ASSOLOMBARDA

IX° 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 nei primi 6 mesi 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 primo semestre del 2024 sono **959**, con una leggera flessione rispetto al semestre precedente (**-18**). È opportuno notare che nel H2 del 2023 sono stati rilevati 977 eventi di sicurezza.

Nel corso di questo primo semestre l'andamento degli attacchi è rimasto costante, confermando soltanto gennaio come mese con un conteggio di eventi inferiore a 100.

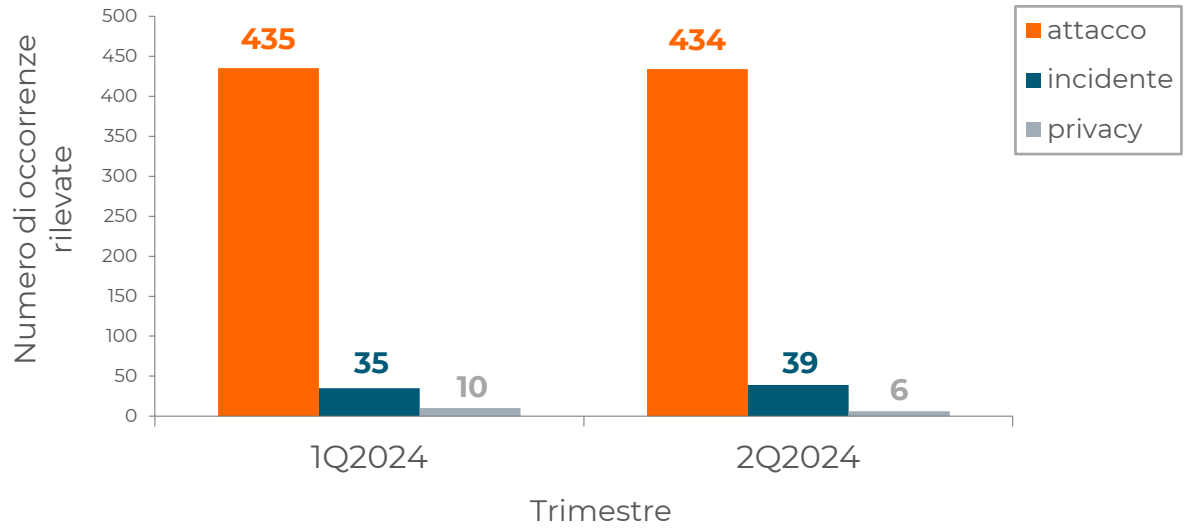
La motivazione che ha spinto ad attaccare è stata principalmente legata ad attività di **cybercrime (903 casi registrati)**, che si conferma la principale modalità mediante la quale gli attaccanti creano i propri introiti.

I settori maggiormente colpiti si confermano essere quello **finanziario** con **385 e quello software e hardware**, con un totale di **265 casi registrati**. Infine, si evidenzia un incremento delle minacce alla sicurezza informatica nell'ambito del **retail**, con un totale di **99 eventi.**

Phishing, social engineering e malware si riconfermano le tecniche maggiormente utilizzate con oltre 859 eventi registrati. Nonostante gli investimenti in tecnologie (software e hardware), la **variabile umana** rimane sempre il **fattore di rischio predominante** e a cui più difficilmente si può porre rimedio, se non attraverso un'efficace e continuativa campagna di sensibilizzazione e formazione.

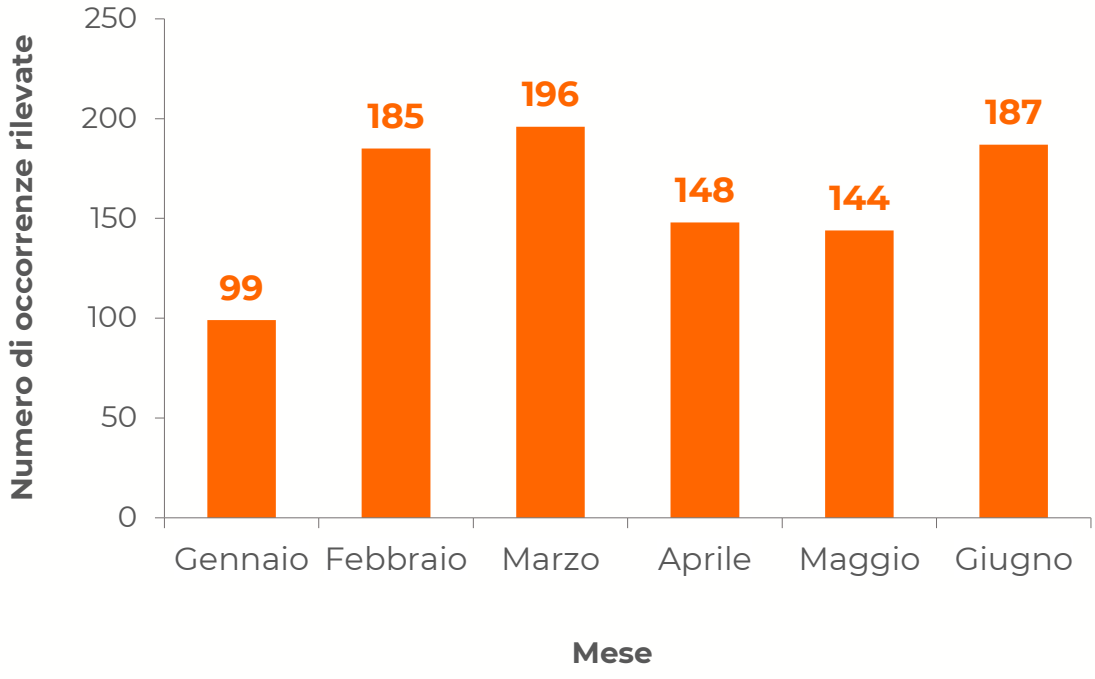
I danni arrecati nel primo semestre del 2023 dai cyber criminali sono stati principalmente legati al **furto dei dati (583)** e all'**estorsione di denaro (217)**.

