Exprivia Threat Intelligence Report

Focus settore finanziario

Italia – 1Q2025

future. perfect. simple.

Sommario

Introduzione 5

Executive Summary 6

Attacchi, incidenti e violazioni privacy 7

Motivazione degli attaccanti 10

Distribuzione geografica 12

Distribuzione vittime per Industria 14

Software/Hardware 15

Finance 16

Retail 17

Tipo di danno 18

Tecniche di attacco 20

Nome e tipo di malware 22

Classificazione MITRE ATT&CK® 27

Sicurezza dei dispositivi IoT 1Q2025 37
- Stato della sicurezza dei dispositivi IoT 1Q2025 47
- Stato della sicurezza dei settori economici italiani 1Q2025 53

Previsioni Cybersecurity 2025 57

Nella Sicurezza Informatica, Mitigare il Rischio Umano Richiede Più della Semplice Formazione 61

L'Intelligenza Artificiale (AI) nella Sicurezza Informatica: Rischi e Opportunità 63

Rising Threat: Protecting Italian Financial Services from DDoS Attacks 68

Malware 1Q2025 70
- PLAYFULGHOST 70
- MintsLoader 70
- Aquabot 70
- MassJacker 71
- StilachiRAT 71
- BackConnect 72
- Astral Stealer 72
- SparkCat 72
- Flesh Stealer 73
- FrigidStealer 73

Autori 74

Sorgenti di Informazioni 79

Indice delle figure

Figura 1 - Tematiche riscontrate di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 6
Figura 2 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi in Italia nel 1Q2025 7
Figura 3 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi nel settore finanziario nel 1Q2025 7
Figura 4 - Numero di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia . 8
Figura 5 - Numero di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 8
Figura 6 - Numero di attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia 8
Figura 7 - Numero di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia . 9
Figura 8 - Numero di attacchi, incidenti e violazioni privacy nel settore finanziario nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 9
Figura 9 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel 1Q2025 in Italia 10
Figura 10 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel settore finanziario nel 1Q2025 in Italia 10
Figura 11 - Conteggio motivazione attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2025 e 1Q2025 in Italia 11
Figura 12 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 12
Figura 13 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia 12
Figura 14 - Distribuzione geografica di attacchi, incidenti e violazioni privacy per abitante nelle diverse aree geografiche nel 1Q2025 in Italia 13
Figura 15 - Distribuzione geografica di attacchi, incidenti e violazioni privacy per abitante nelle diverse aree geografiche nel settore finanziario nel 1Q2025 in Italia 13
Figura 16 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 14
Figura 17 - Attacchi, incidenti e violazione privacy del settore Software/Hardware nel 1Q2025 in Italia 15
Figura 18 - Attacchi, incidenti e violazioni privacy del settore Finance nel 1Q2025 in Italia 16
Figura 19 - Attacchi, incidenti e violazioni privacy del settore Retail nel 1Q2025 in Italia 17
Figura 20 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 18
Figura 21 - Tipologia danno di attacchi, incidenti e violazioni privacy nel settore finanziario in Italia nel 1Q2025 18
Figura 22 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 19
Figura 23 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia 20
Figura 24 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia 20
Figura 25 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 21
Figura 26 - Tipologie di malware relative ad attacchi e incidenti registrate nel 1Q2025 in Italia 22
Figura 27 - Tipologie di malware relative ad attacchi e incidenti registrate nel settore finanziario nel 1Q2025 in Italia 22
Figura 28 - Tipologie di malware relative attacchi e incidenti registrate nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024 e 1Q2025 in Italia 23
Figura 29 - RAT relativi ad attacchi e incidenti registrati nel 1Q2025 in Italia 24
Figura 30 - Infostealer relativi ad attacchi e incidenti registrati nel 1Q2025 in Italia 25
Figura 31 - Keylogger relativi ad attacchi registrati nel 1Q2025 in Italia 26
Figura 32 - Classificazione MITRE ATT&CK® 1Q2025 Italia 28
Figura 33 - Distribuzione degli incidenti legati ad attacchi Supply Chain sulla totalità degli incidenti registrati nel 1Q2025 in Italia 29
Figura 34 - Distribuzione degli incidenti legati ad attacchi Supply Chain sulla totalità degli incidenti registrati nel 1Q2024, 2Q2024, 3Q2024 e 1Q2025 in Italia 30
Figura 35 - Distribuzione degli incidenti legati ad attacchi influenzati dall'AI sulla totalità degli incidenti registrati nel 1Q2025 in Italia .. 31
Figura 36 - Distribuzione degli incidenti legati ad attacchi influenzati dall'AI sulla totalità degli incidenti registrati nel settore finanziario nel 1Q2025 in Italia 31
Figura 37 - Distribuzione degli incidenti legati ad attacchi influenzati dall'AI sulla totalità degli incidenti registrati nel 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 32
Figura 38 - AI nelle tattiche MITRE ATT&CK® nel 1Q2025 in Italia 33

Figura 39 - AI nelle tattiche MITRE ATT&CK® nel 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 34
Figura 40 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel 1Q2025 in Italia 35
Figura 41 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel settore finanziario nel 1Q2025 in Italia 35
Figura 42 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia 36
Figura 43 - Situazione italiana dei dispositivi IPv4 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 37
Figura 44 - IoT/ICS vs Others IPv4 1Q2025 38
Figura 45 - Dispositivi IoT e OT individuati 38
Figura 46 - ICS/PLC individuati 1Q2025 39
Figura 47 - Sistemi industriali 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 39
Figura 48 - Distribuzione dei dispositivi IoT nelle regioni italiane 1Q2025 40
Figura 49 - Distribuzione dei dispositivi IoT per milione di abitanti nelle regioni italiane 1Q2025 41
Figura 50 - Protocolli senza autenticazione 1Q2025 42
Figura 51 - Distribuzione protocolli senza autenticazione in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 43
Figura 52 - Distribuzione dispositivi VoIP in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 44
Figura 53 - Distribuzione telecamere in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 44
Figura 54 - Distribuzione stampanti in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 45
Figura 55 - Distribuzione firewall in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 45
Figura 56 - Distribuzione router in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 46
Figura 57 - Distribuzione dispositivi medicali in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 46
Figura 58 - Unsecurity IoT Index nel 1Q2025 47
Figura 59 - Unsecurity IoT Index per Area Geografica 49
Figura 60 - Unsecurity IoT Index per dispositivo 50
Figura 61 - IoT Vulnerability Entropy Index 52
Figura 62 - Rappresentazione grafica dell'Investment Index media per ogni settore economico analizzato 55
Figura 63 - Investment Index per Area Geografica 56

Introduzione

La CyberSecurity si distingue da molte altre scienze in quanto i reali competitor non sono coloro che forniscono soluzioni migliori, ma gli attaccanti che ogni giorno sviluppano tecniche e metodologie per compromettere i servizi utilizzati da coloro che si difendono per averne un beneficio. Exprivia crede nel valore della condivisione e mette a disposizione i dati rilevati su attacchi, incidenti e violazioni privacy dal suo Osservatorio a beneficio di chi lavora nel mondo della CyberSecurity.
L'Osservatorio colleziona informazioni pubbliche e non, anche se abbiamo deciso di condividere e creare statistiche solo utilizzando informazioni pubbliche. Questa decisione si basa sulla volontà di non compromettere in alcun modo la confidenzialità delle informazioni consegnateci dai nostri clienti e per avere un insieme di dati statisticamente validi e il più possibile solidi. Le statistiche 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.
Al fine di ottenere e condividere dati statisticamente rilevanti, si è attuata un'analisi del perimetro italiano e un focus sul settore finanziario. I valori della ricerca hanno però valenza a livello globale in quanto indicatori di tendenze consolidate.
In caso di scostamenti da cosa è stato osservato a livello globale, questo scostamento verrà discusso e analizzato ulteriormente nel rapporto.
I record registrati relativamente ad attacchi, incidenti e violazioni privacy sono consolidati al 31/03/2025. Eventuali dati la cui evidenza è successiva a questa data possono non essere oggetto dell'analisi in questione.

Executive Summary

Se il 2024 si è chiuso con dei dati che suggeriscono un leggero ottimismo avendo registrato una diminuzione di attacchi ed incidenti, il 2025 si apre in controtendenza. Nei primi tre mesi, infatti, si nota una considerevole inversione di tendenza con un numero di attacchi (630) ed incidenti (217) mai riscontrati negli scorsi dodici mesi. Infatti, non deve essere dimenticato che le informazioni analizzate sono relative a sorgenti aperte e pertanto seppure valide per analisi del rischio e valutazioni statistiche, rappresentano una piccola parte di quanto accade nella realtà. Dunque, se da un lato evitare di essere vittima di un incidente è una necessità che prescinde le normative introdotte e vigenti, dall'altro è necessario investire per ridurre il tempo di reazione ad un incidente tramite piattaforme integrate con tutte le funzioni aziendali che rendano efficiente questo processo.
Anche sul tema della cybersecurity l'Italia non è però uniforme. I numeri assoluti ci suggeriscono che il nord è maggiormente colpito, ma se analizziamo attacchi ed incidenti di sicurezza per milione di abitanti, il quadro si rovescia ed è il nord a sembrare meno esposto al fenomeno, mentre le regioni più a rischio sono quelle centrali.
Il phishing e social engineering continuano ad essere tra le tecniche più utilizzate anche se in diminuzione. Sicuramente gli investimenti su formazione (che include simulazione di campagne di phishing, red-blue team...) hanno avuto dei risultati: malgrado l'utilizzo di AI generativa, oggi sembra meno banale catturare le vittime con semplici inganni. Tuttavia, è necessario non abbassare la guardia in quanto le tecniche di attacco vengono modificate ed è pertanto necessario pianificare formazione che sia in grado di adattarsi sia alle nuove minacce, sia che si adatti alle competenze già acquisite dalla parte del soggetto.
Non tutto però può essere fatto con la formazione. La consapevolezza dell'individuo resta il firewall più importante, ma l'individuo non può essere lasciato solo. Aumentano, infatti, gli attacchi con Malware, ma soprattutto aumentano attacchi di tipo DDoS.
Continua a salire il numero di incidenti di sicurezza legati ad attacchi collegati ad uso di AI dal 30% al 40% (44% nel mondo finanziario).
Un'ultima considerazione sui dispositivi IoT. Migliora generalmente la sicurezza delle telecamere di videosorveglianza e dispositivi medici, ma peggiora la sicurezza degli ICS (Industrial Control System).

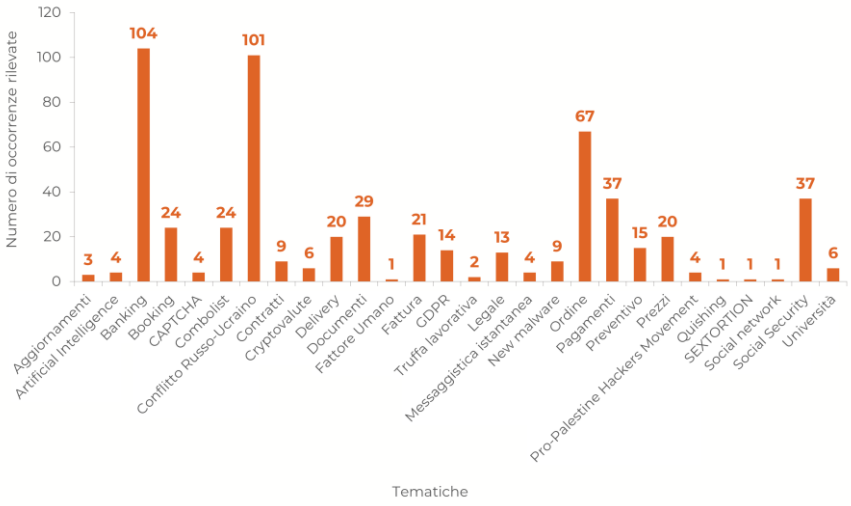


Figura 1 - Tematiche riscontrate di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

Attacchi, incidenti e violazioni privacy

Nei rapporti è necessario identificare con dettaglio gli oggetti delle statistiche. Il presente rapporto include dati che fanno riferimento a diversi elementi.

- **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, anche se non ci sono prove esplicite che la campagna abbia compromesso clienti italiani.
- **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.

Il primo trimestre del 2025 evidenza un andamento in costante crescita del numero di attacchi, incidenti e violazioni privacy, registrando un totale di 862 casi con un picco di 341 casi nel mese di marzo, circa il 9% in più rispetto al mese di febbraio (313 casi) e 64% in più rispetto a gennaio (208 casi) (Figura 2). Numerosi sono stati gli attacchi sferrati nell'ultimo mese del primo trimestre, il più delle volte coinvolgendo non solo il settore privato ma anche quello pubblico. Tutto ciò, evidenzia come le tecniche di attacco adottate dai cybercriminali siano in costante evoluzione e continuino ad infliggere ingenti danni verso istituzioni, aziende, organizzazioni di vario genere ma soprattutto verso cittadini privati, vittime primarie del cybercrime.

Il settore finanziario si conferma tra i settori maggiormente colpiti dai cybercriminali anche nei primi mesi del 2025 (Figura 3). L'andamento del numero di attacchi, incidenti e violazioni privacy nel suddetto settore segue il trend della totalità dei casi nel 1Q2025. Nello specifico nel mese di gennaio si sono verificati 46 casi pari al 22% del totale dei casi dello stesso mese, nel mese di febbraio si sono verificati 78 casi su 313 totali (25%) e nel mese di marzo sono stati registrati 87 casi, il 26% del totale dei casi dello stesso mese. Anche per il settore finanziario assistiamo ad un picco del numero di attacchi, incidenti e violazioni privacy nel mese di marzo. Il settore finanziario è un obiettivo privilegiato per i criminali informatici. Banche, assicurazioni, fornitori di pagamenti digitali e piattaforme di criptovalute sono frequentemente nel mirino degli attaccanti, attratti dalla prospettiva di ottenere rapidamente ingenti somme di denaro.

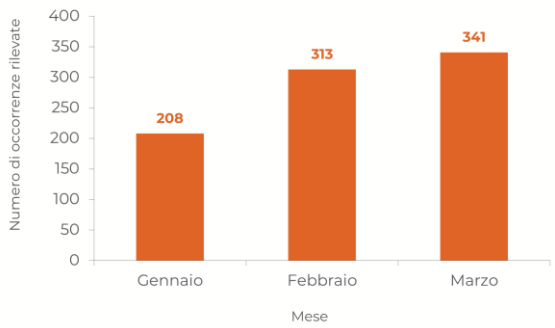


Figura 2 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi in Italia nel 1Q2025

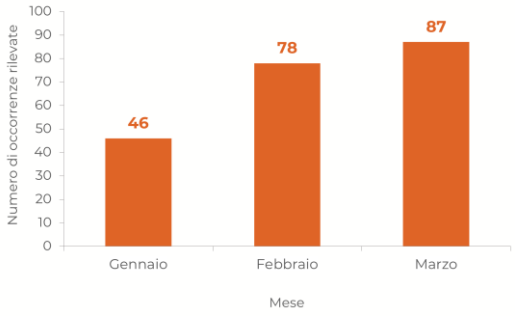


Figura 3 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi nel settore finanziario nel 1Q2025

I dati aggregati su base trimestrale relativi agli eventi di sicurezza rilevati dall'Osservatorio Cybersecurity di Exprivia, raffigurati nella figura seguente, evidenziano rilevanti tendenze.
La variazione del numero di occorrenze rilevate, misurata rispetto al trimestre precedente, è superiore al 34%. Infatti, nel 1Q2025 sono stati registrati 862 eventi di sicurezza rispetto ai 641 del 4Q2024. Anche la variazione tendenziale del numero di casi di sicurezza analizzati, misurata rispetto allo stesso trimestre dell'anno precedente, è superiore al 54%.
Questo trend può indicare sia una maggiore esposizione digitale delle organizzazioni e degli individui, sia una crescente attività da parte di cybercriminali, hacktivisti o altre tipologie di attaccanti.

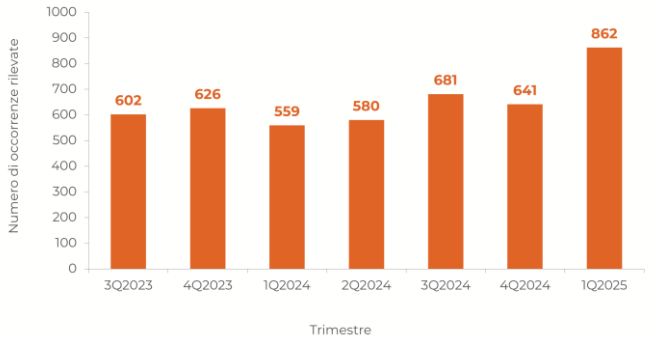


Figura 4 - Numero di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Nel 1Q2025 sono stati registrati in Italia 630 attacchi, 217 incidenti di sicurezza e 15 violazioni della privacy, come mostrato nella prima figura a sinistra.
Il rapporto tra incidenti e attacchi risulta essere in ascesa rispetto ai trimestri precedenti, indicando una persistente vulnerabilità nelle difese dei vari settori.

La figura 6 evidenzia che il settore finanziario italiano, nei primi mesi del 2025, ha subito 203 attacchi, oltre il 90% del totale dei casi registrati per il settore finanziario e 8 incidenti, circa il 4% del totale.
In questo contesto, il panorama della sicurezza informatica in Italia si conferma critico, con avversari sempre più evoluti.

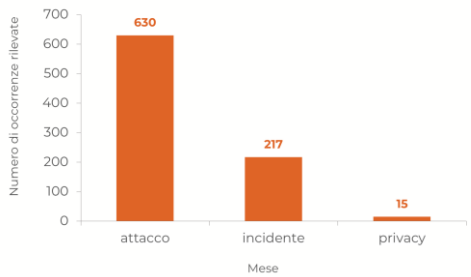


Figura 5 - Numero di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

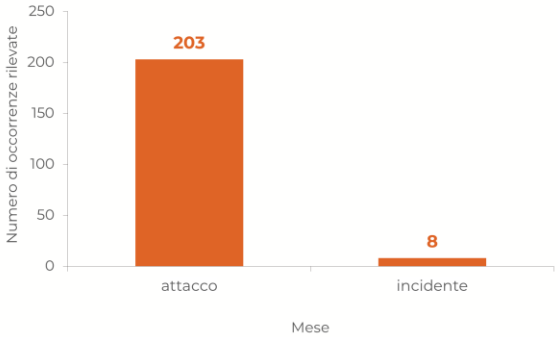


Figura 6 - Numero di attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia

Una visione completa del numero di attacchi, incidenti di sicurezza e violazioni privacy è presente nell'istogramma di seguito rappresentato. Si può osservare come nel 1Q2025 il rapporto tra incidenti e attacchi è superiore al 34%.
Analizzando l'evoluzione temporale, dopo una flessione del 13%, relativamente al numero di incidenti di sicurezza individuati tra il 3Q2024 e il 4Q2024, il primo trimestre dell'anno corrente segna un nuovo picco, rappresentando il valore più alto riscontrato a partire dal 3Q2023.

Sul versante finanziario è possibile osservare, dal grafico a destra, un andamento variabile dei dati raccolti su attacchi, incidenti e violazioni privacy, con un picco nel 4Q2023. In particolare, nel 1Q2025 si assiste ad un aumento di occorrenze raccolte nel settore finanziario del 23%, rispetto al 4Q2024, passando da un numero totale di casi di 171(4Q2024) ad un numero pari a 211(1Q2025).
Nel 1Q2025 restano invariati gli incidenti di sicurezza nel settore finanziario rispetto al 4Q2024. Le violazioni della privacy, invece risultano stabili nel corso dei trimestri in analisi.

Si può quindi affermare che, dopo una fase di crescita degli attacchi nel settore finanziario, i primi mesi del 2025 registrano un nuovo aumento, con livelli comparabili a quelli del primo trimestre dell'anno precedente.

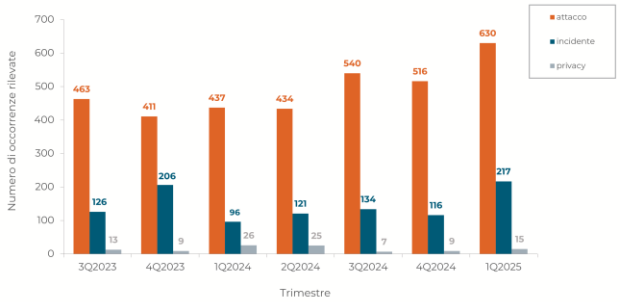


Figura 7 - Numero di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

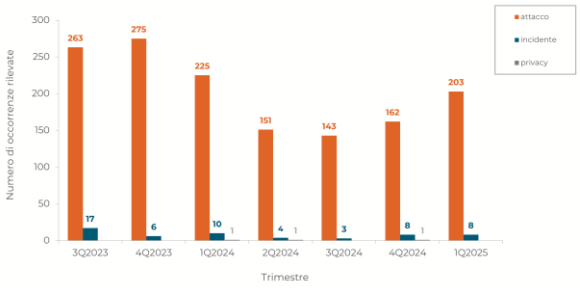


Figura 8 - Numero di attacchi, incidenti e violazioni privacy nel settore finanziario nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Motivazione degli attaccanti

Nel corso del 1Q2025, le analisi condotte dall'Osservatorio di Cybersecurity di Exprivia hanno rilevato che la motivazione più comune dietro gli attacchi informatici è, ancora una volta, il cybercrime con 717 casi registrati. Questo fenomeno è generalmente associato a guadagni illeciti o estorsioni, spesso orchestrato da organizzazioni criminali che sfruttano le vulnerabilità dei sistemi informatici per ottenere vantaggi economici.
Tale dato risulta estremamente elevato rispetto alle altre categorie, ricoprendo (nel grafico di sinistra) oltre l'80% rispetto alla totalità delle evidenze acquisite.
L'hacktivism segue al secondo posto con quasi il 15% dei casi, pari a 127 casi di sicurezza. L'hacktivism si distingue per la sua motivazione ideologica o politica. Infatti, l'obiettivo principale, per questa tipologia di attaccante, è solitamente quello di promuovere un cambiamento sociale o politico o sensibilizzare l'opinione pubblica su determinati temi, mettendo sotto pressione le istituzioni e le organizzazioni che considerano colpevoli.

Il grafico a destra illustra la situazione nel settore finanziario. Dall'analisi è possibile notare, anche in tal caso, che il cybercrime sia decisamente la motivazione principale dietro i vari attacchi, incidenti e violazioni della privacy. Questa disparità sottolinea come le attività malevole nel settore finanziario siano prevalentemente guidate da intenti criminali volti al guadagno illecito, all'estorsione di denaro o al furto di informazioni sensibili. Le motivazioni ideologiche o di protesta, tipiche dell'hacktivism, appaiono marginali in questo specifico contesto.

