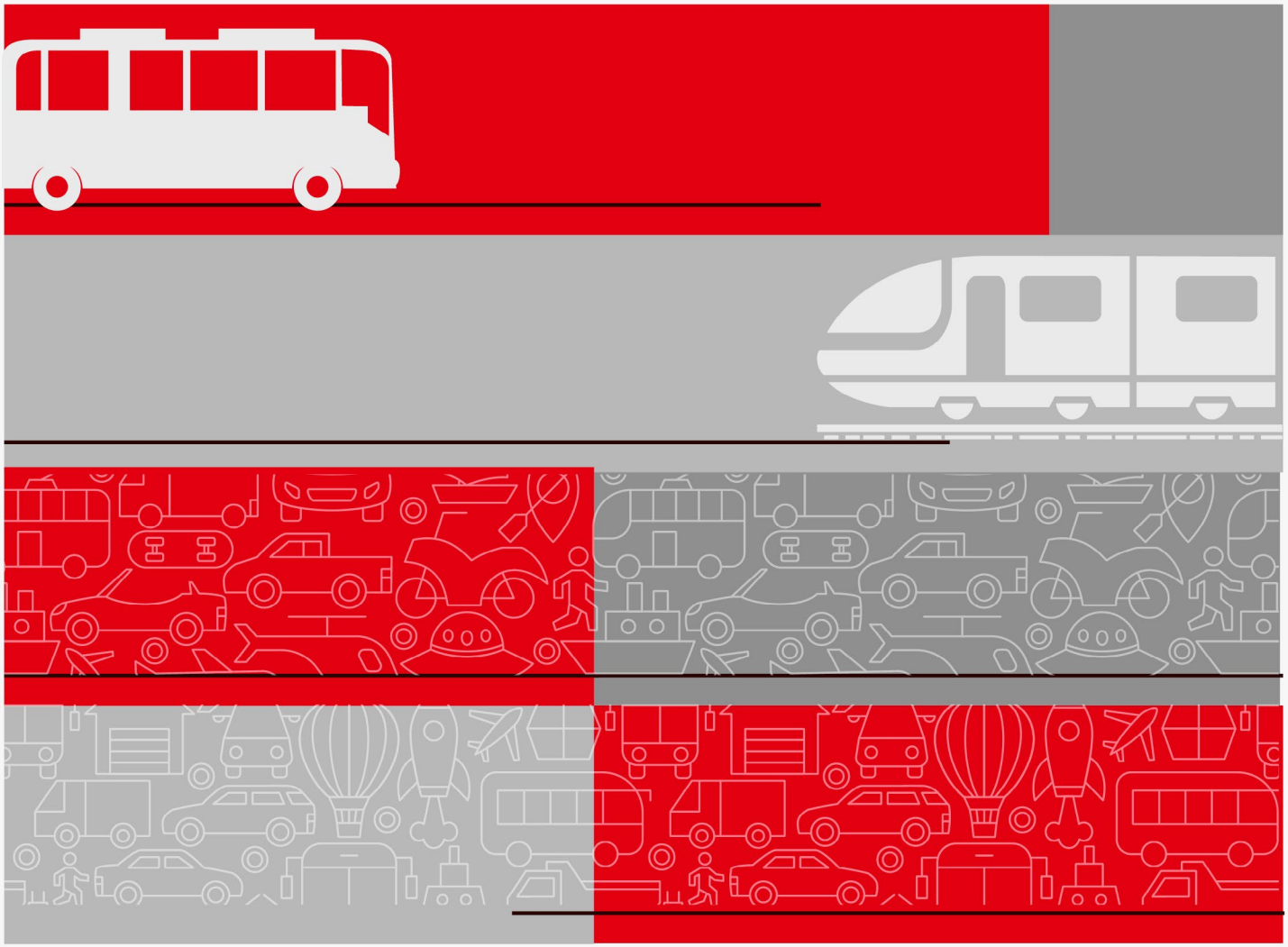
MATICMIND®
MAKES IT EASY

CYBERSECURITY NEL SETTORE TRASPORTI

Analisi delle Minacce e delle Vulnerabilità

By BU CyberSecurity



www.maticmind.it

Sommario

Executive Summary 03

Trend e previsioni 06

Worldwide 07

Sottosettori 17

Europa 27

Italia 32

Danni e impatti economici degli attacchi cyber 37

Rischi specifici per il settore Trasporti 38

Normative e investimenti in cybersecurity 41

Strategie di mitigazione e Best Practices 45

Conclusioni 46

Cyber Framework Maticmind 48

Una Cyber Acies 49

Bibliografia 50

Disclaimer 51

Executive Summary

Nel corso degli ultimi cinque anni, il comparto trasporti si è trasformato in un bersaglio privilegiato per i cybercriminali, testimoniando un'impennata degli attacchi che da poco più di una dozzina di casi significativi nel 2020 sono schizzati fino a quasi sessanta nel 2024. Questo trend, con un tasso di crescita medio annuo del 48%, sottolinea come la digitalizzazione delle infrastrutture di trasporto, se da un lato offre efficienza e connettività, dall'altro esponga a minacce sempre più sofisticate, che spaziano dal ransomware — responsabile di oltre un terzo delle intrusioni — agli attacchi DDoS e alle campagne di phishing.

L'impatto economico è altrettanto allarmante: il **costo medio** di un incidente **nel settore aereo supera i 580 000 €**, mentre **nel ferroviario** si attesta intorno ai **420 000 €**. Anche il mondo **marittimo** e quello **stradale** non restano indietro, con danni medi rispettivamente di **320 000 € e 180 000 €**.

A fronte di queste cifre, gli investimenti in cybersecurity nel comparto trasporti italiano sono cresciuti più del doppio rispetto alla media nazionale — passando dai 45 M€ del 2020 ai 152 M€ stimati per il 2025 — ma restano ancora al di sotto dei livelli europei rapportati al PIL.

Le vulnerabilità emergono soprattutto nella convergenza tra IT e OT: dai sistemi di controllo ferroviari ai network aeroportuali, dove tecniche di spoofing e jamming rischiano di paralizzare intere reti. Allo stesso tempo, l'esplosione di dispositivi IoT e l'adozione del 5G hanno ampliato la superficie di attacco, dando vita a nuove minacce come le botnet intelligenti e le insidie della "shadow AI". Nel trasporto su gomma, poi, quasi il 60 % degli attacchi ransomware prende di mira la supply chain terrestre, esponendo milioni di credenziali e dati sensibili.

Per rispondere a questo scenario, emerge con forza la necessità di un cambio di paradigma: non più sole tecnologie difensive, ma un approccio basato sul rischio che integri segmentazione Zero Trust, monitoraggio continuo e simulazioni di attacco. Formazione specialistica per operatori IT, OT e personale di bordo, insieme a piani di risposta agli incidenti definiti e testati con partner pubblici e privati, diventano strumenti imprescindibili. Inoltre, la compliance con la direttiva NIS2 non deve limitarsi a un mero adempimento normativo, ma trasformarsi in un'opportunità per rafforzare la resilienza e la reputazione delle aziende.

Questo report vuole raccontare, con numeri concreti e analisi approfondite, un settore in rapida evoluzione, dove l'unione tra esperienza operativa e fonti aperte diventa la chiave per anticipare i rischi e costruire una difesa cyber all'altezza delle sfide future.

Obiettivo del Report

Questo report si propone di fornire un'analisi approfondita e strutturata dello stato della cybersecurity nel settore dei Trasporti, con particolare attenzione al contesto italiano ed europeo.

Gli obiettivi specifici includono:

- **Mappare il panorama** delle minacce cyber che interessano il settore Trasporti, identificando trend, vettori di attacco prevalenti e attori malevoli.
- **Quantificare l'impatto economico** degli attacchi informatici.
- **Valutare lo stato degli investimenti** in cybersecurity nel settore Trasporti, identificando gap e opportunità.
- **Fornire raccomandazioni** pratiche per migliorare la resilienza cyber delle organizzazioni del settore.

Il documento intende servire come risorsa strategica per decision maker, responsabili della sicurezza e professionisti del settore Trasporti, offrendo una base informativa solida per orientare strategie di investimento e prioritizzazione degli interventi di sicurezza.

Metodologia

La ricerca si basa su un approccio multi-fonte che integra l'analisi critica di dati quantitativi e qualitativi. Un elemento distintivo della metodologia è l'integrazione dell'esperienza operativa maturata sul campo con evidenze raccolte dalle strutture specializzate della Business Unit Cyber di Maticmind (Offensive Team, Cyber Defence Center, Twin4Cyber, Cyber Threat Intelligence Team, Incident Response Management Team). Queste forniscono un riscontro diretto sulle minacce emergenti, sulla verifica proattiva delle difese e sulla gestione degli incidenti reali. I dati quantitativi sono stati analizzati per individuare trend e correlazioni, mentre quelli qualitativi hanno contribuito a contestualizzare e arricchire l'analisi.

Il processo metodologico ha seguito le seguenti fasi principali:

- **Raccolta dati:** integrazione di fonti primarie (esperienza diretta dei team operativi Maticmind) con contributi provenienti da studi, pubblicazioni e documentazione tecnica di pubblico accesso
- **Analisi comparativa:** confronto tra diversi sottosettori del comparto trasporti e benchmarking a livello internazionale
- **Sintesi e visualizzazione:** produzione di grafici e infografiche per rappresentare con chiarezza trend, pattern e correlazioni rilevanti

- **Formulazione di raccomandazioni:** sviluppo di linee guida operative e best practice basate su evidenze osservate e validazioni empiriche

Questo approccio consente di coniugare insight operativi e fonti aperte, offrendo una visione concreta e aggiornata del panorama di minaccia, con particolare attenzione alla trasversalità dei rischi e alla loro evoluzione.

Considerazioni

Nell'interpretazione dei risultati presentati in questo report, è importante considerare alcuni fattori contestuali:

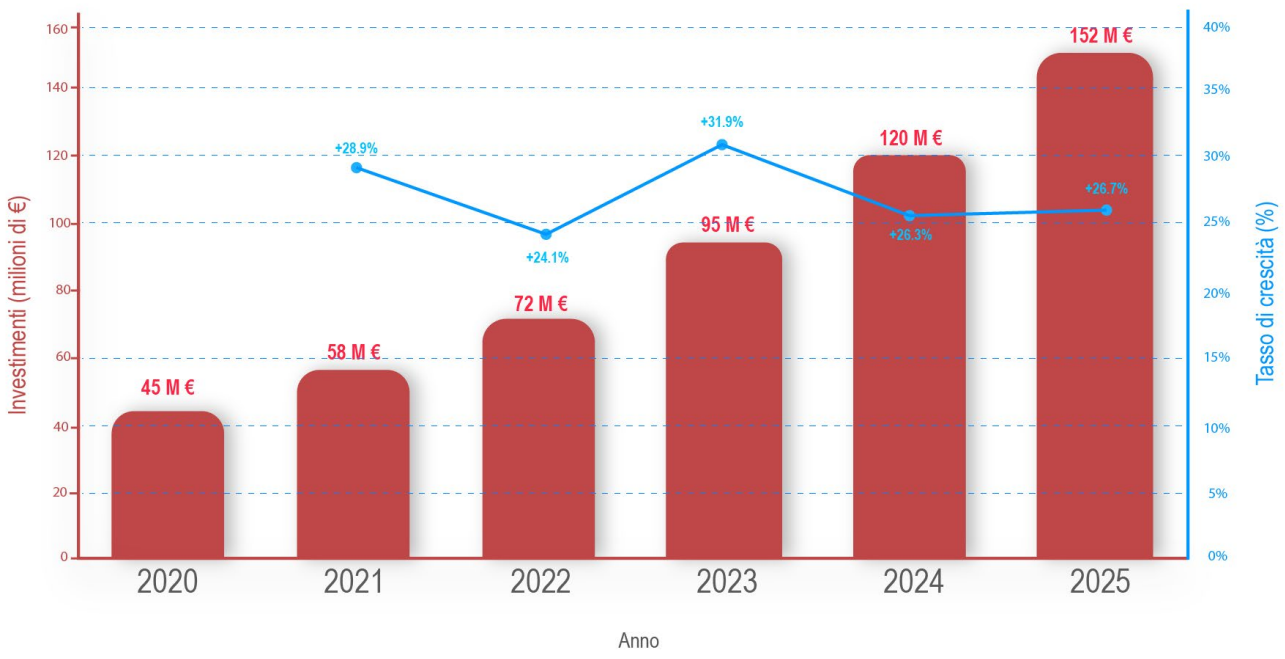
- **Underreporting:** I dati sugli incidenti cyber rappresentano solo gli attacchi noti e segnalati, con una probabile sottostima del fenomeno reale
- **Evoluzione rapida delle minacce:** Il panorama delle minacce cyber è in costante evoluzione, con nuove tecniche e tattiche che emergono continuamente
- **Specificità settoriali:** Ciascun sottosettore del trasporto presenta peculiarità tecnologiche e operative che influenzano il profilo di rischio cyber
- **Contesto geopolitico:** Molti attacchi al settore trasporti hanno possibili motivazioni geopolitiche, rendendo il panorama delle minacce sensibile a tensioni internazionali
- **Impatto della regolamentazione:** L'implementazione della Direttiva NIS2 sta modificando significativamente l'approccio alla cybersecurity nel settore

Questo report offre una fotografia del panorama attuale, ma deve essere interpretato come parte di un processo continuo di monitoraggio e adattamento alle minacce in evoluzione.

