ASSOLOMBARDA

X° 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], saranno l'occasione per avere una panoramica dello stato dei territori dell'associazione in tema di sicurezza informatica. [2]

Di seguito verrà analizzato quanto emerso nel **secondo semestre del 2024**.

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.
- **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.

[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.

ASSOLOMBARDA

Executive Summary

Gli **eventi di sicurezza** che hanno colpito il territorio di Assolombarda nel secondo semestre del 2024 sono **1120**, in aumento rispetto al semestre precedente (+**161**).

L'analisi mensile degli eventi di sicurezza mostra un andamento costantemente superiore ai 120 casi, con un **picco a settembre (252)**, probabilmente legato al rientro dalla pausa estiva, quando la minore attenzione degli utenti può aumentare l'esposizione ai rischi informatici.

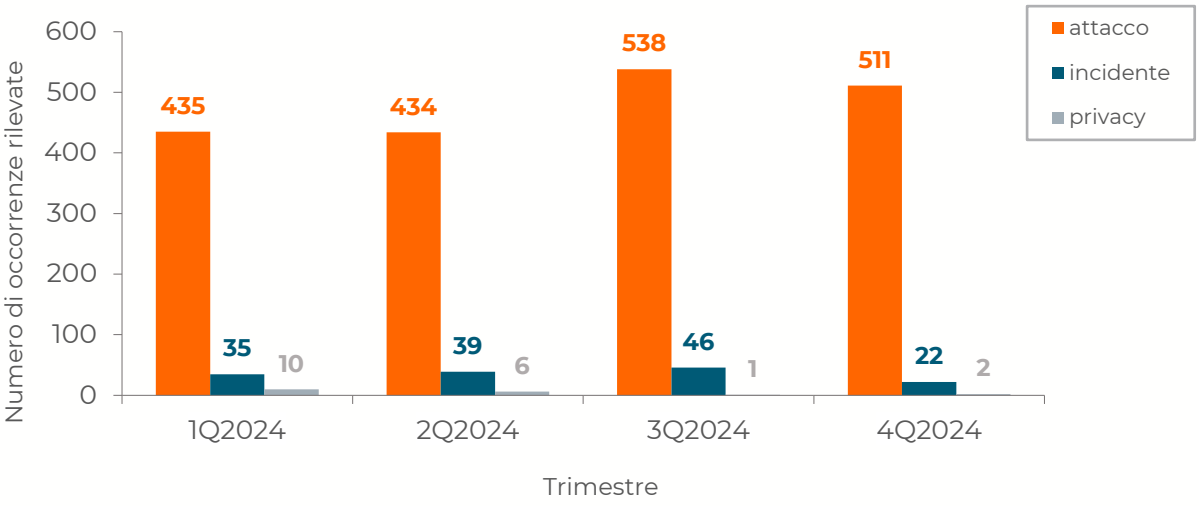
La motivazione che ha spinto ad attaccare è stata principalmente legata ad attività di **cybercrime (1102 casi registrati)**, che si conferma la principale modalità mediante la quale gli attaccanti ottengono i maggiori benefici.

Si registra un marcato aumento delle minacce alla sicurezza informatica nel settore **software e hardware**, che risulta essere il più colpito con **487** casi segnalati, ben 222 in più rispetto al semestre precedente, evidenziando la necessità di integrare la sicurezza sin dalla fase di progettazione di nuovi dispositivi e applicazioni (*security by design*). Il settore **finanziario** si posiziona al secondo posto con **312 eventi**, in lieve calo rispetto al semestre precedente (**-73**).

Phishing, social engineering e malware si riconfermano le tecniche maggiormente utilizzate, con **1052 eventi** registrati. Nonostante gli investimenti in tecnologie (software e hardware), la **variabile umana** rappresenta il **fattore di rischio predominante** evidenziando la necessità di concentrarsi sempre di più su un'efficace e continuativa campagna di sensibilizzazione e formazione.