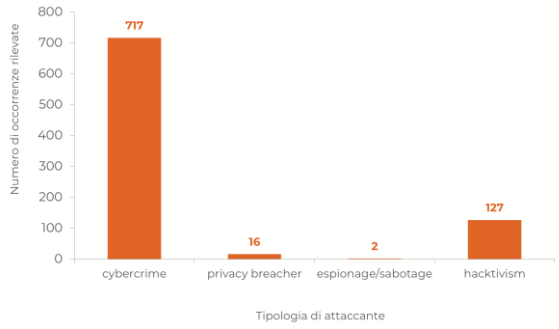


Figura 9 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel 1Q2025 in Italia

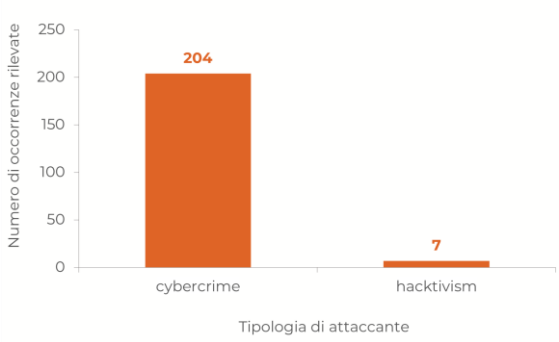


Figura 10 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel settore finanziario nel 1Q2025 in Italia

I dati raccolti evidenziano una netta escalation degli attacchi, con una prevalenza marcata del cybercrime, ma anche con nuove preoccupazioni legate alla privacy e alla sicurezza strategica.
Nel dettaglio il Cybercrime registra un incremento del 21% circa rispetto al trimestre precedente. Questo dato conferma la costanza e la pericolosità di un fenomeno sempre più diffuso e sofisticato, particolarmente attrattivo per chi mira a colpire istituzioni finanziarie e non solo per finalità economiche.
Dal grafico si osserva anche un incremento legato al fenomeno dell'Hacktivism pari al 253% circa, che mostra un'intensificazione nei primi mesi dell'anno, rispetto al 4Q2024. Questo incremento è attribuibile principalmente alle campagne del gruppo filorusso NoName057, che ha condotto numerose azioni contro infrastrutture critiche italiane per diffondere le proprie ideologie legate al conflitto russo-ucraino.
Le analisi del 1Q2025 mettono in luce anche un'impennata delle violazioni privacy causate da privacy breacher, cresciute del 78% circa, rispetto al 4Q2024. Questo trend sottolinea come la gestione dei dati personali stia diventando una questione sempre più delicata, con conseguenti sanzioni disposte dal Garante per la protezione dei dati personali (GDPR) sia verso utenti che organizzazioni.
Per le attività di Espionage/Sabotage e Redirection si rileva una presenza marginale, segnalando una scarsa incidenza di queste motivazioni nel contesto nazionale attuale.

Nel complesso, i valori del 1Q2025 confermano un'intensificazione degli attacchi informatici, con una diversificazione delle motivazioni che pone nuove sfide alle strategie di difesa e protezione delle organizzazioni.

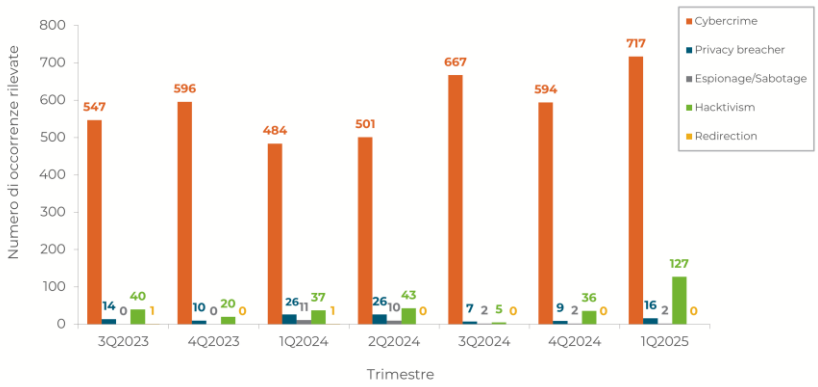


Figura 11 - Conteggio motivazione attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2025 e 1Q2025 in Italia

Distribuzione geografica

La rappresentazione delle mappe sottostanti identifica la distribuzione geografica degli attacchi informatici, degli incidenti e delle violazioni privacy registrati in Italia nel 1Q2025, con un focus specifico sul settore finanziario.
In entrambi i casi, il Nord Italia risulta l'area più colpita: 792 casi di sicurezza complessivi e 211 nel solo ambito finanziario. La maggiore esposizione è verosimilmente attribuibile all'elevata concentrazione di infrastrutture digitali, operatori economici strategici e sistemi critici.
Il Centro Italia presenta una casistica lievemente inferiore (727 eventi totali, 206 nel settore finanziario), ma comunque significativa, data dalla presenza di poli amministrativi e industriali.
Il Sud e le isole, con 685 eventi e 206 nel comparto finanziario, seppur registrando dei valori più contenuti, mostrano una crescente esposizione, segnale che le minacce cyber interessano l'intero territorio nazionale.

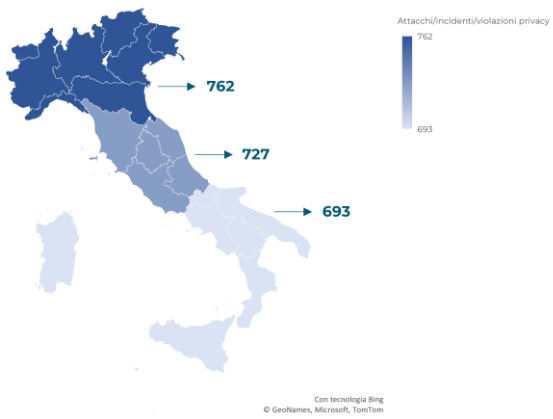


Figura 12 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

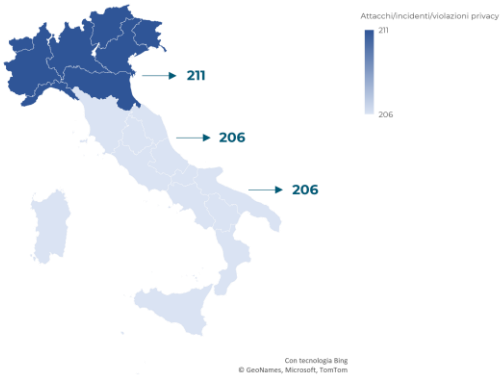


Figura 13 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia

Oltre a individuare i casi di sicurezza nelle diverse aree geografiche italiane, l'Osservatorio Cybersecurity di Exprivia analizza anche la distribuzione degli attacchi informatici, degli incidenti e delle violazioni della privacy in rapporto al numero di abitanti (per milione), considerando sia il quadro generale sia un approfondimento sul settore finanziario.
L'analisi evidenzia disparità tra le macroregioni. Il Centro Italia si distingue per la maggiore incidenza, con un picco di 63 casi ogni milione di abitanti. Al contrario, il Nord registra un'incidenza sensibilmente più bassa, pari a 28 casi per milione, nonostante sia un'area fortemente digitalizzata e con un'economia avanzata. Questo dato potrebbe riflettere un livello più elevato di consapevolezza e un'adozione più diffusa di misure di protezione informatica. Il Sud e le Isole si collocano in una posizione intermedia, con 35 casi ogni milione di abitanti.

Anche nel settore finanziario italiano si riscontrano dinamiche simili a quelle rilevate nel contesto generale, seppur con valori numerici differenti. In particolare, il Centro Italia continua a registrare il maggior numero di casi di sicurezza per milione di abitanti, mantenendo il primato rispetto alle altre aree geografiche del Paese.

L'analisi per abitante evidenzia come la vulnerabilità cyber possa distribuirsi in modo eterogeneo sul territorio nazionale in relazione alla densità demografica e, potenzialmente, a fattori socio-economici e culturali specifici di ciascuna macroregione.

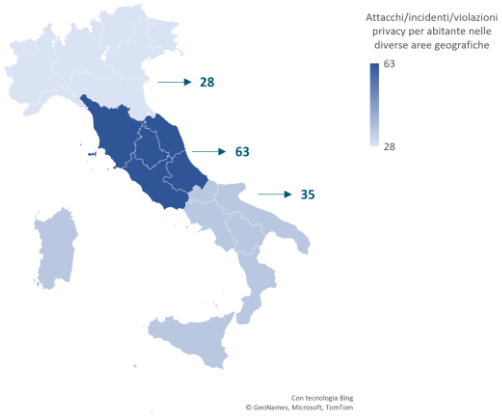


Figura 14 - Distribuzione geografica di attacchi, incidenti e violazioni privacy per abitante nelle diverse aree geografiche nel 1Q2025 in Italia

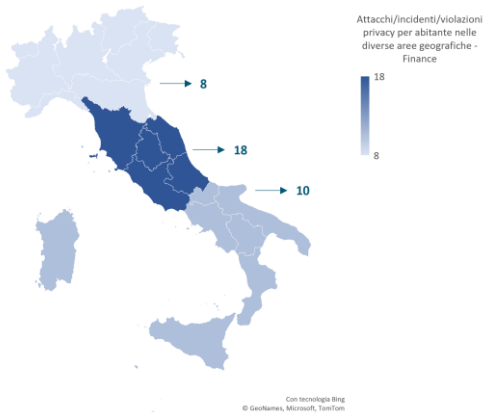


Figura 15 - Distribuzione geografica di attacchi, incidenti e violazioni privacy per abitante nelle diverse aree geografiche nel settore finanziario nel 1Q2025 in Italia

Distribuzione vittime per Industria

Il grafico analizza la distribuzione degli attacchi informatici nei diversi settori industriali, mettendo in luce quali ambiti risultano essere più frequentemente nel mirino dei cybercriminali. Colpisce subito l'elevato numero di casi di sicurezza registrati nel settore Software/Hardware, con ben 226 occorrenze rilevate. Questo suggerisce che spesso gli attaccanti mirano ai fornitori stessi di soluzioni digitali, nel tentativo di sfruttare eventuali vulnerabilità presenti nei prodotti distribuiti su larga scala.
Segue a breve distanza il settore finanziario, con 211 attacchi. Banche, assicurazioni e altri attori del mondo della finanza sono bersagli privilegiati, considerata l'attrattività che rappresentano in termini economici e la natura riservata delle informazioni che gestiscono.
Il settore del Retail, con 115 attacchi, rappresenta un'altra categoria ampiamente compromessa. Questo dato riflette vulnerabilità strutturali legate alla natura stessa del settore, fortemente orientato all'interazione digitale con l'utenza e alla gestione di dati sensibili, come informazioni personali, dati di pagamento e credenziali di accesso.
Il dato relativo alla Pubblica Amministrazione è anch'esso significativo, perché mette in luce la crescente pressione che questo settore sta subendo sul fronte della cybersecurity. Con oltre un centinaio di casi di sicurezza registrati in un solo trimestre, la PA si conferma come uno degli obiettivi privilegiati dai cybercriminali. I motivi sono molteplici: la PA gestisce grandi volumi di dati sensibili (anagrafici, sanitari, fiscali), ha una struttura diffusa e articolata, e spesso presenta infrastrutture IT eterogenee, in parte legacy, che offrono punti di ingresso facilmente sfruttabili.

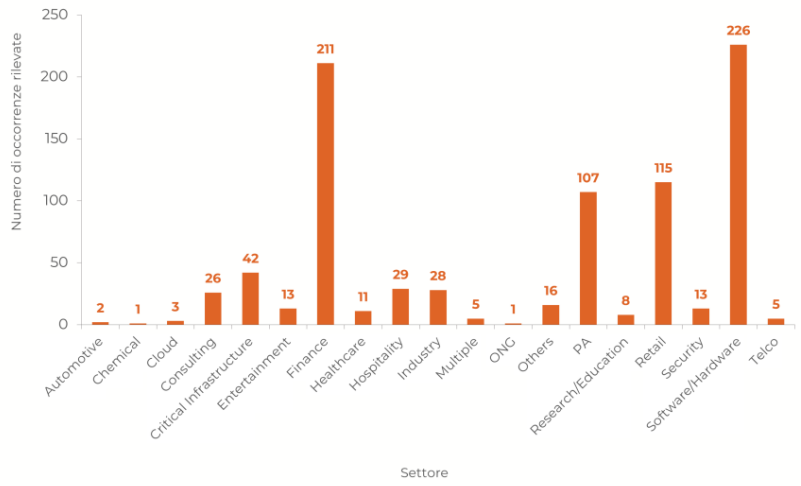


Figura 16 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

Software/Hardware

Il grafico rappresenta l'andamento mensile degli attacchi informatici registrati nel settore Software/Hardware durante il primo trimestre dell'anno, mettendo in evidenza un incremento progressivo e rilevante. Questo andamento segnala un trend in netta crescita, con un incremento complessivo dell'88% tra l'inizio e la fine del trimestre.
Si tratta di un dato particolarmente significativo, se si considera che il settore software/hardware rappresenta l'infrastruttura di base su cui poggiano molte altre aree industriali e servizi digitali. Colpire questi sistemi significa, in molti casi, compromettere a cascata altri ambienti, rendendo queste aziende obiettivi particolarmente strategici per i cybercriminali.

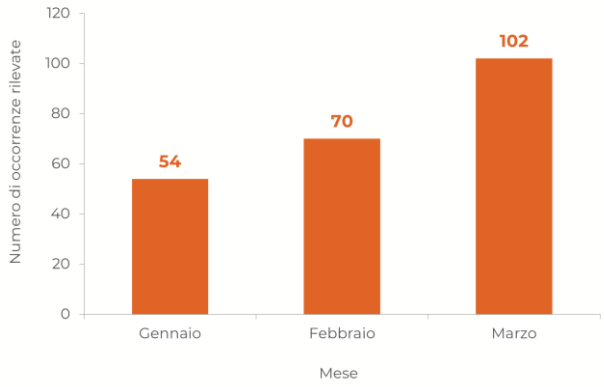


Figura 17 - Attacchi, incidenti e violazione privacy del settore Software/Hardware nel 1Q2025 in Italia

Finance

Nel primo trimestre del 2025, la distribuzione mensile degli attacchi, degli incidenti e delle violazioni della privacy nel settore finanziario in Italia ha evidenziato che marzo è stato il mese con il numero più elevato di casi di sicurezza registrati, con un totale di 87 occorrenze.
Febbraio si è distinto con un numero considerevole di 78 casi di sicurezza, mentre a gennaio si è registrata una diminuzione, con 46 occorrenze.

L'accentuarsi dei fenomeni analizzati per questo settore, potrebbe essere dovuto non solo a un'espansione delle minacce, ma anche ad una maggiore capacità di rilevamento da parte delle organizzazioni finanziarie. Questo trend porta a riflettere non solo sull'efficacia delle difese, ma anche sulla maturità dei sistemi di monitoraggio e sulla tempestività della risposta, fattori che potrebbero aver contribuito alla visibilità degli eventi piuttosto che alla loro effettiva incidenza.

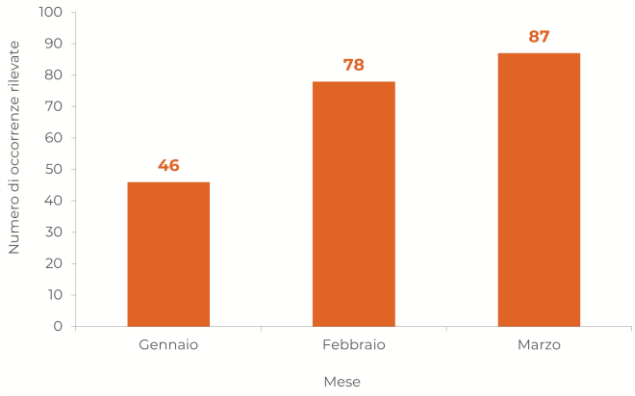


Figura 18 - Attacchi, incidenti e violazioni privacy del settore Finance nel 1Q2025 in Italia

Retail

La visualizzazione dei dati per il settore retail nel primo trimestre del 2025 in Italia evidenzia che febbraio è il mese con il numero più elevato di casi di sicurezza registrati, con un totale di 49 occorrenze. Marzo segue con un numero di 43 fenomeni, mentre gennaio ha registrato una diminuzione, con solo 23 occorrenze.

Nonostante la flessione registrata verso la fine del trimestre, il settore retail si conferma una componente essenziale nella quotidianità dei consumatori, spinta dalla crescente diffusione dell'e-commerce. Proprio questa centralità lo rende un bersaglio particolarmente attrattivo per i criminali informatici, che vi intravedono ampie opportunità di profitto.

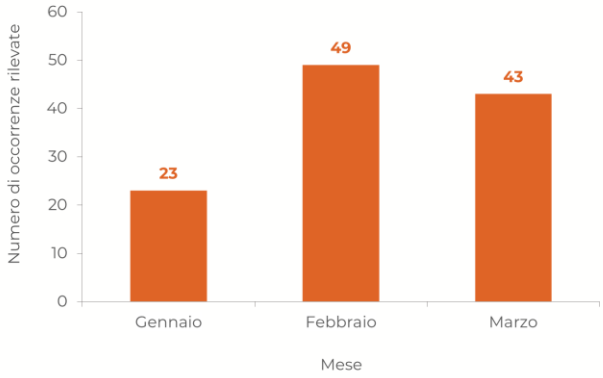


Figura 19 - Attacchi, incidenti e violazioni privacy del settore Retail nel 1Q2025 in Italia

Tipo di danno

Nel primo trimestre del 2025, i danni causati da attacchi informatici, incidenti e violazioni della privacy in Italia hanno colpito in modo diverso a seconda dei settori, con una netta prevalenza del furto di dati.
A livello nazionale, il furto dati è stato di gran lunga il danno più frequente (607 casi), confermando quanto le informazioni sensibili siano, ormai, l'obiettivo principale dei cybercriminali. Seguono l'interruzione dei servizi (117 casi), che causa il blocco delle operazioni aziendali e infrastrutture, e i danni economici diretti (100 casi), legati a furti di denaro o riscatti. Le violazioni della privacy (16 casi), i defacement di siti web (11), altre tipologie di danno (10) e i danni reputazionali (1 solo caso) sono meno comuni, anche se non meno rilevanti.

Nel settore finanziario, lo scenario è simile, ma presenta alcune peculiarità. Anche qui il furto di dati è il danno più frequente (109 casi), seguito molto da vicino dai danni economici (95 casi), che risultano particolarmente rilevanti in questo ambito, data la natura sensibile delle informazioni trattate e le potenziali perdite dirette. Le interruzioni di servizio sono meno comuni (7 casi), ma comunque significative per un settore che si basa sull'affidabilità e la continuità operativa.

In sintesi, il furto di dati si conferma la minaccia principale, ma nel settore finanziario i danni economici pesano in modo maggiore.

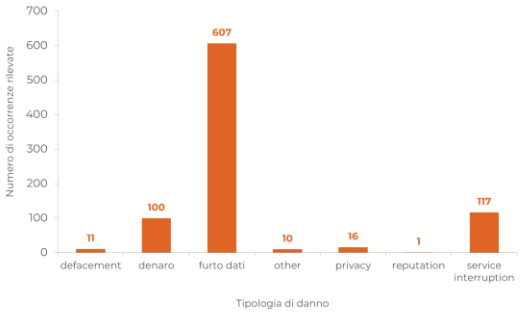


Figura 20 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

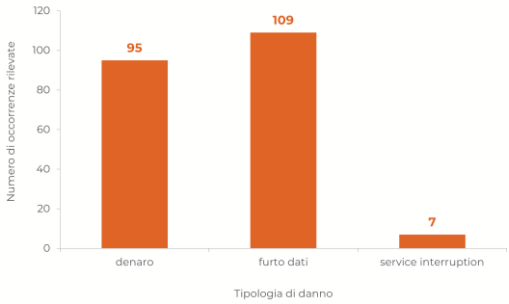


Figura 21 - Tipologia danno di attacchi, incidenti e violazioni privacy nel settore finanziario in Italia nel 1Q2025

Nel periodo esaminato, che ricopre i trimestri a partire dal 3Q2023 al 1Q2025, in Italia si è registrato un forte aumento degli attacchi informatici mirati al furto di dati, con una crescita del 95% su base annua. Questa tipologia di danno provoca esfiltrazione di credenziali, cookie, wallet e informazioni sensibili, spesso tramite campagne di phishing e malware.
I danni economici, hanno mostrato un andamento altalenante, ma restano significativi grazie all'uso di strumenti persistenti. Meno frequenti, ma complessi, gli attacchi mirati allo spionaggio e al furto di proprietà intellettuale.
Le violazioni della privacy, pur numericamente contenute, presentano rischi elevati per le sanzioni legali, mentre i danni reputazionali derivano da pubblicazioni su data leak site.
L'interruzione dei servizi ha registrato un incremento, con impatti su e-commerce, banking, cloud e infrastrutture critiche.
Il defacement, invece, appare marginale, confermando la tendenza degli attaccanti a puntare su obiettivi più redditizi.

La crescente sofisticazione delle minacce impone l'adozione di strumenti avanzati di rilevamento, segmentazione di rete e automazione della threat intelligence.

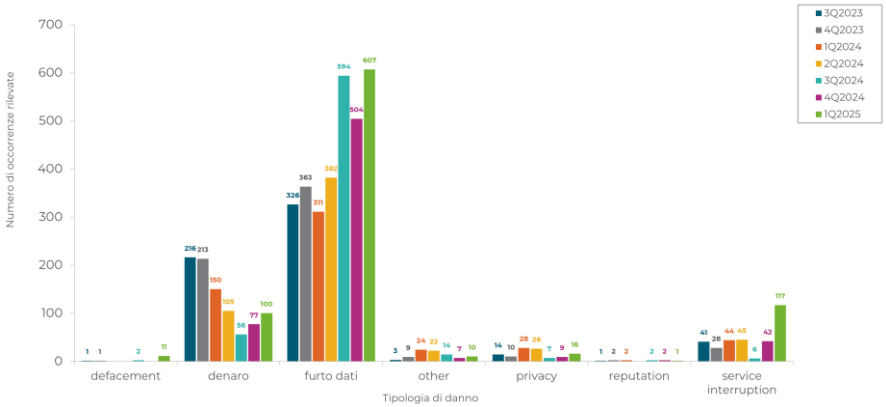


Figura 22 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Tecniche di attacco

Nel 1Q2025 in Italia, il panorama degli attacchi informatici, incidenti e violazioni della privacy è stato dominato da tecniche basate su malware (394 occorrenze), seguite da phishing/social engineering (281), e attacchi Distributed Denial of Service (DDoS) (116), come evidenziato nel grafico. Queste tre categorie rappresentano complessivamente oltre il 90% degli eventi rilevati, con il malware che da solo costituisce il 46% circa del totale. Seguono con frequenze inferiori le known vulnerabilities (23), attacchi di tipo unknown (34), web defacement (11), e con solo un'occorrenza ciascuno gli attacchi 0-Day, brute force e vishing.

Focalizzando l'attenzione al settore finanziario italiano, le tecniche di attacco informatico più rilevate, nel trimestre in esame, sono state principalmente quelle legate ai malware, con 135 evidenze, che rappresentano circa il 64% del totale dei casi di sicurezza considerati. Questo dato conferma il ruolo dominante delle minacce veicolate tramite software malevolo nel panorama finanziario.
A seguire, il phishing e social engineering ha registrato 68 casi (32%), mostrando ancora una volta come le tecniche basate sulla manipolazione degli utenti siano fortemente sfruttate dagli attaccanti nel contesto designato.

La netta predominanza di malware e phishing/social engineering evidenzia un contesto in cui gli attaccanti puntano principalmente sulla compromissione degli endpoint e sulla manipolazione psicologica degli utenti.

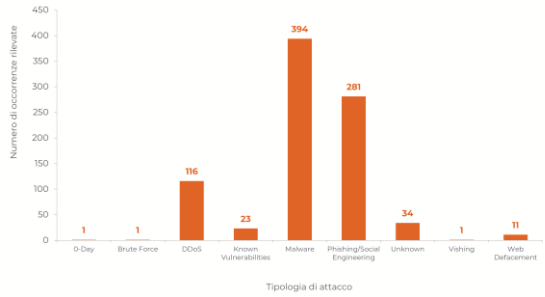


Figura 23 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

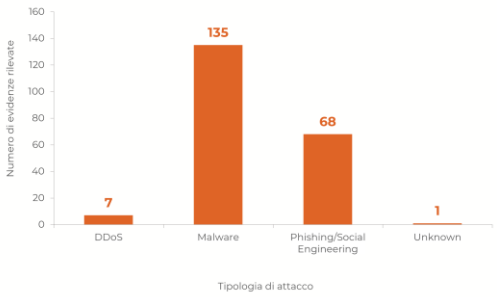


Figura 24 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel settore finanziario nel 1Q2025 in Italia

Una rappresentazione temporale evidenzia un forte aumento degli attacchi DDoS, cresciuti di oltre il 200% rispetto al trimestre precedente. Questo picco è stato in gran parte causato dalle offensive del gruppo hacktivista filorusso NoName057, che ha intensificato le sue azioni contro infrastrutture critiche, pubbliche amministrazioni, banche e altri enti italiani, provocando interruzioni di servizio.
Parallelamente, lo sfruttamento di malware risulta il principale vettore di attacco sfruttato dai cybercriminali, con un rialzo del quasi 80%, rispetto al 4Q2024.
Per quanto riguarda il phishing/social engineering si può osservare un trend positivo, legato alla riduzione delle rilevazioni effettuate attorno a questa categoria di attacco, rispetto al 3Q2024 (-22%) e 4Q2024 (-18%).