Trend e previsioni

L'analisi dei dati mostra un trend in crescita sia per quanto riguarda la frequenza degli attacchi che il loro impatto economico. La Figura illustra l'evoluzione degli investimenti in cybersecurity nel settore trasporti, che riflette la crescente consapevolezza delle organizzazioni riguardo alla necessità di proteggersi.

Trend degli investimenti in cybersecurity nel settore trasporti (2020-2025)

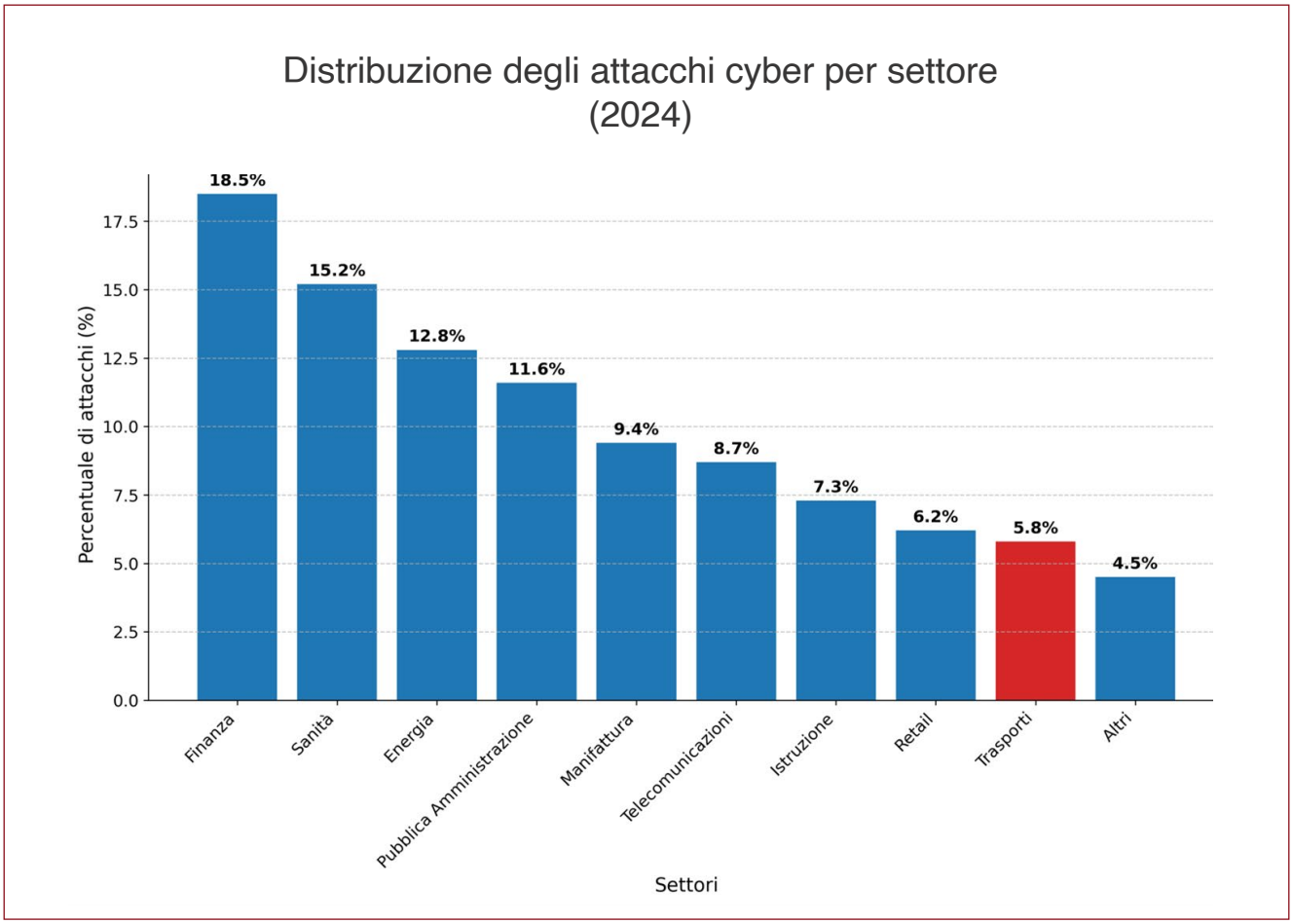


Gli investimenti sono passati da 45 milioni di euro nel 2020 a 152 milioni di euro nel 2025, con un tasso di crescita annuo composto (CAGR) del 27,5%. Questo incremento è in parte attribuibile alla spinta normativa della direttiva NIS2, ma riflette anche la crescente consapevolezza delle organizzazioni riguardo alla necessità di investire in sicurezza informatica.

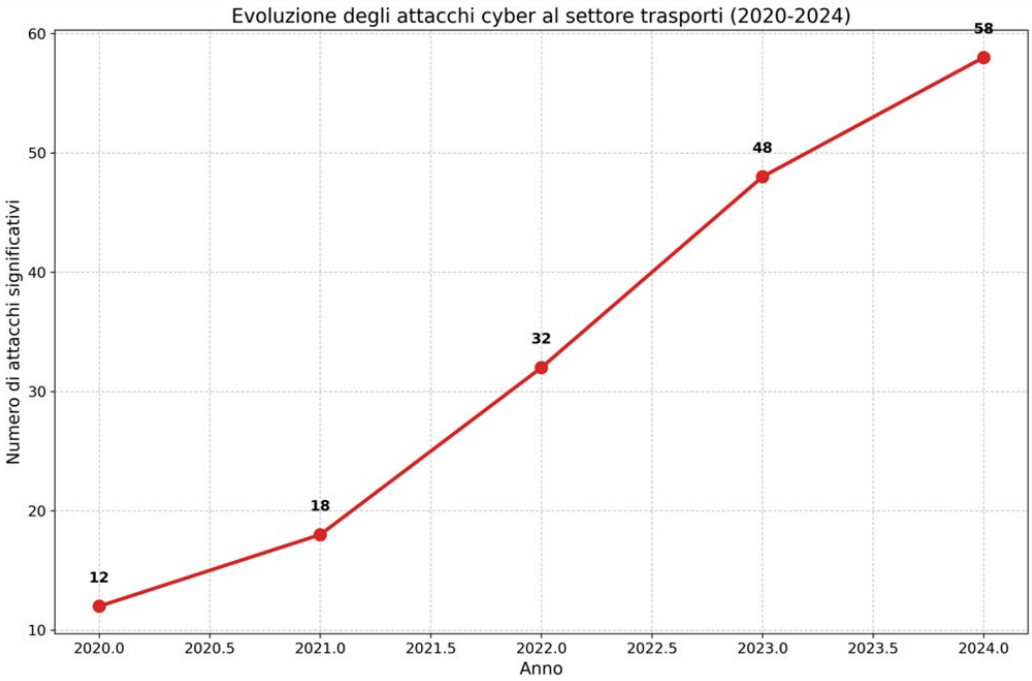
Secondo l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano (2025), si prevede che gli investimenti in cybersecurity nel settore trasporti continueranno a crescere con un CAGR del 18-20% nel periodo 2025-2030, raggiungendo i 350 milioni di euro entro il 2030.

Worldwide

Nel 2024, il settore dei trasporti ha rappresentato il **5,8%** degli attacchi cyber globali, posizionandosi al nono posto tra i settori più colpiti, come illustrato nella Figura Sebbene questa percentuale possa sembrare relativamente contenuta rispetto ad altri settori come la finanza (18,5%) o la sanità (15,2%), l'impatto potenziale degli attacchi al settore trasporti è particolarmente significativo per la loro capacità di causare interruzioni di servizio con effetti a cascata sull'economia e sulla società.



L'analisi dell'evoluzione degli **attacchi cyber al settore trasporti** nel periodo 2020-2024 mostra un trend in costante crescita, con un incremento particolarmente significativo negli ultimi anni. Il numero di attacchi significativi è passato da 12 nel 2020 a 58 nel 2024, con un **tasso di crescita medio** annuo del **48%**.



Questo incremento è attribuibile a diversi fattori:

1. **Maggiore digitalizzazione:** l'adozione accelerata di tecnologie digitali nel settore trasporti ha ampliato la superficie di attacco
2. **Crescente interconnessione:** l'integrazione tra sistemi IT e OT (Operational Technology) ha creato nuove vulnerabilità
3. **Motivazioni geopolitiche:** l'aumento di attacchi con possibili motivazioni geopolitiche, come quelli condotti dal gruppo russo Noname057 contro infrastrutture di trasporto italiane
4. **Evoluzione delle tecniche di attacco:** l'utilizzo di tecnologie avanzate, inclusa l'intelligenza artificiale, per rendere gli attacchi più sofisticati ed efficaci

La maggior parte dei log relativi a malware di tipo stealer è associata al settore Transportation and Warehousing (64,33%).

Questi colossi globali sono tra i principali bersagli delle minacce informatiche, a causa del loro ruolo strategico nel commercio e nella logistica internazionale.

- Gli Stati Uniti (13,72%) risultano essere il principale obiettivo degli attori delle minacce, seguiti da Ucraina e Regno Unito. Gli USA rappresentano un target prioritario per via della vasta rete logistica nazionale, mentre la situazione geopolitica dell'Ucraina la espone a cyberattacchi di

matrice statale.

- Il sotto-settore Truck Transportation (59,66%) risulta essere il più colpito dagli attacchi ransomware, evidenziando la vulnerabilità dei sistemi di gestione flotte e coordinamento logistico. Anche i segmenti Water e Air Transportation sono frequentemente presi di mira, a conferma di una strategia d'attacco ampia, orientata a interrompere le catene del commercio globale.
- Sono state esposte oltre 2,28 milioni di credenziali e 117.000 indirizzi IP di vittime tramite malware stealer, indicando compromissioni diffuse di dispositivi personali o aziendali del personale impiegato nella logistica. Anche hash di password e dati di carte di credito risultano a rischio, sottolineando la necessità di rafforzare le misure di endpoint protection e gestione delle credenziali.
- DHL è frequentemente oggetto di campagne di phishing, nelle quali gli attaccanti sfruttano pagine di tracciamento spedizioni o stato della consegna per sottrarre dati sensibili.