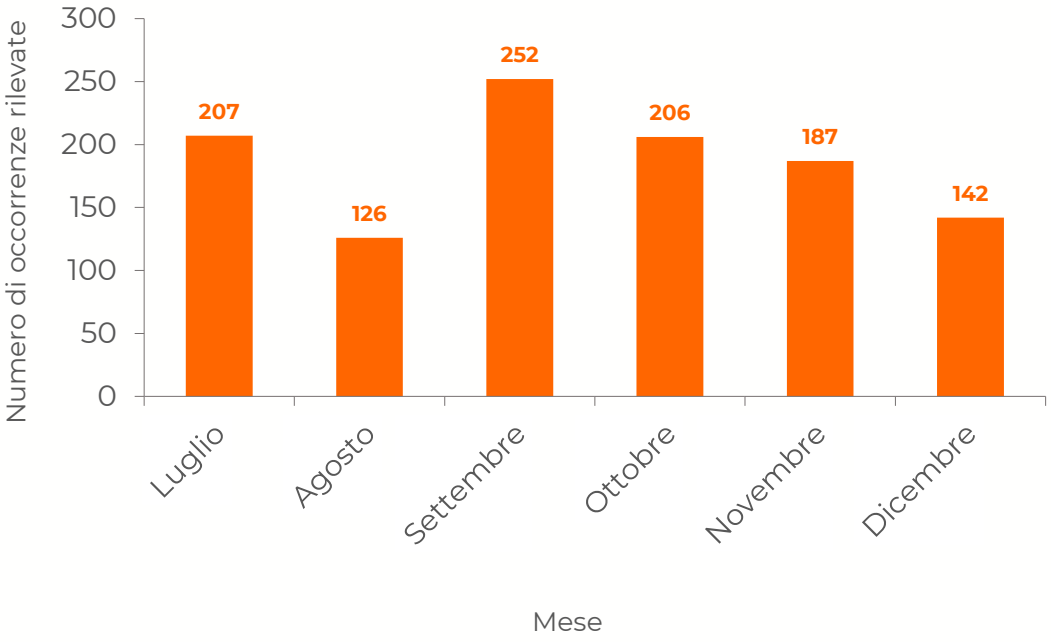
I danni arrecati nel secondo semestre del 2024 dai cyber criminali sono stati principalmente legati al **furto dei dati (956)** e all'**estorsione di denaro (129)**.