Il tasso di sfruttamento di vulnerabilità critiche, torna in rialzo ed è aumentato del 53% rispetto al trimestre precedente, seppur con valori più bassi rispetto ai primi due trimestri dell'anno precedente. Questa tendenza conferma, comunque, come la divulgazione di nuove falle (CVE) venga rapidamente utilizzata da attori malevoli.

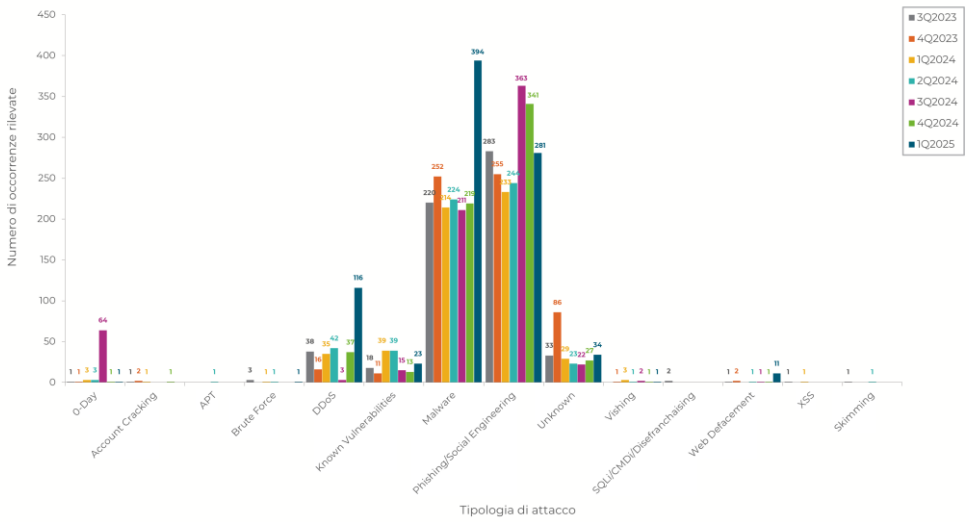


Figura 25 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Nome e tipo di malware

Nei grafici che seguono vengono illustrate le principali tipologie di malware associate ad attacchi ed incidenti di sicurezza registrati nel 1Q2025.
Si evidenziano i casi relativi a Remote Access Trojan (RAT), Infostealer, Keylogger e Ransomware.
Nel dettaglio, i casi relativi al malware RAT, che consentono all'attaccante di controllare da remoto il sistema della vittima, hanno totalizzato un valore di 128 casi, più del 30% di tutte le occorrenze rilevate nel 1Q2025 dall'Osservatorio CyberSecurity di Exprivia. Altra categoria rilevante è rappresentata dai malware di tipo Infostealer, che permettono di sottrarre informazioni sensibili dall'apparato colpito, con 99 casi (circa il 25% del totale).

Per il settore finanziario, si rileva un aumento, in percentuale, delle occorrenze relative ad attacchi veicolati tramite Keylogger, che vanno a pareggiare i numeri relativi ad Infostealer.
Inoltre, i Trojan bancari, nonostante siano sempre in numero inferiore rispetto alle tre tipologie con più occorrenze, ovvero RAT, keylogger e Infostealer, in questo contesto risultano più rilevanti: rappresentano infatti più dell'8% dei casi totali registrati nel settore finanziario, contrariamente al 3% rilevato nei dati totali del Paese e non specializzati per settore.

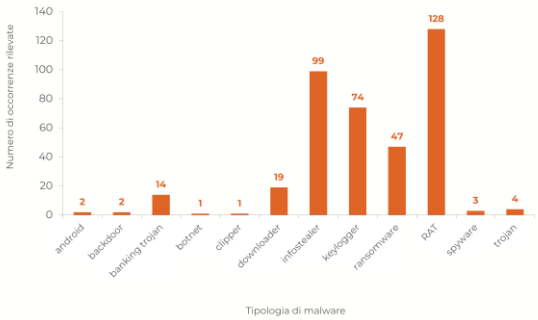


Figura 26 - Tipologie di malware relative ad attacchi e incidenti registrate nel 1Q2025 in Italia

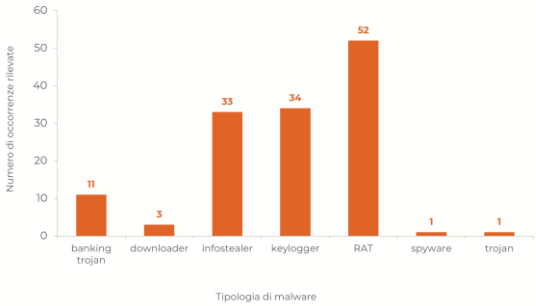


Figura 27 - Tipologie di malware relative ad attacchi e incidenti registrate nel settore finanziario nel 1Q2025 in Italia

Nella rappresentazione di seguito è possibile confrontare le numeriche complessive relative alle tipologie di malware, rilevate dal 3Q2023 fino al 1Q2025, nel territorio italiano.
Nel 1Q2025 si è registrata un'impennata nell'utilizzo dei malware di tipo RAT (+80% rispetto al 4Q2024), Keylogger (+393%) e Infostealer (+77% circa). Queste appena descritte sono le tipologie di malware che hanno subito maggiori variazioni in termini di evidenze raccolte, mentre il numero di casi di sicurezza relativi al ransomware è rimasto sostanzialmente stabile rispetto ai trimestri precedenti.

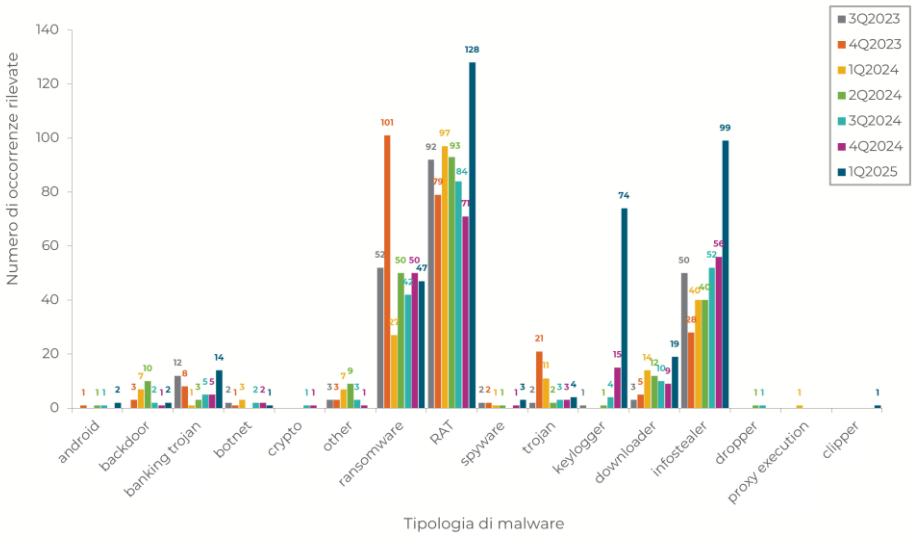


Figura 28 - Tipologie di malware relative attacchi e incidenti registrate nel 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024 e 1Q2025 in Italia

RAT

Il grafico rappresenta il numero di occorrenze rilevate su base mensile nei primi tre mesi dell'anno corrente, relativamente al malware RAT.
Il trend evidenziato nel grafico è nettamente crescente. Dopo un incremento significativo del 76% tra gennaio e febbraio, si registra un ulteriore aumento, più contenuto, pari a circa 34% tra febbraio e marzo.
L'incremento complessivo da gennaio a marzo è di 34 unità, rappresentando un aumento complessivo del 136% nel trimestre.
Questo andamento evidenzia una accelerazione iniziale seguita da una crescita più moderata, indicando un fenomeno in espansione, ma con un possibile rallentamento del tasso di crescita.

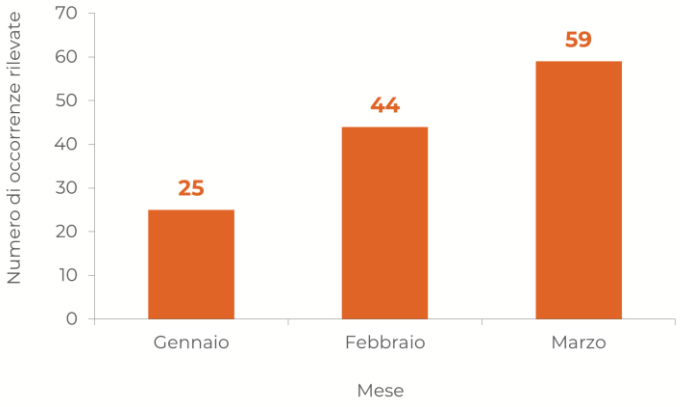


Figura 29 - RAT relativi ad attacchi e incidenti registrati nel 1Q2025 in Italia

Infostealer

Nel primo trimestre 2025, il numero di attacchi e incidenti informatici legati a Infostealer in Italia ha evidenziato un trend in crescita.
Complessivamente, da gennaio a marzo si è registrato un incremento del 58%, a indicare una pressione crescente di questa minaccia. Sebbene tra febbraio e marzo il numero di casi di sicurezza rilevati, per questa tipologia di malware, si sia mantenuto costante, il numero rimane elevato e segnala una fase di consolidamento della minaccia.

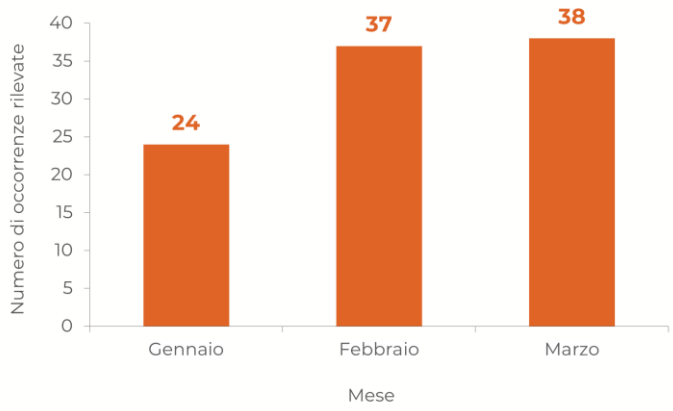


Figura 30 - Infostealer relativi ad attacchi e incidenti registrati nel 1Q2025 in Italia

Keylogger

Nel primo trimestre del 2025, l'andamento degli attacchi che coinvolgono i Keylogger mostra un trend irregolare. Il passaggio da gennaio a febbraio evidenzia un incremento del 63%, mentre il calo da febbraio a marzo si attesta al 22%. Nonostante questa diminuzione, il dato di marzo risulta comunque superiore a quello di gennaio, con una crescita del 26% rispetto all'inizio del trimestre.
I Keylogger continuano a rappresentare una minaccia rilevante per il furto di credenziali, considerando che l'accesso ai sistemi costituisce spesso il primo step per compromissioni più complesse.

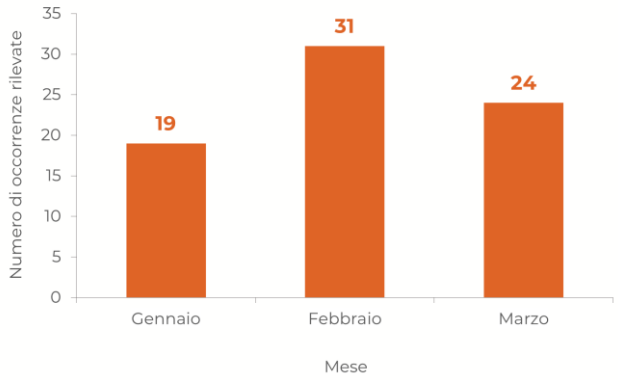


Figura 31 - Keylogger relativi ad attacchi registrati nel 1Q2025 in Italia

Classificazione MITRE ATT&CK®

Di seguito è rappresentata un'analisi delle tattiche e delle corrispondenti tecniche (appartenenti alle matrici Enterprise e Mobile) del MITRE ATT&CK® individuate nei fenomeni di sicurezza esaminati dall'Osservatorio Cybersecurity di Exprivia durante il 1Q2025 per il territorio Italiano. Ad ogni tecnica è associata la percentuale di occorrenza della stessa rispetto alla totalità degli eventi esaminati.

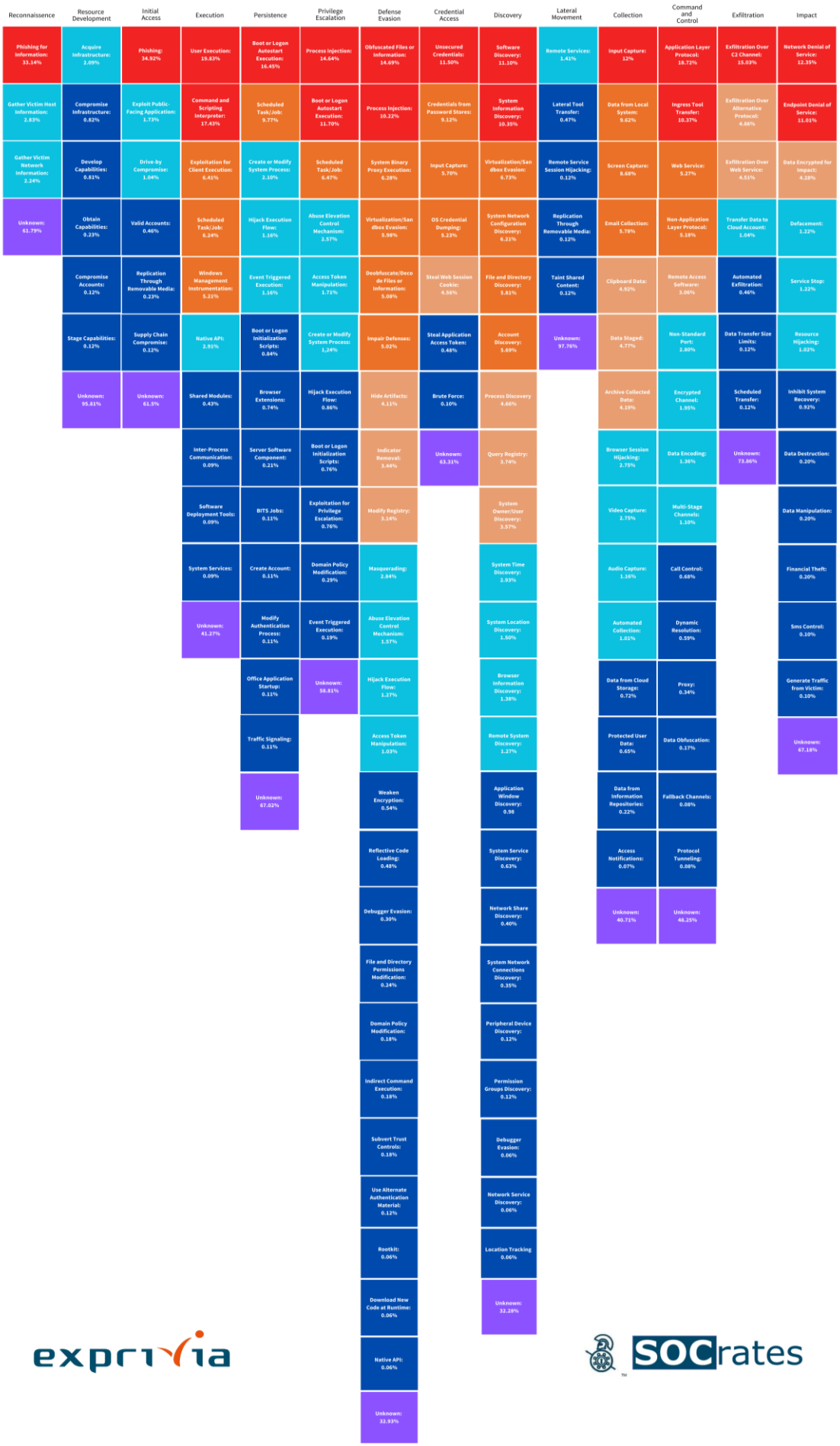


Figura 32 - Classificazione MITRE ATT&CK® 1Q2025 Italia

Incidenti di sicurezza AI e Supply Chain

Gli attacchi alla supply chain, che puntano a compromettere fornitori di software, servizi gestiti (MSP) e componenti open-source o firmware, rappresentano una minaccia particolarmente critica a causa dell'elevata interconnessione tra i sistemi, della crescente pressione normativa (NIS2, DORA) e del potenziale impatto reputazionale.
Tuttavia, come mostra il grafico sottostante relativo al primo trimestre del 2025, in Italia la maggior parte degli incidenti di sicurezza non è riconducibile a compromissioni della supply chain, evidenziando una riduzione della frequenza di tali episodi nel contesto nazionale della cybersecurity.

È interessante notare come, all'interno di questo contesto critico, il settore finanziario non abbia registrato alcun incidente riconducibile ad attacchi alla supply chain nel periodo analizzato.

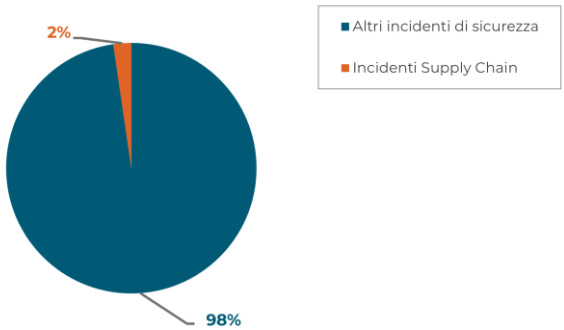


Figura 33 - Distribuzione degli incidenti legati ad attacchi Supply Chain sulla totalità degli incidenti registrati nel 1Q2025 in Italia

L’analisi tendenziale degli incidenti relativi alla supply chain, in Italia, mostra un picco massimo nel 3Q2024 (+940%), con oltre la metà degli incidenti causata da compromissioni di fornitori. Questo dato è attribuibile ad una compromissione di un vendor software critico, che ha causato un attacco su larga scala.
Dopo il picco, il numero degli incidenti è diminuito drasticamente nel 4Q2024 (-90%), tornando allo stesso valore del 2Q2024, stabilizzato poi al 1Q2025 con il 2%, ancora sotto il livello di inizio anno, ma con oscillazioni che indicano un rischio ancora instabile.

Le implicazioni di rischio includono interruzioni nei sistemi di pagamento, ritardi nei servizi online e rischi reputazionali, con sanzioni regolatorie che potrebbero arrivare fino al 2% del fatturato annuo in caso di mancata notifica tempestiva.

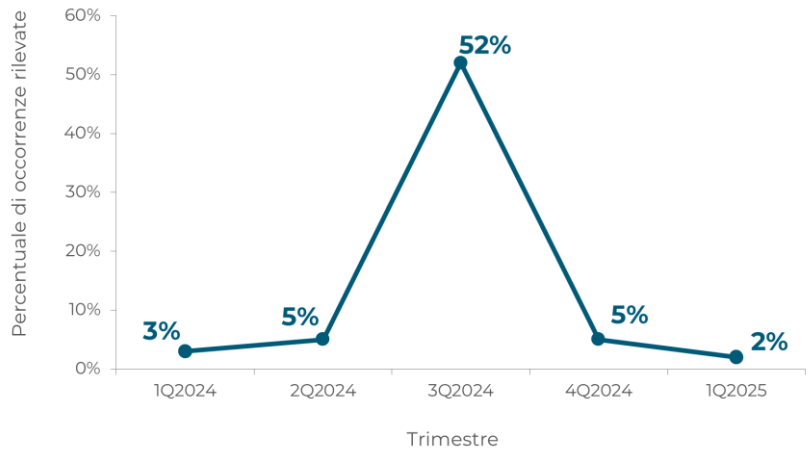


Figura 34 - Distribuzione degli incidenti legati ad attacchi Supply Chain sulla totalità degli incidenti registrati nel 1Q2024, 2Q2024, 3Q2024 e 1Q2025 in Italia

Come mostrato nel grafico a sinistra, nel primo trimestre del 2025 in Italia il 40% degli incidenti di sicurezza informatica è ricondotto ad attacchi influenzati dall'intelligenza artificiale, mentre il restante 60% deriva da metodologie convenzionali.
L'utilizzo di agenti AI per la ricognizione automatizzata consente di scansionare reti, identificare vulnerabilità e orchestrare campagne offensive su larga scala con velocità e precisione superiori alle operazioni manuali. Le reti neurali generative, inoltre, sono sfruttate per creare deepfake, e-mail di phishing iperrealistiche e documenti contraffatti, aumentando l'efficacia delle operazioni di ingegneria sociale.
Quasi metà degli incidenti rilevati nel periodo preso in esame presenta quindi elementi di sofisticazione, con processi automatizzati e modelli predittivi compromessi che giocano un ruolo centrale nello scenario delle minacce informatiche.

Il grafico a destra identifica la percentuale di sfruttamento dell'AI negli attacchi andati a buon fine per il settore finanziario italiano nel primo trimestre del 2025. In particolare, il 44% degli incidenti di sicurezza informatica è associato ad attacchi influenzati dall'intelligenza artificiale, mentre il restante 56% è attribuibile a minacce cibernetiche tradizionali.
Questi dati evidenziano un cambiamento strutturale nel profilo del rischio, confermando il ruolo determinante dell'AI nel rimodellare il contesto della sicurezza nel settore finanziario.

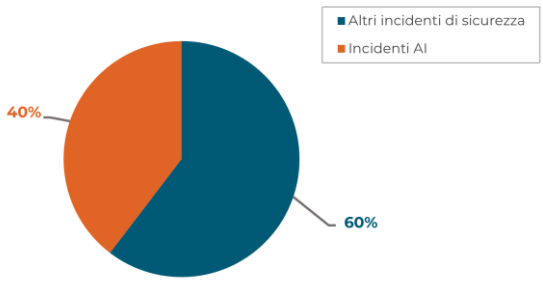


Figura 35 - Distribuzione degli incidenti legati ad attacchi influenzati dall'AI sulla totalità degli incidenti registrati nel 1Q2025 in Italia

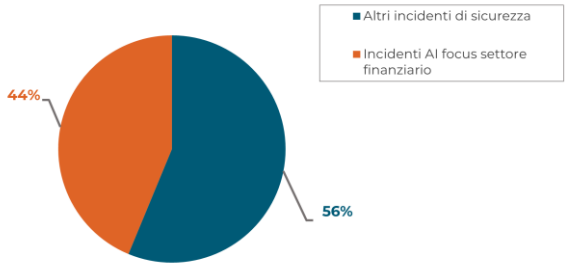


Figura 36 - Distribuzione degli incidenti legati ad attacchi influenzati dall'AI sulla totalità degli incidenti registrati nel settore finanziario nel 1Q2025 in Italia

L’andamento sottostante evidenzia una tendenza generale alla crescita nello sfruttamento dell’AI.
L’aumento osservato nel primo trimestre del 2025 suggerisce un uso sempre più pervasivo dell’AI nei contesti malevoli, probabilmente legato all’affinamento delle tecnologie come i deepfake vocali, gli attacchi di phishing avanzati e le tecniche automatizzate di elusione delle difese.
In conclusione, la figura conferma che l’intelligenza artificiale sta diventando uno strumento chiave nei moderni attacchi informatici.