Sebbene il protocollo HTTPS sia impiegato nella maggior parte dei tentativi di **phishing (58,22%)**, **l'uso del meno sicuro HTTP (41,78%)** rimane ancora significativo. Ciò evidenzia l'importanza di sistemi di web filtering e di formazione degli utenti sulle pratiche di navigazione sicura.

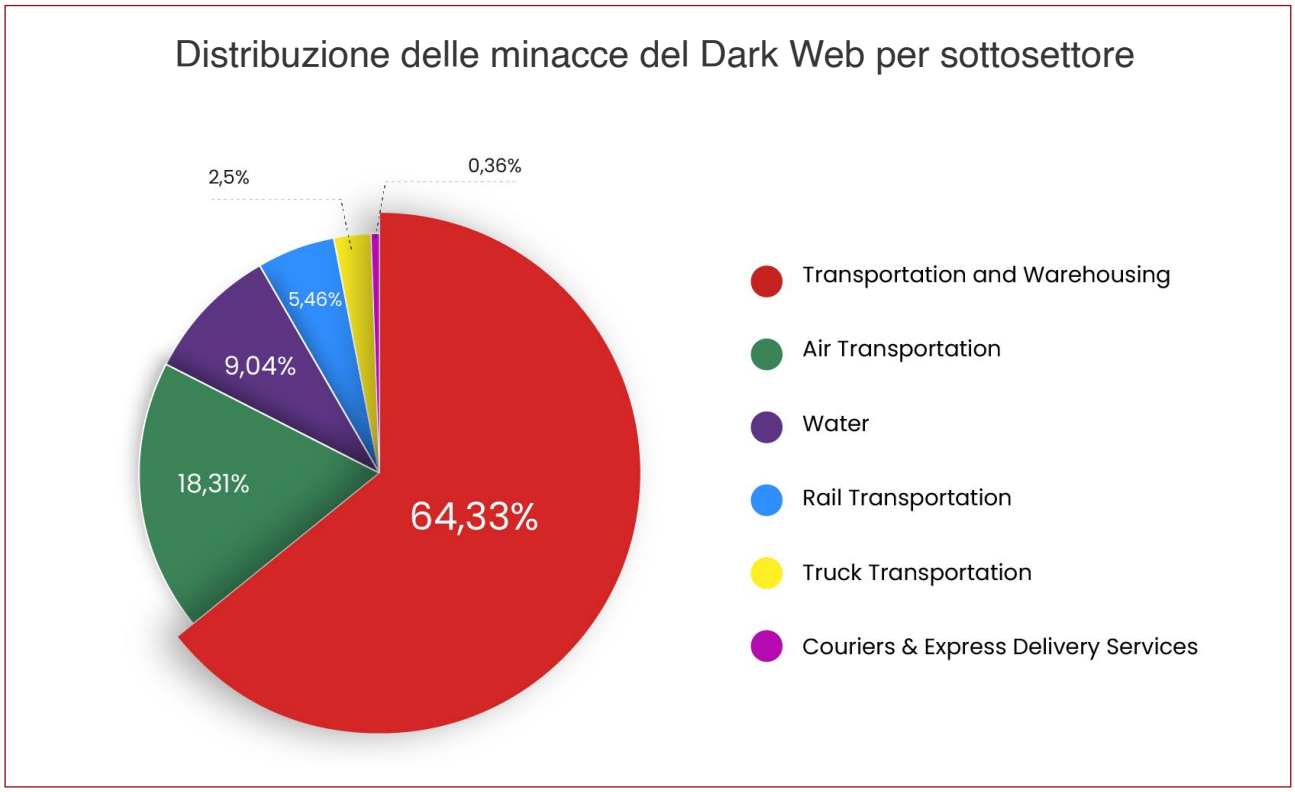
Dark Web Threats

Il settore ***Transportation and Warehousing*** risulta essere il più colpito **(64,33%)**, a conferma del fatto che i cybercriminali mirano principalmente a generare **interruzioni estese nella supply chain,** con un focus particolare sui fornitori di logistica terzi (*third-party logistics providers*) e sui sistemi di gestione dei magazzini (*warehouse management systems*).

Segue il comparto ***Air Transportation*** (**18,31%**), verosimilmente a causa della natura critica delle operazioni aeree e del valore dei dati relativi a passeggeri e carichi. I settori *Water* (9,04%) e *Rail Transportation* (5,46%) registrano un numero inferiore di attacchi, ma restano comunque rilevanti in quanto componenti fondamentali del commercio globale e della movimentazione delle merci.

I segmenti *Truck Transportation* (2,50%) e *Couriers & Express Delivery Services* (0,36%) evidenziano una **minore esposizione**, suggerendo una **superficie d'attacco digitale più limitata** o dati meno appetibili dal punto di vista economico per gli attori delle minacce.

Questa distribuzione evidenzia la necessità di rafforzare le misure di **cybersecurity nei principali snodi logistici e nelle reti della supply chain**, con particolare attenzione ai magazzini e ai fornitori di trasporto su larga scala



Fonte 3

Gli **Stati Uniti** (13,72%) risultano essere il Paese più colpito, verosimilmente a causa dell'estesa infrastruttura logistica nazionale e della presenza di hub strategici per la supply chain globale. Segue l'**Ucraina** (4,57%), la cui posizione è presumibilmente legata a dinamiche di **cyber warfare** geopolitico e ad attacchi mirati alle reti di trasporto critiche.

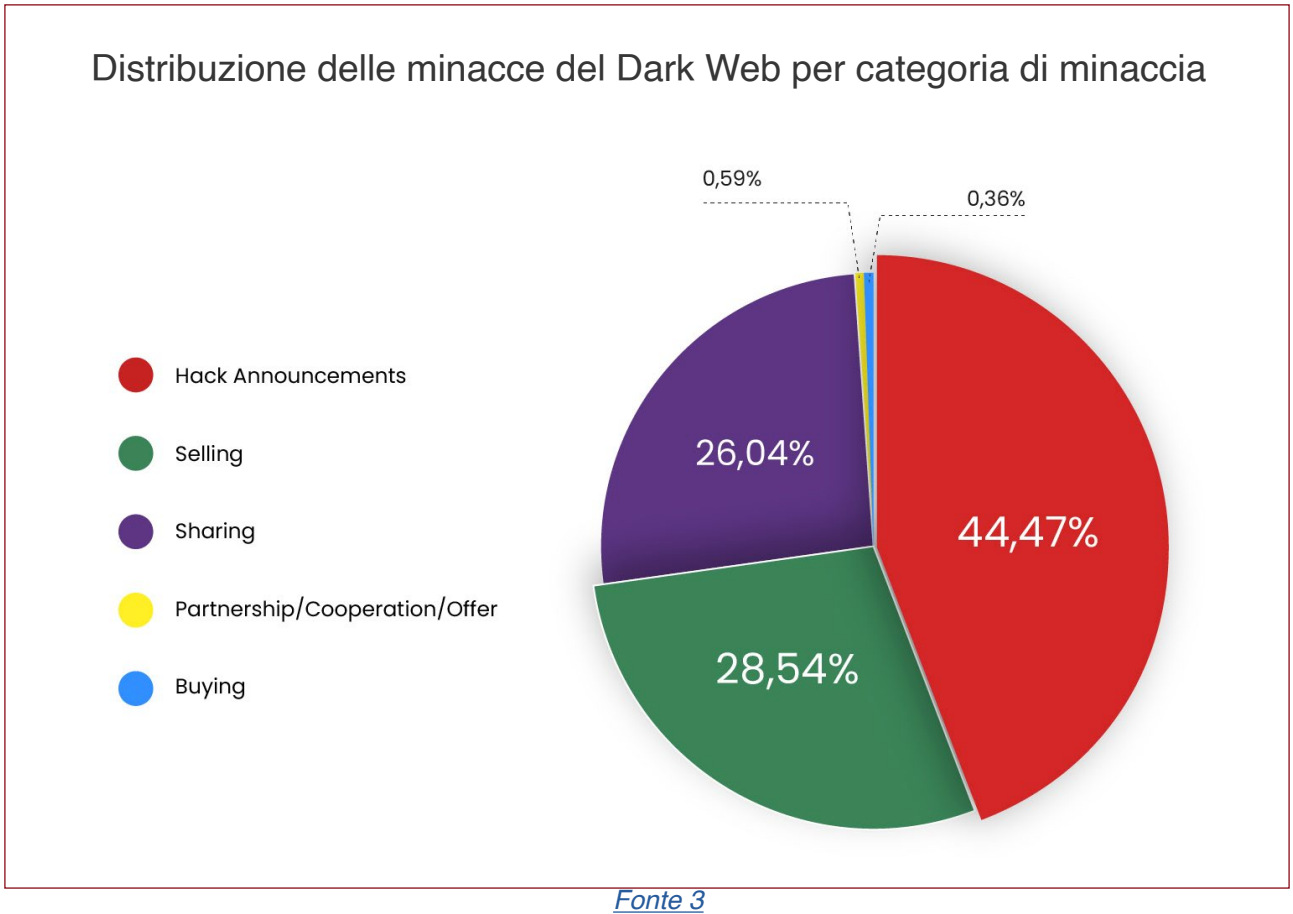
Questi dati indicano che gli attori delle minacce tendono a colpire le **grandi economie** e le **aree geopoliticamente instabili**, evidenziando l'urgenza di una c**ollaborazione regionale in ambito cybersecurity** e di una **condivisione trasversale dell'intelligence sulle minacce** all'interno del settore.

L'elevata percentuale di ***Hack Announcements*** (44,47%) mostra come i cybercriminali diano priorità alla pubblicizzazione delle violazioni, con l'obiettivo di **accreditarsi nella scena underground, intimidire le vittime** o **attirare acquirenti** interessati ai dati trafugati.

Le categorie ***Selling*** (28,54%) e ***Sharing*** (26,04%) indicano che le violazioni legate alla logistica spesso sfociano in attività di **monetizzazione o distribuzione gratuita dei dati sottratti,** aumentando il rischio di **credential stuffing**, **frodi** e **interruzioni della supply chain.**

Le categorie P***artnership/Cooperation/Offer*** (0,59%) e ***Buying*** (0,36%) risultano marginali, suggerendo che **acquisti diretti** o **forme di collaborazione tra attori malevoli** siano meno diffuse rispetto alle pratiche di vendita e divulgazione pubblica.

Questo trend sottolinea la necessità di adottare un approccio proattivo alla difesa informatica, con particolare attenzione a **monitoraggio delle violazioni, sorveglianza del dark web** e **intercettazione tempestiva dei dati compromessi**, al fine di prevenire l'utilizzo illecito delle informazioni sottratte.