Totale eventi



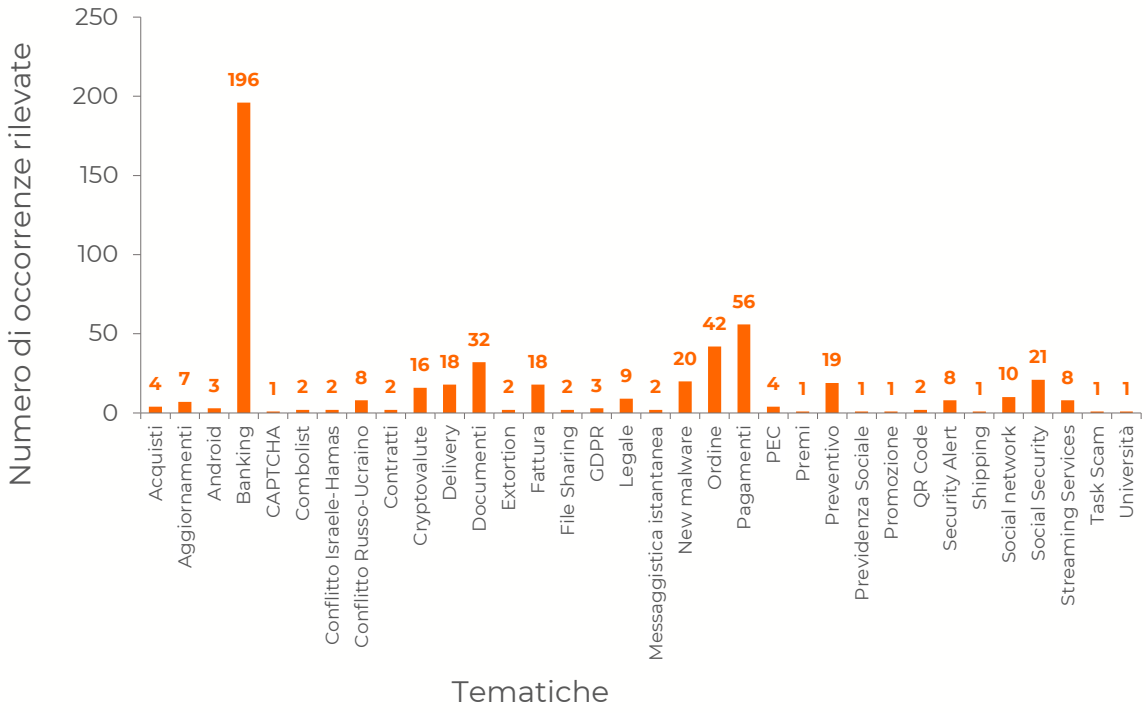
Distribuzione temporale

L'analisi mensile del numero di attacchi, incidenti e violazioni della privacy evidenzia un andamento costantemente superiore ai 120 eventi, con un **picco registrato nel mese di settembre (252 eventi)**. Questo aumento potrebbe essere riconducibile al rientro dalla pausa estiva, periodo in cui un calo dell'attenzione da parte degli utenti può aumentare la vulnerabilità ai rischi informatici.



Tematiche degli attacchi

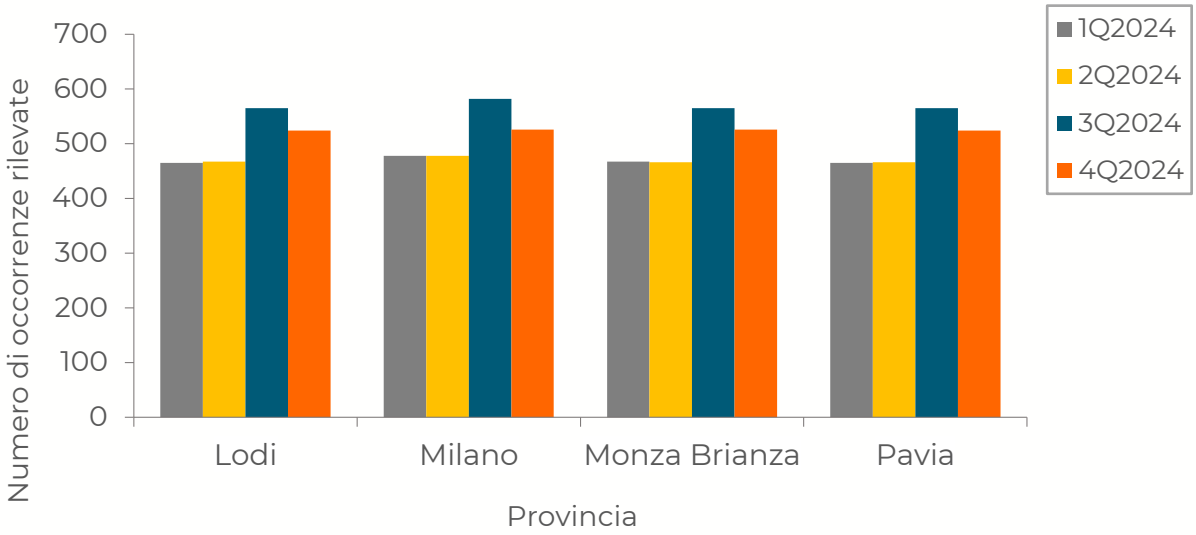
La tematica che ha registrato il maggior numero di attacchi è stata il **banking**, con 196 casi, nettamente al primo posto, seguita dai **pagamenti** (56). Si osserva, inoltre, un costante aumento nella diversificazione dei trend di attacco, con **34 tematiche** differenti nel secondo semestre (+5 rispetto al H1 del 2024).