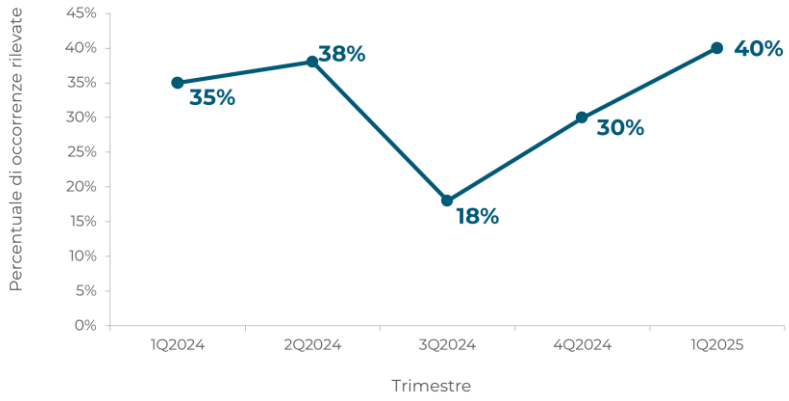


Figura 37 - Distribuzione degli incidenti legati ad attacchi influenzati dall’AI sulla totalità degli incidenti registrati nel 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Il panorama della cyber sicurezza in Italia è stato marcatamente influenzato dall'impiego crescente dell'intelligenza artificiale, sia da parte degli attori delle minacce che dei difensori. L'analisi delle offensive rilevate ha posto in evidenza una concentrazione preponderante sulle fasi terminali degli attacchi, quelle volte a causare danno tangibile alle vittime.

Le tattiche orientate all'impatto hanno mostrato una diffusione elevata. Queste includono azioni malevole come la cifratura dei dati (ransomware), la distruzione sistematica di dati o l'interruzione di servizi critici. L'AI gioca un ruolo di rilievo per gli attaccanti, ad esempio attraverso l'uso di algoritmi di reinforcement learning per ottimizzare le strategie di dispiegamento del ransomware o per automatizzare decisioni che massimizzino il danno economico ed operativo.
Le fasi di esecuzione del codice malevolo hanno mantenuto una presenza significativa. L'utilizzo dei modelli generativi può permettere la creazione di varianti di malware difficilmente rilevabili.
L'evasione delle difese è rimasta una priorità per gli attaccanti. L'AI viene impiegata per sviluppare tecniche per ingannare i modelli di rilevamento basati su AI utilizzati dalle difese.

Le fasi di accesso iniziale (Initial Access), ricognizione (Reconnaissance) e accesso alle credenziali (Credential Access), pur meno prevalenti nelle osservazioni aggregate, beneficiano anch'esse dell'impiego dell'AI, che automatizza scansioni di alla ricerca di vulnerabilità.

Nel settore finanziario italiano, l'analisi dell'influenza dell'intelligenza artificiale sulle varie tattiche del framework MITRE ATT&CK®, ha evidenziato che la tattica Impact è l'unica a emergere in modo significativo negli incidenti di sicurezza rilevati. Essa registra la percentuale più alta di occorrenze, confermando una netta correlazione con gli attacchi DDoS, che rappresentano la tipologia di minaccia prevalente nel settore e sono classificati proprio all'interno della categoria Impact della knowledge base del Mitre.

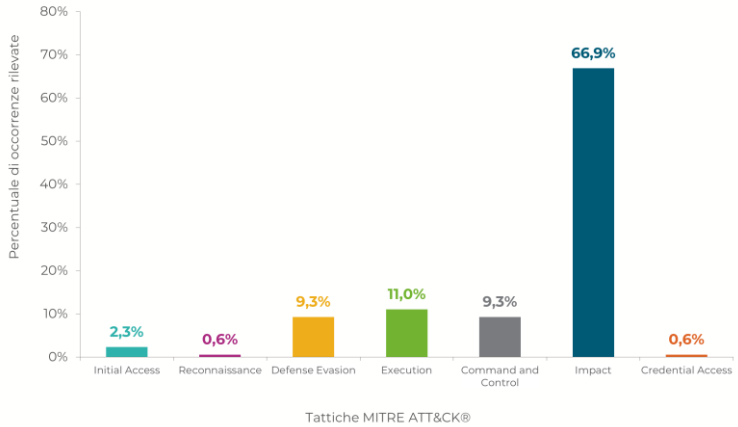


Figura 38 - AI nelle tattiche MITRE ATT&CK® nel 1Q2025 in Italia

Nel grafico sottostante sono rappresentati le varie percentuali di occorrenze rilevate in relazione alle principali tattiche di attacco, secondo il framework MITRE ATT&CK®, sfruttate dall'intelligenza artificiale.
In particolare, si è considerato come intervallo temporale l'intero 2024 e il primo trimestre del 2025. Si può notare come la tattica Impact sia ampiamente utilizzata dagli attaccanti per sferrare attacchi che mirano alla compromissione e/o distruzione di dati aziendali, impattando sulla loro disponibilità, integrità e la confidenzialità. Durante il 2024, si sono registrati valori percentuali molto alti, con una media del 33,25%, che risulta essere superiore a tutti i massimi valori registrati, durante l'intervallo temporale considerato, per le altre tattiche rappresentate. Con l'avvento del 2025, inoltre, si è registrato un picco del 66,9% di occorrenze rilevate (circa il 13% in più rispetto al primo trimestre del 2024), a testimonianza di quanto l'AI possa rendere sempre più automatizzato l'utilizzo di questa tattica.

Per quanto riguarda le altre tattiche considerate nel grafico, sono da sottolineare le percentuali, durante il 4Q2024, delle tattiche di Defence Evasion, Command and Control e Execution, con un valore percentuale del 22,9%.
Si può notare come l'andamento delle tattiche di Defence Evasion e Command and Contro sia crescente durante il 2024, ma calante durante il 1Q2025, mentre per la tattica di Execution si può notare come, durante il 2Q2024 e il 3Q2024, non siano stati rilevati incidenti di sicurezza caratterizzati dalla suddetta tattica MITRE.

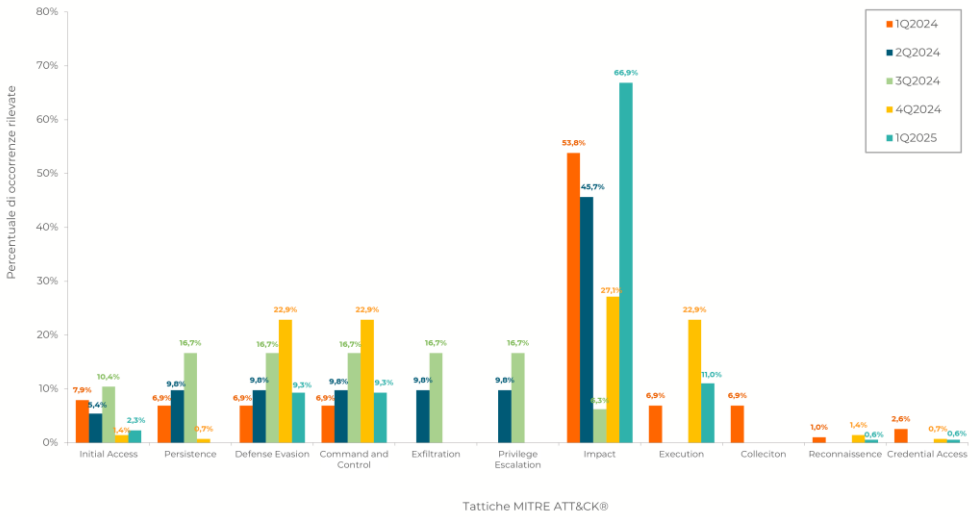


Figura 39 - AI nelle tattiche MITRE ATT&CK® nel 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Incidenti di sicurezza appartenenti alle tattiche e tecniche della Cloud Matrix MITRE ATT&CK®

I due grafici a torta illustrano la distribuzione degli incidenti di sicurezza per il periodo di riferimento del primo trimestre del 2025 in Italia, con particolare attenzione a quelli classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK®.

Nel primo grafico a sinistra, relativo al contesto generale per il periodo di riferimento, si osserva che l'83% degli incidenti è riconducibile a tattiche classificate dalla Cloud Matrix MITRE ATT&CK®.
Questo evidenzia la predominanza di attacchi strutturati e riconducibili a tattiche note all'interno dell'ambiente cloud.

Nel secondo grafico a destra relativo allo stesso periodo di riferimento, ma focalizzato sul settore finanziario, la tendenza è ancora più marcata: ben l'88% degli incidenti è classificato secondo la Cloud Matrix MITRE ATT&CK®, mentre solo il 13% rientra in altre tipologie. Questo dato sottolinea come, nel settore finanziario, la maggior parte degli attacchi sia sofisticata e rispecchi pattern ben documentati.

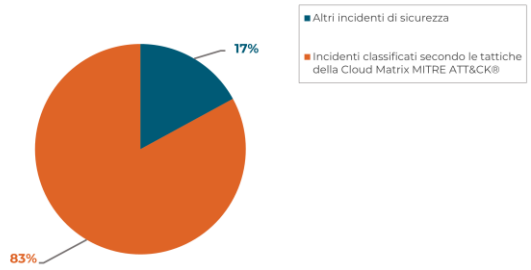


Figura 40 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel 1Q2025 in Italia

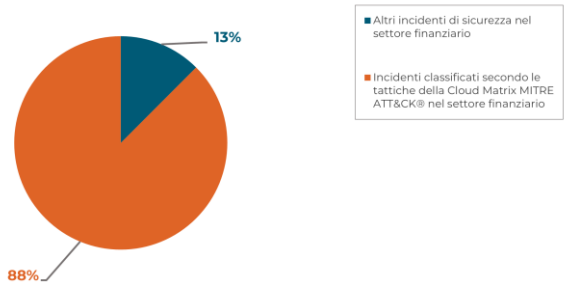


Figura 41 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel settore finanziario nel 1Q2025 in Italia

Nel contesto della crescente adozione di tecnologie cloud, l'analisi degli incidenti di sicurezza appartenenti alle tattiche e tecniche della Cloud Matrix MITRE ATT&CK® fornisce un quadro chiaro del trend in esame.
Osservando il periodo compreso tra il secondo trimestre 2024 e il primo trimestre 2025, si rileva un andamento altalenante ma significativo. Nel 2Q2024, il 74% degli incidenti risultava classificabile secondo le tattiche MITRE ATT&CK®, un dato già elevato che segnala la diffusione di attacchi strutturati e mappabili. Questo valore cresce ulteriormente nel 3Q2024, raggiungendo l'81%, con un incremento del 9% rispetto al trimestre precedente, a conferma della consolidata adozione di tecniche codificate da parte degli attaccanti.
Tuttavia, nel 4Q2024 si assiste a un'inversione di tendenza significativa: solo il 49% degli incidenti rientra nelle tattiche MITRE, segnando un calo del 39% rispetto al trimestre precedente.
La situazione si ribalta nuovamente nel 1Q2025, con una netta risalita fino all'83%, ovvero un aumento del 69% rispetto al trimestre precedente. In particolare, questo dato rappresenta il valore più alto del periodo considerato.

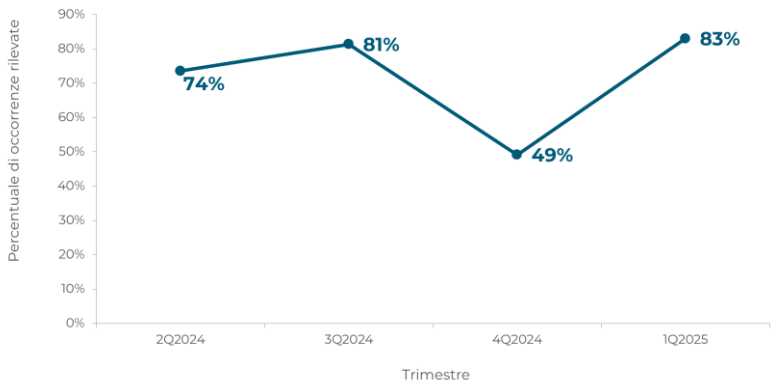


Figura 42 - Distribuzione degli incidenti classificati secondo le tattiche della Cloud Matrix MITRE ATT&CK® nel 2Q2024, 3Q2024, 4Q2024 e 1Q2025 in Italia

Sicurezza dei dispositivi IoT 1Q2025

In questa rubrica si discute sull'evoluzione della distribuzione dei dispositivi IoT, con riferimento ai dati del 1Q2025. In prima analisi abbiamo notato come i dispositivi IPv4 connessi in rete siano diminuiti di circa 220 mila dispositivi.

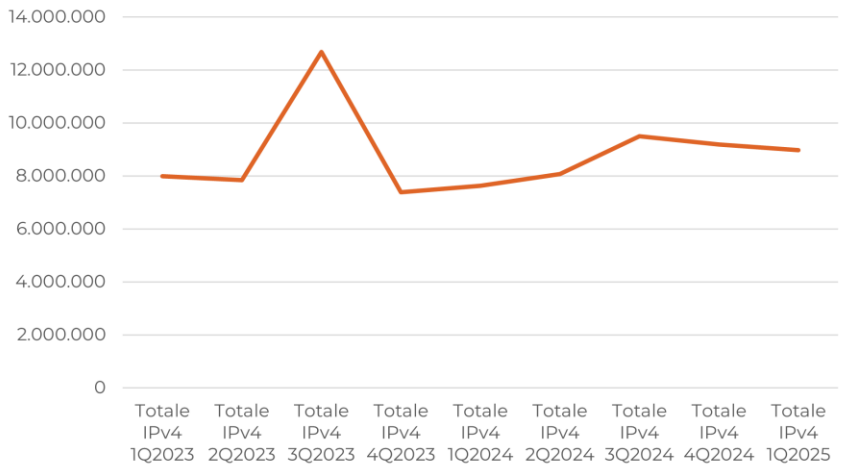


Figura 43 - Situazione italiana dei dispositivi IPv4 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

In Italia, le industrie con una maggiore presenza di dispositivi IoT sono:

- smart car;
- smart home;
- industrial IoT;
- smart health;
- smart metering;
- smart building.

In questa rubrica è stata mantenuta la distinzione tra dispositivi IT e dispositivi Operational Technology (OT). Nella figura 44, è mostrato il numero dei dispositivi specifici IoT sottoelencati, rilevati nel 1Q2025. Attualmente sono stati individuati 8.972.091 indirizzi IPv4 di cui 92.406 riferiti a:

- telecamere;
- stampanti;
- firewall;
- router;
- VoIP;
- dispositivi medicali.

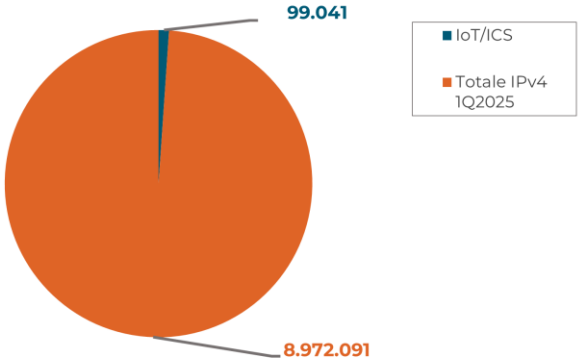


Figura 44 - IoT/ICS vs Others IPv4 1Q2025

Oltre ai dispositivi IoT sono stati individuati 6.635 dispositivi OT. Nel seguente grafico si mostra il numero di dispositivi IT e OT individuati, facenti parte degli 8.972.091.

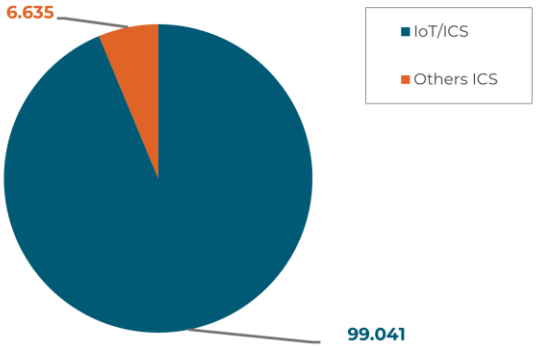


Figura 45 - Dispositivi IoT e OT individuati

Si ricorda che l'esposizione delle informazioni fornite da questi dispositivi potrebbero essere cruciali per la sicurezza del dispositivo stesso e in modo indiretto, per tutta l'infrastruttura IT che li ospita.

L'analisi è focalizzata sulle tecnologie ICS (Industrial Control System) che includono sistema di controllo per la supervisione e acquisizione dati (SCADA), sistemi di controllo distribuiti (DCS), sistemi di automazione industriale e controllo (IACS), controllori logici programmabili (PLC), controllori di automazione programmabili (PAC), unità terminali remote (RTU), server di controllo, dispositivi elettronici intelligenti (IED) e sensori.
L'analisi è focalizzata anche sui PLC (Programmable Logic Controller), ovvero computer specializzati nella gestione dei processi industriali. Nel 1Q2025 sono stati rilevati 1.345 dispositivi, in decremento rispetto ai 1.494 rilevati nel 4Q2024.
Tra i vari PLC analizzati rientrano quei dispositivi riconducibili ai sistemi ICS e che comunicano con protocollo TCP utilizzando la porta 102 (comunicazione con note vulnerabilità).

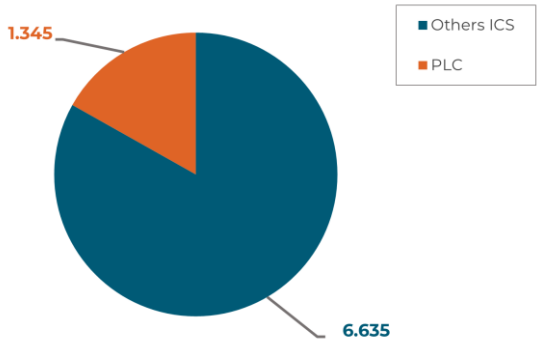


Figura 46 - ICS/PLC individuati 1Q2025

Questo è un dato che continua ad essere allarmante, poiché tali dispositivi risultano essere poco protetti: per molti di essi vengono mostrate informazioni come “riferimenti hardware” e “versione firmware” semplicemente interrogandoli. Esse sono informazioni molto utili nella prima fase di un attacco, ovvero quella della ricognizione, consentendo di ricercare vulnerabilità note o specifici exploit facilmente applicabili.

Con riferimento al grafico sottostante, si nota un decremento dei sistemi industriali rispetto al 4Q2024 di circa il 22% del numero di dispositivi connessi riconducibili alla categoria OT (insieme dei sistemi utilizzati tipicamente in ambito industriale per il monitoraggio e/o il controllo automatizzato degli impianti).

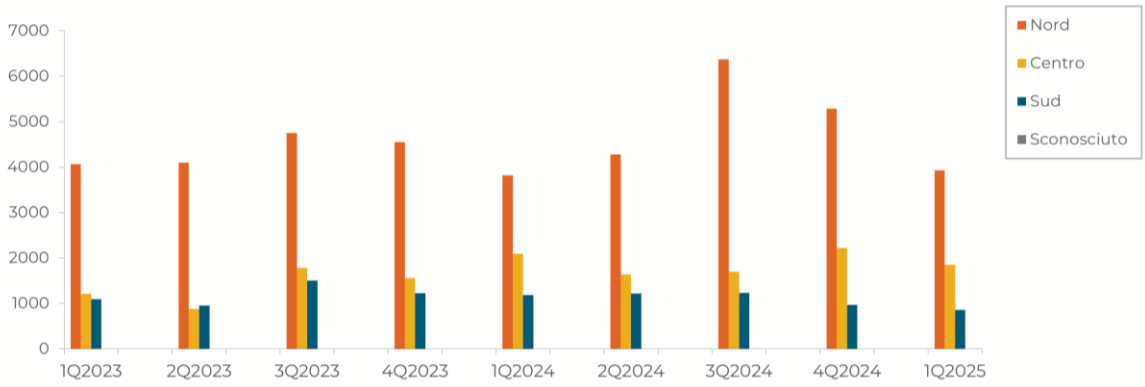


Figura 47 - Sistemi industriali 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

La distribuzione dei circa 9 milioni di dispositivi IoT rilevati nel nostro Paese mostra una relazione piuttosto stretta con i livelli di industrializzazione attribuibili alle differenti regioni. La Lombardia si conferma la regione con il più elevato numero di dispositivi IoT connessi, 24.753 i dispositivi individuati, seguita da Lazio (14.450), Campania (9.152) e Emilia Romagna (8.116). In fondo a questa particolare classifica la Valle D'Aosta con 33 dispositivi. Come si può notare, rispetto al trimestre precedente, il numero totale di dispositivi esposti è diminuito. Si è, infatti, passati da 118.827 dispositivi a 92.406 (un decremento di circa il 22%). Questo risultato deve essere accolto positivamente poiché si riflette in un decremento della facilità da parte di un attaccante nel riuscire ad accedere ai dispositivi esposti.

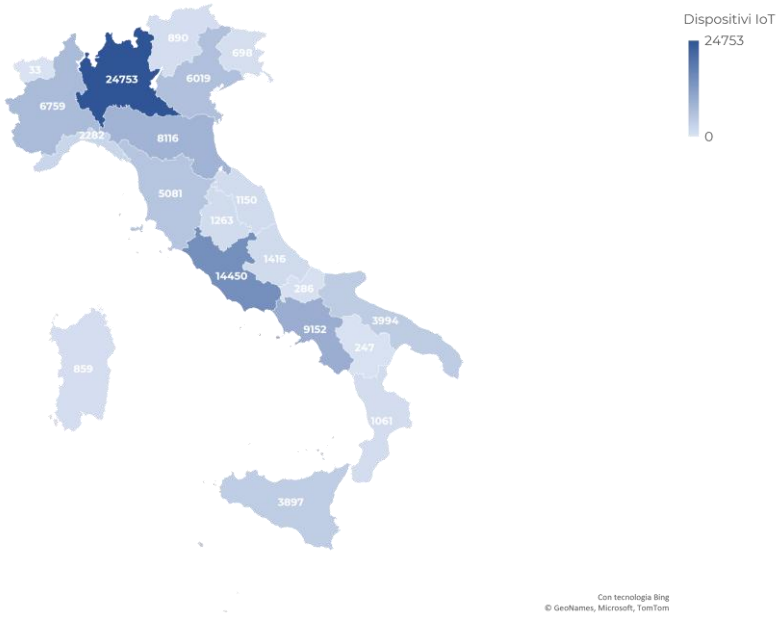


Figura 48 - Distribuzione dei dispositivi IoT nelle regioni italiane 1Q2025

Il grafico successivo rappresenta la distribuzione dei dispositivi IoT per milione di abitanti in ciascuna regione italiana. I dati evidenziano il rapporto tra il numero di dispositivi connessi e la popolazione residente, fornendo un'indicazione della densità tecnologica sul territorio. Un valore più alto indica una maggiore diffusione della tecnologia IoT rispetto agli abitanti, mentre valori più bassi suggeriscono una presenza minore.

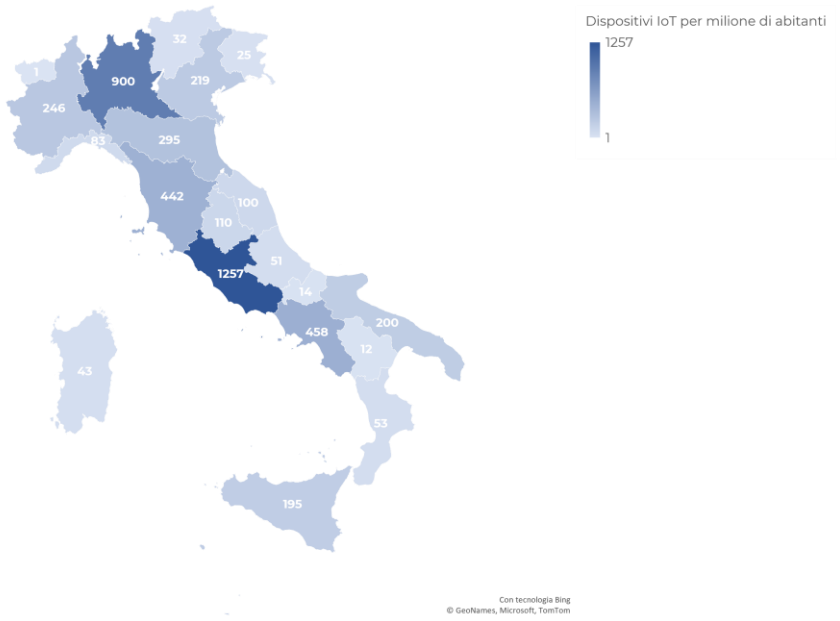


Figura 49 - Distribuzione dei dispositivi IoT per milione di abitanti nelle regioni italiane 1Q2025

Sono stati analizzati anche i dispositivi che utilizzano protocolli privi di autenticazione. In Italia ne sono stati rilevati 3.828 (un decremento di circa il 15% rispetto ai 4.512 rilevati nel 4Q2024) come si evince in Figura 50:

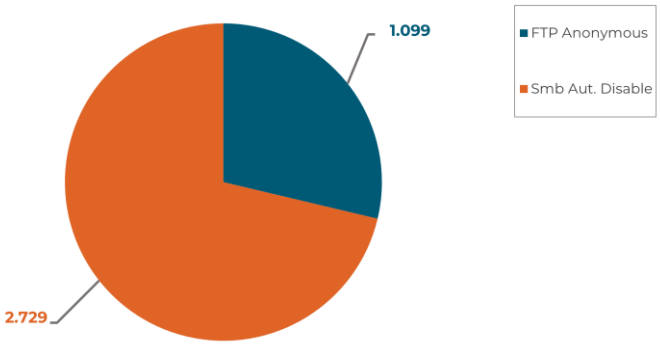


Figura 50 - Protocolli senza autenticazione 1Q2025

È opportuno far osservare che attraverso i dispositivi privi di protocolli di autenticazione è possibile accedere alla rete aziendale e ciò potrebbe essere utilizzata come backdoor indesiderata nella propria rete o comportare una perdita di dati sensibili che esporrebbe l'azienda al pagamento di sanzioni previste dal GDPR, oltre che provocare importanti danni di immagine.