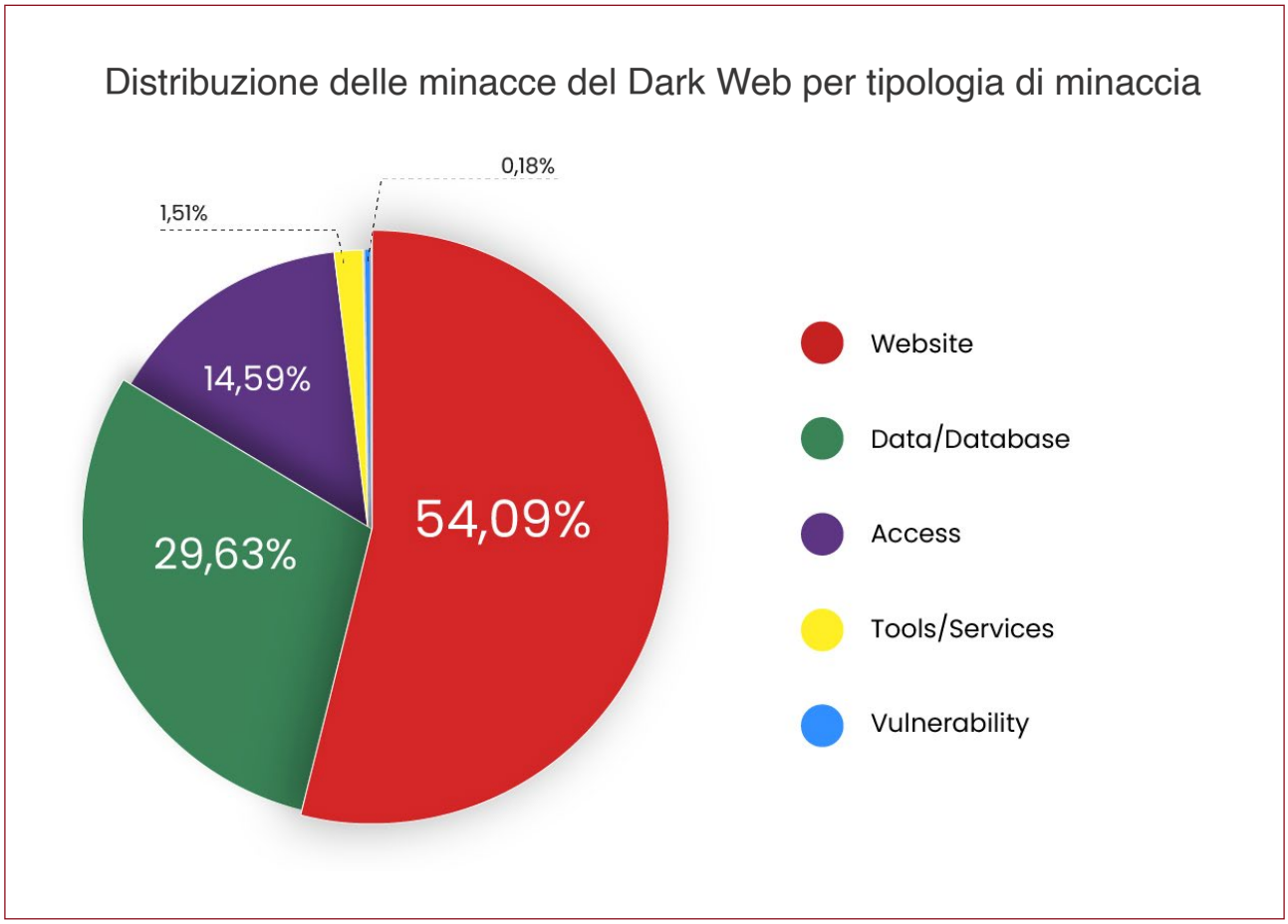
Fonte 3

La predominanza di contenuti relativi a ***Website*** (54,09%) evidenzia come i cybercriminali prendano frequentemente di mira – o discutano nei forum underground – **siti web compromessi del settore logistico**, potenzialmente per attività di **defacement, phishing o esfiltrazione di credenziali.**

I post classificati come **Data/Database** (29,63%) indicano un forte interesse per la vendita o la condivisione di **record sensibili sottratti**, tra cui **informazioni sui clienti, dettagli delle spedizioni o dati provenienti da sistemi logistici interni.**

La categoria ***Access*** (14,59%) suggerisce che gli attori delle minacce sono attivamente impegnati nella vendita o diffusione di **punti di accesso non autorizzati**, presumibilmente tramite **credenziali compromesse, accessi RDP/VPN**, o **presidi iniziali** all'interno delle reti aziendali.

Queste evidenze sottolineano l'importanza di implementare **misure avanzate** di sicurezza per i siti web, crittografia dei dati sensibili e **controlli rigorosi** sugli accessi, al fine di ridurre l'esposizione su forum e marketplace del dark web.



Fonte 3

Minacce Ransomware

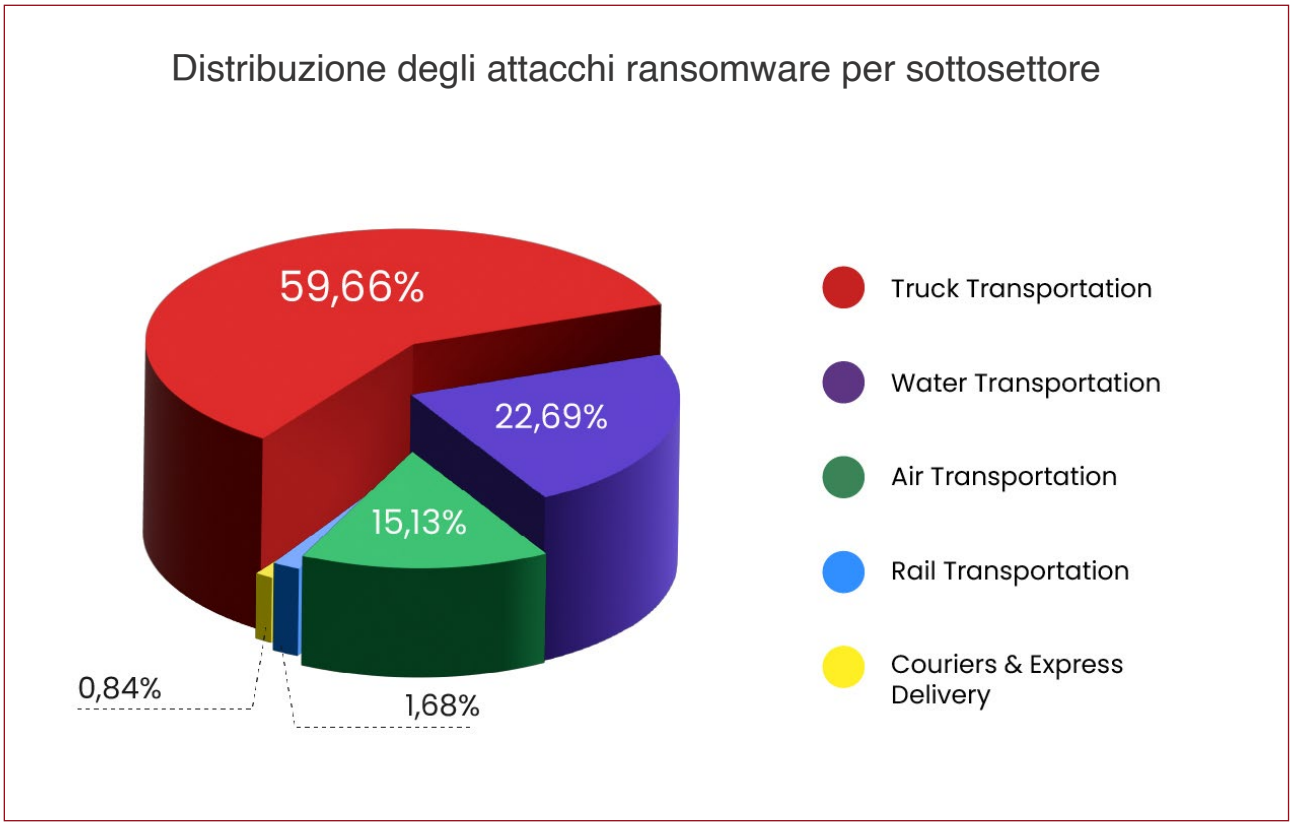
Il settore ***Truck Transportation*** risulta essere il principale obiettivo dei gruppi ransomware, con una quota del **59,66%**, verosimilmente a causa della forte dipendenza da sistemi digitali per la gestione della flotta, tracciamento GPS e coordinamento logistico. Il blocco di tali attività può generare gravi ritardi nella supply chain, aumentando la probabilità che le aziende colpite decidano di pagare il riscatto.

Anche i settori ***Water Transportation*** (22,69%) e ***Air Transportation*** (15,13%) risultano significativamente esposti, in linea con il loro ruolo critico nel commercio globale e nella mobilità di passeggeri e merci. Attacchi in questi ambiti possono tradursi in interruzioni operative nei porti, ritardi nei voli e blocchi nel traffico merci.

Al contrario, i settori ***Rail Transportation*** (1,68%) e ***Couriers & Express Delivery*** (0,84%) mostra-

no una bassa incidenza, probabilmente dovuta a una minore digitalizzazione o a misure di resilienza più efficaci.

Questa distribuzione evidenzia come i gruppi ransomware puntino a obiettivi ad alto impatto operativo e con potenziale di forte interruzione, rafforzando la necessità per le aziende logistiche di implementare **segmentazione della rete, backup regolari** e **sistemi di rilevamento delle minacce specifiche ransomware** all'interno delle loro strategie di cybersecurity.



Fonte 3

Gli **Stati Uniti** rappresentano la maggioranza assoluta degli incidenti ransomware nel settore (**53,85%**), un dato attribuibile all'estensione della rete di supply chain, all'elevata digitalizzazione delle piattaforme logistiche e alla presenza di obiettivi ad alto valore economico. Il Paese è quindi un bersaglio privilegiato per i gruppi ransomware, che puntano a interruzioni operative critiche e richieste di riscatto elevate.

La Croazia si posiziona sorprendentemente al secondo posto (**15,38%**), suggerendo potenziali attacchi mirati a infrastrutture marittime critiche o a hub logistici regionali strategici per il commercio europeo.

Il **Regno Unito** (**9,49%**) continua a registrare una minaccia costante, coerente con il suo ruolo chiave nel trasporto marittimo globale, nel cargo aereo e nelle operazioni di supply chain.

L'elevata concentrazione di attacchi negli Stati Uniti evidenzia come i gruppi ransomware prediligano economie **digitalmente avanzate** e ricche, rafforzando la necessità di **strategie di cyber-resilienza avanzate**, **capacità di risposta rapida agli incidenti** e **collaborazione intersettoriale** per contrastare queste minacce.

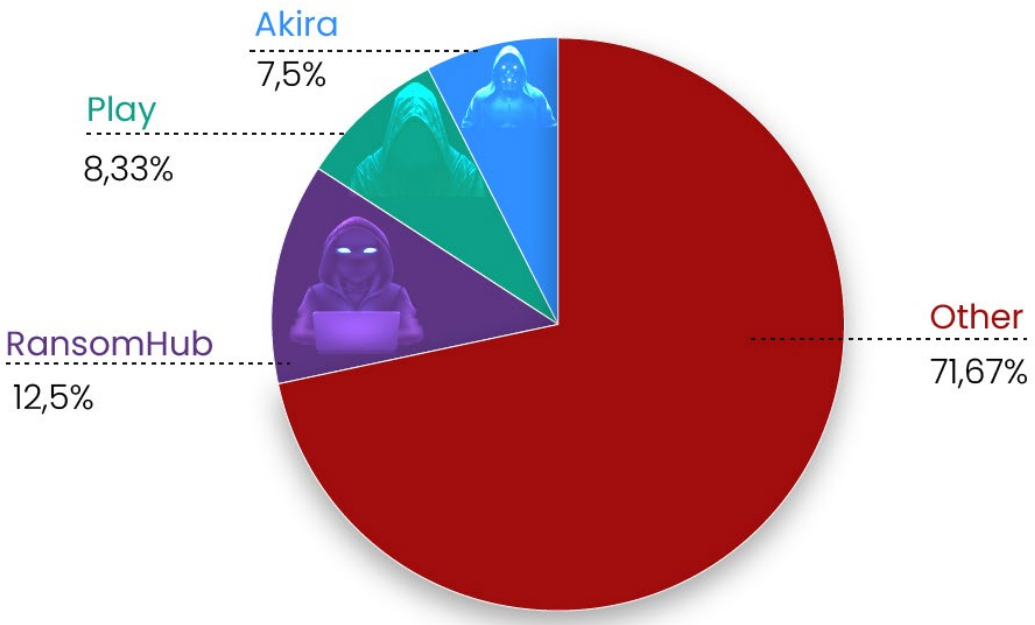
Principali Gruppi Ransomware

Il gruppo **RansomHub** emerge come il più attivo nel colpire il settore logistico (**12,5%**), grazie al suo focus su obiettivi ad alto valore e all'utilizzo di tecniche di doppia estorsione (esfiltrazione + cifratura dei dati).