Totale eventi



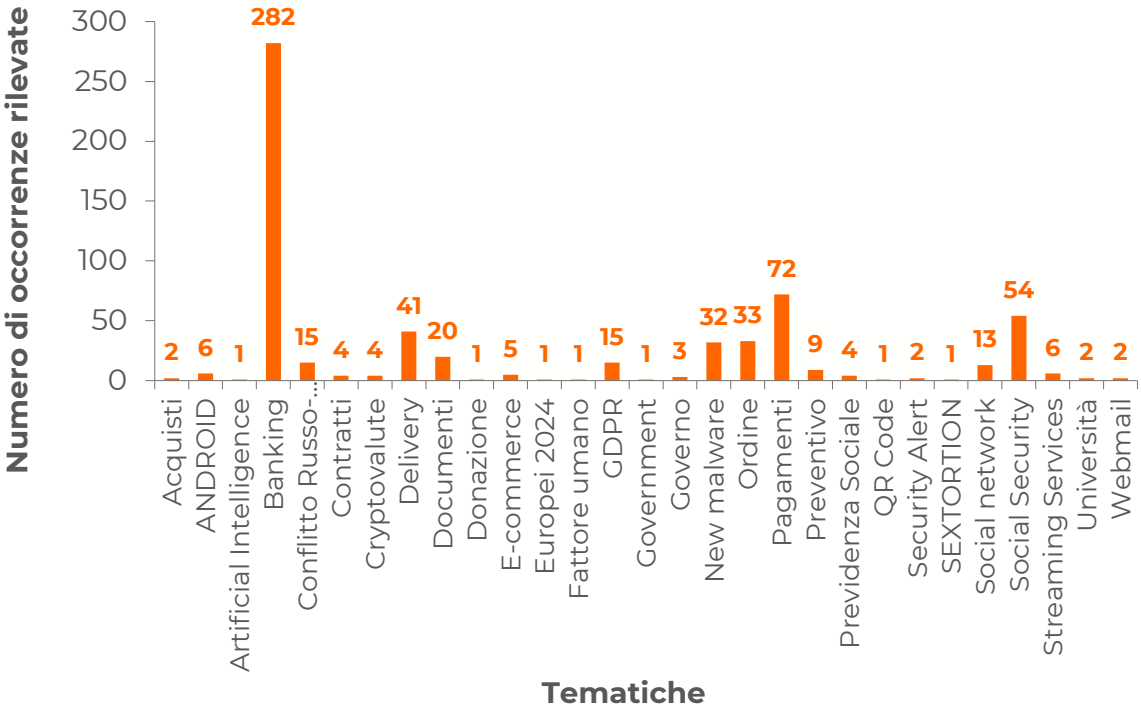
Distribuzione temporale

Gli eventi di sicurezza registrati nel corso del primo semestre del 2024 mostrano un andamento stabilmente sopra i 140 attacchi al mese, ad esclusione di **gennaio**, che registra **99** eventi. Il mese con il maggior numero di eventi analizzati è **marzo**, con ben **196** casi tra attacchi, incidenti e violazioni privacy.



