ASSOLOMBARDA

XII° USCITA

Cyber Security News

La Cyber Security News è un'indagine semestrale dedicata agli eventi di cyber security sul territorio di Assolombarda. Le pubblicazioni, realizzate grazie ad una partnership con Exprivia [1], forniscono una panoramica dello stato dei territori dell'associazione in tema di sicurezza informatica. [2]

Di seguito verrà analizzato quanto emerso nei **primi 6 mesi del 2025**.

Nel primo semestre del 2025, sul territorio di Assolombarda sono stati registrati **1795 eventi di sicurezza**, con un aumento significativo rispetto allo stesso periodo del 2024 (+**836**), suddivisi in:

- **1663** attacchi informatici (+65% dal 1Q2025 al 2Q2025);
- **115** incidenti di sicurezza (+50% dal 1Q2025 al 2Q2025);
- **17** violazioni privacy.

Sebbene il numero complessivo degli attacchi sia in crescita, è opportuno notare che gli **incidenti** rappresentano il **6,4% del totale degli eventi**, in calo rispetto al 7,7% registrato nel primo semestre del 2024, un dato probabilmente riconducibile al progressivo rafforzamento delle misure di cybersecurity adottate dalle imprese.

Quando si parla di eventi di sicurezza si considerano:

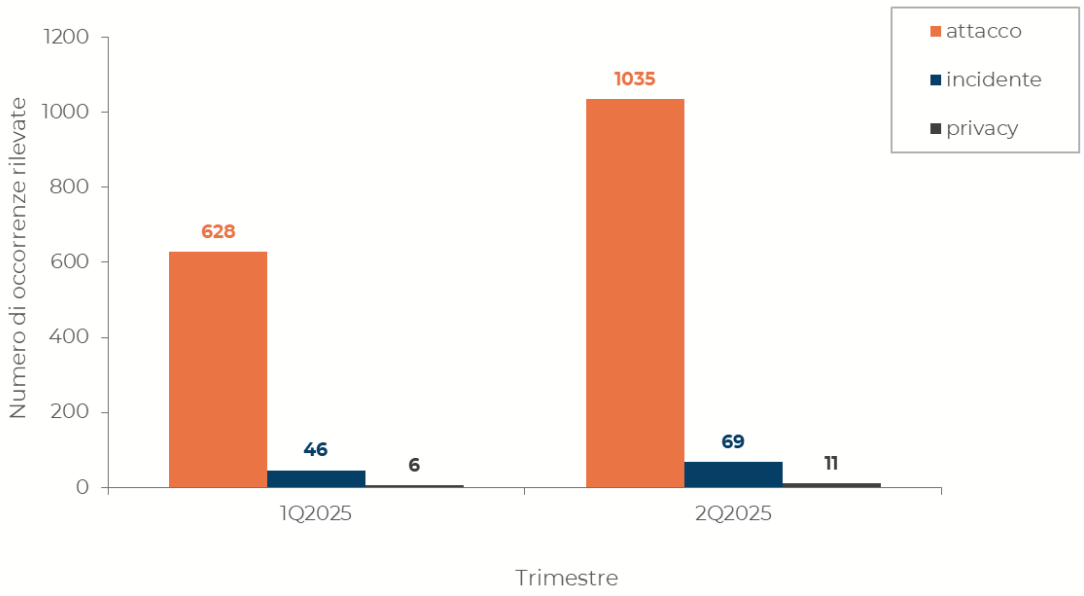
- **Attacchi**: insieme di azioni intraprese per compromettere un servizio. In presenza di una campagna di phishing indirizzata a molti target, verrà contabilizzata la campagna come un attacco. Il rapporto include campagne criminali intese a sfruttare vulnerabilità di servizi ampiamente utilizzati in Italia.
- **Incidenti**: un attacco che ha avuto successo. Nel caso di un attacco che abbia avuto successo su diverse entità, verranno contabilizzate tutte le istanze di incidenti nei confronti delle varie vittime.

---

[1] Azienda internazionale specializzata nel settore dell'Information and Communication Technologies.

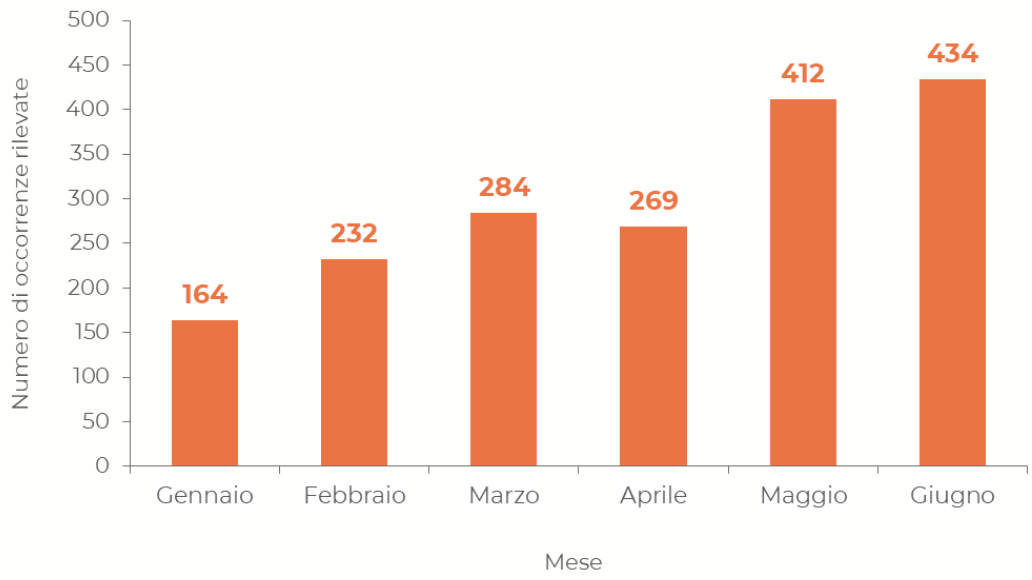
[2] L'Osservatorio Cyber Security di Exprivia colleziona informazioni pubbliche e non, ma crea statistiche utilizzando solo le prime per garantire la confidenzialità delle informazioni e per avere un insieme di dati statisticamente validi e il più possibile solidi. Le statistiche, infatti, vengono aggiornate modificando il numero di sorgenti. Nuove sorgenti vengono inserite solo e soltanto se i dati acquisti sono rilevanti dal punto di vista statistico e integrabili. A ogni record inserito nel rapporto corrisponde una precisa informazione sulla sorgente da cui questo record è stato preso.