Seguono **Play** (**8,33%**) e **Akira** (**7,5%**), entrambi noti per l'aggressività con cui colpiscono infrastrutture critiche e per l'impiego di payload ransomware personalizzati in grado di massimizzare l'interruzione operativa.

La categoria **Other** (**71,67%**) indica un panorama eterogeneo composto da numerosi gruppi ransomware minori o emergenti, che rendono più complesse le attività di rilevamento, analisi e mitigazione.

Questi dati confermano l'urgenza di adottare **strategie proattive di difesa ransomware**, tra cui **modelli di sicurezza zero trust**, **segmentazione della rete**, e **piani strutturati di incident response**, per fronteggiare un ecosistema di minacce in costante evoluzione.



Fonte 3

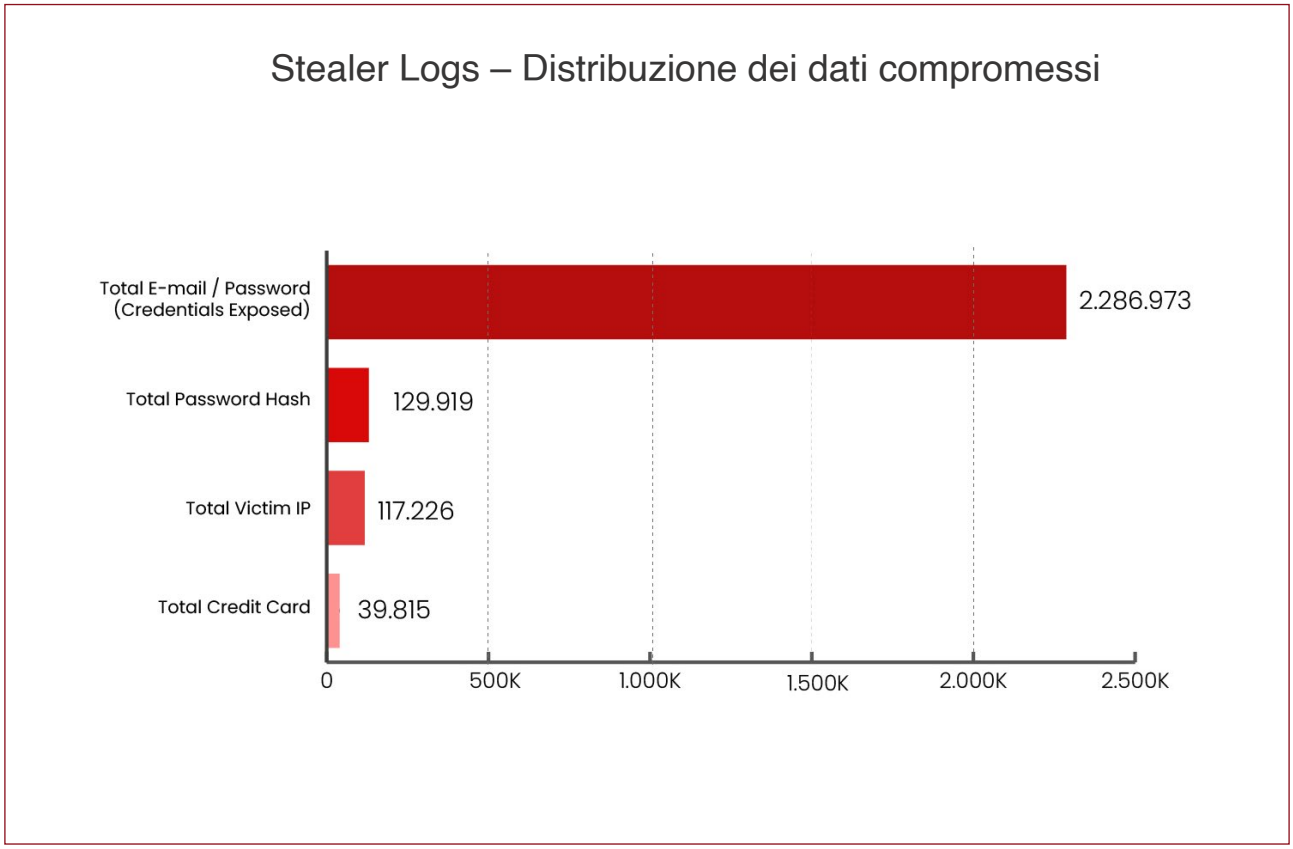
Stealer Logs

L'elevato volume di credenziali esposte (2,28 milioni) indica che un gran numero di dipendenti o contractor nel settore utilizza dispositivi compromessi, verosimilmente a causa di phishing, scarsa sicurezza o assenza di adeguate soluzioni di endpoint protection.

L'esposizione di 117.200 indirizzi IP delle vittime evidenzia un rischio significativo di attacchi mirati, poiché gli attori malevoli possono effettuare geolocalizzazione degli utenti, sfruttare vulnerabilità o condurre intrusioni successive nelle reti aziendali.

Le 39.800 carte di credito esposte indicano potenziali rischi di frodi finanziarie, presumibilmente connesse a piattaforme e-commerce della logistica, sistemi di pagamento aziendali o all'utilizzo di fuel card.

Questi dati sottolineano l'urgenza di implementare misure quali l'autenticazione multi-fattore (MFA), soluzioni avanzate di endpoint security e programmi di formazione mirati alla consapevolezza cyber-security del personale, al fine di mitigare le minacce derivanti dai malware stealer nel settore della logistica, in particolare in ambiti come transportation and warehouse.



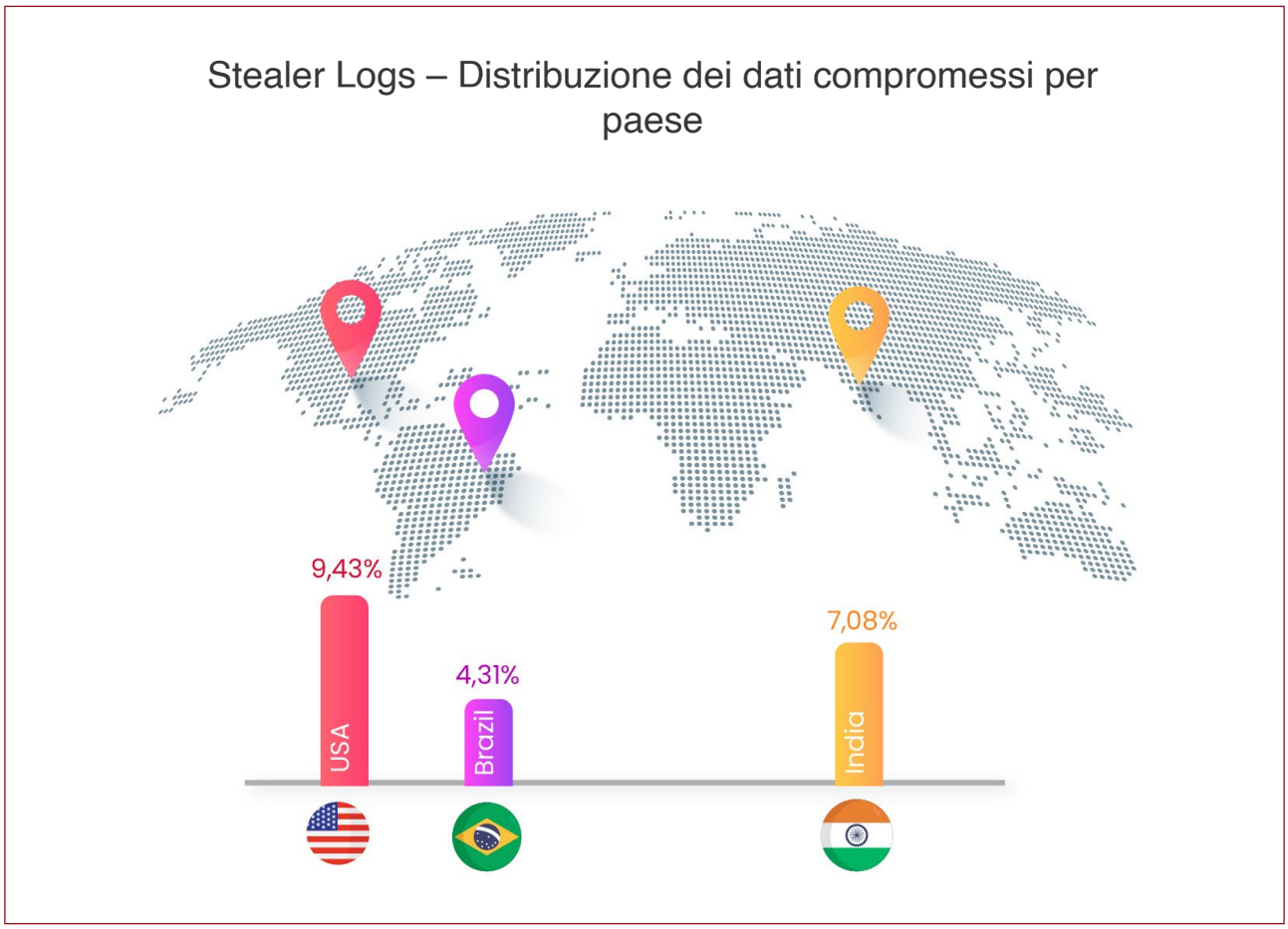
Fonte 3

Gli **Stati Uniti** (**9,43%**) registrano il più alto numero di infezioni da malware, probabilmente a causa dell'ampia forza lavoro nel settore e dell'elevata integrazione digitale nelle operazioni di supply chain. L'utilizzo, da parte dei dipendenti, di dispositivi personali o aziendali compromessi rappresenta un rischio significativo per la sicurezza dell'impresa.

Segue **l'India** (**7,08%**), che riflette il rapido sviluppo del settore e la presenza di una vasta forza lavoro; in questo contesto, lacune nella cyber hygiene e l'uso frequente di dispositivi personali per attività lavorative possono contribuire alla diffusione delle infezioni.

Il **Brasile** (**4,31%**) evidenzia una problematica regionale di cybercrime nell'infrastruttura logistica dell'America Latina, probabilmente correlata a un'intensificata trasformazione digitale e a protezioni endpoint insufficienti.

Questa distribuzione indica che i dipendenti nel settore, nei principali mercati globali, risultano frequentemente compromessi, rafforzando la necessità di adottare soluzioni avanzate di endpoint protection, controlli di accesso alle reti e meccanismi di autenticazione resistenti al phishing, al fine di prevenire ulteriori fughe di dati.



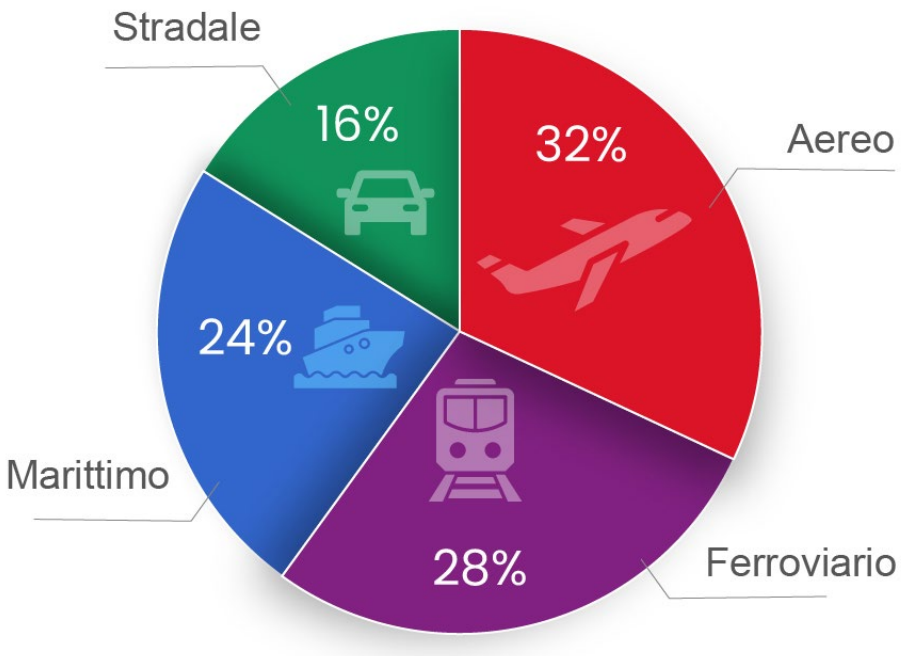
Fonte 3

Sottosettori

Distribuzione degli attacchi per sottosettore

All'interno del settore trasporti, gli attacchi non sono distribuiti uniformemente tra i vari sottosettori. Come illustrato nella Figura, a livlelo globale il trasporto aereo è il più colpito (32%), seguito dal ferroviario (28%), dal marittimo (24%) e dallo stradale (16%).