Tematiche degli attacchi

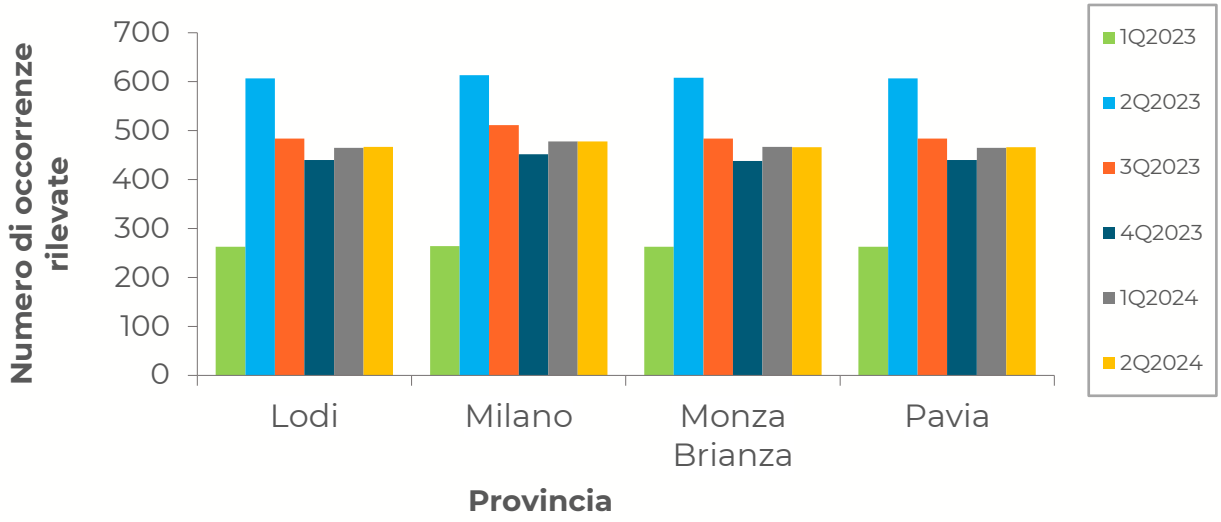
I principali temi intorno ai quali è stato registrato il maggior numero di attacchi sono stati il **banking (282)**, i **pagamenti (72)** e la **social security (54)**. Differentemente dai report degli anni precedenti si segnala come le tematiche degli attacchi siano notevolmente aumentate.



La distribuzione Geografica

Dall'analisi della distribuzione geografica di attacchi, incidenti e violazioni 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.

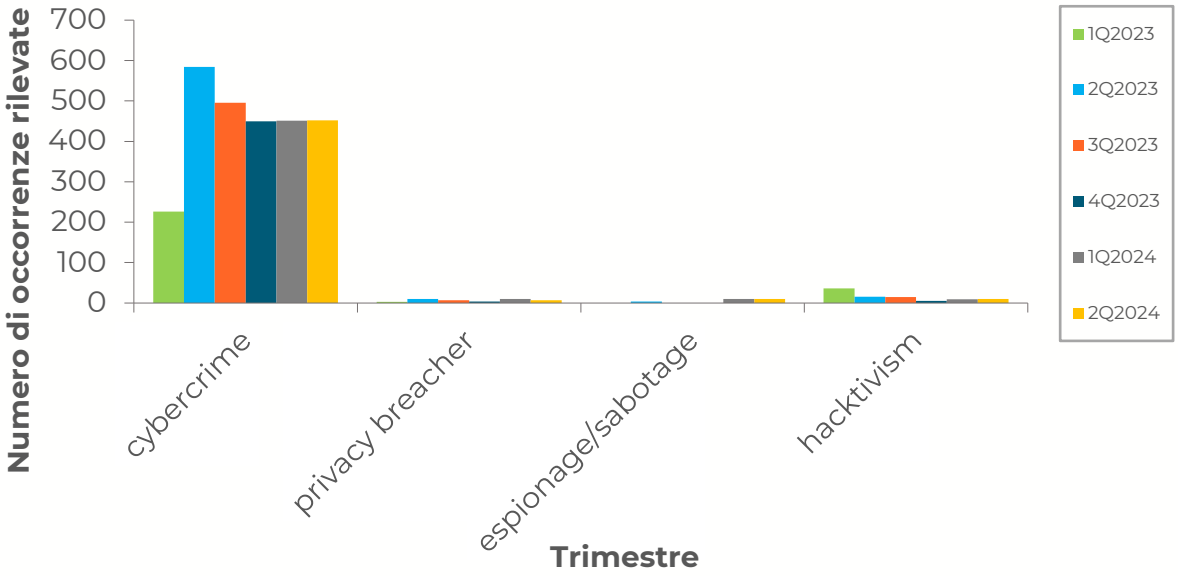
Il numero degli attacchi è riportato considerando che alcuni eventi riguardano tutti i territori ed altri, invece, sono rilevati soltanto in una determinata provincia.



	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024	2Q2024
Lodi	263	607	484	440	465	467
Milano	264	613	511	452	478	478
Monza Brianza	263	608	484	438	467	466
Pavia	263	607	484	440	465	466

Le motivazioni

Analizzando complessivamente il primo semestre del 2024, la motivazione che ha spinto ad attaccare è stata principalmente legata ad attività di **cybercrime (903 casi registrati)**, che si conferma la principale modalità mediante la quale gli attaccanti creano i propri introiti. Al secondo posto, ma con una rilevanza in termini numerici decisamente inferiore, si posizionano le attività di **espionage/sabotage (20)**, seguite dalle attività di **hacktivism (19)**.