- **Violazioni privacy**: vengono contate non solo le violazioni segnalate dalle istituzioni (ad esempio GDPR), ma anche quelle pubbliche quando queste ultime dovessero essere eclatanti. Ovviamente manterremo il riserbo e non esporremo la vittima, anche se la violazione dovrà essere descritta in una sorgente aperta, ma il dato riteniamo che abbia rilevanza statistica, al pari di incidenti e attacchi.



Distribuzione temporale

Gli eventi di sicurezza registrati nei primi sei mesi del 2025 mostrano un **andamento in crescita**. Il mese di **gennaio** presenta il numero più basso di episodi (**164**), mentre **giugno** risulta il più critico, con ben **434** casi tra attacchi, incidenti e violazioni della privacy. A titolo di confronto, nello stesso periodo del 2024, il mese con il maggior numero di eventi era stato marzo, con 196 attacchi. Il confronto evidenzia quindi un incremento significativo nel primo semestre del 2025, con cinque mesi su sei che superano ampiamente tale soglia.



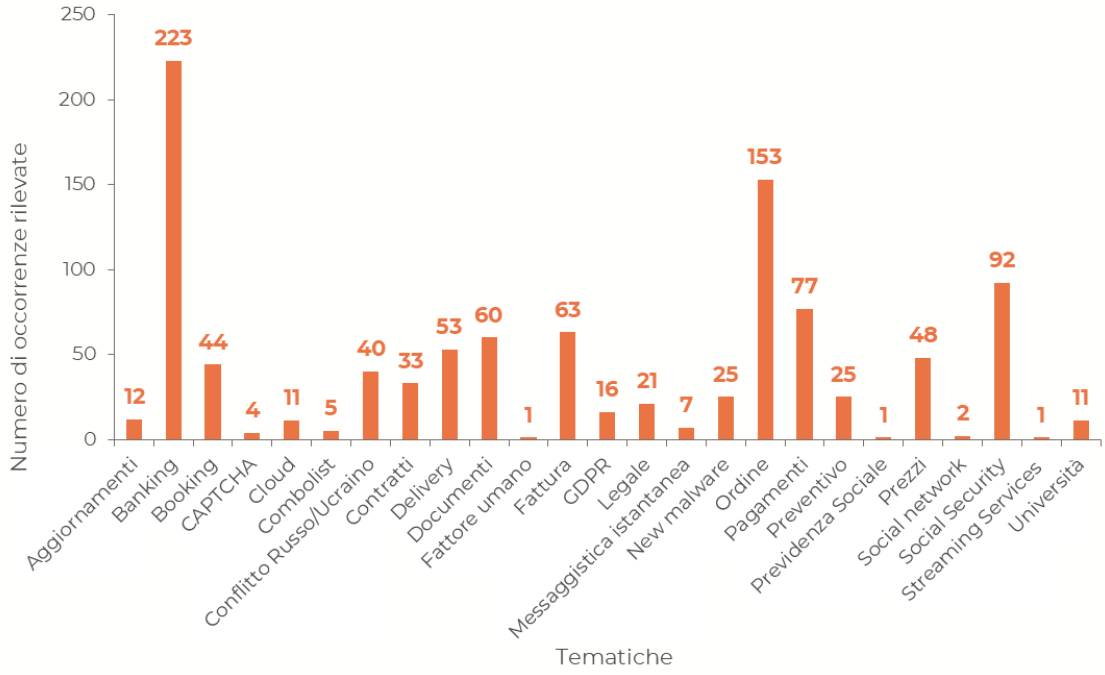
Tematiche degli attacchi

Il grafico sottostante mostra come, sebbene un numero limitato di tematiche continui a concentrare la maggior parte degli attacchi, stia emergendo una progressiva diversificazione dei trend di attacchi, incidenti e violazioni della privacy nel nostro territorio, con un numero crescente di tematiche che mostra occorrenze rilevanti.

Ancora una volta, la categoria **Banking** risulta la più colpita, con **223 occorrenze**, a conferma della vulnerabilità dei servizi finanziari digitali, legata sia al valore economico dei dati gestiti sia al potenziale ritorno di un attacco riuscito.

Segue la categoria **Ordine (153)**, che riguarda i processi di acquisto e vendita online, spesso sfruttati tramite phishing o spoofing per sottrarre credenziali o informazioni sensibili. Al terzo posto si colloca la categoria **Social Security (92)**, indice di un crescente interesse da parte dei cybercriminali verso le informazioni anagrafiche e le identità digitali dei cittadini, sempre più centrali nei servizi pubblici e privati.

