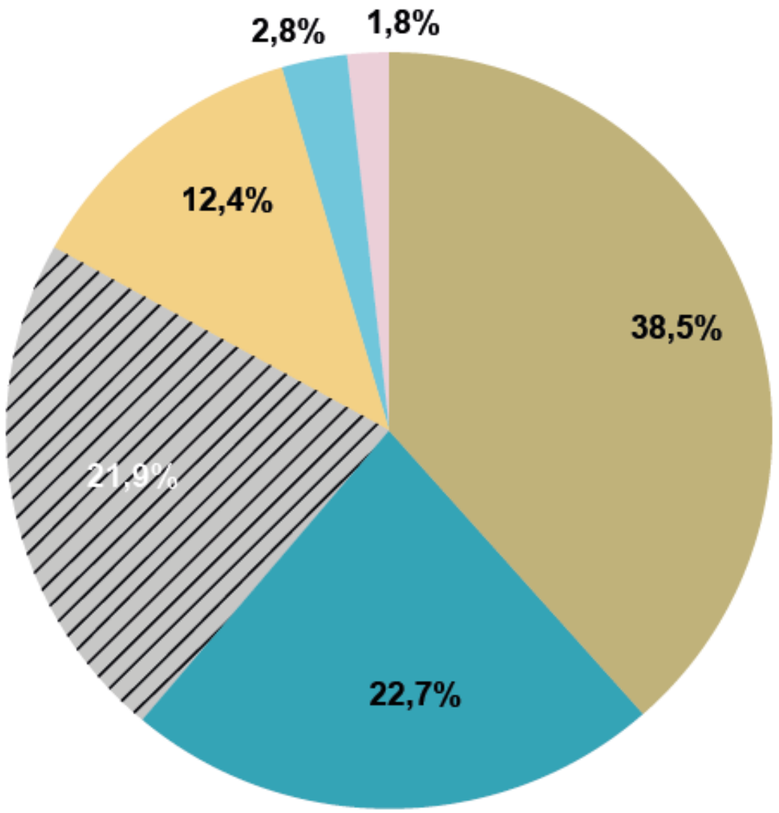
è la crescita di incidenti di tipo Phishing / Social Engineering in Italia

-14%

è la diminuzione degli incidenti Malware in Italia rispetto al 2024

-79%

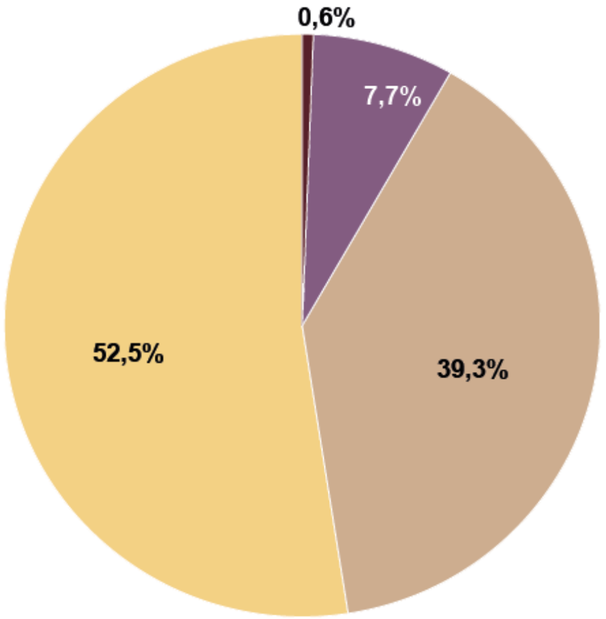
è la diminuzione degli incidenti basati su vulnerabilità in Italia rispetto al 2024