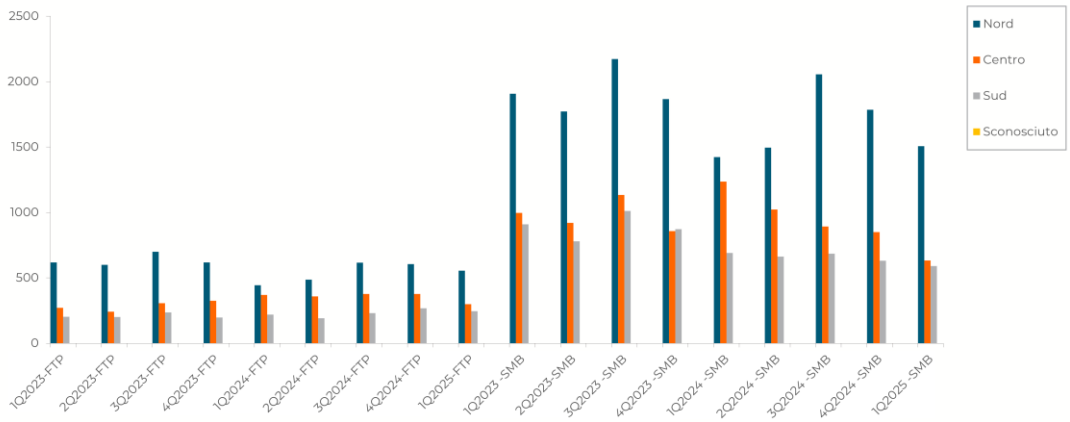


Figura 51 - Distribuzione protocolli senza autenticazione in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

Quanto ai grafici relativi alla distribuzione dei dispositivi IoT, si nota che tutti i numeri sono in decremento. Dai dati analizzati, infatti, risulta un decremento di 13.170 telecamere, 1500 router, 10 dispositivi medicali, 302 stampanti e 58 VoIP ed un incremento di 541 firewall per un totale di 14.499 dispositivi in meno. Secondo l'Osservatorio CyberSecurity di Exprivia, questo decremento dei dispositivi esposti rispetto al 4Q2024, è un bene in quanto riduce la superfice di attacco.
In questo primo trimestre del 2025 sono riportate le analisi effettuate sui sistemi VoIP. È possibile osservare una diminuzione del numero dei dispositivi rispetto al trimestre precedente, rilevando attualmente 192 dispositivi rispetto ai precedenti 250. Si nota, inoltre, come la presenza di questi dispositivi è particolarmente significativa al centro Italia rispetto al nord e sud Italia nonostante le oscillazioni osservate nei trimestri analizzati.

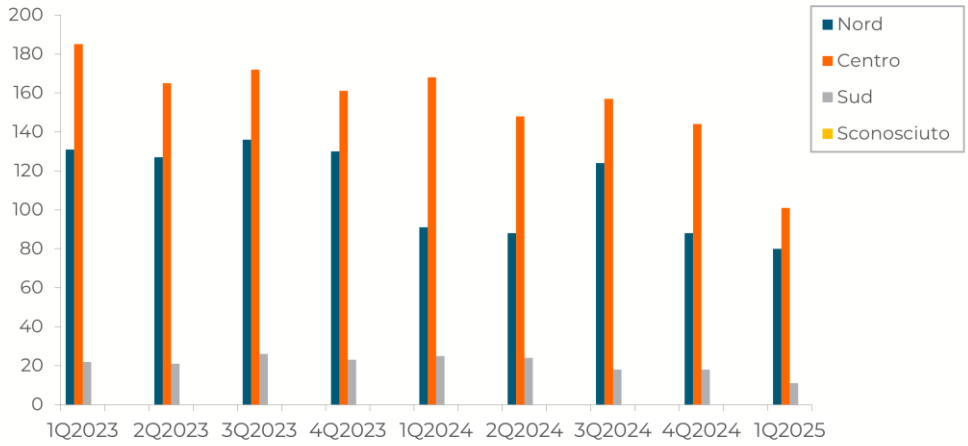


Figura 52 - Distribuzione dispositivi VoIP in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

La distribuzione delle telecamere mantiene sempre il primato nel nord Italia con un decremento rispetto al 4Q2024.

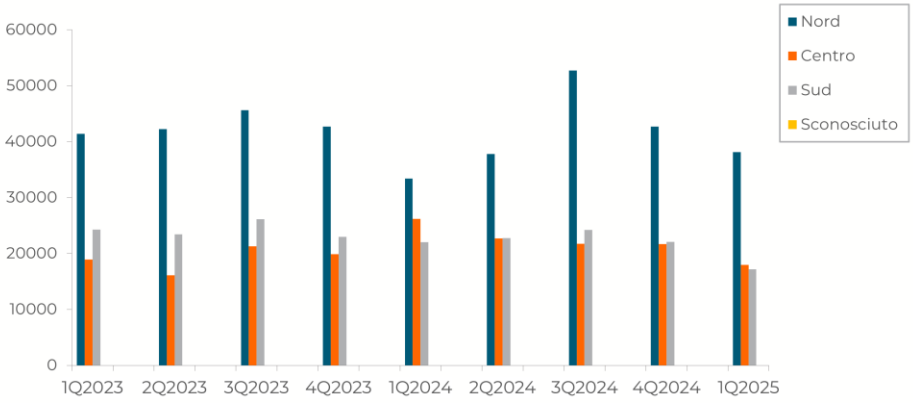


Figura 53 - Distribuzione telecamere in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

La distribuzione delle stampanti mantiene sempre il primato nel nord Italia con un decremento da 1.640 a 1.338 rispetto al 4Q2024.

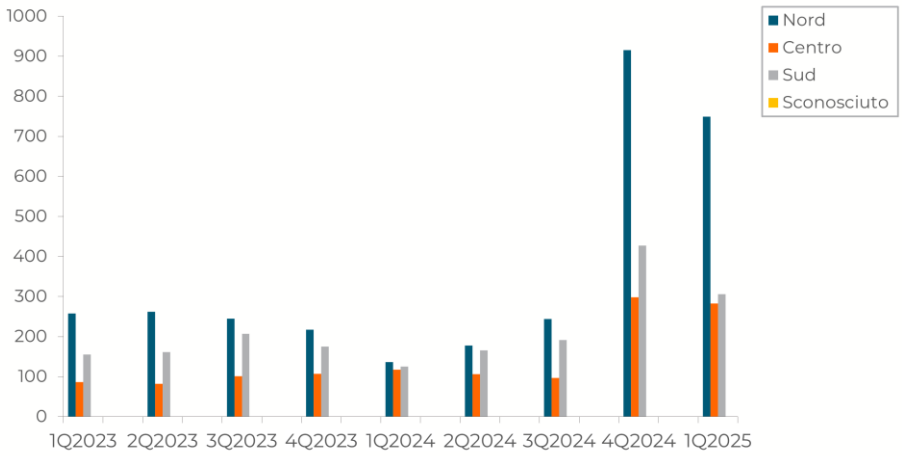


Figura 54 - Distribuzione stampanti in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

Per quanto riguarda i firewall si può notare che c'è stato un incremento dei dispositivi totali, in particolare nel nord Italia.

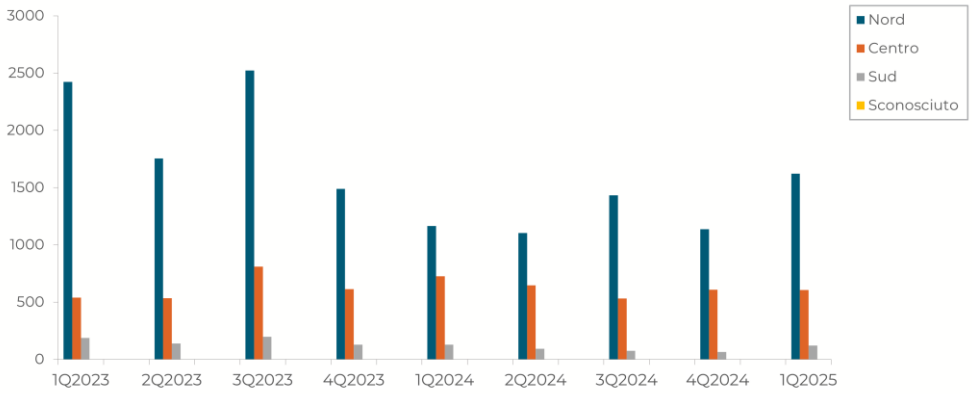


Figura 55 - Distribuzione firewall in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

Per quanto riguarda i router, si evidenzia una riduzione dei dispositivi individuati per un totale di 1500 dispositivi in meno rispetto al 4Q2024.

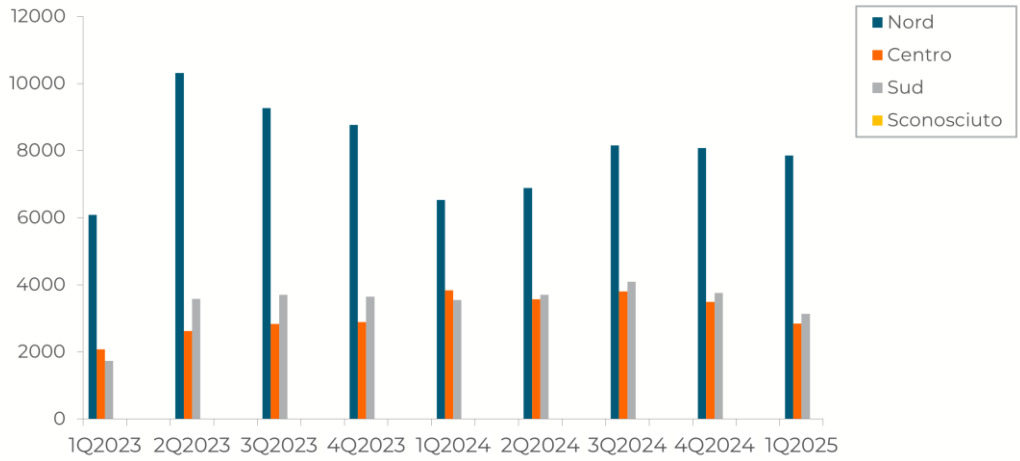


Figura 56 - Distribuzione router in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

In questo trimestre del 2025 sono riportate le analisi effettuate sui dispositivi medicali, iniziate nel 3Q2022. Come è possibile osservare dalla figura si nota un decremento di tali dispositivi che passa dai 1.409 rilevati nel 4Q2024 ai 1.399 nel 1Q2025. Si può notare, inoltre una maggiore presenza di questi dispositivi a nord Italia, seguiti da centro e sud.

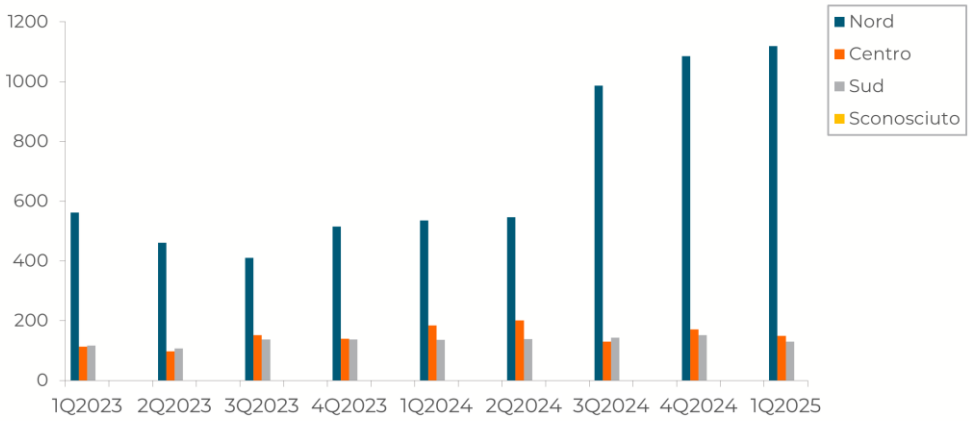


Figura 57 - Distribuzione dispositivi medicali in Italia per area geografica 1Q2023, 2Q2023, 3Q2023, 4Q2023, 1Q2024, 2Q2024, 3Q2024, 4Q2024 e 1Q2025

Stato della sicurezza dei dispositivi IoT 1Q2025

In questa rubrica si illustra l'evoluzione del livello di sicurezza dei dispositivi IoT osservati nel 1Q2025. Per valutare questo livello di sicurezza l'azienda Exprivia ha introdotto un nuovo indice di valutazione detto Unsecurity IoT Index (UII). Il valore calcolato mette in relazione il numero di dispositivi IoT vulnerabili con il numero di protocolli privi di autenticazione. Al fine di rendere i risultati più leggibili a partire da questo trimestre i valori ottenuti sono stati normalizzati in un intervallo compreso tra 1 e 10. In tabella 1 sono riportati i valori di tale indice ottenuti per il 1Q2025:

	1Q2025
N° Protocolli Vulnerabili	3.828
N° Protocolli Totali	108.138
N° dispositivi IoT vulnerabili	24.612
N° dispositivi IoT totali	84.200
Unsecurity_IoT_Index	5,656

Tabella 1 - Unsecurity IoT Index Totale

Il valore ottenuto è riportato graficamente in figura 58:

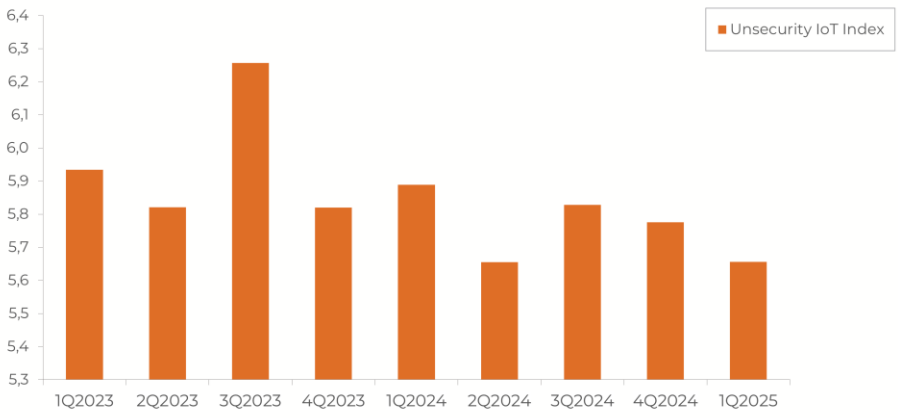


Figura 58 - Unsecurity IoT Index nel 1Q2025

Come si può osservare dalla figura 58 il valore dell'UII nel 1Q2025 è inferiore di circa il 2% a quello del 4Q2024. Ciò è dovuto ad un decremento sia del tasso di vulnerabilità dei protocolli sia del tasso di vulnerabilità dei dispositivi IoT.

È stato ritenuto opportuno mostrare l'incidenza dell'Unsecurity IoT Index nelle tre aree geografiche del nostro Paese, al fine di evidenziare l'area che presenta il maggiore rischio dovuto alla rilevazione di questi dispositivi.

I valori di questo indice per il 1Q2025 sono riportati in tabella 2:

	Nord	Centro	Sud	Sconosciuto	Totale
N°Protocolli Senza Autenticazione	2.061	931	836	0	3.828
N° Protocolli totali	57.141	33.469	17.528	0	108.138
N° dispositivi IoT vulnerabili	12.842	5.637	6.143	0	24.622
N° dispositivi IoT totali	44.757	20.635	18.808	0	84.200
Unsecurity_IoT_Index	5,6571	4,4195	8,0101	1,0000	5,6563

Tabella 2 - Unsecurity IoT Index per Area Geografica

I valori riportati in tabella 2 sono mostrati graficamente in figura 59:

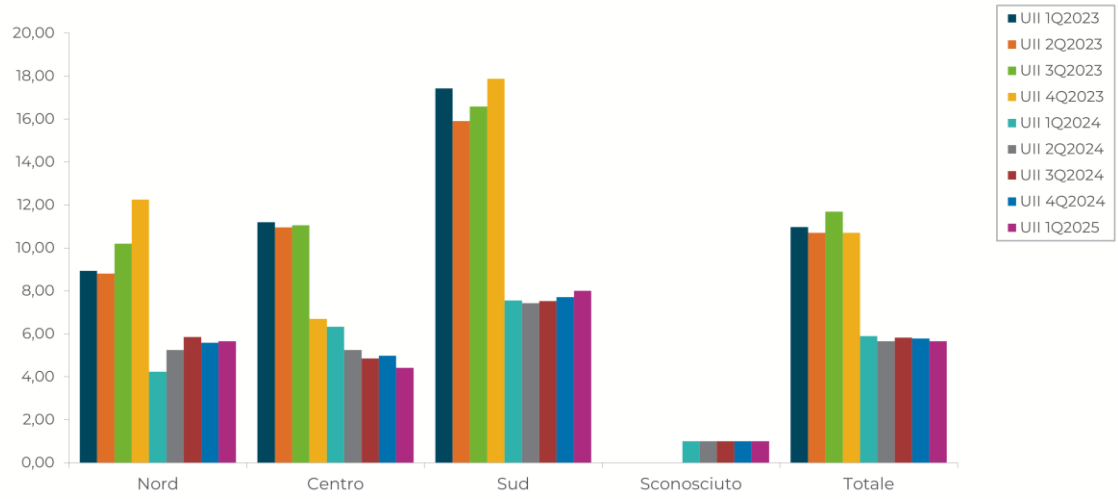


Figura 59 - Unsecurity IoT Index per Area Geografica

L'indice calcolato ci consente di stabilire il livello di rischio cyber per area geografica. Il valore calcolato per l'Unsecurity IoT Index delle varie aree geografiche, rapportato a quello totale, deve essere considerato come valore pesato in base sia al numero dei dispositivi osservati e protocolli totali utilizzati, sia all'insieme dei sistemi che presentano vulnerabilità di protocollo e di autenticazione.
Se il valore dell'indice per area geografica è inferiore al valore dell'indice totale italiano il rischio è minimo, come accade per il centro. Al contrario, se tale valore supera l'indice totale, il rischio di esposizione ad attacchi cyber per i dispositivi IoT in questa area geografica è alto, come accade, ad esempio al sud. Per quanto riguarda il nord, il rischio di esposizione è medio in quanto il valore dell'indice è circa pari a quello totale.
È evidente come il decremento del valore dell'UII nazionale si riflette anche sulle varie aree geografiche italiane.
A questo punto dello studio sono stati valutati quali dispositivi analizzati presentavano il maggior rischio procedendo con il calcolo dell'UII per ogni dispositivo IoT considerato. A partire dal 3Q2022 sono stati aggiunti all'analisi anche i dispositivi medicali.

I risultati ottenuti sono di seguito riportati in tabella:

	Stampanti	Telecamere	VoIP	ICS	PLC	Dispositivi medicali	Totale
1Q2025	1,6585	5,9784	1,0819	3,5254	2,9184	2,5182	5,6563

Tabella 3 - Unsecurity IoT Index per Dispositivo

I valori riportati in tabella sono mostrati graficamente in Figura 60:

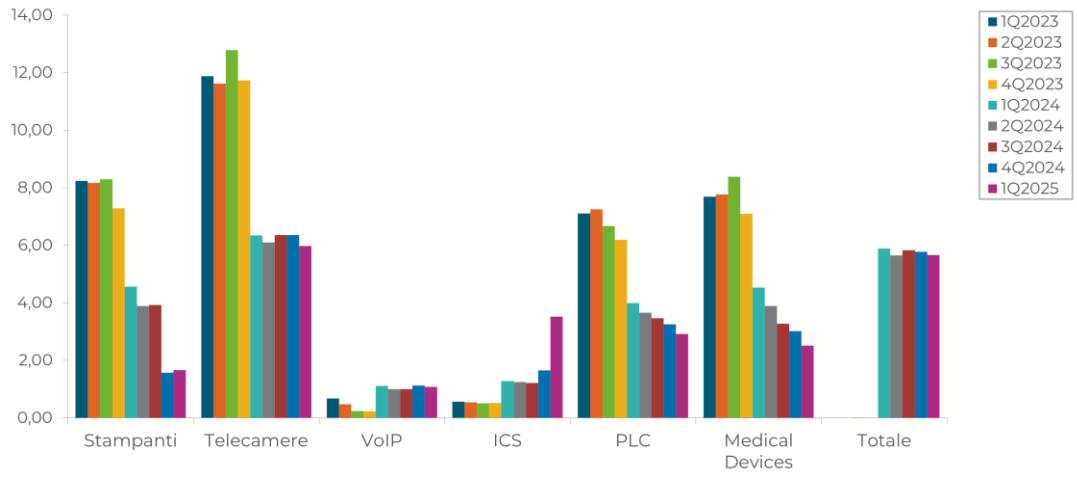


Figura 60 - Unsecurity IoT Index per dispositivo

Dall'analisi si evince che i dispositivi a maggior rischio sono le telecamere. Questo è evidente se si considera che 23.191 telecamere su un totale di 73.291 sono vulnerabili (circa il 32%).
Per quanto riguarda i dispositivi medicali, i PLC e gli ICS, si ha che solo il 10%, il 12% e il 16% dei dispositivi è vulnerabile, pertanto questi presentano un basso rischio.
Una considerazione analoga può essere fatta per i dispositivi VoIP e le stampanti che presentano un rischio molto basso poiché si ha che solo lo 0,5% e il 4% dei dispositivi risulta essere vulnerabile.
Oltre all'analisi dei grafici ricavati dal calcolo dell'indice UII, viene introdotto un nuovo valore adimensionale detto IoT Vulnerability Entropy Index (IVEI), dato dal rapporto tra il numero di vulnerabilità dei dispositivi IoT ed il numero totale delle vulnerabilità. I risultati ottenuti sono riportati in tabella 4:

Data	IoT_Vulnerability_Entropy_Index (IVEI)
01/09/2020	0,00096
01/12/2020	0,02032
01/03/2021	0,00045
01/06/2021	0,01898
01/09/2021	0,00108
01/12/2021	0,00173
01/03/2022	0,00050
01/06/2022	0,00042
01/09/2022	0,00084
01/12/2022	0,00064
01/03/2023	0,00106
01/06/2023	0,00397
01/09/2023	0,00000
01/12/2023	0,00153
01/03/2024	0,00254
01/06/2024	0,00042
01/09/2024	0,00086
01/12/2024	0,00076
01/03/2025	0,00117

Tabella 4 - IoT Vulnerability Entropy Index

I risultati ottenuti vengono mostrati graficamente in figura 61:

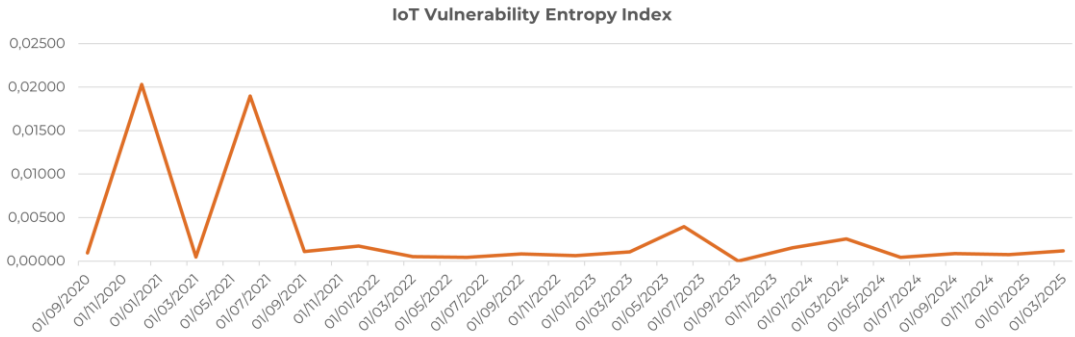


Figura 61 - IoT Vulnerability Entropy Index

Dall'analisi delle vulnerabilità correlate a tali dispositivi sono emerse delle criticità che hanno fatto registrare un picco dell'indice nei periodi compresi tra settembre e dicembre 2020 e tra marzo e giugno 2021, dovuti principalmente alla scoperta di vulnerabilità di uno specifico componente hardware utilizzato su numerosi dispositivi IoT.
Si è potuto osservare che delle 1064 vulnerabilità IoT rilevate nel periodo preso in esame, 901 erano dovute a potenziali rischi nell'utilizzo di tali componenti in ambito mobile su dispositivi quali smartphone, tablet e smartbook, con un'incidenza di circa l'85%. A partire da giugno 2021 il numero di vulnerabilità correlate a tali componenti è tendenzialmente diminuito, pertanto, da questa data in poi, è stato possibile notare come l'IVEI tenda a diminuire fino a raggiungere un andamento quasi costante a partire da settembre 2021.