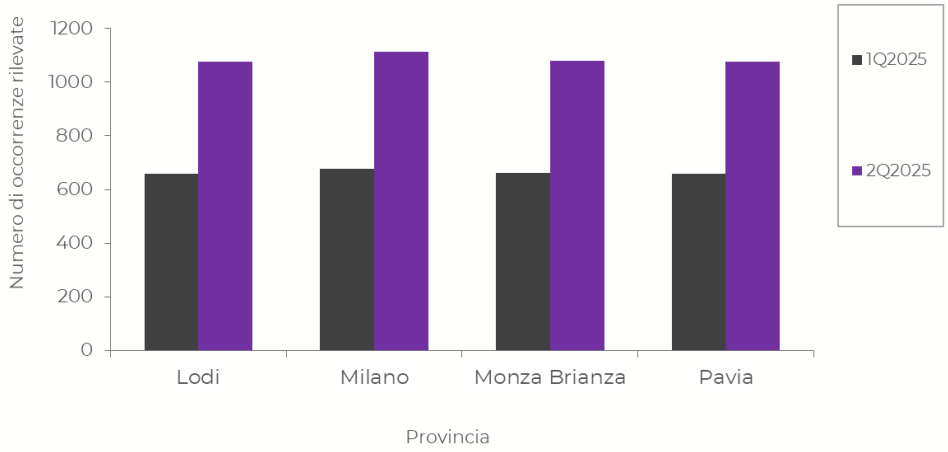
Infine, le aree **Pagamenti (77)** e **Fattura (63)** mantengono un peso significativo, riflettendo una tendenza agli attacchi mirati ai processi economico-amministrativi, attraverso campagne finalizzate alla manipolazione dei flussi di pagamento.



La distribuzione Geografica

Dall'analisi della distribuzione geografica di attacchi, incidenti e violazioni della privacy, viene evidenziata una **concentrazione equamente distribuita tra le diverse provincie**, a dimostrazione del fatto che gli attacchi sono ormai pregnanti in tutto il territorio in cui l'associazione opera.

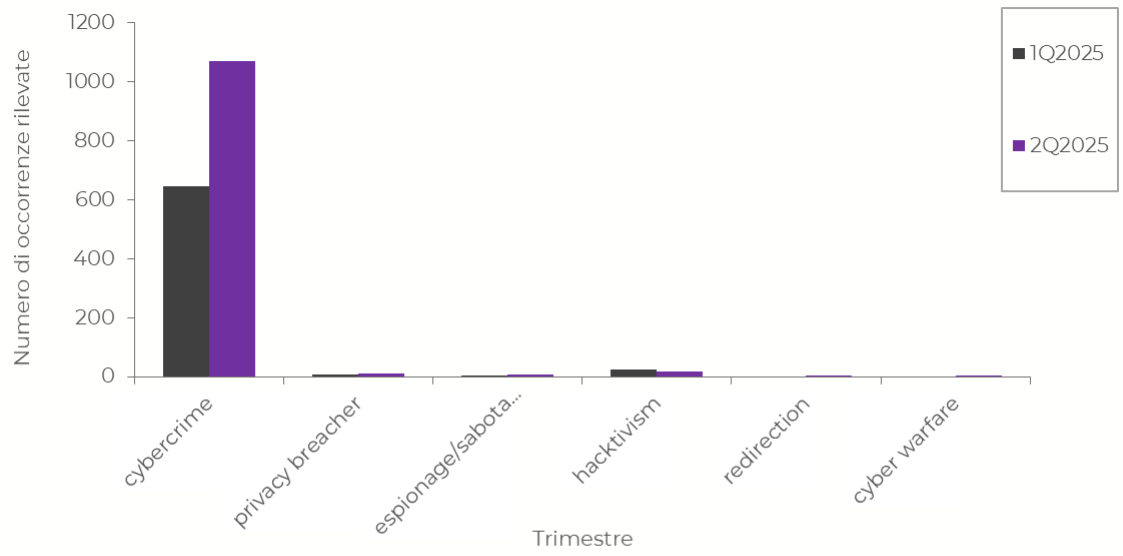
Il numero degli attacchi è riportato considerando che alcuni eventi riguardano tutti i territori ed altri, invece, sono rilevati soltanto in una determinata provincia.



	1Q2025	2Q2025
Lodi	660	1077
Milano	677	1113
Monza Brianza	663	1079
Pavia	660	1077

Le motivazioni

Dall'analisi delle motivazioni emerge che su un totale di 1795 casi, oltre il **95%** (1717 casi) è riconducibile ad attività criminali (**cybercrime**), ovvero reati informatici perpetrati attraverso l'ausilio di tecniche e strumenti acquisibili in rete (ad esempio nel Dark Web esiste una vera e propria industria del Malware come le piattaforme di malware-as-a-service). In confronto, i casi legati ad **hacktivism**, ovvero quelli che mirano a promuovere un'agenda politica o principi sociali, sono stati significativamente meno frequenti, con **42** episodi. Ancora meno numerosi sono stati i casi di violazione della sicurezza dei dati (**privacy breacher**), che si sono attestati a **19**, e quelli legati a **espionage/sabotage** (**11**).



	1Q2025	2Q2025
cybercrime	646	1071
privacy breacher	7	12
espionage/sabotage	2	9
hacktivism	25	17
redirection	0	5
cyber warfare	0	1

Le vittime

Appartiene al settore **Software/Hardware** il maggior numero di vittime di eventi di sicurezza registrati nel corso del primo semestre del 2025, precisamente **641** vittime (**35,7%**). L'elevato numero di vittime può essere spiegato dal ruolo centrale che le imprese di questo comparto rivestono nel fornire servizi e infrastrutture digitali ad altre organizzazioni: un singolo attacco riuscito, infatti, può generare effetti a catena su un ampio numero di soggetti interconnessi.