	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024	2Q2024
cybercrime	226	584	496	450	451	452
privacy breacher	3	10	7	4	10	7
espionage/sabotage	0	4	0	0	10	10
hacktivism	36	16	15	5	9	10

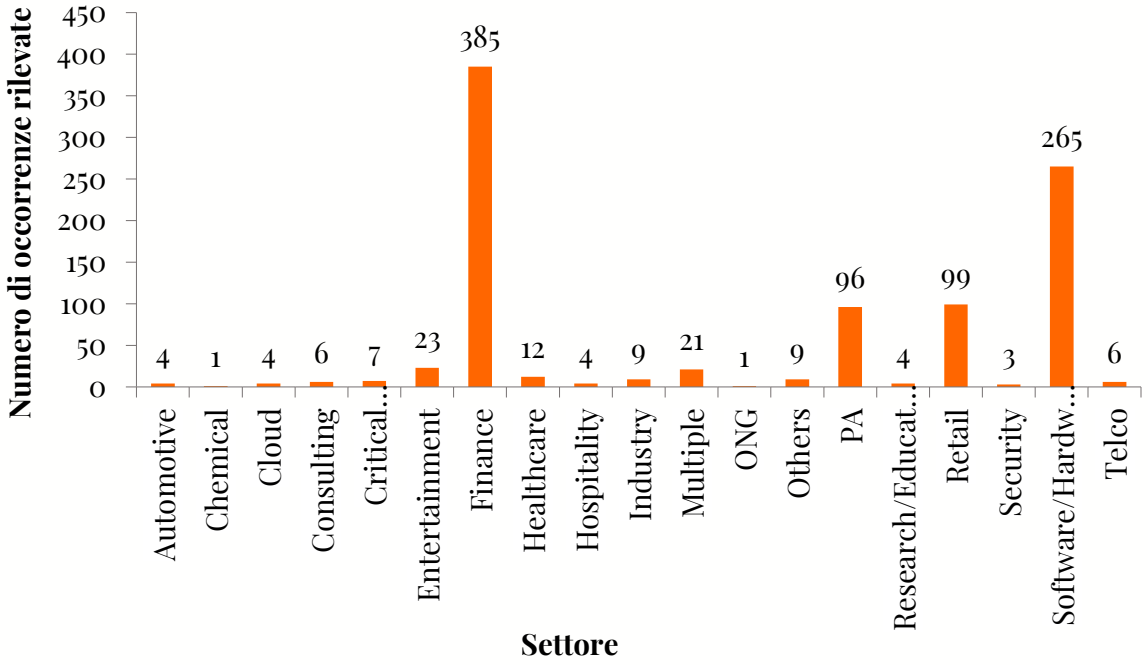
Le vittime

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

Il **settore finanziario** rimane quello più colpito, registrando un totale di **385 eventi**. Ciò è probabilmente dovuto al fatto che questo settore coinvolge considerevoli quantità di denaro, che gli aggressori possono mirare attraverso il furto diretto di fondi o richiedendo un riscatto tramite ransomware. Al secondo posto si collocano **software e hardware**, con un totale di **265 casi registrati**. Questo spesso deriva da una mancanza di adeguata considerazione per la sicurezza durante la fase di progettazione di nuovi dispositivi e applicazioni software.

Infine, si evidenzia un incremento delle minacce alla sicurezza informatica nell'ambito Retail, con un totale di **99 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.