La distribuzione Geografica

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

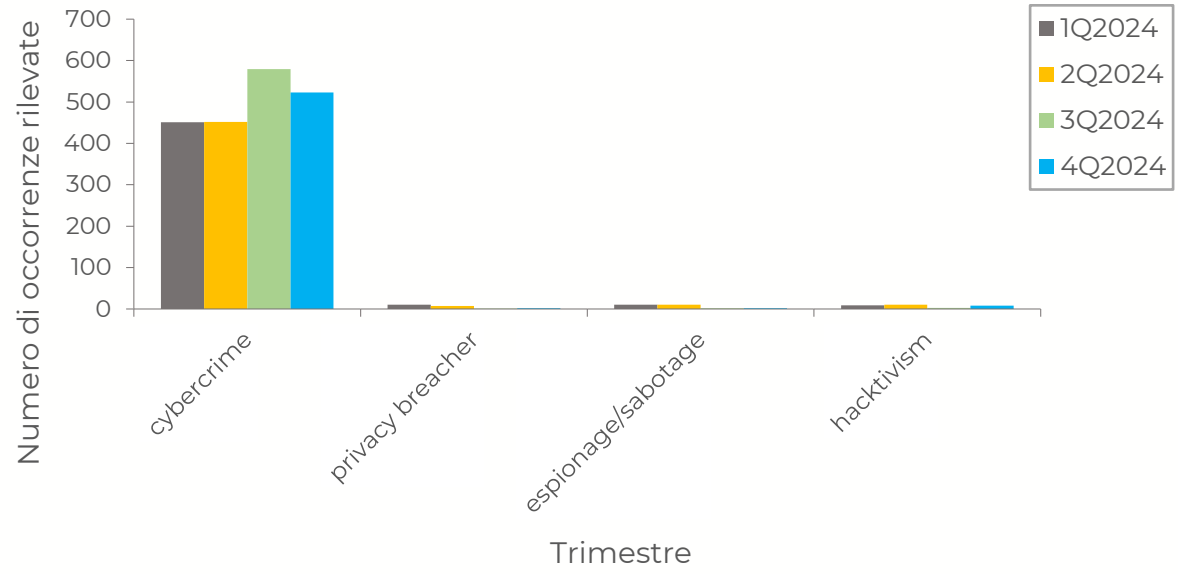
Il numero degli attacchi è riportato considerando che alcuni eventi riguardano tutti i territori ed altri, invece, sono rilevati soltanto in una determinata provincia.



	1Q2024	2Q2024	3Q2024	4Q2024
Lodi	465	467	565	524
Milano	478	478	582	526
Monza Brianza	467	466	565	526
Pavia	465	466	565	524

Le motivazioni

Analizzando complessivamente il secondo semestre del 2024, la motivazione che ha spinto ad attaccare è stata principalmente legata ad attività di **cybercrime (1102 casi registrati)**, che si conferma la principale modalità mediante la quale gli attaccanti ottengono i maggiori benefici.



	1Q2024	2Q2024	3Q2024	4Q2024
cybercrime	451	452	579	523
privacy breacher	10	7	1	2
espionage/sabotage	10	10	2	2
hacktivism	9	10	3	8