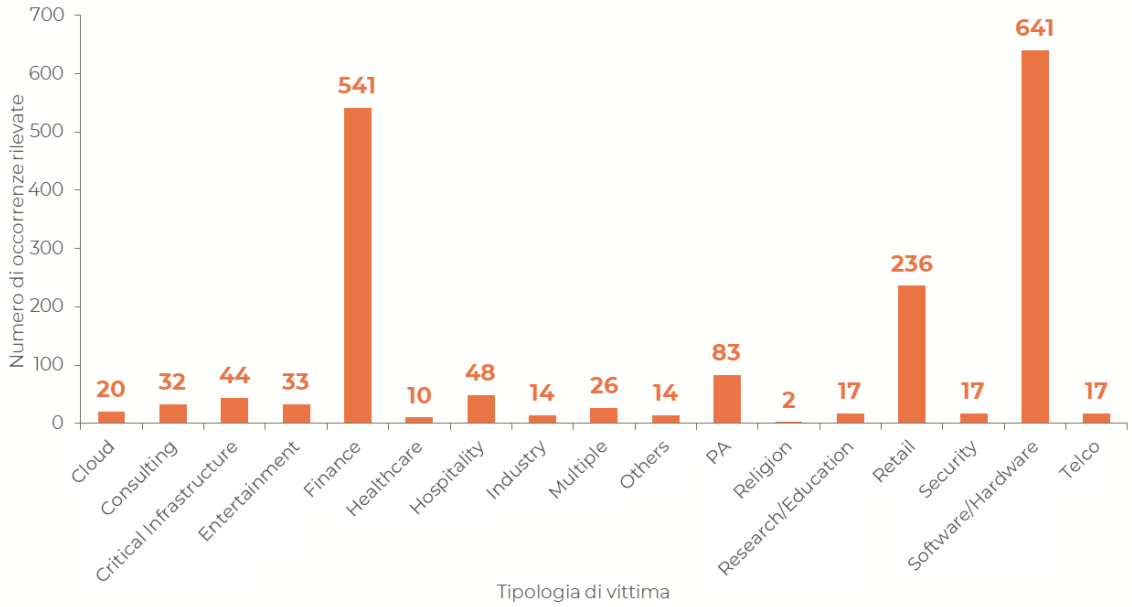
Il secondo settore maggiormente colpito è il **Finance**, con **541** vittime (**30,1%**). Le aziende finanziarie, infatti, gestiscono grandi quantità di dati sensibili e denaro, rendendole un obiettivo attraente per gli attaccanti. Inoltre, il settore finanziario è altamente regolamentato e le conseguenze di una violazione della sicurezza possono essere molto severe, sia in termini di sanzioni che di danni alla reputazione.

Segue il **Retail**, che si conferma come settore altrettanto vulnerabile, con numeri di vittime importanti (**236**).

Per quanto riguarda la **Pubblica Amministrazione (83)**, essa gestisce molti dati sensibili dei cittadini e ha responsabilità importanti nell'amministrazione dello Stato; di conseguenza può rappresentare un bersaglio per i cybercriminali. Spesso le tecnologie utilizzate sono datate e i sistemi obsoleti, risultando quindi meno sicuri rispetto alle soluzioni più aggiornate. È importante che la PA investa in robuste misure di sicurezza per proteggere i sistemi informativi, nonché i dati dei cittadini.

Gli altri settori si attestano al disotto delle 50 vittime.

Ricordiamo che questa classifica non tiene conto del grado di severità degli attacchi. Infatti, è possibile trovare dei settori in cui gli attacchi sembrano avere numeri residuali, ma hanno avuto un impatto notevole sull'intera supply chain.