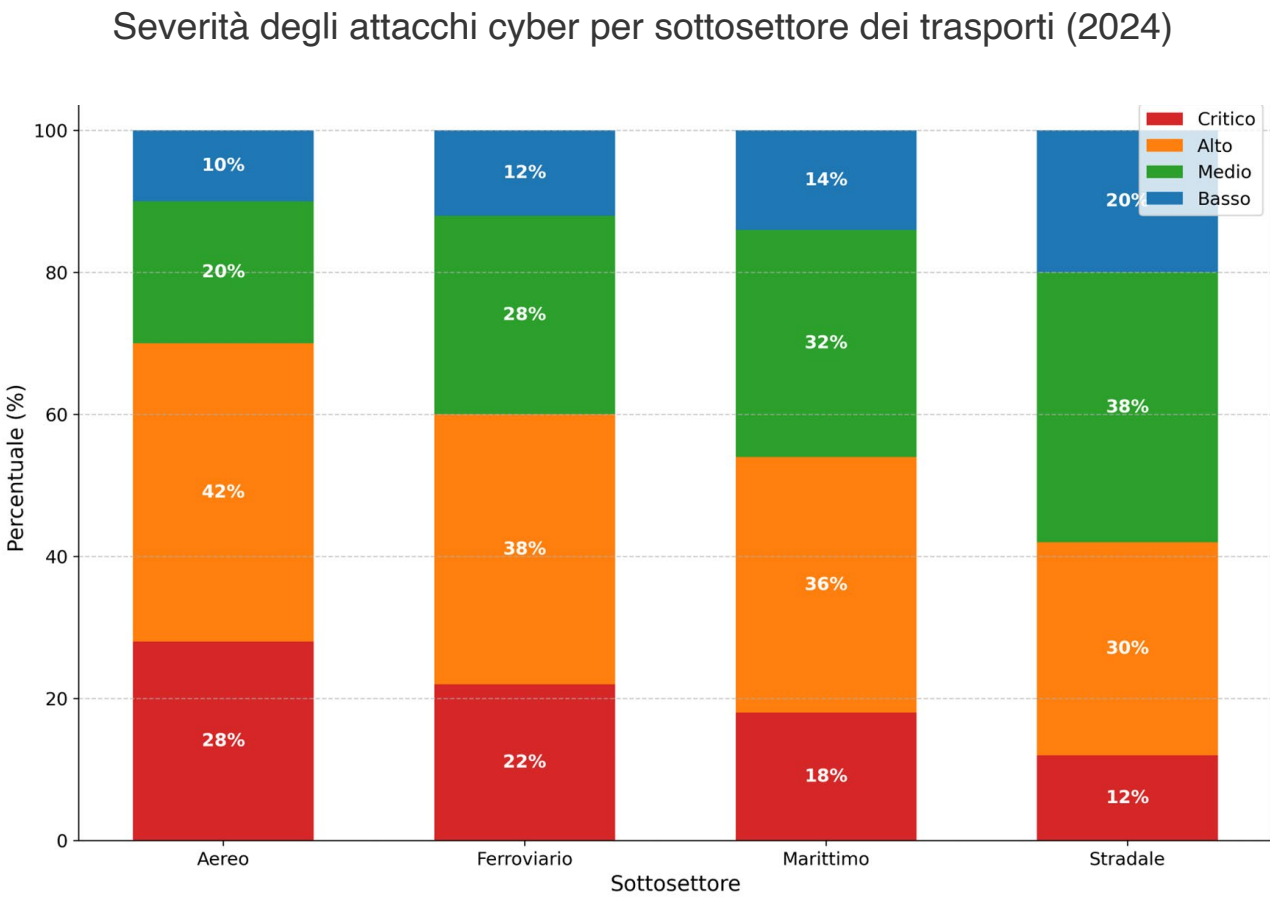
Distribuzione degli attacchi cyber per sottosettore dei trasporti (2024)



Questa distribuzione riflette sia il livello di digitalizzazione e interconnessione dei vari sottosettori, sia la loro criticità strategica ed economica. Il trasporto aereo, con i suoi sistemi altamente digitalizzati e la sua importanza strategica, rappresenta un target particolarmente appetibile. Il trasporto stradale, nonostante sia il sottosettore con la minore percentuale di attacchi, sta registrando un incremento significativo con la crescente adozione di sistemi di trasporto intelligenti (ITS) e veicoli connessi.

Severità degli attacchi

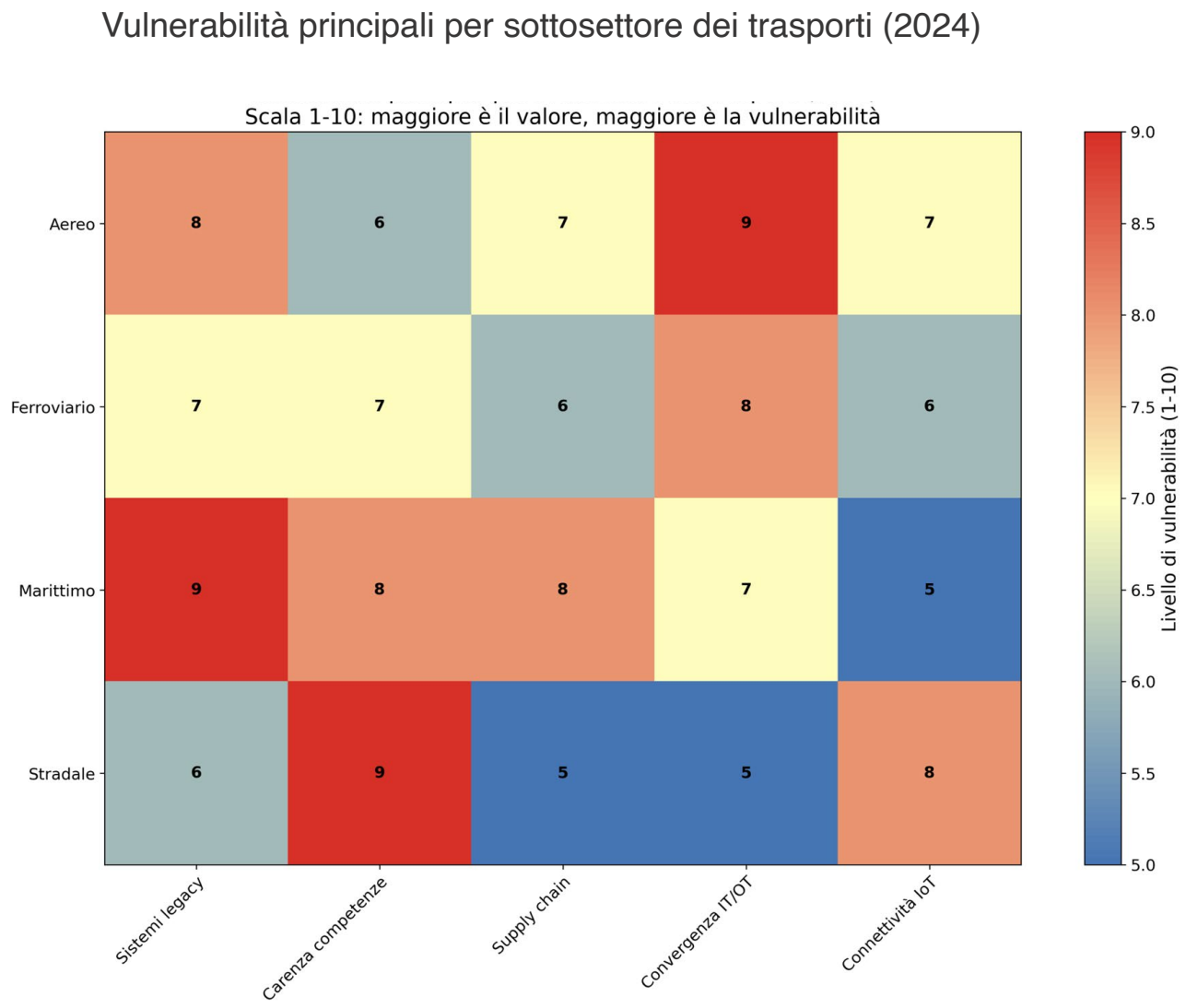
La severità degli attacchi varia significativamente tra i diversi sottosettori del trasporto, come mostrato nella Figura. Il trasporto aereo non solo è il più colpito in termini di volume, ma registra anche la maggiore percentuale di attacchi critici (28%), seguito dal ferroviario (22%).



La maggiore severità degli attacchi al trasporto aereo è attribuibile alla criticità dei sistemi coinvolti e al potenziale impatto sulla sicurezza dei passeggeri e delle operazioni. Il trasporto stradale, pur avendo la minore percentuale di attacchi critici (12%), presenta la maggiore percentuale di attacchi di media e bassa severità, spesso finalizzati al furto di dati o a interruzioni temporanee del servizio.

Vulnerabilità principali per sottosettore

La figura illustra le principali vulnerabilità per ciascun sottosettore del trasporto, evidenziando come diversi fattori di rischio abbiano un impatto differente a seconda del contesto specifico.



Aviazione

Nel 2024, si sono verificati importanti attacchi ransomware che hanno colpito infrastrutture critiche nei settori trasporti e aerospaziale, evidenziando tendenze e tecniche sofisticate di intrusione.

Gruppo Ransomware	Data	Obiettivo	Descrizione Sintetica
Akira	Luglio	Aeroporto croato	Ha causato il blocco totale dell'infrastruttura IT, con conseguenti cancellazioni e deviazioni di voli. Accesso iniziale tramite SSH, possibile sfruttamento di CVE-2023-27532 (Veeam Backup). Uso di LOLBAS per esfiltrazione dati e movimento laterale. Attacco critico a infrastruttura nazionale.
Helldown	Agosto	Azienda statunitense del settore aerospaziale	Data breach con accesso a dati sensibili (NDA, dati dipendenti, finanziari). Vettori sospetti: phishing, software non aggiornato o vulnerabilità nella supply chain. Indagine in corso.
Fancy Bear (APT28)	Settembre	Organizzazione tedesca per il controllo del traffico aereo	Breach sulla infrastruttura IT amministrativa (non ha impattato il controllo del traffico aereo). Attacco attribuito a APT28, gruppo legato al GRU russo, con attività di cyber-spionaggio. Indagine in corso su entità e impatto della compromissione.

Attività APT:

MuddyWater ha intensificato le attività di cyber-spionaggio nel settore aviazione, con focus sul Medio Oriente.

Ha utilizzato campagne spear-phishing per distribuire il malware custom **BugSleep** tramite strumenti legittimi RMM (es. Atera, ScreenConnect).

Ha ottenuto accesso persistente per monitorare e controllare sistemi compromessi di compagnie aeree.