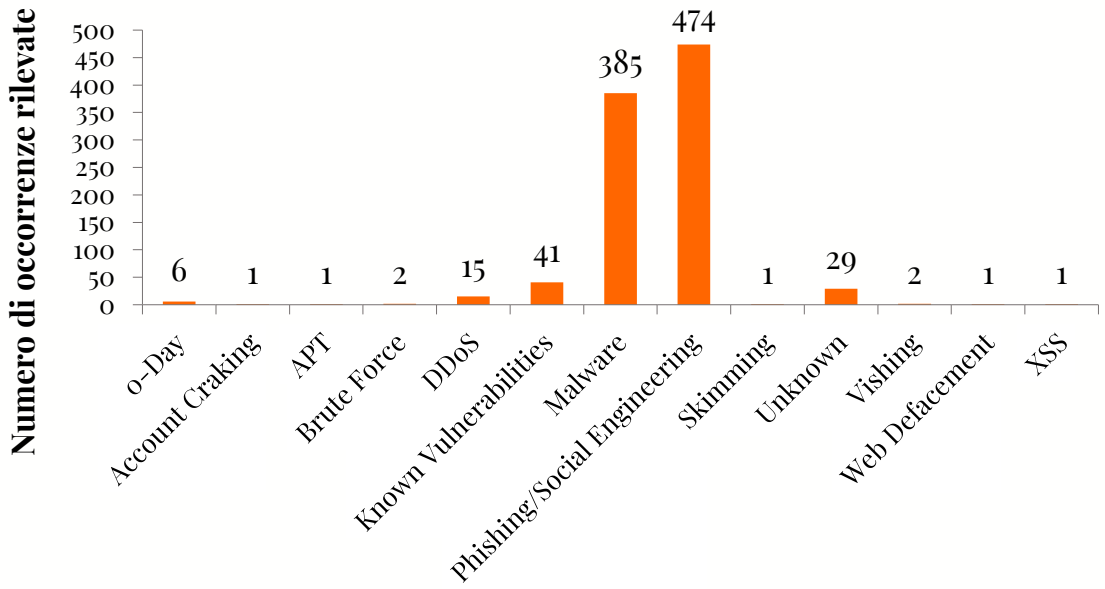


Le tecniche di attacco

Phishing/Social Engineering e Malware si riconfermano le tecniche maggiormente utilizzate. La ragione sottostante a questa chiara disproporzione nell'uso è legata alle misure di sicurezza adottate dalle vittime stesse. Nonostante gli investimenti in tecnologie (software e hardware), la **variabile umana** rimane sempre il **fattore di rischio predominante** e a cui più difficilmente si può porre rimedio, se non attraverso un'efficace e continuativa campagna di sensibilizzazione e formazione.

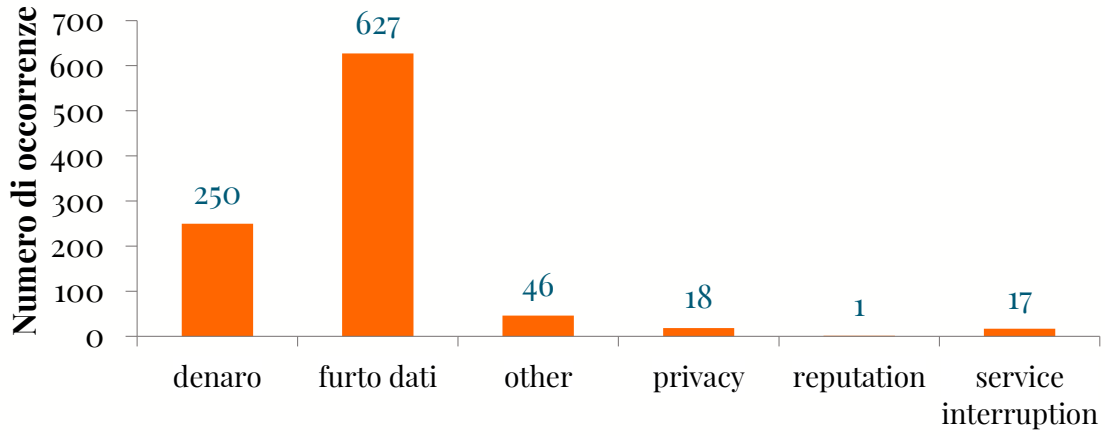
Proprio su questo anello debole fanno leva le tecniche di attacco che stanno alla base del social engineering. Questo tipo di attacco, noto come ingegneria sociale, non ha origini informatiche, ma si concentra sul lato psicologico, mirando alle vittime attraverso aspetti emotivamente "sensibili". L'obiettivo 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.

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.



Il fine ultimo

I danni arrecati nel primo semestre del 2024 dai cyber criminali sono stati principalmente legati al **furto dei dati (627)** e all'**estorsione di denaro (250)**. In aggiunta, si osserva un interessante numero di casi di violazioni con l'intento di **interrompere un servizio (17)**, in un contesto sempre più orientato alla connessione e all'uso dei servizi online.



Approfondimento Dispositivi Connessi

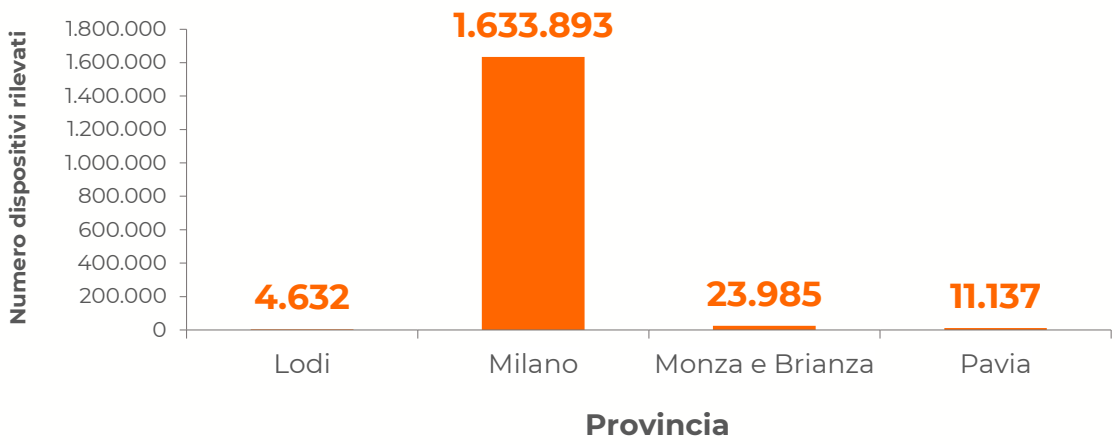
Visto il contesto digitale in piena evoluzione è fondamentale capire se tale progresso corre in parallelo alla messa in sicurezza dei servizi?