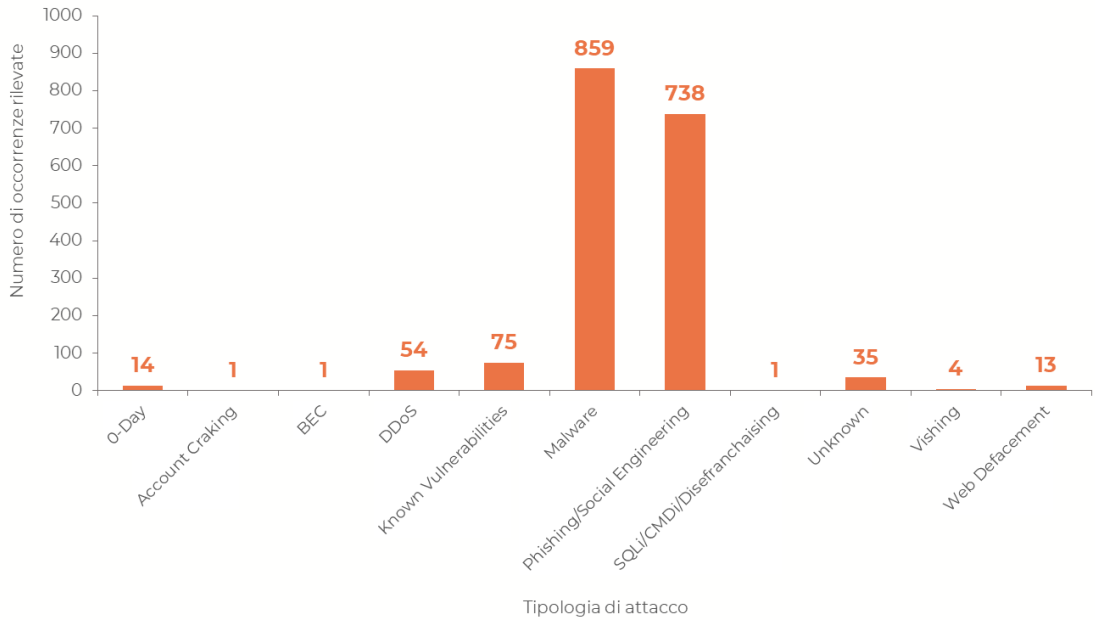
Le tecniche di attacco

Un attacco informatico è qualsiasi tipo di azione condotta contro un computer, un sistema informatico, un server o un'infrastruttura di rete, con l'obiettivo di rubare, modificare o distruggere dati, oppure compromettere il funzionamento dei sistemi stessi. Può essere perpetrato non solo verso organizzazioni private, ma anche contro un'infrastruttura critica, rischiando così di mettere in ginocchio intere economie di paesi.

Di seguito si riportano i valori numerici e il relativo grafico delle diverse tipologie di attacchi. Nello specifico due sono gli attacchi maggiormente riscontrati, nell'ordine: casi relativi ad installazione ed esecuzione di **Malware**, a quota **859** casi (poco meno del **48%**) e **Phishing/Social Engineering**, con **738** casi totali (circa il **41%**).

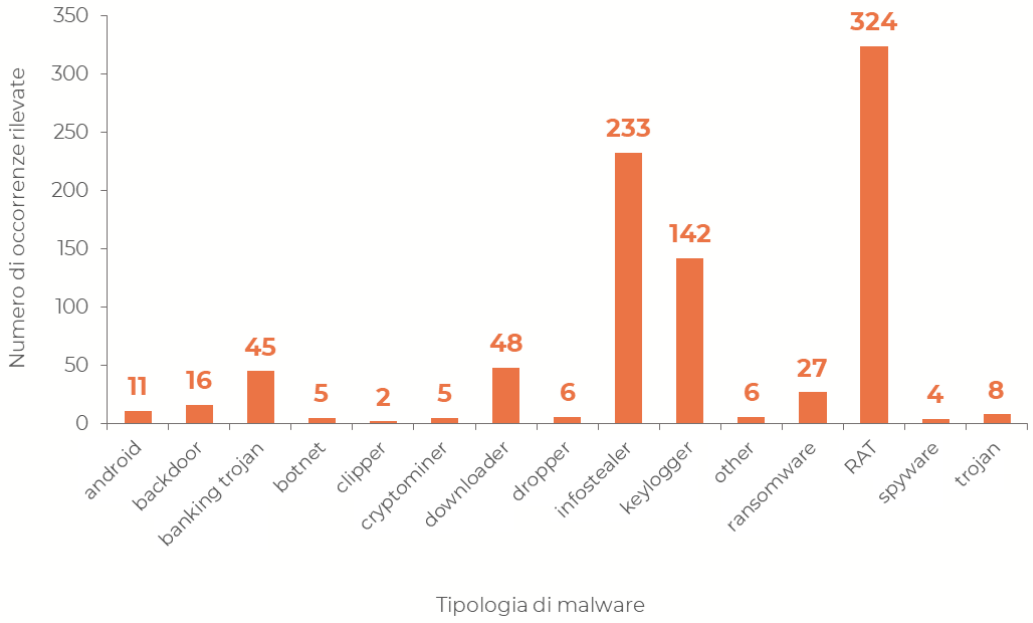
Restano invece in numero più contenuto gli attacchi **DDoS** (**54** casi), per cui ormai esistono metodi di protezione/mitigazione altamente efficienti.

È opportuno evidenziare il costante aumento dei Malware (+**506** rispetto al semestre precedente), probabilmente causato dal massiccio impiego dell'AI, che consente agli attaccanti di introdurre Malware sempre più pericolosi e difficili da individuare.



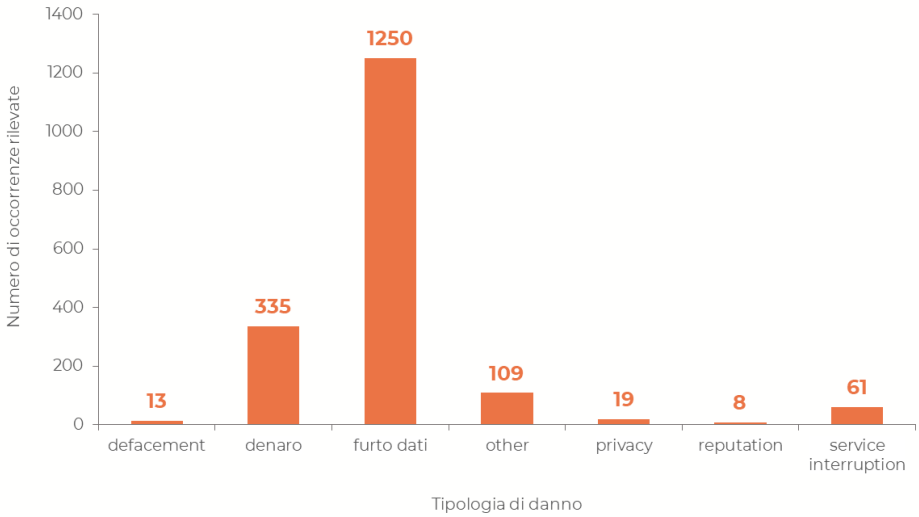
Analizzando nel dettaglio le tipologie di malware relative agli eventi di sicurezza registrati sul territorio di Assolombarda nel 1H2025, emerge il seguente scenario:

- **RAT** - Remote Access Trojan (324 casi);
- **Infostealer** (233 casi);
- **Keylogger** (142 casi);
- presenza stabile di **banking trojan** e **downloader**, indicatori di campagne mirate (oltre 40 casi);
- **Ransomware** (oltre 20 casi, ma con impatti economici elevati).