Rispetto al trimestre precedente sono state registrate 15 nuove vulnerabilità nel settore IoT.

Stato della sicurezza dei settori economici italiani 1Q2025

In questo approfondimento si osserva l''evoluzione del livello di sicurezza dei settori economici italiani in riferimento al 1Q2025.
Per valutare tale livello di sicurezza Exprivia ha introdotto un nuovo indice di valutazione detto "Investment Index (II)" che mette in correlazione l'impatto di ogni vulnerabilità rilevata da Exprivia e il numero di occorrenze di queste ultime, per ognuna delle aziende monitorate.
A partire dal 2Q2024 ed al fine di rendere i risultati maggiormente leggibili è stata modificata la formula per il calcolo di tale indice normalizzando i valori in un intervallo compreso tra 1 e 100 anziché tra 1 e 10.
Il valore 1 rappresenta un livello di sicurezza molto alto, indicando che l'azienda analizzata ha una bassa esposizione al rischio cyber mentre il valore 100 rappresenta uno scarso livello di sicurezza con conseguente maggiore esposizione al rischio di subire attacchi informatici.
Nell'analisi sono state prese in considerazione le cinque aziende leader dei seguenti settori economici:

- Automotive
- Consulting
- Critical Infrastructure
- Educational
- Entertainment
- Finance
- Healthcare
- Hospitality
- Industrial
- ONG
- Public Administration
- Religion
- Retail
- Security
- Software
- Telco

Per ognuna delle cinque aziende di ogni settore economico sono state valutate tutte le vulnerabilità, è stata applicata la formula vista precedentemente e successivamente è stata fatta una media per calcolare l'II del settore economico analizzato.
In tabella 5 vengono riportati i risultati ottenuti comparati con quelli dei trimestri dell'anno 2024:

	Investment Index 1Q2024	Investment Index 2Q2024	Investment Index 3Q2024	Investment Index 4Q2024	Investment Index 1Q2025
Automotive	50,7205	51,1306	50,4044	48,8396	49,0025
Consulting	69,2408	71,0796	71,7234	71,0439	70,6478
Critical Infrastructure	71,3480	71,4649	70,0455	70,4983	70,6693
Education	68,8977	68,9094	68,7454	68,9326	68,4551
Entertainment	63,7691	71,7331	72,0035	72,6909	73,5832
Finance	58,5568	58,3345	57,5737	53,4576	58,3858
Healthcare	44,3464	44,3096	43,6522	44,1803	43,0286
Hospitality	37,5986	37,4692	34,3503	39,4052	37,3689
Industrial	36,1804	37,2518	32,5160	36,3603	35,8714
ONG	50,3806	50,0394	46,7690	47,0209	46,6406
PA	51,0306	51,3922	51,3730	51,8432	52,0261
Religion	30,0367	31,5885	28,7142	30,2780	28,7595
Retail	55,3325	62,8453	62,7901	55,6423	63,3095
Security	37,3622	36,3925	37,4614	37,0807	34,6876
Software	37,4993	38,8307	38,5753	39,5617	39,3890
Telco	67,1287	66,8961	66,2506	66,4051	66,8286

Tabella 5 - Investment Index media di ogni settore economico analizzato nel 1Q2025

I risultati ottenuti vengono mostrati graficamente in figura 62:

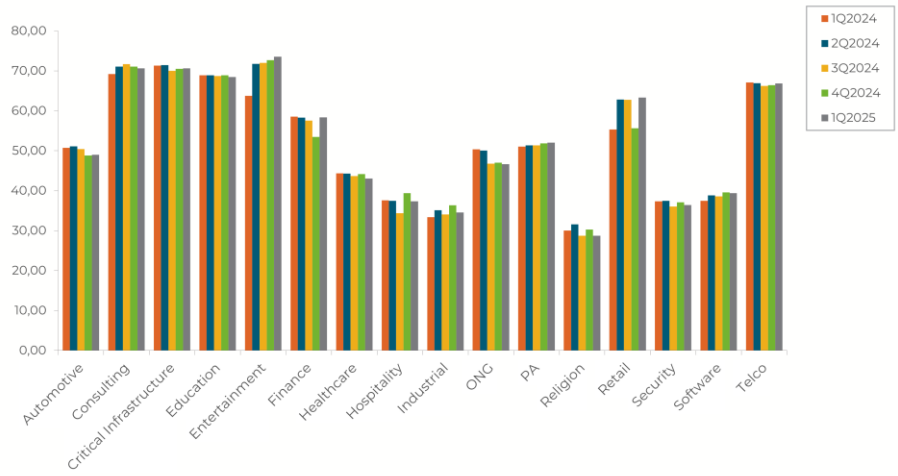


Figura 62 - Rappresentazione grafica dell'Investment Index media per ogni settore economico analizzato

Dalla figura precedente risulta che il settore avente il minor numero di vulnerabilità, ovvero la minor esposizione al rischio, è il settore Religion con il valore di II più basso (pari a 28,7595).
Il settore con il più alto numero di vulnerabilità, ovvero la più alta esposizione al rischio, è il settore dell'Entertainment presentando un II pari a 73,5832 (in incremento rispetto a quello del 4Q2024 in cui era stato rilevato un II pari a 72,6909).
Rispetto al trimestre passato è evidenziabile un impercettibile miglioramento nell'efficienza degli investimenti in tutti i settori economici analizzati ed in particolare nei settori Hospitality, Industrial e Religion, ed un lieve peggioramento per quanto riguarda Finance e Retail.
A questo punto dell'analisi si vuole valutare in quale area geografica si abbia il miglior livello di sicurezza possibile.
I valori per nord, centro e sud Italia sono riportati in tabella 6 comparati con i trimestri del 2024:

	Investment Index 1Q2024	Investment Index 2Q2024	Investment Index 3Q2024	Investment Index 4Q2024	Investment Index 1Q2025
Nord	54,9675	56,6872	55,9078	55,8414	56,6714
Centro	52,0711	52,7345	51,3539	52,6122	52,2816
Sud	42,7654	42,8249	42,2960	42,4894	39,5138

Tabella 6 - Investment Index per Area Geografica

I risultati mostrati in tabella vengono mostrati graficamente in figura 63:

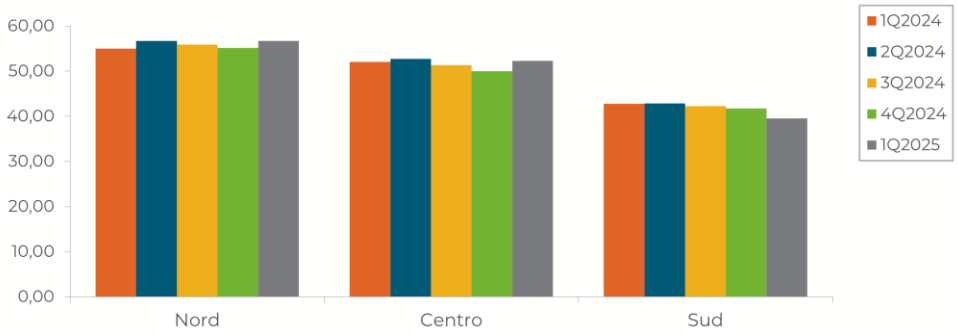


Figura 63 - Investment Index per Area Geografica

Dalla figura si evince come, rispetto al trimestre precedente, ci sia stato un lieve peggioramento dell'efficienza degli investimenti in tutte le aree geografiche, ad eccezione del sud Italia.

Il nuovo indice (Investment Index) appena introdotto, mostra quanto siano efficaci gli investimenti aziendali in ambito cybersecurity, fortemente influenzato dalla velocità con cui le aziende affrontano il progresso tecnologico senza un adeguato supporto alla protezione delle nuove soluzioni introdotte.

Previsioni Cybersecurity 2025

Domenico Raguseo – Head of Cybersecurity di Exprivia

Nel 2024, il panorama della cybersecurity è stato segnato da eventi significativi che hanno evidenziato l'importanza di proteggere le infrastrutture critiche e i dispositivi connessi. Tra questi, spiccano attacchi sofisticati che hanno sfruttato vulnerabilità nei sistemi industriali e nei dispositivi IoT, dimostrando ancora una volta quanto sia cruciale la sicurezza informatica.
Nulla di quanto accaduto non era prevedibile. Nel 2010 infatti Stuxnet ha mostrato come un attacco informatico possa colpire infrastrutture critiche, utilizzando chiavette USB e vulnerabilità sconosciute per sabotare sistemi SCADA. Ha evidenziato l'importanza della cybersecurity nella vita quotidiana, non solo nei data center. Nel 2016 invece. Mirai ha sfruttato credenziali deboli nei dispositivi IoT per creare una botnet capace di lanciare attacchi DDoS su larga scala. Ha cambiato il modo di valutare il ritorno di investimento sulle contromisure di sicurezza, dimostrando che anche dispositivi insignificanti possono essere pericolosi.
Entrambi i casi sottolineano la necessità di investire nella sicurezza informatica come valore intrinseco, indipendentemente dal ritorno di investimento immediato, e di implementare normative come la NIS2 per proteggere l'ecosistema digitale.
Nel 2025 pertanto prevediamo investimenti su contromisure che da un lato possono garantire la conformità alle normative recenti, dall'altro e contemporaneamente riducono il rischio a minacce concrete che hanno un impatto sempre maggiore.

Monitoraggio continuo della sicurezza della infrastruttura

Utilizzo di tecniche come il ransomware-as-a-service, gli attacchi supply chain, e gli attacchi zero-day, utilizzo di strumenti automatizzati e basati su intelligenza artificiale per identificare vulnerabilità con velocità e precisione, fanno sì che nel 2025 ci sarà una crescente attenzione nel controllare la suscettibilità delle infrastrutture a subire attacchi. Fare infatti vulnerability assessment e penetration test solo qualche volta in un anno per identificare vulnerabilità da potere sfruttare non è più sufficiente in quanto la migrazione al cloud ha reso necessaria la protezione di infrastrutture ibride e complesse, l'uso di dispositivi personali e connessioni non protette introduce nuove vulnerabilità continuamente, dispositivi intelligenti (IoT) sono sempre più pervasivi rappresentando un potenziale punto di ingresso per gli attaccanti. Se da un lato il tempo necessario agli attaccanti per sfruttare una vulnerabilità appena scoperta si è drasticamente ridotto, spesso a pochi giorni o addirittura ore e questo richiede una risposta rapida e continua per prevenire danni, dall'altro la sicurezza di una singola organizzazione dipende spesso dalla sicurezza delle aziende partner (es. fornitori, appaltatori). Gli attacchi alla supply chain sono diventati un vettore di minaccia sempre più comune. Non sarà pertanto una sorpresa che normative come GDPR, NIS2, CCPA e altre impongono requisiti di sicurezza più stringenti e richiedono controlli continui per evitare sanzioni.

Caratteristiche delle soluzioni da adottare:

1. Monitoraggio continuo delle vulnerabilità all'interno delle infrastrutture IT e cloud, utilizzando tecniche di simulazione di attacchi e di analisi del percorso degli attaccanti.
2. Identificazione delle potenziali catene di attacco sfruttabili all'interno dell'infrastruttura, dai punti di ingresso fino agli asset critici
3. Fornire una lista prioritaria di azioni di mitigazione, indicando le misure che avranno il maggior impatto sulla riduzione del rischio.
4. Valutazione della sicurezza delle terze parti e nel monitoraggio della postura di sicurezza di un'organizzazione.
5. Fornire un'analisi continua del rischio, con particolare attenzione alla superficie di attacco esposta (ad esempio, configurazioni errate, certificati scaduti, e-mail vulnerabili).

6. Generare report con suggerimenti prioritari per la mitigazione, supportando il miglioramento della postura di sicurezza.
7. Valutazione della sicurezza sia interna che di terze parti attraverso il monitoraggio di metriche di rischio, assegnando un punteggio alla postura di sicurezza.

Monitoring degli eventi di sicurezza

Identificare le vulnerabilità non è però sufficiente a garantire la sicurezza di una infrastruttura. Gli attaccanti potrebbero indentificare delle vulnerabilità non conosciute (zero day) utilizzando strumenti di AI o semplicemente non sempre è possibile risolvere le vulnerabilità tempestivamente. Quando questo accade Monitorare tutti gli eventi, sia interni che esterni, di un'organizzazione è cruciale per garantire la sicurezza informatica e proteggere i sistemi critici. Il monitoraggio continuo consente di rilevare tempestivamente attività sospette come accessi non autorizzati o intrusioni, individuare attacchi in corso riduce il tempo di permanenza degli attaccanti all'interno dei sistemi, limitando i danni, proattivamente consentire di migliorare la configurazione della infrastruttura per garantire migliore resilienza operativa. Il monitoraggio continuo è richiesto anche da normative come GDPR, ISO 27001 o NIS2. Il mercato offre soluzioni che si adattano sia in termini di spending che caratteristiche tecnologiche ed architetturali alla domanda.

Caratteristiche delle soluzioni da adottare:

1. Raccogliere, normalizzare, analizzare e correlare i log e gli eventi di sicurezza da un'ampia gamma di fonti (dispositivi di rete, server, applicazioni, endpoint, ecc.).
2. Integrare nativamente diverse fonti di sicurezza (endpoint, rete, cloud, e-mail, ecc.) per rilevare e rispondere a minacce in modo più efficace per rilevare e rispondere rapidamente a minacce che colpiscono endpoint, reti o ambienti cloud.
3. Utilizzo di intelligenza artificiale e il machine learning per rilevare comportamenti anomali senza dover configurare regole manualmente.

Formazione

In Italia la tecnica di attacco più utilizzata è il phishing e la maggiore vulnerabilità sfruttata è la mancanza di consapevolezza. Sensibilizzare il personale sulle tematiche di cybersecurity creando consapevolezza su come reagire di fronte ad un cyber attacco aumentando la resilienza di tutti i dipendenti resta una delle contromisure più efficaci.
Non si tratta però di fornire solo soluzioni a supporto o costringere la popolazione aziendale a partecipare a corsi di formazion. È necessario far comprendere ai dipendenti il rischio associato a minacce relative agli attacchi trovando soluzioni che avvicinino la popolazione alla tematica. In altre parole migliorare il livello di engagement.

Caratteristiche delle soluzioni/approcci da adottare:

1. Offrire contenuti formativi brevi e mirati (spesso sotto i 10 minuti) per massimizzare l'attenzione e l'efficacia dell'apprendimento.
2. Fare contenuti su un tema specifico (ad esempio phishing, l'ingegneria sociale o la gestione delle password)
3. Fare in modo che le lezioni siano disponibili su più dispositivi, consentendo agli utenti di apprendere in modo flessibile.
4. Verificare l'apprendimento tramite d simulazioni di phishing nelle sue forme più svariate (quishing, chiavette USB..)
5. Personalizzare gli scenari verifica per riflettere minacce specifiche o realistiche per l'organizzazione.
6. Fornire report dettagliati sul comportamento degli utenti, identificando chi ha cliccato su link sospetti o ha condiviso credenziali.
7. Utilizzare giochi per incentivare l'apprendimento, come quiz, punteggi e classifiche.

8. Inventarsi aree dove i dipendenti possono competere in modo sano, rendendo la formazione più divertente e memorabile.
9. Evitare di far fare la stessa formazione a tutti. Gli utenti che mostrano comportamenti ad alto rischio, come cadere nelle simulazioni di phishing, devono ricevere formazione mirata per migliorare le loro competenze.
10. La formazione deve essere adattiva e cambiare in base ai risultati dei test e ai progressi degli utenti.
11. Avere contenuti aggiornati e contestualizzati
12. Creare campagne di sensibilizzazione personalizzate, come e-mail educative, poster digitali (oppure modifica sito intranet aggiungendo avatar o chatbot a supporto).
13. Riconoscere i comportamenti sicuri. La formazione non si limita a insegnare cosa fare, ma si concentra anche sullo sviluppo di abitudini sicure per riconoscere e reagire alle minacce.
14. Integrare le piattaforme con presentazioni da speaker riconosciuti dal mercato.
15. Integrare la piattaforma con programmi di certificazione formali.

Difendersi contro attacchi di tipo DDoS

Negli ultimi anni, gli attacchi DDoS (Distributed Denial of Service) si sono evoluti in frequenza, complessità e impatto. Le aziende si trovano ad affrontare minacce sempre più sofisticate, spesso multi-vettore e capaci di colpire con precisione millimetrica le vulnerabilità dell'infrastruttura IT. Non si tratta più soltanto di rendere irraggiungibile un sito web: oggi, un attacco DDoS può compromettere la disponibilità di servizi essenziali, interrompere operazioni critiche, danneggiare la reputazione aziendale e generare perdite economiche consistenti.

A rendere il contesto ancora più critico è la difficoltà di rilevare tempestivamente questi attacchi, specialmente quelli meno evidenti come i "carpet bombing", che distribuiscono il traffico malevolo su molteplici IP e segmenti della rete per sfuggire ai controlli tradizionali. Le soluzioni basate su soglie statiche, firme predefinite o analisi manuali non sono più sufficienti per garantire una protezione efficace e reattiva.

In questo scenario, diventa sempre più rilevante aumentare la velocità di elaborazione dei dati e consolidare il rilevamento degli attacchi in un'unica piattaforma intelligente e automatizzata. L'adozione di tecniche avanzate, come l'identificazione della vittima e la profilazione del traffico in tempo reale, consente di contrastare con maggiore precisione attacchi volumetrici e a tappeto. Questo approccio si basa sull'analisi di indicatori comportamentali per apprendere dinamicamente i pattern di traffico legittimo, ridurre i falsi negativi e accelerare i tempi di rilevamento e risposta.

Un ulteriore aspetto sempre più richiesto dal mercato è la capacità delle soluzioni di adattarsi in tempo reale, sfruttando baseline dinamiche e soglie flessibili che evolvono in base al contesto operativo. Questa capacità di adattamento è fondamentale per affrontare minacce zero-day o campagne DDoS particolarmente sofisticate, senza dover ricorrere continuamente all'intervento umano.

In questo contesto così complesso, le aziende cercano soluzioni che offrano protezione continua, automazione, visibilità e prestazioni elevate, elementi chiave per garantire la resilienza dell'infrastruttura digitale.

Security Orchestration, Automation, and Response (SOAR)

Rispondere efficacemente agli incidenti è sempre maggiormente rilevante con informazioni accurate e con la migliore efficienza possibile, non sorprende pertanto che si stiano affermando sempre di più nel mondo della cybersecurity soluzioni SOAR che consentono di gestire in modo più efficiente le minacce, automatizzare le operazioni di sicurezza e rispondere agli incidenti in maniera rapida e coordinata. L'obiettivo principale è

quello di ridurre al minimo l'intervento umano, lasciando che sia la piattaforma a rilevare, analizzare e intervenire automaticamente sugli eventi di sicurezza.

Tra le funzionalità maggiormente richieste troviamo la capacità di identificare e dare priorità alle minacce più rilevanti, valutare il loro potenziale impatto e intervenire in modo mirato.

Nella Sicurezza Informatica, Mitigare il Rischio Umano Richiede Più della Semplice Formazione

Giulia Dragone - Channel Account Manager Italy and Iberia – Mimecast

Con l'aumento costante delle minacce informatiche, le organizzazioni stanno destinando sempre più risorse a nuovi servizi e tecnologie all'avanguardia per fronteggiare gli attacchi. Tuttavia, molte continuano a seguire un approccio uniforme e generico per proteggere il vettore di rischio più critico: l'elemento umano.
Nonostante i progressi, l'elemento umano resta uno dei principali fattori di vulnerabilità in ambito cybersecurity. La pratica comune di imporre corsi generici sulla consapevolezza della sicurezza non ha portato ai miglioramenti sperati, visto che furti di credenziali, perdite di dati e attacchi di phishing sono ancora all'ordine del giorno. Per affrontare questa vulnerabilità cruciale, i CISO devono adottare strategie più mirate e basate sui dati, andando oltre la formazione tradizionale. È necessario sviluppare soluzioni di sicurezza informatica pensate e progettate con l'essere umano al centro.

Quantificare il Rischio

La formazione sulla consapevolezza della sicurezza è utile, ma non risolve completamente il problema, poiché adotta un approccio uniforme per tutti i dipendenti. In realtà, alcuni utenti sono particolarmente abili nel riconoscere le minacce, mentre altri necessitano di un supporto maggiore. Inoltre, alcuni gruppi di dipendenti sono regolarmente presi di mira, mentre altri ricevono pochissimi tentativi di phishing. Pertanto, un approccio alla sicurezza centrato sull'essere umano deve partire da una comprensione approfondita della distribuzione del rischio all'interno dell'organizzazione.
Il primo passo consiste nell'individuare le persone più vulnerabili. Gli studi hanno dimostrato che solo l'8% dei dipendenti è responsabile dell'80% degli incidenti di sicurezza, e molti di questi sono recidivi. Alcuni dipendenti sono anche presi di mira più frequentemente a causa del loro ruolo: i manager ricevono in media 2,5 volte più email di phishing rispetto ai non-manager, e il numero di tentativi aumenta per tutti i dipendenti man mano che rimangono nell'azienda, raddoppiando quasi ogni tre anni.
Questi dati possono variare significativamente tra le diverse organizzazioni, per cui è essenziale che le aziende conducano un'analisi approfondita. Ciò può essere fatto esaminando dati spesso ignorati, come i log generati dai sistemi di sicurezza quando bloccano il malware, e raccogliendo modelli comportamentali. In un approccio ideale, gli amministratori della sicurezza dovrebbero poter raccogliere dati da tutti gli strumenti di protezione, per valutare costantemente quali decisioni di sicurezza sono sicure o rischiose per ciascun utente, costruendo così un profilo di rischio personalizzato per ogni individuo.