Per rispondere al quesito, Exprivia ha elaborato un'analisi sullo stato di sicurezza dei dispositivi italiani connessi in rete. Per competenza dell'Associazione si analizzeranno i dati dei territori di riferimento.

Obiettivo è da un lato osservare l'impatto che l'IoT ha nella sicurezza dell'ecosistema digitale, dall'altro verificare se i risultati degli investimenti fatti in cybersecurity bilanciano quelli fatti nello sviluppo del digitale.

Innanzitutto, si osserva che il numero di **indirizzi IPv4 (dispositivi connessi)** esposti su internet sul territorio di Assolombarda è diminuito rispetto all'anno precedente nel 1H2024 (**-162.453**). È opportuno notare che il numero complessivo di dispositivi esposti in rete indica il perimetro di un potenziale attacco.

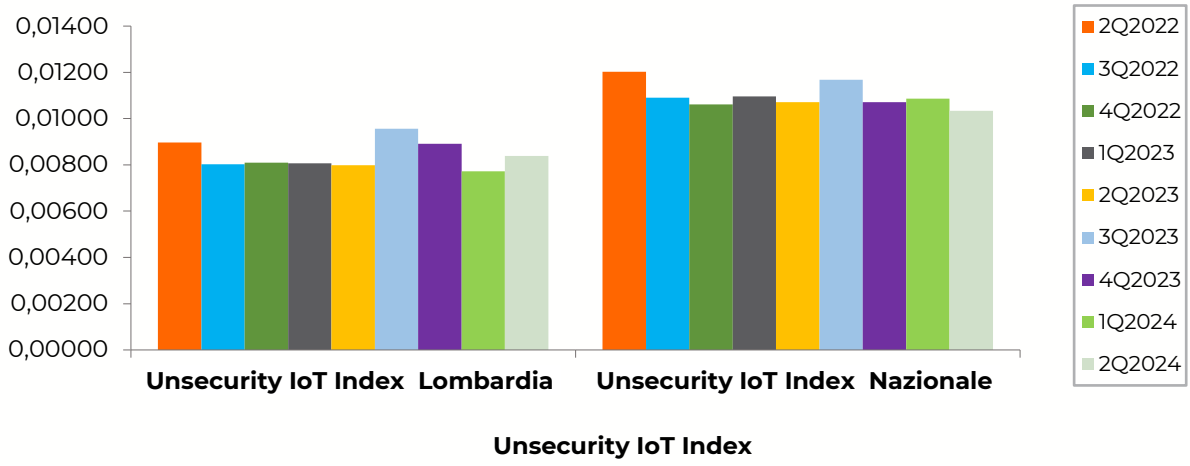
I dispositivi connessi in Lombardia sono 1.940.757 e sul territorio di Assolombarda sono 1.673.647. La suddivisione è la seguente:



Milano	1.633.893
Lodi	4.632
Monza Brianza	23.985
Pavia	11.137
Totale	**1.673.647**

Per avere ulteriori informazioni ***Exprivia*** ha definito un nuovo indice: **Unsecurity IoT Index (UII),** che prende in considerazione il numero totale di dispositivi esposti su internet e le maggiori vulnerabilità identificate su dispositivi e protocolli di autenticazione.

Questo nuovo indice è stato rilevato per la prima volta nel secondo quarter del 2022. Tale indice viene poi comparato con quello nazionale.