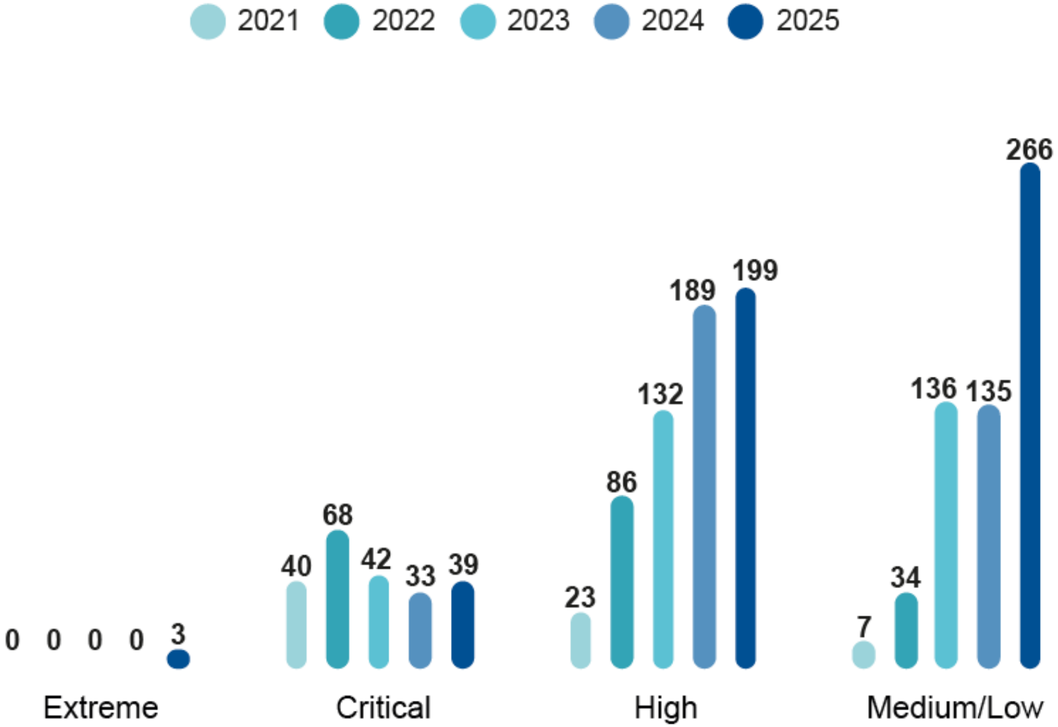
- DDos 38,5%
- Malware 22,7%
- Undisclosed 21,9%
- Phishing / Social Engineering 12,4%
- Vulnerabilities 2,8%
- Multiple Techniques 1,8%
- Web Attack 0%

Severity in Italia 2021 - 2025

52%+
degli incidenti in Italia hanno il livello più basso di severity (Medium/Low)



- Extreme 0,6%
- Critical 7,7%
- High 39,3%
- Medium/Low 52,5%



Attività e segnalazioni del Servizio Polizia Postale e per la Sicurezza Cibernetica

- Panoramica Generale: Oltre **52.590 casi gestiti** su tutto il territorio nazionale
- **Protezione Infrastrutture Critiche** (C.N.A.I.P.I.C.): Gestione di **9.440 eventi** cibernetici e invio di oltre **50.445 alert** di sicurezza
- **Financial Cybercrime**: Più di **27.600 casi** trattati con una sottrazione stimata di capitali pari a oltre **275 milioni** di euro
- Contrasto alla **Pedopornografia** (C.N.C.P.O.): Un incremento significativo dell'efficacia repressiva con **224 arresti** (**+52%** rispetto al 2024)
- Reati contro la persona: Un totale di **9.768 casi**, con 487 attivazioni del protocollo "Codice Rosso" per reati come **stalking e revenge porn**

Minori e Social

1. Adescamento Online (**Grooming**): il fenomeno è in costante crescita, con **434 casi** trattati nel 2025 (**+16%** rispetto al 2024)
    - Mentre i casi tra i bambini 0-9 anni sono diminuiti, si registra un incremento allarmante del **69% nella fascia 14-16 anni**, dove la vulnerabilità emotiva viene sfruttata nonostante le maggiori competenze tecniche dei ragazzi
2. **Sextortion** (Estorsione Sessuale): Questa è considerata l'emergenza di maggiore gravità del 2025, con un incremento del **+72%** dei casi (da 130 a 223)
3. Cyberbullismo e Revenge Porn
    - **Cyberbullismo**: I casi sono aumentati del **+13%** (365 totali), manifestandosi con minacce, diffamazione e aggressioni psicologiche sui social
    - **Revenge Porn**: La diffusione non consensuale di immagini intime ha registrato una flessione del **-31%** (29 casi nel 2025), segno di una possibile maggiore consapevolezza tra i giovani, anche se l'**impatto** resta **devastante** per la reputazione e l'identità sociale del minore

Tavola rotonda

moderata da **Alessio Pennasilico**, CS Clusit, con gli esperti di security di alcuni dei principali fornitori di prodotti e servizi di sicurezza ICT, che arricchiranno il dibattito con le loro esperienze sul campo:

- **Nicola Dalla Vecchia**, Akamai
- **Luca Nilo Livrieri**, CrowdStrike
- **Umberto Pirovano**, Palo Alto Networks
- **Maurizio Taglioretti**, Netwrix

Contatti

rapporti@clusit.it
info@astrea.pro
avaccarelli@clusit.it
gdragoni@clusit.it
apennasilico@clusit.it
sscozzari@clusit.it
lbechelli@clusit.it
Silvio.ferrari@fastweb.it