Tipologie di danno

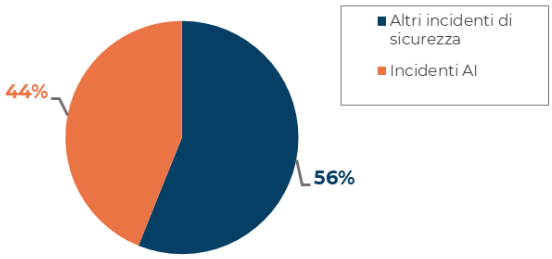
La principale tipologia di danno causato da attacchi informatici, incidenti e violazioni della privacy nel corso del primo semestre del 2025 è senza dubbio il **furto dati**, che caratterizza circa il **70%** della totalità delle evidenze acquisite (**1250** casi). Non è da sottovalutare il **danno economico** (**335** casi), il quale risulta associato al **18,7%** degli attacchi informatici individuati e il **service interruption** (**61** casi, pari al **3,4%**).

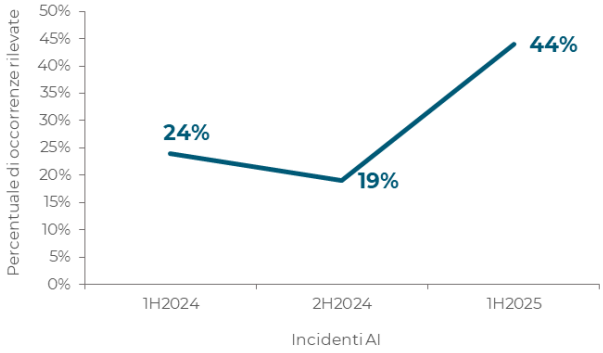


Incidenti di sicurezza AI

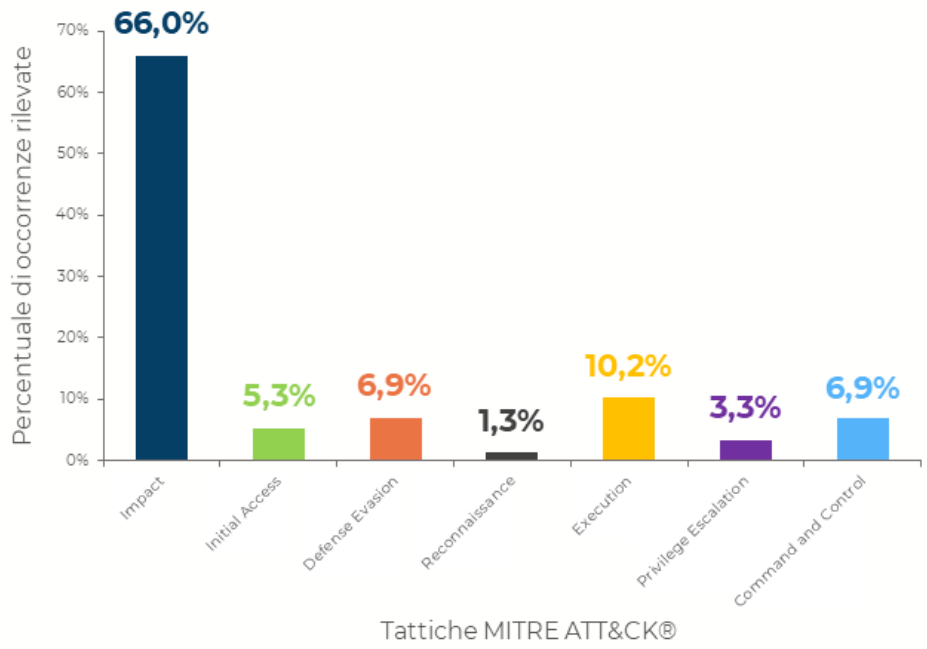
Come si evince dai seguenti grafici, gli incidenti legati ad attacchi influenzati dall'AI hanno rappresentato, nel 1H2025, il **44**% della totalità degli incidenti registrati.

Si tratta di una percentuale in aumento rispetto ai semestri precedenti, indicando una tendenza crescente nell'utilizzo dell'intelligenza artificiale a fini malevoli.





Sotto, inoltre, si riporta il grafico relativo agli incidenti di sicurezza AI nelle tattiche MITRE ATT&CK®.



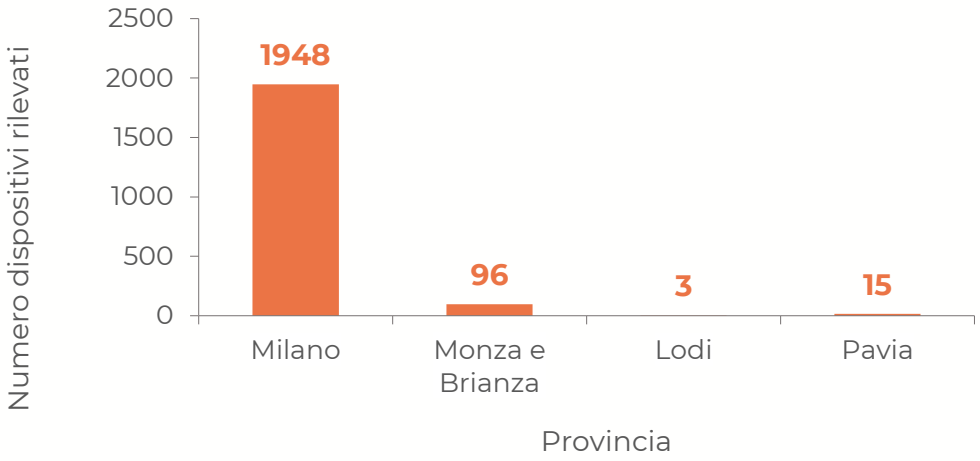
Trend dispositivi IoT più vulnerabili - Unsecurity IoT Index (UII)