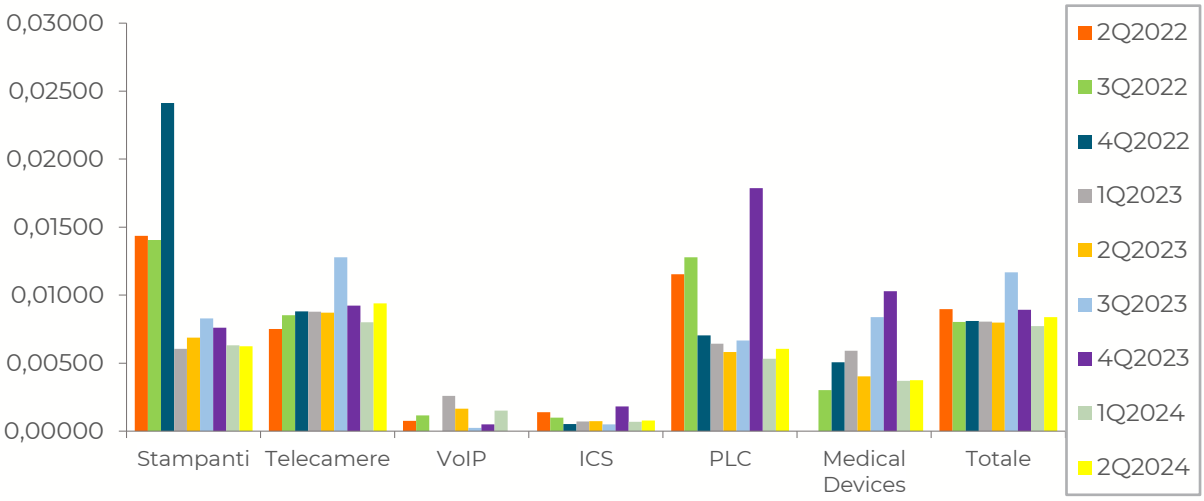


Unsecurity IoT Index

	2Q2022	3Q2022	4Q2022	1Q2023	2Q2023	3Q2023	4Q2023	1Q2024	2Q2024
Unsecurity IoT Index Lombardia	0,00896	0,00802	0,00809	0,00806	0,00798	0,00956	0,00892	0,00772	0,00838
Unsecurity IoT Index Nazionale	0,01202	0,01091	0,01061	0,01096	0,01071	0,01168	0,01071	0,01086	0,01034

È stato successivamente calcolato l'UII per ogni dispositivo IoT analizzato, al fine di valutare quale dispositivo IoT presenti il maggior livello di rischio in Lombardia.

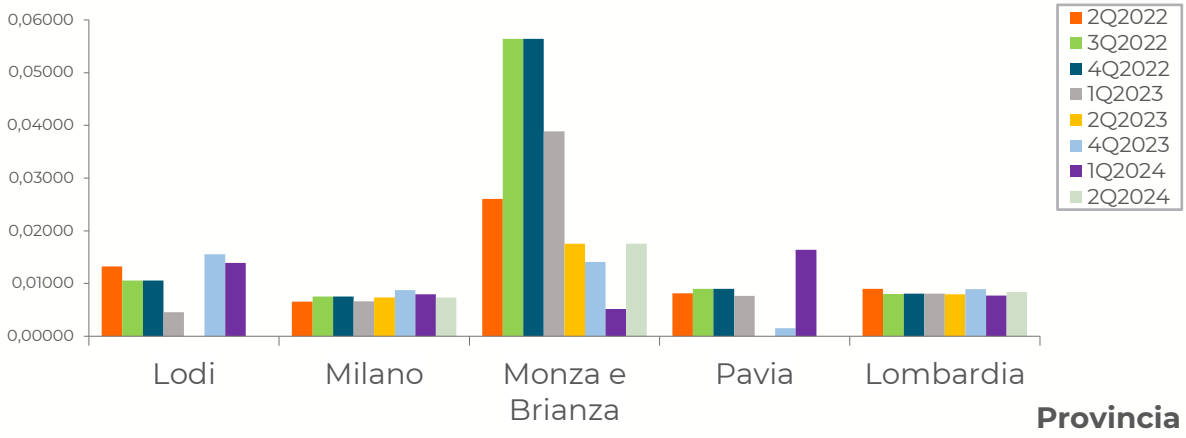
Con riferimento al H1 del 2024, i dispositivi a maggior rischio sono le **telecamere**, poiché superano il valore totale (+9% circa). **Stampanti, PLC e medical devices** hanno un rischio medio, in quanto il loro valore è prossimo a quello totale. Per quanto riguarda, invece, **ICS e VoIP Systems** si evince che questi hanno un rischio basso, in quanto hanno un valore inferiore rispetto all'indice totale.



	Stampanti	Telecamere	VoIP	ICS	PLC	Medical Devices	Totale
2Q2022	0,01436	0,00751	0,00076	0,00140	0,01154	0,00000	0,00896
3Q2022	0,01405	0,00852	0,00116	0,00099	0,01279	0,00301	0,00802
4Q2022	0,02413	0,00879	0,00000	0,00053	0,00703	0,00506	0,00809
1Q2023	0,00605	0,00878	0,00259	0,00072	0,00643	0,00592	0,00806
2Q2023	0,00688	0,00872	0,00165	0,00074	0,00581	0,00404	0,00798
3Q2023	0,00829	0,01279	0,00023	0,00051	0,00667	0,00839	0,01168
4Q2023	0,00762	0,00923	0,00049	0,00181	0,01786	0,01029	0,00892
1Q2024	0,00631	0,00800	0,00152	0,00068	0,00533	0,00370	0,00772
2Q2024	0,00625	0,00940	0,00000	0,00078	0,00605	0,00376	0,00838

Esaminando le province di riferimento di Assolombarda (sempre con riferimento al H1 del 2024), possiamo notare che a **Lodi e Pavia** il rischio connesso all'utilizzo di dispositivi IoT risulta basso in quanto il valore dell'indice è inferiore a quello regionale (è opportuno evidenziare, tuttavia, che nel 1Q del 2024 l'indice di entrambe le province è risultato superiore a quello regionale nello stesso periodo), mentre a **Milano e Monza Brianza** il rischio risulta moderato considerato che i due grafici tendono quasi a coincidere (si noti, in particolare, il picco nel 2Q del 2024 nella provincia di MB, che supera l'indice regionale).