Gestire il Rischio

Proprio come le compagnie di assicurazione utilizzano i premi per personalizzare le polizze, anche le organizzazioni possono adottare i punteggi di rischio per creare un approccio alla sicurezza personalizzato e adattivo, iniziando con una formazione su misura.
Invece di far completare a tutti i dipendenti gli stessi moduli generici di consapevolezza della sicurezza (che, ammettiamolo, molti finiranno per completare rapidamente senza prestare molta attenzione), le persone a basso rischio potrebbero ricevere promemoria leggeri delle politiche aziendali e delle liste di controllo. Al contrario, coloro che sono frequentemente presi di mira, o che potrebbero esserlo, potrebbero essere obbligati a seguire una formazione più approfondita, mirata ai rischi specifici che affrontano.
Con una conoscenza dettagliata dei modelli comportamentali, le organizzazioni possono anche premiare le buone pratiche di sicurezza attraverso riconoscimenti. Inoltre, possono adottare misure per correggere comportamenti scorretti, come suggerimenti adattivi—messaggi personalizzati inviati al momento e nel contesto giusto per evitare che gli utenti diventino vittime di attacchi—oppure strategie come un filtraggio più rigoroso delle email, restrizioni più severe sulla navigazione web o la riduzione del periodo di validità dei token di autenticazione a più fattori sui dispositivi degli utenti a rischio.

È fondamentale che queste pratiche siano implementate con trasparenza, affinché i dipendenti siano consapevoli di come il team di sicurezza intenda utilizzare i dati raccolti. Quando i team di sicurezza adottano un approccio costruttivo—ad esempio inviando report che evidenziano i comportamenti positivi e suggeriscono aree di miglioramento—i dipendenti rispondono generalmente con apertura e apprezzamento. Per la piccola percentuale di utenti nel gruppo ad alto rischio, è necessario un maggiore impegno nel spiegare come la formazione aggiuntiva e le misure adattive siano pensate per aiutarli a migliorare.

Monitorare i Miglioramenti

Raccogliere e analizzare gli eventi di sicurezza consente agli amministratori di adottare un approccio più basato sui dati per misurare i risultati e, idealmente, i miglioramenti. Misurando la baseline iniziale, i team di sicurezza possono monitorare nel tempo l'evoluzione dei comportamenti rischiosi nella rete e affinare le migliori metodologie per "rafforzare" i sottoinsiemi di utenti, riducendo così il numero di incidenti futuri.
Questa misurabilità si distingue nettamente dalle pratiche tradizionali di mitigazione del rischio umano (come la formazione generica sulla consapevolezza della sicurezza), che spesso risultano in un "buco nero" per quanto riguarda la comprensione dell'impatto e, di conseguenza, del ROI. Adottando un approccio oggettivo e orientato ai risultati, i CISO possono non solo migliorare la sicurezza, ma anche dimostrare in modo chiaro il successo dell'investimento alla direzione aziendale.
Con l'intelligenza sempre maggiore degli attori delle minacce nel mirare agli utenti, è responsabilità delle organizzazioni e dei loro partner di sicurezza informatica costruire una difesa solida—dove l'elemento umano gioca un ruolo fondamentale. Le aziende che adotteranno un approccio più mirato e personalizzato per ridurre i comportamenti rischiosi avranno le migliori probabilità di proteggere le loro infrastrutture dagli attacchi informatici, ottimizzando allo stesso tempo l'uso del budget per la sicurezza.

L'Intelligenza Artificiale (AI) nella Sicurezza Informatica: Rischi e Opportunità

Armando Crisafo - Advisory Solution Consultant, Security Operations ServiceNow

L'uso dell'Intelligenza Artificiale (AI) nella sicurezza informatica sta diventando sempre più diffuso, grazie alla sua capacità di analizzare grandi volumi di dati e individuare minacce in tempo reale. Tuttavia, l'impiego dell'AI in questo settore presenta anche alcuni rischi e limitazioni. Se da un lato offre strumenti avanzati per la prevenzione e la gestione degli attacchi cyber, dall'altro rappresenta una minaccia concreta, fornendo agli hacker nuovi mezzi per sviluppare attacchi sempre più sofisticati. Questo dualismo rende l'AI una vera e propria "croce e delizia" della cybersecurity. In questo articolo, analizzeremo le principali contromisure per affrontare gli attacchi cyber, focalizzandoci però sui motivi per cui l'AI rappresenta un'opportunità per la cybersecurity e le ragioni per cui il suo utilizzo va comunque ponderato e analizzato accuratamente.

L'aumento degli attacchi cyber nel settore bancario: minacce e strategie di difesa

Negli ultimi anni, il settore finanziario, subito dopo il settore Software/Hardware, è diventato uno dei bersagli principali dei cybercriminali, come si può vedere dalla figura 1, in base alle analisi condotte dall'Osservatorio Cybersecurity di Exprivia, nel corso del primo trimestre del 2025. Le banche e le istituzioni finanziarie gestiscono enormi quantità di dati sensibili e transazioni di alto valore, rendendole obiettivi privilegiati per attacchi informatici sempre più sofisticati. Tra le principali minacce emergenti troviamo il furto di dati, attacchi ransomware, phishing mirati e l'uso dell'intelligenza artificiale per compromettere la sicurezza.

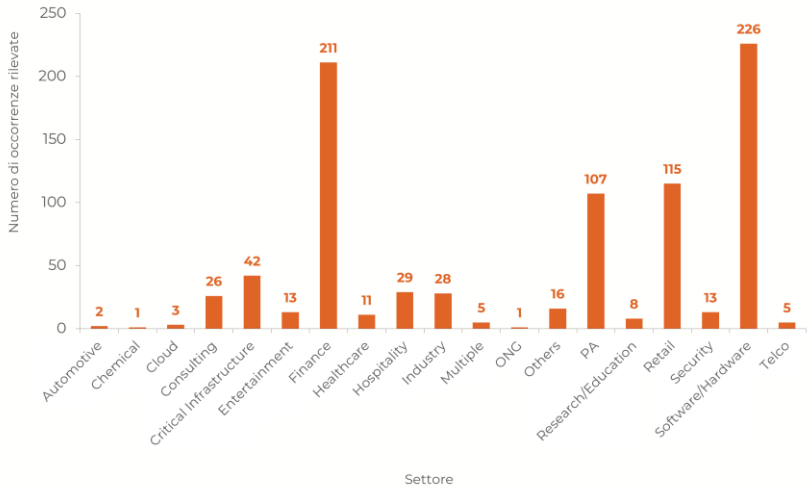


Figura 1 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 1Q2025 in Italia

Le banche investono miliardi ogni anno in sicurezza informatica, cercando di rimanere un passo avanti rispetto agli attaccanti. In questo scenario, l'AI emerge come uno strumento di grande impatto per rafforzare la difesa informatica e di cui non si può e non si potrà più fare a meno. Analizzeremo nelle prossime pagine i principali strumenti che si possono utilizzare per la difesa dagli attacchi cyber e, come anticipato, approfondiremo pro e contro dell'AI, nel campo della sicurezza informatica.

Le strategie di difesa: strumenti e metodologie avanzate

Per proteggere le aziende da questi attacchi, è fondamentale adottare un approccio multi-livello che integri tecnologie avanzate e best practice di sicurezza informatica. Vediamo ora le principali tecnologie che possiamo mettere in campo.

Implementazione del framework MITRE ATT&CK

Il framework MITRE ATT&CK fornisce una panoramica dettagliata delle tattiche e tecniche utilizzate dai cybercriminali. Le aziende possono utilizzarlo per:

- Mappare le minacce e identificare vulnerabilità nei loro sistemi.
- Creare strategie di difesa basate su attacchi reali.
- Migliorare la risposta agli incidenti grazie a un'analisi dettagliata del comportamento degli attaccanti.

Threat Intelligence per una protezione proattiva

Le piattaforme di Threat Intelligence consentono di raccogliere, analizzare e condividere informazioni sulle minacce emergenti, permettendo alle aziende di:

- Anticipare attacchi grazie all'analisi di percorsi sospetti.
- Integrare dati sulle minacce nei sistemi di sicurezza per bloccare attività malevole in tempo reale.
- Collaborare con altre istituzioni per una difesa più efficace.

Security Orchestration, Automation and Response (SOAR)

Le piattaforme SOAR migliorano la gestione degli incidenti di sicurezza attraverso l'automazione. I principali vantaggi includono:

- Riduzione del tempo di risposta agli attacchi.
- Automazione delle indagini su eventi sospetti.
- Integrazione con altri strumenti di sicurezza per un'azione coordinata.

Zero Trust: un modello di sicurezza indispensabile

L'approccio Zero Trust si basa sul principio "mai fidarsi, ma verificare sempre". Le aziende devono implementare:

- Autenticazione multi-fattore (MFA) per ogni accesso.
- Segmentazione della rete per limitare i movimenti laterali degli attaccanti.
- Monitoraggio continuo per rilevare attività sospette e bloccare accessi non autorizzati.

Simulazioni di attacco e Red Teaming

Un'altra strategia efficace è la simulazione continua di attacchi per testare la resilienza della banca e di qualunque altra tipologia di azienda. Le tecniche di Red Teaming includono:

- Penetration testing per valutare la robustezza delle difese.
- Simulazioni di attacchi phishing per verificare la consapevolezza dei dipendenti.
- Test di risposta agli incidenti per migliorare la rapidità di reazione.

L'uso dell'AI nella sicurezza informatica

Perché Usare l'AI nella Sicurezza Informatica

Uno degli aspetti più innovativi dell'AI è la sua capacità di analizzare enormi quantità di dati in tempo reale per individuare comportamenti anomali e possibili attacchi informatici. Attraverso l'apprendimento automatico

e l'analisi predittiva, questi sistemi possono identificare tentativi di intrusione, schemi fraudolenti e attività malevole prima che possano causare danni. Tuttavia ciò che spesso viene trascurato è il ruolo cruciale giocato dai dati – e **in particolare dalla qualità, varietà e integrazione delle fonti informative** – nel determinare l'efficacia delle soluzioni basate su AI. Per poter generare risposte coerenti, contestuali e realmente utili, **un sistema di AI deve attingere, in modo sicuro e protetto, da una molteplicità di fonti**: database aziendali, sistemi CRM, documentazione interna, knowledge base, archivi email, ticketing system e molto altro. Le multi-sorgenti di dati non solo arricchiscono il contesto, ma eliminano o riducono sensibilmente il rischio di risposte parziali o fuorvianti. Una AI che può "vedere" l'intera storia di un cliente, il suo contratto, le conversazioni pregresse con il supporto e le condizioni commerciali in tempo reale, può rispondere in modo preciso e personalizzato. Questo è il salto di qualità che l'AI porta rispetto a soluzioni generiche. Inoltre, avere più fonti non basta: è essenziale consolidare queste informazioni in **un'unica e sicura piattaforma** che permette di agire come un layer intelligente che normalizza, arricchisce e rende interrogabili tutti i dati. Solo così si può garantire che l'AI lavori su dati consistenti, aggiornati e privi di ambiguità. Infine, una piattaforma unificata consente una governance efficace, fondamentale per garantire sicurezza, compliance e controllo degli accessi. L'adozione di una strategia di unificazione dei dati permette non solo di potenziare le performance dell'AI, ma anche di aumentare la fiducia degli utenti nei risultati generati. L'uso dell'AI nella cybersecurity può rafforzare le difese delle aziende in particolare attraverso:

Rilevamento delle Minacce in Tempo Reale. L'AI può analizzare grandi quantità di dati e identificare schemi sospetti più velocemente di quanto potrebbero fare gli esseri umani. Gli algoritmi di machine learning possono apprendere dai dati storici e riconoscere nuove minacce informatiche prima che possano causare danni.

Automazione dei Processi di Sicurezza. Grazie all'AI, molte operazioni di sicurezza, come il monitoraggio delle reti e la risposta agli attacchi, possono essere automatizzate, riducendo il carico di lavoro per gli analisti umani e migliorando la tempestività degli interventi.

Riduzione del Fattore Umano negli Errori. Gli errori umani sono tra le principali cause di falle nella sicurezza informatica. L'AI, essendo meno soggetta a distrazioni ed errori di valutazione, può ridurre significativamente questi rischi.

Analisi Predittiva e Adattabilità. Le tecnologie AI possono prevedere attacchi futuri analizzando percorsi e comportamenti anomali, adattandosi rapidamente ai nuovi metodi utilizzati dai cybercriminali.

Migliore Gestione degli Incidenti. I sistemi AI possono fornire risposte automatiche agli incidenti, mitigando rapidamente i danni e migliorando la resilienza complessiva di un'infrastruttura IT. In particolare possiamo mettere in evidenza le seguenti funzionalità:

Sintesi Intelligente degli Incidenti. La funzionalità di sintesi utilizza l'intelligenza artificiale e il machine learning per generare automaticamente riassunti degli incidenti di sicurezza. Questo permette agli analisti di ottenere una panoramica chiara e dettagliata senza dover esaminare manualmente enormi quantità di dati. I vantaggi principali includono:

- Riduzione del tempo necessario per analizzare un incidente.
- Migliore comprensione delle cause e degli impatti.
- Facilità di condivisione delle informazioni tra i team di sicurezza.

Correlazione: associazione Intelligente degli Eventi di Sicurezza. La correlazione aiuta a collegare tra loro eventi di sicurezza apparentemente isolati, identificando percorsi comuni e attacchi su larga scala. Grazie a questa funzionalità, si riesce a:

- Riconoscere minacce avanzate che altrimenti potrebbero passare inosservate.

- Ridurre il numero di falsi positivi eliminando eventi duplicati o irrilevanti.
- Fornire un contesto più ampio per un'analisi più accurata degli incidenti.

Chiusura Automatica degli Incidenti. Grazie all'AI e all'automazione dei processi, e' possibile la chiusura automatica degli incidenti, una volta che tutte le azioni necessarie sono state completate e validate. Questo comporta:

- Maggiore efficienza nella gestione della sicurezza.
- Riduzione degli errori umani nella fase di chiusura.
- Ottimizzazione dei tempi di risposta e gestione delle risorse.

Perché serve cautela nell'utilizzo dell'AI soprattutto nella Sicurezza Informatica

Sebbene l'AI offra vantaggi significativi, è anche una risorsa nelle mani degli attaccanti. Gli hacker stanno sfruttando sempre più l'AI per automatizzare, perfezionare e potenziare le loro offensive. Ecco alcuni esempi:

- **Creazione di Malware e Attacchi Automatizzati.** L'AI può essere utilizzata dai cybercriminali per generare malware in grado di eludere i sistemi di rilevamento tradizionali. Grazie alla capacità dell'AI di adattarsi in tempo reale, i malware possono essere costantemente aggiornati per superare le difese più avanzate.

- **Deepfake e Frodi Bancarie.** Una delle minacce più preoccupanti è rappresentata dai deepfake. Queste tecnologie permettono di creare video, immagini e registrazioni audio altamente realistiche, che possono essere usate per ingannare i sistemi di autenticazione biometrici e per perpetrare frodi finanziarie.

- **Inganno nei Sistemi di AI Defensivi.** Gli attaccanti possono sfruttare l'AI per ingannare i modelli di sicurezza delle aziende. Ad esempio, attraverso il "data poisoning", si possono alterare l'insieme di dati utilizzati per addestrare i sistemi di AI, rendendoli inefficaci nel riconoscere minacce reali.

- **Lo Shadow AI: l'AI non controllata.** Un ulteriore problema emergente è quello dello "Shadow AI", ovvero l'utilizzo non autorizzato o non monitorato dell'AI da parte di dipendenti e team IT/Sicurezza. L'uso di strumenti AI non approvati può introdurre vulnerabilità critiche, esponendo i dati aziendali a rischi non calcolati.

- **AI-Powered Social Engineering.** L'AI sta rendendo gli attacchi di social engineering più sofisticati. Gli hacker possono generare email o messaggi di testo che imitano perfettamente il linguaggio e il tono dei dirigenti aziendali, aumentando il rischio di truffe come il Business Email Compromise (BEC).

Conclusione: un equilibrio tra opportunità e minacce

L'aumento degli attacchi cyber, in particolare nel settore bancario, richiede una strategia di difesa avanzata e multilivello. L'integrazione di strumenti come MITRE ATT&CK, Threat Intelligence, SOAR, Zero Trust, Red Teaming e AI permettono di ridurre i rischi e migliorare la resilienza delle istituzioni finanziarie ed in generale di tutte le aziende. Solo attraverso un approccio proattivo e innovativo le banche potranno proteggere i propri dati e garantire la sicurezza delle transazioni per i loro clienti. In particolare l'AI rappresenta una rivoluzione per la cybersecurity bancaria e non solo, offrendo strumenti potenti sia per la difesa che per l'attacco. L'AI è intelligenza data-driven al servizio dell'efficienza, della personalizzazione e dell'innovazione continua e che è essenziale consolidare tutte informazioni in un'unica e sicura piattaforma che agisce come un layer intelligente che normalizza, arricchisce e rende interrogabili tutti i dati. Solo così si può garantire che l'AI

lavori su dati consistenti, sicuri, aggiornati e privi di ambiguità. Il futuro della sicurezza informatica dipenderà dalla capacità delle aziende di sfruttare i vantaggi dell'AI, senza sottovalutare i rischi che essa comporta. Solo con un approccio equilibrato e una gestione attenta sarà possibile garantire la protezione dei dati e delle transazioni finanziarie in un mondo sempre più digitalizzato. L'AI rappresenta pertanto un potente alleato nella sicurezza informatica, offrendo strumenti avanzati per il rilevamento delle minacce, l'automazione dei processi e la riduzione degli errori umani. Tuttavia, la sua implementazione deve essere ponderata, tenendo conto dei rischi associati, come falsi positivi, vulnerabilità agli attacchi e costi elevati. Per un'efficace strategia di cybersecurity, l'ideale è combinare l'intelligenza artificiale con l'esperienza umana, sfruttando il meglio di entrambi i mondi per garantire protezione e reattività ottimali contro le minacce informatiche.

Rising Threat: Protecting Italian Financial Services from DDoS Attacks

Brett Ley VP, Technical Sales - A10 Networks

All modern businesses must contend with the threat of a cyberattack. Every day, thousands of businesses and individuals fall victim to ransomware, data breach, or distributed denial of service (DDoS) threats, enacted by cybercriminals looking to exfiltrate valuable data. While this issue is universal, certain sectors suffer more than others, with one of the most popular targets being organisations operating within the financial services sector.

The European finance sector is a prime target for cybercriminals due to the vast amounts of sensitive personally identifiable information (PII) and financial data it handles, making it lucrative for monetary gain and reputational damage. Cybercriminals seek to steal this information for resale, identity theft, or to cripple operations – potentially leading to significant financial losses for affected institutions and customers.

Why are DDoS attacks so popular in financial services?

DDoS is a favoured method for cybercriminals because attacks are easy to launch, especially with dark web "as-a-service" kits requiring little skill. This means cybercriminals can enact large-scale DDoS campaigns with little or no specialised knowledge – and AI tools now enable even larger, more complex automated attacks.
While the financial sector is a particular target for DDoS attacks worldwide, European organisations are particularly at risk. Research from FS-ISAC has shown that financial businesses in EMEA were the victims of 66% of all DDoS attacks, compared with only 28% in North America. Unlike ransomware, which focuses on data theft and extortion, DDoS mainly aims to cause disruption, a key goal for hacktivists and nation-state actors.

DDoS is also favoured by hackers for 'smokescreen' attacks, causing chaos that masks other cybercrimes. While key applications are taken offline, admins are forced to focus their efforts on restoring access to their sites. Threat actors can use this distraction to explore the edges of an organisation's network, searching for vulnerabilities or a way to breach the system and gain access to sensitive data.

DDoS and the Italian Financial Services Industry

Italian financial services organisations have been a frequent target for DDoS attacks. In February 2025, a wave of DDoS attacks was launched against a number of high-profile Italian institutions, particularly targeting banks, specifically Intesa Sanpaolo, Banca Monte dei Paschi, and Iccrea Banca. The attack was claimed by a hacker group known as 'NoName057(16)', with its apparent motives being political in nature.

These recent attacks are a prime example of how DDoS has been used by cybercriminals to cause disruption for Italian financial institutions. High-profile financial services companies are not only crucial to Italy but also have significant international ties. Attacks on Italian banks can affect the broader European and global financial ecosystem, which adds an additional layer of appeal for cybercriminals seeking to cause global disruption.

Research has shown that the number of financial firms that fall victim to DDoS attacks is only increasing, with FS-ISAC finding an increase of 154% between 2022 and 2023. As DDoS attacks become increasingly easy for threat actors to carry out, financial organisations in Italy need to stay vigilant to protect the sensitive data they carry.

How Financial Services Can Protect Themselves

While DDoS is often seen as one type of attack, there are many different forms they can take. These include volumetric attacks, where the target system is overwhelmed with a huge number of false requests, as well as protocol attacks, which aim to overwhelm defence resources like firewalls and load balancers. It is vital for organisations to have a robust, multi-layered security solution that can mitigate every kind of DDoS attack.

While AI is being leveraged by attackers to enhance their DDoS capabilities, it is also a powerful tool to defend against threats. Italian financial institutions can use AI to perform traffic analysis much more efficiently than ever before, allowing them to detect and mitigate attacks in real-time. Furthermore, AI also excels at behavioural analysis and traffic baselining, which help identify anomalies and block malicious traffic.

The attack surface for Italian financial institutions will only widen as they continue with digital transformation initiatives. This will lead to technology stacks becoming increasingly complex, making it harder to defend from external threats. In most large-scale DDoS events, attackers aim to overwhelm cloud bandwidth, which on-premises solutions cannot defend against. Companies should look to employ a hybrid defence solution which absorbs and mitigates traffic surges, providing an additional layer of protection and preventing the internal network from being overwhelmed.

At the same time, whilst cloud adoption in Italy continues to increase, and legacy solutions dwindle, financial institutions are also grappling with how to ensure regulatory compliance. With disparate regulations across Europe – not just in Italy – this can take significant time and resources, complicating organisations' ability to effectively defend its perimeters.

Securing Against DDoS Threats

The Italian financial sector faces an escalating threat from DDoS attacks. As DDoS incidents increase in Italy overall, financial services could be disproportionately affected. To mitigate these risks, financial institutions must invest in robust, best-of-breed cybersecurity solutions to protect their own perimeter – and that of companies within their supply chains.

Malware 1Q2025

PLAYFULGHOST

PLAYFULGHOST è un malware che prende il nome dalla natura apparentemente "giocosa" con cui comunica nei sistemi compromessi. Si comporta come una backdoor avanzata, ispirata a Gh0st RAT, uno strumento di controllo remoto il cui codice sorgente è pubblico da anni, ma introduce diverse variazioni nei pattern di traffico e nei metodi di cifratura, rendendosi più difficile da identificare.
Il malware presenta diverse funzionalità avanzate, tra cui la registrazione dei tasti digitati, la possibilità di catturare schermate e audio, l'accesso remoto alla shell del sistema, la capacità di trasferire ed eseguire file, e tecniche per eludere i meccanismi di rilevamento.
La distribuzione avviene principalmente tramite email di phishing, dove i file dannosi sono spesso nascosti in archivi compressi che appaiono come immagini innocue, oppure attraverso una tecnica chiamata SEO poisoning, che manipola i risultati dei motori di ricerca per dirottare le vittime su siti fraudolenti da cui scaricare software apparentemente legittimi.
Una volta installato, PLAYFULGHOST si assicura di rimanere attivo nel sistema, modificando il registro di Windows, pianificando attività automatiche o installandosi come servizio di sistema. Questo gli permette di riattivarsi ad ogni riavvio e mantenere l'accesso al computer della vittima nel tempo.

MintsLoader

MintsLoader è un malware loader basato su PowerShell, diffuso principalmente tramite email di spam contenenti link a pagine ClickFix o a file dannosi. Una volta che l'utente clicca su un link di phishing, il file JavaScript offuscato viene scaricato e esegue un comando PowerShell per caricare MintsLoader in modo automatico. Una volta attivo, MintsLoader implementa payload secondari, come StealC e il client BOINC, che consentono il furto di dati sensibili da browser, applicazioni e portafogli di criptovalute, che vengono poi esfiltrati verso un server di comando e controllo (C2).
Il malware, inoltre, incorpora meccanismi che gli consentono di escludere automaticamente i dispositivi localizzati in specifiche aree geografiche, evitando così di attivarsi in quei territori.
MintsLoader è progettato per eludere i sistemi di sicurezza, sfruttando tecniche avanzate per migliorare l'efficacia dell'attacco.
Tra i principali bersagli del malware figurano settori strategici come quello dell'energia elettrica, del gas e del petrolio.