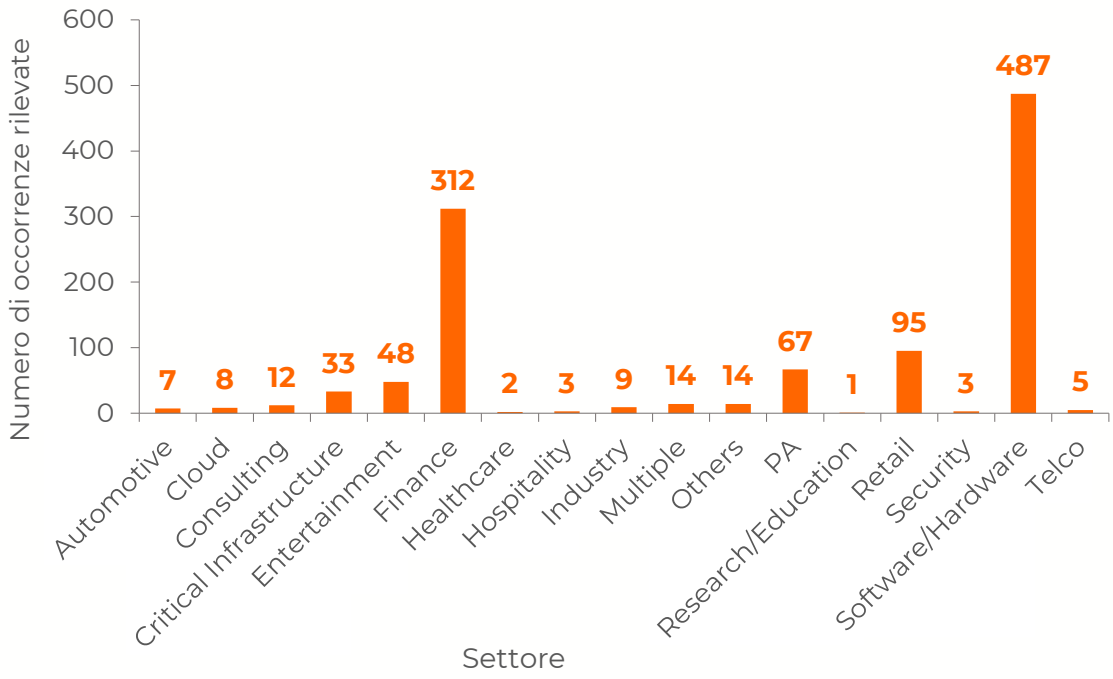
Le vittime

Gli obiettivi principali per i cybercriminali sono target specifici, quali aziende, istituzioni e organizzazioni di vario genere.

Si evidenzia un notevole incremento delle minacce alla sicurezza informatica nel settore **software e hardware**, che risulta il più colpito con un totale di **487** casi registrati (+**222** rispetto al semestre precedente). Questo dato sottolinea l'importanza di adottare un approccio di *security by design*, integrando la sicurezza fin dalle prime fasi di progettazione di dispositivi e applicazioni software.

Il **settore finanziario** si colloca al secondo posto con **312** eventi, in lieve calo rispetto al semestre precedente (**-73**). Infine, si mantiene relativamente stabile il numero di minacce alla sicurezza informatica nell'ambito **Retail**, con un totale di **95** eventi.

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.



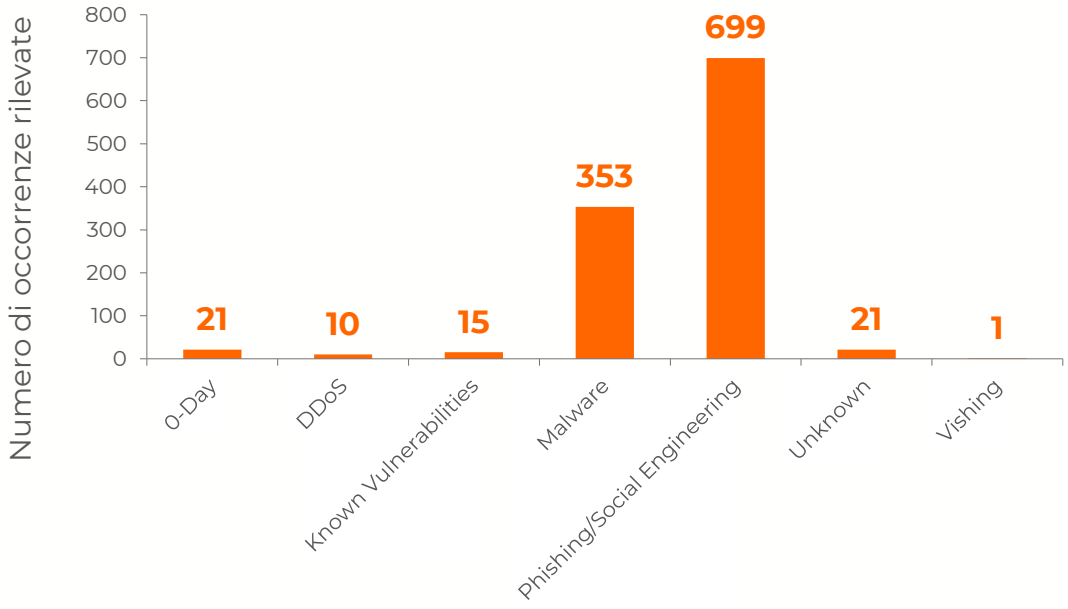
Le tecniche di attacco

Phishing/Social Engineering e **Malware** si confermano ancora una volta come le tecniche più utilizzate, con rispettivamente **699** e **353** casi registrati. La causa principale è riconducibile alle misure di sicurezza adottate dalle vittime stesse. Nonostante gli investimenti in tecnologie, sia software che hardware, la **variabile umana** continua a rappresentare il **principale fattore di rischio**, difficile da mitigare se non attraverso campagne di sensibilizzazione e formazione efficaci e continuative.