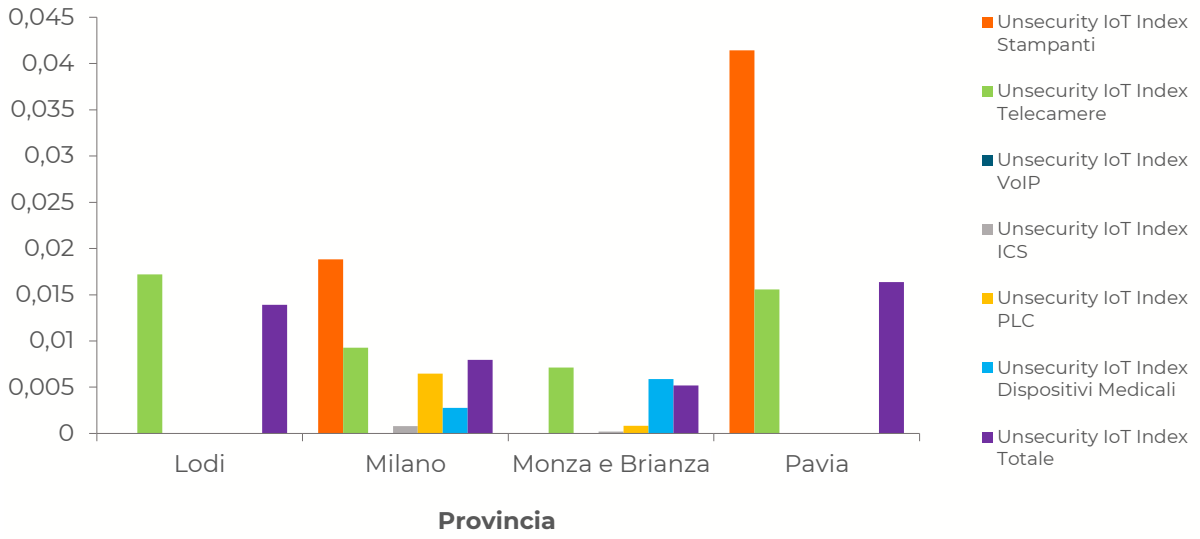
Per quanto riguarda Monza e Brianza il rischio è elevato in quanto l'indice supera di molto (tre volte e mezzo circa) il valore dell'indice regionale.



Unsecurity IoT Index	2Q2022	3Q2022	4Q2022	1Q2023	2Q2023	4Q2023	1Q2024	2Q2024
Lodi	0,01325	0,01058	0,01058	0,00457	0,00000	0,01554	0,01392	0,00000
Milano	0,00654	0,00754	0,00754	0,00660	0,00747	0,00877	0,00795	0,00738
Monza e Brianza	0,02606	0,05638	0,05638	0,03884	0,01768	0,01408	0,00518	0,01756
Pavia	0,00813	0,00902	0,00902	0,00764	0,00000	0,00154	0,01637	0,00000
Lombardia	0,00896	0,00802	0,00809	0,00806	0,00798	0,00892	0,00772	0,00838

Se scorporiamo i dati per dispositivo, si evince che a **Pavia** i dispositivi più vulnerabili sono le **stampanti**, mentre a **Lodi** le **telecamere**[3].

[3] Nell'analisi corrente è stato sostituito, all'interno del campo Unsecurity IoT Index Totale, il valore dell'Unsecurity IoT Index della Lombardia con il valore dell'UII totale per ogni singola provincia, in modo tale da rendere più accurati i confronti.



1Q2024	Unsecurity IoT Index Stampanti	Unsecurity IoT Index Telecamere	Unsecurity IoT Index VoIP	Unsecurity IoT Index ICS	Unsecurity IoT Index PLC	Unsecurity IoT Index Dispositivi Medicali	Unsecurity IoT Index Totale
Lodi	0,0000	0,0172	0,0000	0,0000	0,0000	0,0000	0,01392
Milano	0,0188	0,0093	0,0000	0,0008	0,0065	0,0028	0,00795
Monza e Brianza	0,0000	0,0071	0,0000	0,0002	0,0008	0,0059	0,00518
Pavia	0,0414	0,0156	0,0000	0,0000	0,0000	0,0000	0,01637

Osservando il tipo di dispositivo, continua ad impressionare il numero di stampanti vulnerabili che superano le telecamere sui territori di Pavia e Milano, nonché il numero di PLC non sicuri, ricordando che un PLC potrebbe controllare l'erogazione di un servizio industriale fondamentale.

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.