Dall'analisi sulla distribuzione dei dispositivi IoT privi di autenticazione all'interno del territorio di Assolombarda, emerge il seguente quadro di vulnerabilità:

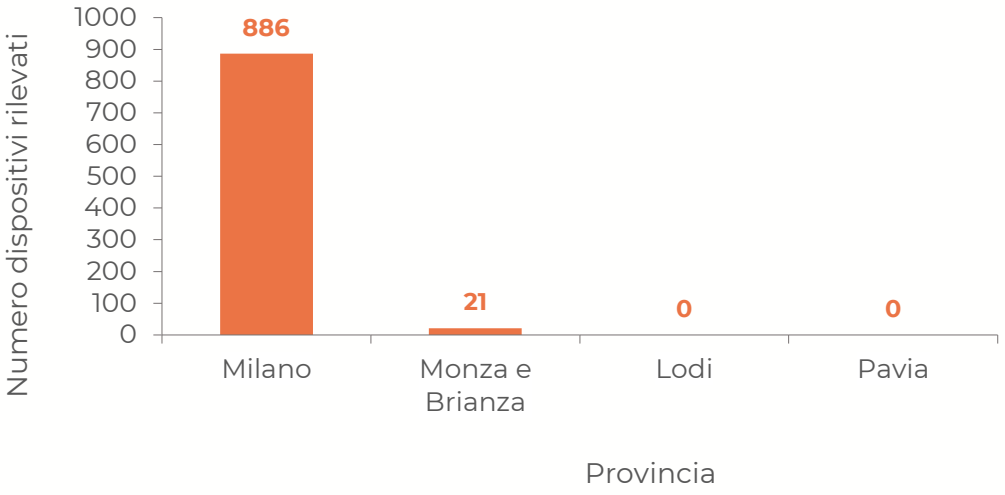
- **ICS** (il 35% dei sistemi ICS risulta vulnerabile);
- **Telecamere** (il 30% delle telecamere risulta vulnerabile);
- **PLC** (il 29% dei sistemi PLC risulta vulnerabile);
- **Medical Devices** (il 23% dei dispostivi medicali risulta vulnerabile).

Nel dettaglio:

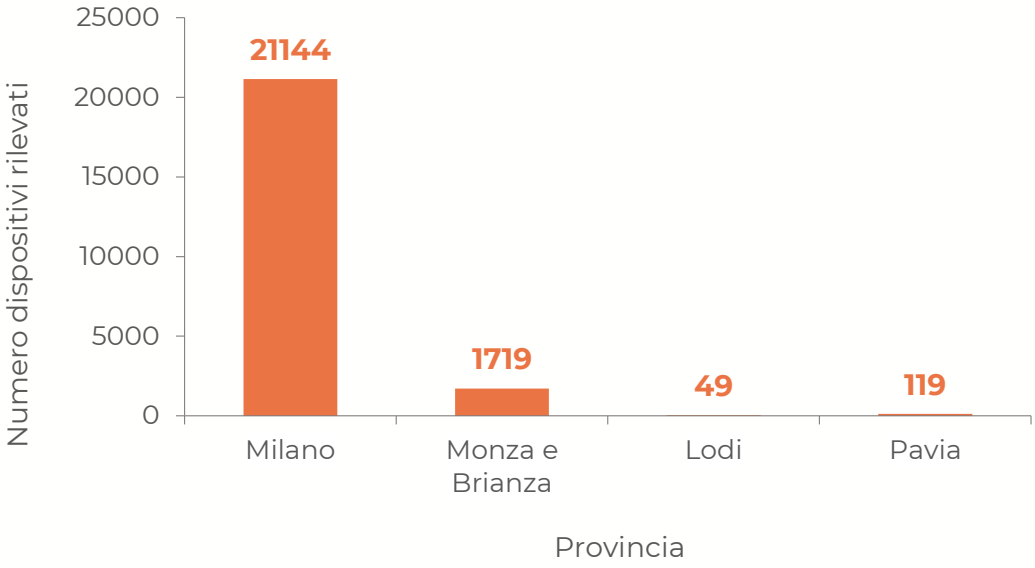
ICS



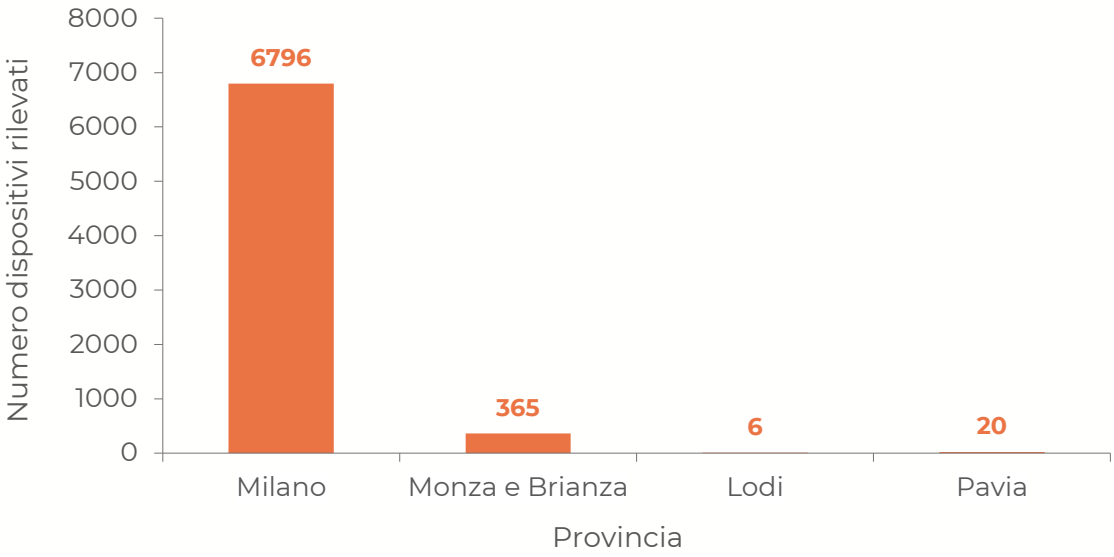
PLC



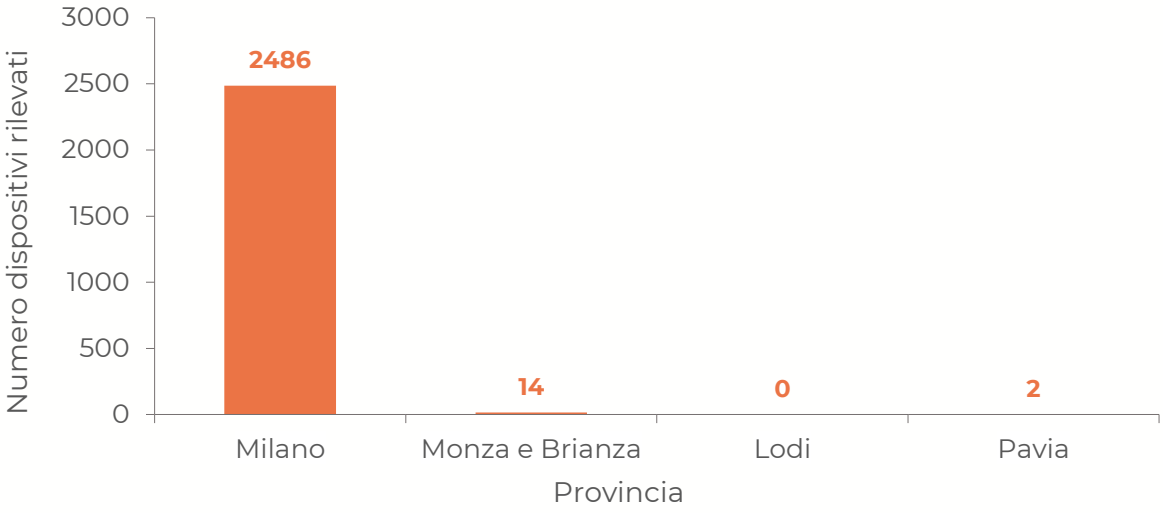
Telecamere senza autenticazione



Router senza autenticazione



Medical Devices senza autenticazione



Glossario

I termini del glossario provengono da CSIRT Italia, istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

Attacco DOS e DDOS (Denial of Service e Distributed Denial of Service)

Attacco informatico che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. Nella versione distribuita (DDoS) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un target. Le botnet sono uno strumento per condurre un attacco DDoS.

Brute Force

Metodo di risoluzione di un problema dato mediante l'impiego di un algoritmo che consiste nel verificare tutte le soluzioni teoricamente possibili fino a quando non si trovi quella effettivamente corretta. Nell'ambito informatico, questo metodo si utilizza soprattutto per individuare le password di accesso a un sistema.

Botnet

Rete di computer utilizzata per attacchi da remoto, o per altre finalità, formata da computer infetti (bot o zombie) che, all'insaputa dei legittimi utenti, sono controllati da un utente malevolo (botmaster).

Backup

Salvataggio, totale o parziale, dei contenuti di una memoria.

Cybercrime

Azioni illecite condotte in danno di sistemi informatici o attraverso l'utilizzo abusivo degli stessi, le cui condotte sono punite dal codice penale.

Cyberwarfare

L'insieme delle operazioni militari condotte nel e tramite il cyberspace per infliggere danni all'avversario, statuale o non, consistenti – tra l'altro – nell'impedirgli l'utilizzo efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyberspace).

Data breach

Violazione dei dati: nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la

distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone.

Defacing

Con il termine Defacing (in italiano con defacciare) si intende la modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco, viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.

Hactivista

"Hacktivism" è un termine portmanteau coniato all'inizio degli anni '90 che identifica l'uso sovversivo di computer o computer network al fine di promuovere un'agenda politica o principi di connotazione sociale. Chi pone in essere tali pratiche è definito hacktivista o attivista digitale.

Malware

Contrazione di malicious software. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Phishing

Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

PLC

Il controllore logico programmabile (in inglese programmable logic controller, spesso in sigla, PLC) è un computer per l'industria specializzato nella gestione o controllo dei processi industriali.

Zero Day

In gergo informatico, si intendono con zero-day (o 0-day) vulnerabilità riferite a sistemi, apparati e applicazioni non ancora note al produttore della tecnologia. La gravità degli zero-day è costituita dall'assenza di aggiornamenti software a fini di mitigazione (cd. patching). Proprio tali caratteristiche rendono gli zero-day oggetto di compravendite illecite da parte di soggetti intenzionati a sfruttarli per finalità intrusive.