Aquabot

Aquabot è un malware di tipo botnet che colpisce principalmente sistemi Windows, con l'obiettivo di trasformarli in host controllabili da remoto, detti zombie, all'interno di una rete malevola. Diffuso tramite phishing, exploit kit o software pirata, Aquabot stabilisce una connessione con un server C2 (Command and Control), dal quale riceve comandi e moduli operativi. È dotato di funzionalità avanzate come keylogging, furto di credenziali, acquisizione di screenshot, esecuzione remota di comandi e download di payload aggiuntivi. Il malware implementa meccanismi di persistenza tramite modifiche al registro di sistema e la creazione di task pianificati, garantendosi l'esecuzione automatica a ogni riavvio. Aquabot adotta tecniche anti-analysis come offuscamento del codice, rilevamento di ambienti sandbox o virtual machine e disabilitazione di strumenti di monitoraggio, rendendosi difficile da rilevare e analizzare.

L’architettura modulare di questo malware permette l'invio dinamico di plugin, che possono estendere le sue capacità, ad esempio per eseguire operazioni di esfiltrazione dei dati, attacchi ransomware o DDoS. Inoltre, è in grado di aggiornarsi o disinstallarsi autonomamente, in risposta a comandi provenienti dal server di comando e controllo (C2).

MassJacker

Nel primo trimestre del 2025, MassJacker si è affermato come una minaccia concreta all'interno del panorama dei malware finanziari, in particolare per gli utenti e le organizzazioni che operano nel mondo delle criptovalute. Si tratta di un malware classificato come *clipper*, progettato per monitorare la clipboard dei dispositivi e sostituire in modo furtivo gli indirizzi di wallet copiati con quelli controllati dagli attaccanti.
MassJacker viene distribuito principalmente tramite siti web che offrono software pirata, che si presentano come fonti affidabili ma sono in realtà veicoli per la diffusione di codice malevolo.
Il malware utilizza una Dynamic Link Library (DLL) crittografata che viene iniettata in processi legittimi di Windows per garantirsi persistenza e invisibilità. Una delle peculiarità di MassJacker è il ricorso a tecniche di evasione sofisticate: sfrutta il *JIT Hooking*, altera i token dei metadati per ostacolare l’analisi statica e si avvale di una macchina virtuale interna personalizzata per eseguire i comandi, rendendo l’analisi dinamica complessa.
L’obiettivo è intercettare transazioni di criptovalute e reindirizzare i fondi verso destinazioni fraudolente.
Infatti, il software dannoso intercetta le operazioni di copia/incolla di indirizzi di wallet di criptovalute. Quando l’utente copia un indirizzo per inviare un pagamento, il malware lo sostituisce automaticamente con un indirizzo controllato dagli attaccanti. I fondi vengono così trasferiti inconsapevolmente a terzi.

StilachiRAT

Il nuovo Remote Access Trojan (RAT) noto come **StilachiRAT** combina capacità di elusione, furto di dati e controllo remoto, con un particolare focus sulla sottrazione di credenziali e informazioni legate alle criptovalute.
Sebbene i vettori di attacco primari non siano ancora del tutto definiti, si ritiene che StilachiRAT venga distribuito attraverso campagne di phishing e software compromessi. Una volta che il malware raggiunge il sistema della vittima, attiva una serie di controlli per verificare se si trova in un ambiente di analisi o sandbox. In caso affermativo, sospende o modifica il proprio comportamento per sfuggire all’identificazione. Questo lo rende particolarmente difficile da rilevare con tecniche convenzionali.
Gli obiettivi di StilachiRAT sono chiaramente orientati al furto di dati sensibili, in particolare credenziali di accesso e informazioni relative a wallet di criptovalute. Inoltre, il malware è progettato per rilevare e interagire con estensioni di wallet digitali installate nel browser.
StilachiRAT, inoltre, monitora le sessioni di desktop remoto (RDP), consentendo potenzialmente agli attori malevoli di esplorare la rete della vittima e compiere movimenti laterali. In ambienti aziendali, questo significa la possibilità concreta di estendere la compromissione ad altri sistemi, aumentando il danno complessivo e potenzialmente esfiltrando grandi volumi di dati o accedendo a infrastrutture critiche.

Per le organizzazioni, un’infezione da StilachiRAT può tradursi in danni operativi, perdita di dati critici, compromissione dell’infrastruttura IT e danni reputazionali. Considerando la sua capacità di agire in modo furtivo, è possibile che una compromissione resti attiva per periodi prolungati prima di essere rilevata.

BackConnect

BackConnect è un malware orientato al controllo remoto persistente dei sistemi compromessi, tipicamente associato ad attività di cybercrime e cyberspionaggio. Il nome deriva dalla tecnica "backconnect", che permette all'attaccante di ottenere una shell remota sul sistema bersaglio, anche se questo si trova dietro un firewall o NAT, stabilendo una connessione inversa verso il server di comando e controllo. Una volta attivo, il malware consente l'esecuzione remota di comandi arbitrari, la manipolazione dei file di sistema e l'installazione di payload.
BackConnect impiega meccanismi stealth per occultare la propria presenza, come rootkit, iniezione di codice nei processi legittimi e crittografia del traffico C2. Può anche sfruttare vulnerabilità note per elevare i privilegi e ottenere accesso a livello di sistema. È spesso utilizzato come primo stadio in attacchi complessi, dove funge da "ponte" per operazioni successive come esfiltrazione dei dati, movimenti laterali o installazione di ransomware. Supporta funzionalità di persistenza avanzate, tra cui la modifica di servizi di sistema e chiavi del registro. Per l'attaccante, BackConnect offre un accesso stabile e discreto alla rete bersaglio, facilitando un'occupazione a lungo termine.
Il suo impiego è particolarmente diffuso in campagne APT (Advanced Persistent Threat) e attacchi mirati contro aziende, enti governativi e infrastrutture strategiche.

Astral Stealer

Astral Stealer è un malware multifunzionale progettato per eseguire una vasta gamma di attività dannose. Tra le principali funzionalità del malware figurano: l'offuscamento per eludere il rilevamento dai sistemi di sicurezza, il furto di dati sensibili come credenziali, cookie, metodi di pagamento salvati nei browser e informazioni sui portafogli di criptovalute, l'esecuzione di operazioni dannose e la garanzia di persistenza sui dispositivi vittima.
Il codice sorgente di Astral Stealer è scritto in diversi linguaggi, tra cui Python, JavaScript e C#, ed è distribuito tramite uno strumento personalizzabile, dotato di un'interfaccia semplice e intuitiva che lo rende facilmente accessibile anche a utenti meno esperti.
Per restare attivo nel sistema colpito, il malware maschera i processi ad alto consumo di risorse affinché non risultino sospetti e può configurarsi per l'esecuzione automatica all'avvio del sistema, creando una cartella nella directory di avvio.
Il tutto rende Astral Stealer una minaccia concreta e versatile, capace di operare in maniera silenziosa ed efficiente all'interno di un sistema compromesso.

SparkCat

Il malware SparkCat fa parte di una categoria nuova nel panorama dell'analisi dei malware. Infatti, utilizza algoritmi di intelligenza artificiale e librerie di apprendimento automatico, disponibili pubblicamente, per sferrare attacchi.
Questo malware ha come target tutti i dispositivi mobili, utilizzando come vettore di attacco applicazioni presenti su Google store e App store considerate legittime dai sistemi di protezione. Una volta atterrato sul dispositivo tramite l'applicazione, il malware, etichettato come trojan, utilizza il riconoscimento ottico dei caratteri (OCR) per scansionare tutti i file multimediali presenti nella galleria, e trovare immagini contenenti parole chiave associate a credenziali per l'accesso ad app sensibili, dati bancari, dati sensibili ed altre informazioni utili al lavoro degli attaccanti.

Flesh Stealer

FleshStealer è un malware progettato per colpire determinati browser web, ma anche per sottrarre dati da alcune applicazioni, ampiamente utilizzate, di messaggistica istantanea, come database e chat archiviate. Scritto in C#, agisce tramite un pannello di controllo web che consente agli attaccanti di gestire da remoto i dispositivi colpiti. La compromissione del sistema avviene principalmente attraverso file dannosi o siti web compromessi. Una volta introdotto nel sistema, il malware sfrutta vulnerabilità mirate per esfiltrare dati sensibili, come credenziali di accesso e informazioni di pagamento. Per evitare il rilevamento e garantire la permanenza sul dispositivo compromesso, adotta tecniche avanzate di offuscamento e persistenza.
Una caratteristica peculiare di FleshStealer è la sua capacità di adattarsi al contesto culturale del dispositivo. Infatti, prima di attivarsi, il malware analizza la lingua di input del sistema operativo. Se rileva una lingua appartenente a un Paese membro della Comunità degli Stati Indipendenti (CSI), il malware evita di installarsi, presumibilmente per eludere conseguenze legali nei territori d'origine degli sviluppatori.

FrigidStealer

FrigidStealer è un malware mirato a colpire i sistemi macOS, sviluppato e distribuito dal gruppo di criminali informatici noto come TA2727, il cui obiettivo principale è di natura economica. Questo malware si diffonde attraverso siti web compromessi che presentano notifiche ingannevoli, che appaiono come aggiornamenti legittimi per i browser web. In realtà, queste notifiche inducono l'utente a scaricare un file Disk Image (DMG) contenente il malware, scritto in linguaggio Go.
Una volta che il file DMG viene aperto e il malware installato, l'eseguibile consente agli attaccanti di accedere a dati sensibili presenti nel sistema colpito. Il processo malevolo si avvale di tecniche di inganno visivo e sfrutta il bypass manuale di Gatekeeper, la funzionalità di sicurezza integrata nei dispositivi macOS, per eludere il blocco delle applicazioni non autorizzate.

Autori

Domenico Raguseo è Responsabile della Unit di CyberSecurity di Exprivia. Precedentemente ha ricoperto il ruolo di CTO della divisione IBM Security nel Sud Europa. Ha una decennale esperienza manageriale e nel campo della CyberSecurity in diverse aree. Domenico collabora con diverse università nell'insegnamento di tematiche relative alla CyberSecurity sia come professore a contratto che invitato come lettore per seminari. Domenico è stato IBM Master Inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è apprezzato speaker, autore e blogger in eventi nazionali e internazionali. In particolare, da diversi anni collabora con il Clusit come autore.

Rosita Galiandro ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'Università di Bari.
Attualmente ricopre il ruolo di Responsabile Osservatorio CyberSecurity presso Exprivia.
Contribuisce alle attività di prevendita e collabora in piani di insegnamento con diverse università e scuole di formazione nell'ambito CyberSecurity.

Valeria Vetrano, ha conseguito la laurea magistrale in Ingegneria Elettronica presso l'Università Politecnica delle Marche, con focus in Smart and Secure Communication Networks.
In Exprivia ricopre il ruolo di Cyber Threat Intelligence Specialist, all'interno della divisione di Cybersecurity.

Ernesto Vignes dal 1998 collabora con diverse realtà del settore IT come sistemista dal 2015 presso Exprivia partecipa a diversi progetti in ambito Telco & Media ricoprendo il ruolo di system engineer.
Attualmente collabora con la DFCY-CY Digital Factory CyberSecurity di Exprivia, ove si occupa delle soluzioni di IdAM.

Michele Cortese, ha conseguito la laurea Magistrale in Ingegneria Informatica presso il Politecnico di Bari.
Attualmente ricopre il ruolo di Cyber Security Consultant presso Exprivia.
Svolge attività di delivery e R&D, si occupa della definizione e formalizzazione dei processi aziendali critici e di tematiche legate al mondo dei GRC (Governance, Risk, Compliance). Inoltre, è impegnato nella progettazione di un framework innovativo per la simulazione di processi aziendali.

Giuseppe Troianiello, CyberSecurity Analyst con particolare esperienza nel mercato finance, in Exprivia è responsabile di progetti in ambito IAM, PAM e Data Protection. Si occupa di A&D per lo sviluppo e il delivery di nuovi software, di installazione configurazione ed integrazione di prodotti di mercato, di customizzazione di applicativi esistenti.
Tra le sue attività, inoltre, vi è la fornitura di soluzioni applicative per l'adeguamento delle aziende alla normativa GDPR.

Luigi Florio, ha conseguito la laurea in Scienze dell'Informazione presso l'Università degli Studi di Pisa.
Project Manager certificato PMP® si occupa principalmente di Privileged Access Management per l'unità cybersecurity di Exprivia. Più recentemente ha seguito progetti in ambito SAP per l'area sistemistica/infrastrutturale e di integrazione svolgendo anche attività di presales.

Mauro Gadaleta, ha conseguito la laurea magistrale in ingegneria delle telecomunicazioni con specializzazione in cybersecurity presso il Politecnico di Bari.
Attualmente svolge attività di gestione del portale CSIRT e ricopre il ruolo di SOC Analyst.

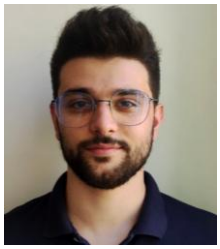
Graziano Specchierla, ICT Security Consultant nella CyberSecurity Digital Factory di Exprivia, precedentemente Security Architect in IBM Security.
È coinvolto nel disegno di soluzioni, sviluppo del business e delivery sulle tematiche di sicurezza orientate principalmente al digital trust, alla gestione degli endpoint, alle implementazioni di soluzioni innovative.
Ha al suo attivo molti progetti, in varie aree dell'Information Technology, nelle discipline del system & network management, mobile management e del monitoraggio, in vari settori d'industria.

Tullio Mario Cozzolino, è diplomato Ragioniere Programmatore, Laureato in Economia e Commercio, incomincia la sua carriera come Account Manager nel settore dell'ICT. Come Project Manager ha seguito diversi appalti nel settore Militare, Sicurezza e Pubblica Amministrazione. Responsabile della Compliance GDPR in ambito Giustizia. Ha conseguito diverse certificazioni quali CCNA, CEH, CSA e dal 2023 riveste il ruolo di SOC Analyst in Exprivia.

Gerardo Pio Giannetta, ha conseguito la laurea triennale in Informatica e Tecnologie per la Produzione del Software presso l'università di Bari. Attualmente ricopre il ruolo di ICT Security Administrator presso Exprivia. Svolge attività di progettazione e sviluppo software in ambito CyberSecurity.

Antonio Minnella, ha conseguito la laurea triennale in Informatica presso l'Università degli Studi di Bari.
Ha maturato più di 15 anni di esperienza nell'ambito dello sviluppo di software, dal 2017 si occupa prevalentemente di Application Security e di come rendere sicuro il software in ogni fase del SDLC.
Attualmente ricopre il ruolo di CyberSecurity Specialist presso Exprivia. Dal 2018 è membro di OWASP.

Lorella Defilippis, ha conseguito una laurea magistrale in "Scienze della criminalità e tecnologie per la sicurezza" presso l'Università Cattolica del Sacro Cuore di Milano.
In Exprivia ricopre il ruolo di Cyber Security Consultant all'interno della DFCY-CY.



Alessandro De Bartolo, è studente laureando in Ingegneria Dei Sistemi Medicali presso il Politecnico di Bari.
Membro della DFCY-Delivery Service, attualmente ricopre il ruolo di Junior Cyber Security Consultant presso Exprivia, svolgendo attività di supporto alle tematiche legate al mondo della Governance, Risk e Compliance.

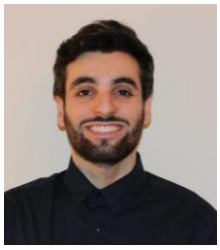
Fabio Massimo Console, ha conseguito il diploma di tecnico superiore presso “Apulia Digital – ITS”. Attualmente ricopre il ruolo di SOC Analyst presso la DFCY di Exprivia.

Antonio Montrone, Diplomato presso l'Istituto Tecnico Superiore (ITS) di Bari, specializzato in cybersecurity. In Exprivia attualmente ricopro la posizione di Cyber Security Analyst svolgendo attività di monitoraggio SOC, contribuendo inoltre allo sviluppo di soluzioni di Threat Intelligence.

Giacomo Gorrieri, ricopre il ruolo di Operation Manager della Unit di CyberSecurity di Exprivia.
È laureato in Informatica ed Odontoiatria ed ha conseguito il Master di II Livello in “Governance e Audit dei Sistemi Informativi” presso il Dipartimento di Informatica dell’Università di Roma “La Sapienza”. I suoi principali settori di competenza sono: il Project Management, IT Governance e Gestione di Processi aziendali.

Roberto Epifanio, è diplomato presso l'ITS Apulia Digital Maker come Cyber Security Expert
Attualmente svolgo il ruolo di SOC Analyst L1 all'interno della Digital Factory Cybersecurity di Exprivia.
Mi occupo principalmente del monitoraggio dei SIEM e di fornire consulenza ad alcuni clienti.

Paolo De Chirico, diplomando presso ITS Apulia Digital Maker come Cybersecurity Expert e laureando in Ingegneria Informatica. Attualmente ricopre il ruolo di Cyber Security Analyst presso Exprivia. Impegnato principalmente nello sviluppo di Cyber Innovation Technologies.



Alessandro Armenise, diplomando presso l'Istituto Tecnico Superiore (ITS) di Bari, con specializzazione in Cybersecurity Expert e laureando in Ingegneria Informatica. In Exprivia attualmente ricopro il ruolo di Cyber Security Analyst all'interno della DFCY-CY e partecipo a progetti in ambito sicurezza informatica e innovazione tecnologica.

Marco Martiradonna, attualmente diplomando come Cybersecurity Expert presso l'Istituto Tecnico Superiore Apulia Digital. Membro del team DFCY-SOC di Exprivia come Cyber Security Analyst, coinvolto in attività di monitoraggio e di sviluppo nei campi di sicurezza informatica e di Threat Intelligence.

Sorgenti di Informazioni

1. https://securityaffairs.co/wordpress/
2. https://www.enforcementtracker.com/
3. https:// thehackernews.com/
4. https://sicurezza.net/
5. https://www.cybertrends.it/
6. https://www.bleepingcomputer.com/
7. https://www.CyberSecurity360.it/
8. https://www. poliziadistato.it/
9. https://www.hackread.com/
10. https://www.forbes.com/
11. https://www. garanteprivacy.it/
12. https://www.cert-pa.it/
13. https://success.trendmicro.com/
14. https://www.commisariatodips.it/
15. https://www.securityinfo.it/
16. https://www.repubblica.it/
17. https://threatpost.com/
18. https://wired.it/
19. https://zerobin.net/
20. https://d3lab.net/
21. https://teconologia.libero.it/
22. https://chietitoday.it/
23. https://cybersecnatlab.it/
24. https://cyware.com/
25. https://medium.com/
26. https://reporterpress.it/
27. https://agi.it/
28. https://csoonline.com/

29. https://cert-agid.it/
30. https://csirt.gov/
31. https://www.ilsole24ore.it/
32. https://www.linkedin.com/
33. https://www.hdmotori.it/
34. https://www.key4biz.it/
35. https://www.cert-agid.gov.it/
36. https://www.ivg.it/
37. https://www.leggo.it/
38. https://yoroi.company/
39. https://www.corriere.it
40. https://www.ferrovie.info
41. https://www.spcnet.eu
42. https://www.trend-online.com
43. https://www.insicurezzadigitale.com
44. https://www.tecnoandroid.it
45. https://www.zeusnews.it
46. https://www.ilsussidiario.net
47. https://smarthome.hwupgrade.it
48. https://www.aboutpharma.com
49. https://www.swascan.com
50. https://www.hdblog.it
51. https://www.lagazzettadelmezzogiorno.it
52. https://leganerd.com
53. https://www.inforisktoday.com
54. https://www.msn.com
55. https://it.sputniknews.com
56. https://tecnologia.libero.it
57. https://techcrunch.com
58. https://hackerjournal.it

59. https://www.money.it
60. https://infopcfacile.it
61. https://it.cointelegraph.com/
62. https://www.ilcrivello.it
63. https://www.smartworld.it
64. https://www.rainews.it
65. https://www.ilrestodelcarlino.it
66. https://www.china-files.com
67. https://corrierealpi.gelocal.it
68. https://www.zoom24.it
69. https://www.nordmilano24.it
70. https://www.lanazione.it/
71. https://www.ilmessaggero.it
72. https://www.mediasetplay.mediaset.it
73. https://www.ictbusiness.it
74. https://www.upguard.com/
75. https://www.techradar.com
76. https://tech.fanpage.it
77. https://www-swascan-com.
78. https://computerweekly.it
79. https://www.helpmetech.it
80. https://www.adnkronos.com
81. https://www.hwupgrade.it
82. https://www.improntaunika.it
83. https://www.laleggepertutti.it
84. https://cyware.com
85. https://www.securityinfo.it
86. https://www.redhotcyber.com
87. https://tech.everyeye.it
88. https://www.corrierecomunicazioni.it

89. https://quifinanza.it
90. https://www.formulapassion.it
91. https://www.corriereromagna.it
92. https://www.tomshw.it
93. https://www.veneziatoday.it
94. https://gamerant.com
95. https://leganerd.com
96. https://dday.it
97. https://english.kyodonews.net
98. https://www.laprovinciacr.it
99. https://www.securityopenlab.it
100. https://www.361magazine.com
101. https://content.upguard.com
102. https://www.itnews.com.au
103. https://www.matricedigitale.it
104. https://www.orticalab.it
105. https://www.html.it
106. https://www.punto-informatico.it
107. https://techfromthenet.it
108. https://www.giornalettismo.com
109. https://www.securityweek.com
110. https://www.itworldcanada.com
111. https://www.commissariatodips.it
112. https://www.ansa.it
113. https://hackmanac.com
114. https://latesthackingnews.com
115. https://www.cshub.com
116. https://www.drcommodore.it
117. https://www.lgpdbrasil.com.br
118. https://cybernews.com

119. https://mattinopadova.gelocal.it
120. https://gbhackers.com
121. https://www.cronacacomune.it
122. https://www.giornalettismo.com
123. https://www.milanofinanza.it
124. https://www.ildolomiti.it
125. https://www.computersecuritynews.it
126. https://ransomfeed.it
127. https://www.cybersecitalia.it
128. https://securelist.ru/
129. https://www.easypark.com/it-it
130. https://roma.repubblica.it
131. https://csirt.exprivia.it/
132. https://www.ilsoftware.it
133. https://www.dylog.it
134. https://www.carabinieri.it
135. https://securityintelligence.com
136. https://ransomfeed.it
137. https://www.ilcentro.it
138. https://www.agenziaentrate.gov.it
139. https://mole24.it
140. https://www.lapresse.it
141. https://www.gpdp.it
142. https://pugliasera.it
143. https://www.repubblica.it
144. https://www.traderlink.it
145. https://www.tgcom24.mediaset.it
146. https://www.passionetecnologica.it/
147. https://www.mimit.gov.it
148. https://www.valleumbrasport.it

149. https://www.romatoday.it
150. https://www.darkreading.com
151. https://blog.giotech.net
152. https://www.corriereadriatico.it
153. https://www.spiceworks.com
154. https://www.ermes.company/phishing-live-ermes-reporting/
155. https://www.bancaditalia.it
156. https://www.fia.com
157. https://cyberinsider.com
158. https://cofense.com
159. https://www.key4biz.it
160. https://www.suspectfile.com
161. https://guide.aruba.it/avvisi
162. https://www.ts-way.com
163. https://roma.corriere.it
164. https://www.open.online/
165. https://www.unionesarda.it
166. https://buonasera24.it
167. https://www.acn.gov.it
168. https://bari.repubblica.it
169. https://citynotizie.it/
170. https://mag212.com
171. https://www.cyfirma.com
172. https://www.ilpost.it
173. https://noipa.mef.gov.it/cl/it/web/guest/home
174. https://puglia.coldiretti.it/
175. https://www.veronaoggi.it
176. https://www.ictsecuritymagazine.com
177. https://www.rsi.ch/
178. https://dailydarkweb.net

179. https://x.com/

exprivia

Sponsor

mimecast®

servicenow®

A10