Proprio su questo anello debole fanno leva le tecniche di attacco che stanno alla base del social engineering. Questo tipo di attacco, noto come ingegneria sociale, non ha origini informatiche, ma si concentra sul lato psicologico, mirando alle vittime attraverso aspetti emotivamente "sensibili". L'obiettivo è convincere la vittima (o potenziale vittima) a compiere un'azione, come cliccare su un link, eseguire un bonifico o fornire credenziali. Ciò apre la porta per ulteriori azioni dell'attaccante, come infiltrarsi nei sistemi e richiedere un riscatto dopo aver criptato i dati presenti.

Inoltre, in questo momento l'utilizzo di tecnologie riconducibili all'intelligenza artificiale rende gli attacchi maggiormente sofisticati.

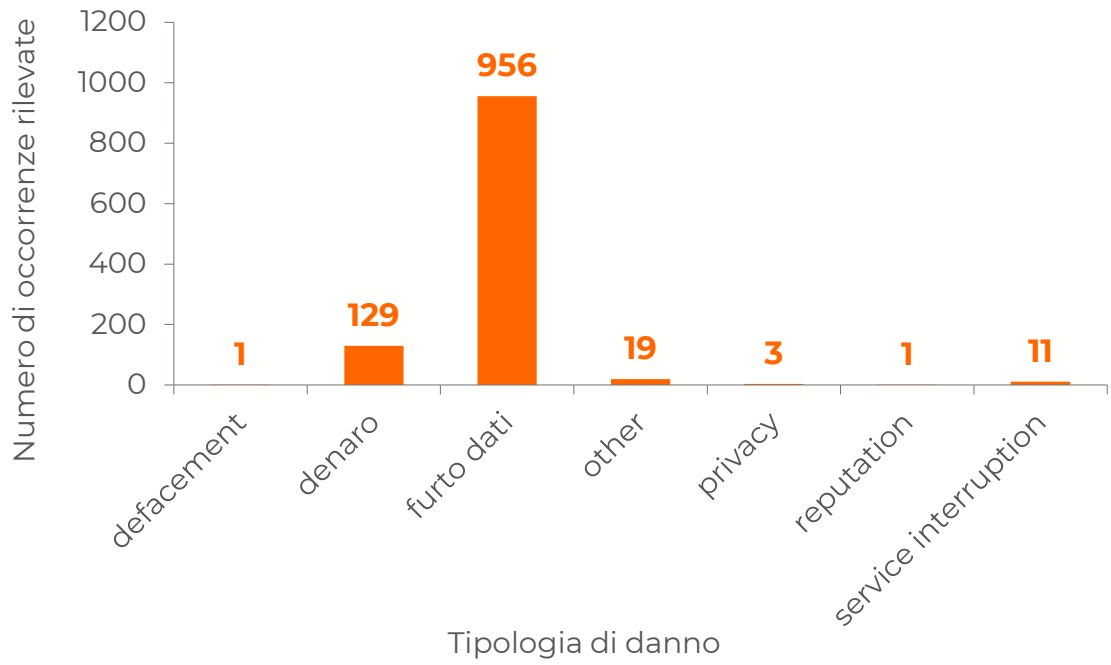
È infatti evidente come il numero di attacchi puramente tecnologici sia di gran lunga minore rispetto agli altri, poiché richiedono senza dubbio un maggior impegno e conoscenza da parte dei malintenzionati.



Tipologia di attacco

Il fine ultimo

I danni arrecati nel secondo semestre del 2024 dai cyber criminali sono stati principalmente legati al **furto dei dati (956)** e all'**estorsione di denaro (129)**. In aggiunta, si osserva un discreto numero di casi di violazioni con l'intento di **interrompere un servizio (11)**, in un contesto sempre più orientato alla connessione e all'uso dei servizi online.



ASSOLOMBARDA

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.