Il trasporto aereo presenta vulnerabilità specifiche nei seguenti ambiti:

- **Sistemi di controllo del traffico aereo (ATC):** dipendenza da sistemi GPS vulnerabili a jamming e spoofing; comunicazioni terra-aria intercettabili; sistemi radar vulnerabili a interferenze.
- **Sistemi aeroportuali:** database passeggeri target di attacchi per furto dati; sistemi di controllo accessi e gestione bagagli vulnerabili a interruzioni.
- **Aeromobili:** avionica di bordo interconnessa; sistemi di intrattenimento in volo come potenziali punti di ingresso; comunicazioni satellitari intercettabili.

Strade e ferrovie

Il trasporto stradale ha subito il 24% degli attacchi nel settore trasporti in Europa. Il ransomware è la principale minaccia per questo sottosettore, rappresentando il 43% dei casi.

Il trasporto ferroviario presenta un livello di maturità cyber intermedio, con vulnerabilità specifiche:

- **Sistemi di segnalamento e controllo:** ERTMS/ETCS con potenziali vulnerabilità nei componenti software; sistemi di interlocking compromettibili; sale operative centralizzate come single point of failure.
- **Materiale rotabile:** sistemi digitali di bordo per gestione trazione, freni e ausiliari; connettività Wi-Fi come punto di ingresso; sistemi di manutenzione predittiva che creano nuove superfici di attacco.
- **Infrastruttura:** sottostazioni elettriche controllate da sistemi SCADA vulnerabili; reti di telecomunicazione dedicate compromettibili; passaggi a livello automatici manipolabili.

Il settore stradale è quello meno maturo dal punto di vista della sicurezza informatica:

- **Sistemi di trasporto intelligenti (ITS):** sistemi di gestione traffico e semaforica manipolabili; pannelli a messaggio variabile compromettibili; sistemi di pedaggio elettronico vulnerabili a frodi.
- **Veicoli connessi e autonomi:** molteplici ECU interconnesse; comunicazioni V2X che creano nuove superfici di attacco; sistemi di guida autonoma ingannabili.
- **Infrastruttura:** stazioni di ricarica elettrica compromettibili; sistemi di monitoraggio strutturale manipolabili; sistemi di emergenza disabilitabili.

Marittimo

Il comparto marittimo, con una quota del 18%, si conferma come una superficie d'attacco critica per la logistica globale, con minacce che includono sia il sabotaggio dei sistemi OT (Operational Technology), sia il furto di informazioni sensibili relative a carichi e rotte. Nel corso del 2024, la maggior parte delle minacce informatiche ha avuto origine non da tecniche di hacking avanzate, bensì dall'utilizzo di credenziali legittime compromesse, quali password sottratte, riutilizzate o configurate con valori di default. È stato osservato che un'ampia porzione degli attacchi si è concretizzata attraverso vettori di accesso remoto. L'impiego di strumenti come VPN e Remote Desktop Protocol (RDP) per il collegamento tra unità navali e team IT a terra o terze parti ha generato superfici d'attacco sfruttate attivamente dagli operatori malevoli.

Una criticità ricorrente riguarda le vulnerabilità di sistemi esposti quali firewall di bordo e software di gestione operativa delle navi, spesso caratterizzati da scarsa frequenza di aggiornamento dovuta a connettività intermittente. Tali condizioni favoriscono l'exploit di vulnerabilità note. Gli endpoint di bordo, come antivirus e firewall, hanno rilevato attività anomale riconducibili a esecuzione di script malevoli o comunicazioni covert verso server esterni.

La telemetria raccolta indica un incremento significativo delle attività di botnet dirette verso l'infrastruttura digitale marittima, dove la convergenza tra sistemi OT (Operational Technology), piattaforme di bordo connesse e infrastrutture IT a terra amplifica la superficie di attacco. Le botnet più frequenti nell'H2 2024 sono risultate:

- Torpig/Mebroot (31%)
- Mozi (19%)
- Mirai (14%)
- SystemBC (13%)
- Prometei (10%)
- UDPoS (8%)
- Bladabindi (2%)

L'impatto primario delle botnet a bordo consiste nell'uso illecito delle risorse di sistema per attività come il cryptomining o l'esecuzione di attacchi di tipo Denial of Service (DoS), i quali provocano rallentamenti operativi e sovraccarico delle risorse. Sebbene tali attacchi non compromettano direttamente i sistemi di navigazione o sicurezza, generano degrado delle prestazioni di rete, riduzione della banda satellitare disponibile e ampliano il rischio di compromissioni successive più gravi.

Nell'H2 2024, i principali gruppi APT (Advanced Persistent Threat) e cybercriminali che hanno preso di mira il settore marittimo sono i seguenti:

Gruppo	Attività principali	Obiettivi specifici nel settore marittimo	Tecniche principali utilizzate
APT28 (Fancy Bear)	Cyber spionaggio e sabotaggio infrastrutturale	Enti governativi, difesa, infrastrutture critiche tra cui operazioni marittime	Attacchi mirati a infrastrutture critiche, cyber spionaggio
APT41 (Winnti)	Spionaggio e attacchi finanziari	Organizzazioni marittime, furto dati sensibili, proprietà intellettuale, ransomware	Malware avanzato, operazioni ransomware, furto dati
Lazarus Group	Guadagno finanziario e spionaggio	Compagnie di navigazione, reti logistiche, istituti finanziari	Malware sofisticato, social engineering
APT34 (OilRig)	Spionaggio e furto dati	Infrastrutture critiche, supply chain marittima	Campagne phishing, malware custom
APT10 (Stone Panda)	Cyber spionaggio	Entità marittime, organizzazioni commerciali, reti logistiche	Exploit vulnerabilità software, raccolta intelligence
APT33 (Elfin)	Spionaggio e sabotaggio	Settore marittimo ed energetico	Phishing, malware
APT29 (Cozy Bear)	Campagne di spionaggio a lungo termine	Organizzazioni marittime, agenzie governative, istituti di ricerca	Spear phishing, zero-day exploits
Iridium	Spionaggio e sabotaggio operativo	Infrastrutture critiche marittime	Malware avanzato, attacchi mirati
SideWinder	Spionaggio e raccolta dati	Enti governativi, militari e marittimi	Phishing, malware custom
Mustang Panda	Spionaggio, sorveglianza e furto dati	Enti governativi, ONG, settori critici tra cui marittimo ed energetico	Spear phishing, exploit vulnerabilità, malware

I principali gruppi ransomware che hanno preso di mira organizzazioni del settore marittimo nell'H2 sono stati identificati come segue:

Gruppo	Descrizione e tattiche principali	Tecniche di accesso e modalità di attacco
RansomHub	Gruppo Ransomware-as-a-Service (RaaS) che cifra dati e richiede riscatto	Phishing e sfruttamento di vulnerabilità non patchate
8Base	Conosciuto per tattiche di doppia estorsione (dati criptati + minaccia di leak)	Phishing e vulnerabilità, mira a PMI
Blackout	Nuovo gruppo che cifra dati e richiede riscatti in criptovalute	Phishing e exploit su protocolli RDP
Akira	Specializzato in doppia estorsione, accede tramite credenziali VPN compromesse o phishing	Compromissione VPN e campagne phishing
Rhysida	Target infrastrutture critiche, usa metodi di cifratura sofisticati	Phishing e configurazioni RDP deboli
Play	Attivo e aggressivo, utilizza doppia estorsione	Sfruttamento vulnerabilità di applicazioni esposte su Internet
Cactus	Gruppo emergente, utilizza cifratura dati e richieste di riscatto	Sfruttamento VPN e phishing
Dragonforce	Campagne aggressive, cifratura dati e riscatti	Phishing e sfruttamento di sistemi non aggiornati
ElDorado	Specializzato in doppia estorsione con phishing e vulnerabilità RDP	Phishing e vulnerabilità RDP
LockBit 3.0	Tra i gruppi più prolifici, RaaS con cifratura veloce e doppia estorsione	Exploit vulnerabilità in sistemi esposti pubblicamente

La dipendenza del settore marittimo da sistemi legacy incrementa la sua esposizione a vulnerabilità note, frequentemente sfruttate dagli attori malevoli. Durante il secondo semestre, sono stati osservati attacchi che hanno preso di mira specifiche vulnerabilità di prodotti comunemente utilizzati.

Top 5 vulnerabilità note sfruttate da Threat Actors nel settore marittimo	CVE
ConnectWise ScreenConnect	CVE-2024-1709
Microsoft Outlook	CVE-2023-23397
Citrix NetScaler (ADC) e NetScaler Gateway	CVE-2023-3519
Apache Log4j2	CVE-2021-44228
Citrix Application Delivery Controller (ADC) e Gateway	CVE-2019-19781

Top 5 vulnerabilità note sfruttate da gruppi ransomware nel settore marittimo	CVE
FortiManager	CVE-2024-47575
Microsoft Outlook	CVE-2023-23397
Windows Common Log File System Driver	CVE-2023-28252
Citrix NetScaler (ADC) e NetScaler Gateway	CVE-2023-3519
Microsoft Netlogon Protocol	CVE-2020-1472

Durante il periodo analizzato, diversi strumenti legittimi sono stati sfruttati dai threat actors per eseguire attacchi sofisticati, bypassare controlli di sicurezza e mantenere l'accesso persistente nei sistemi compromessi:

PowerShell

WinSCP

AnyDesk

Metasploit

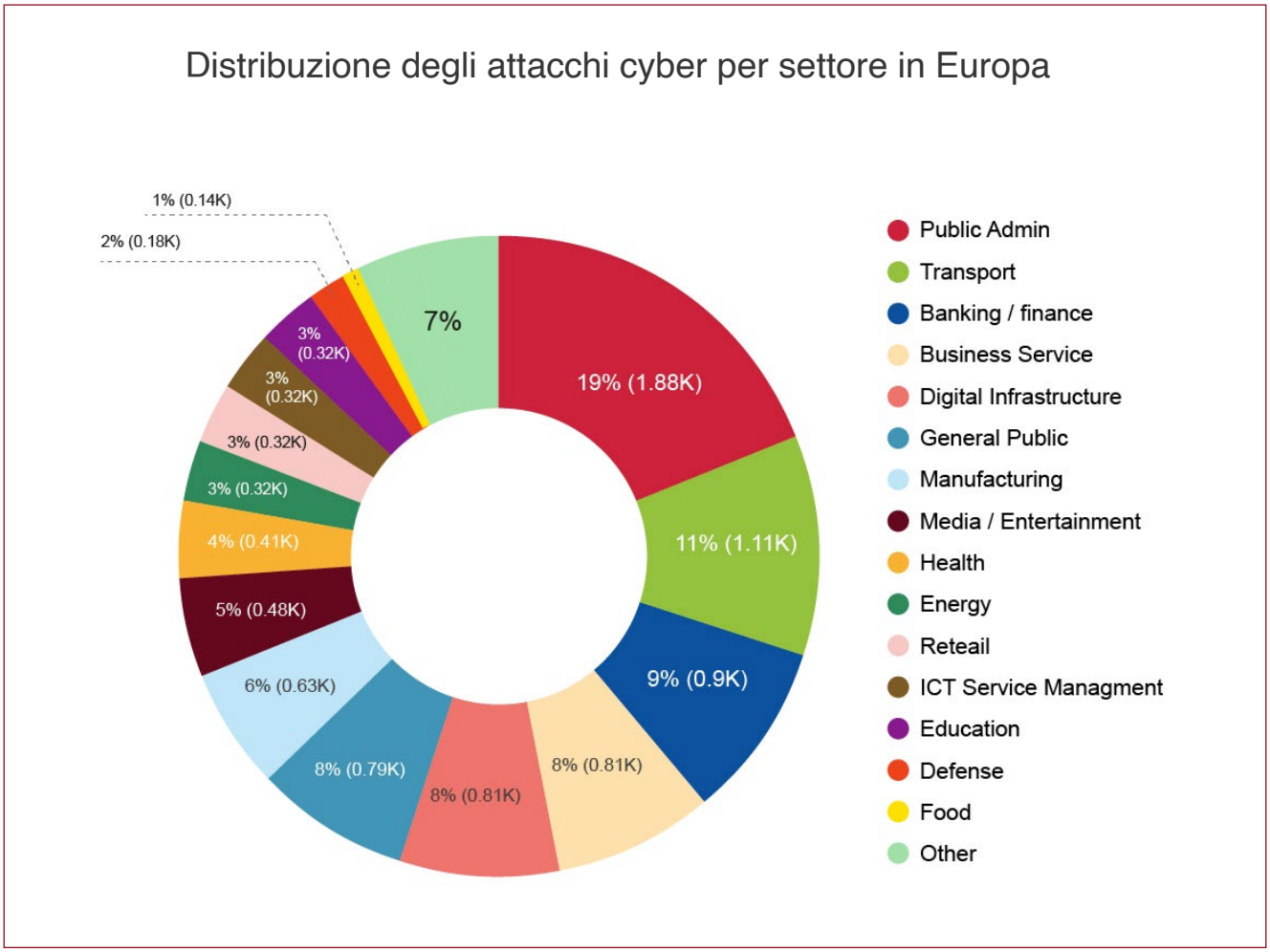
ScreenConnect

Cobalt Strike

Europa

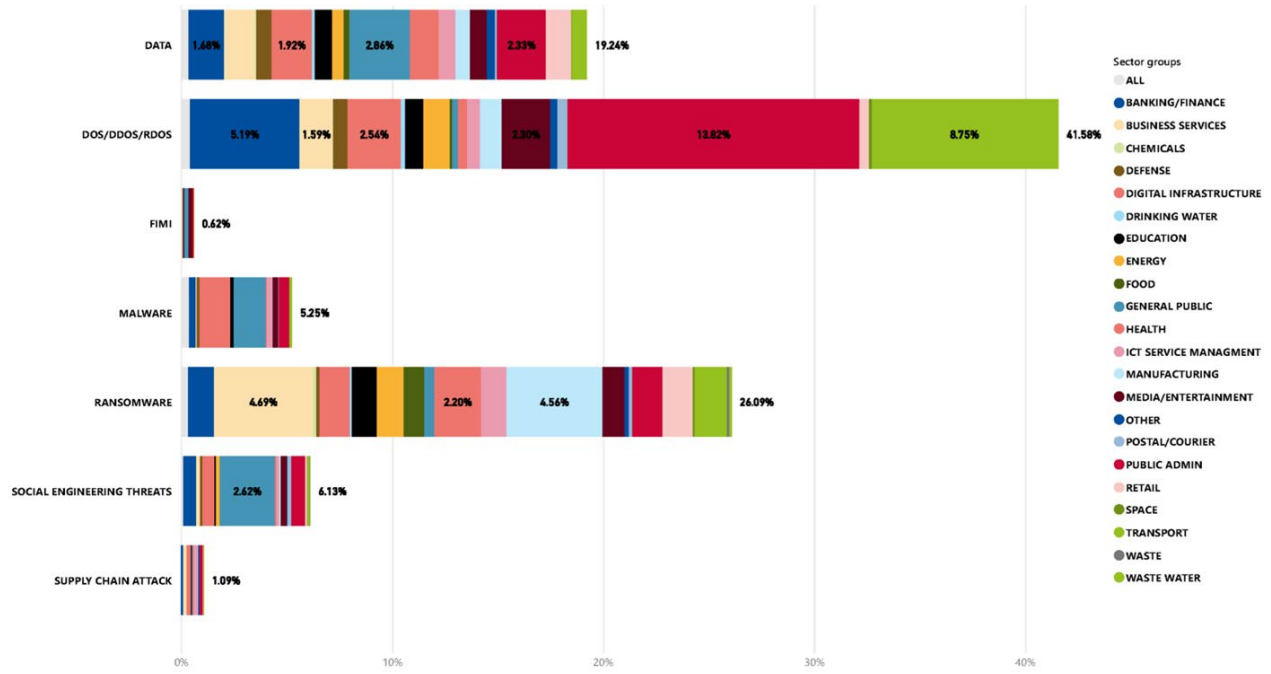
Secondo alcuni report, tra cui quello dall'agenzia europea ENISA, certifica che tra luglio 2023 e giugno 2024 il settore **transportation** è stato tra i tre più colpiti da offensive cyber.

Nel dettaglio, è stato evidenziato che i settori maggiormente impattati sono stati le organizzazioni della pubblica amministrazione (19%), il settore transportation (11%) e quello finanziario (9%). Le entità operanti nel settore transportation si sono classificate al secondo posto tra i bersagli di attacchi DDoS, rappresentando il 21% degli eventi registrati nel periodo di riferimento. Il settore dei trasporti si è dunque posizionato al secondo posto per numero di incidenti cyber nell'Unione Europea, con 1.110 incidenti segnalati, dietro solo alla pubblica amministrazione.



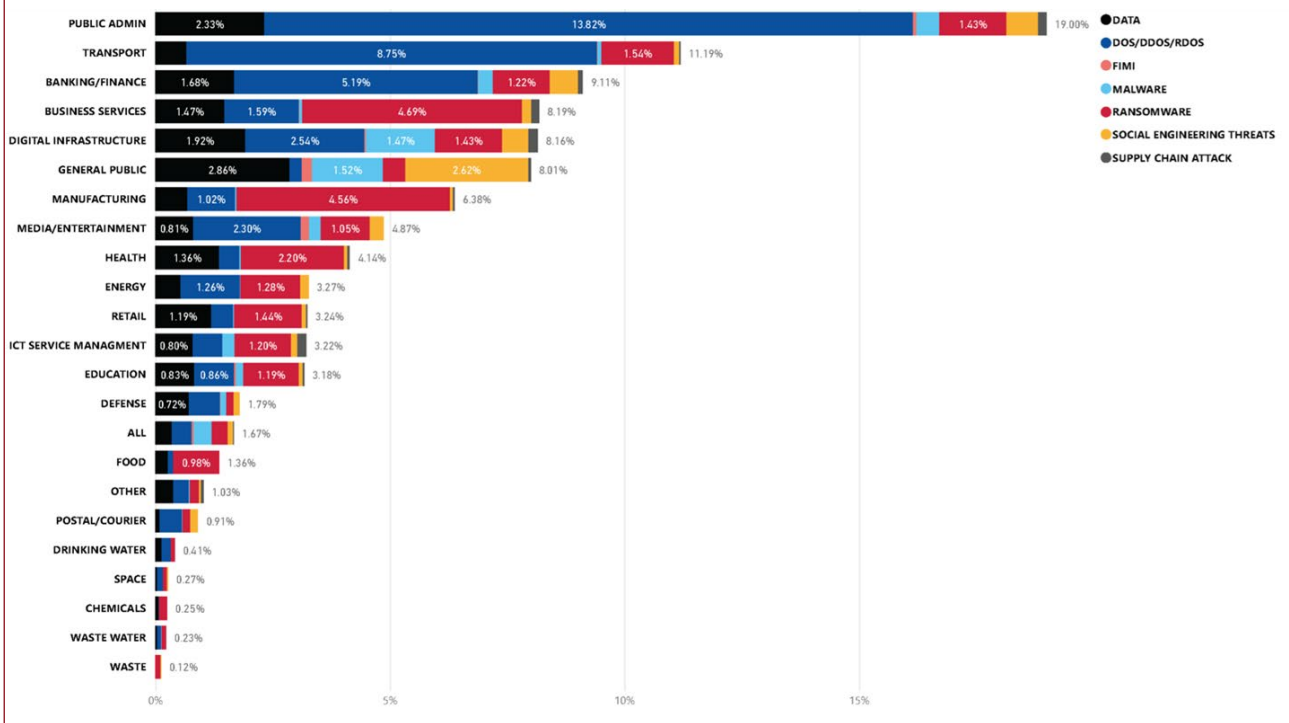
Fonte 4

Observed events related to prime ETL threats in terms of the affected sectors

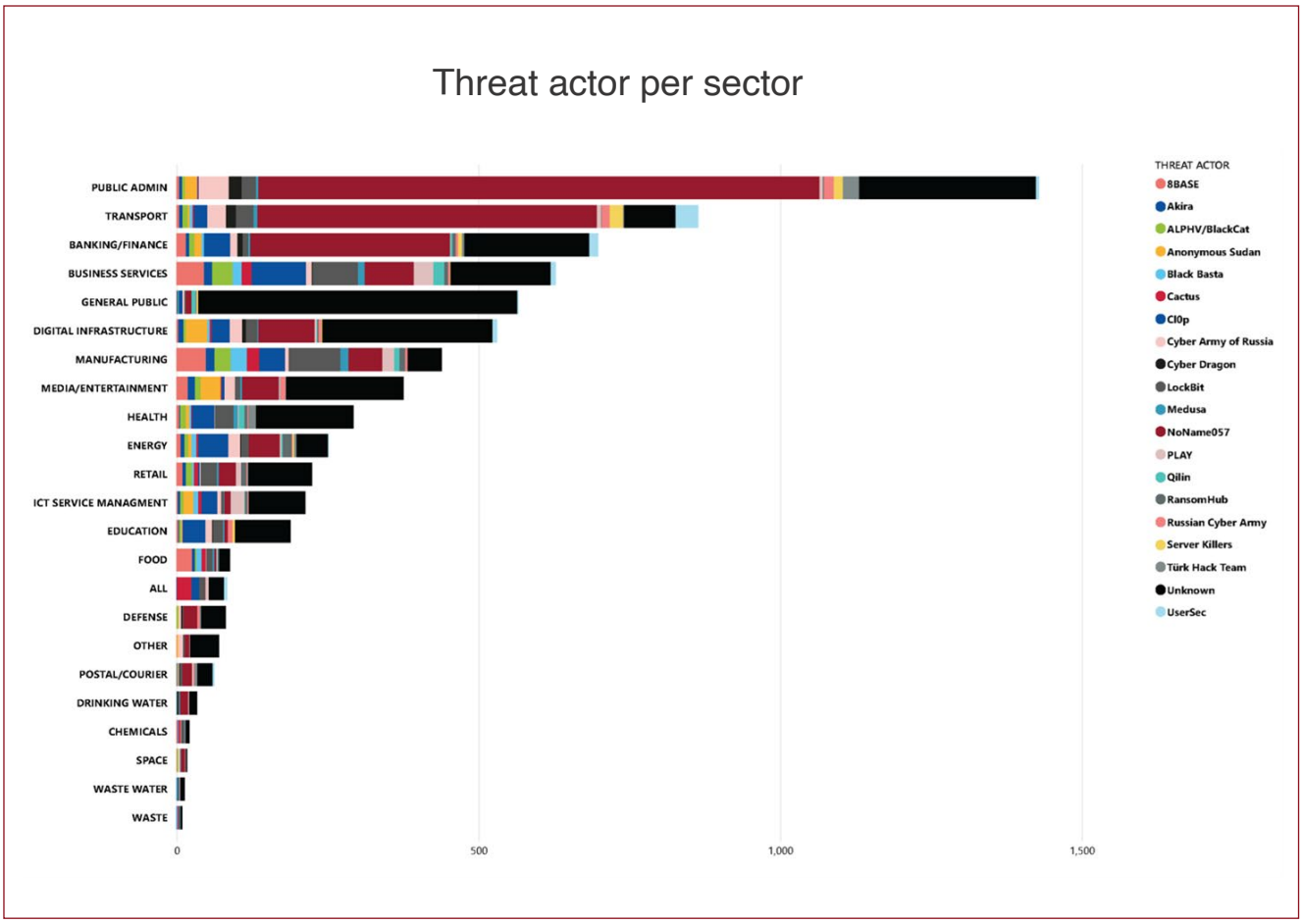


Fonte 4

ETL threats per sector



Fonte 4



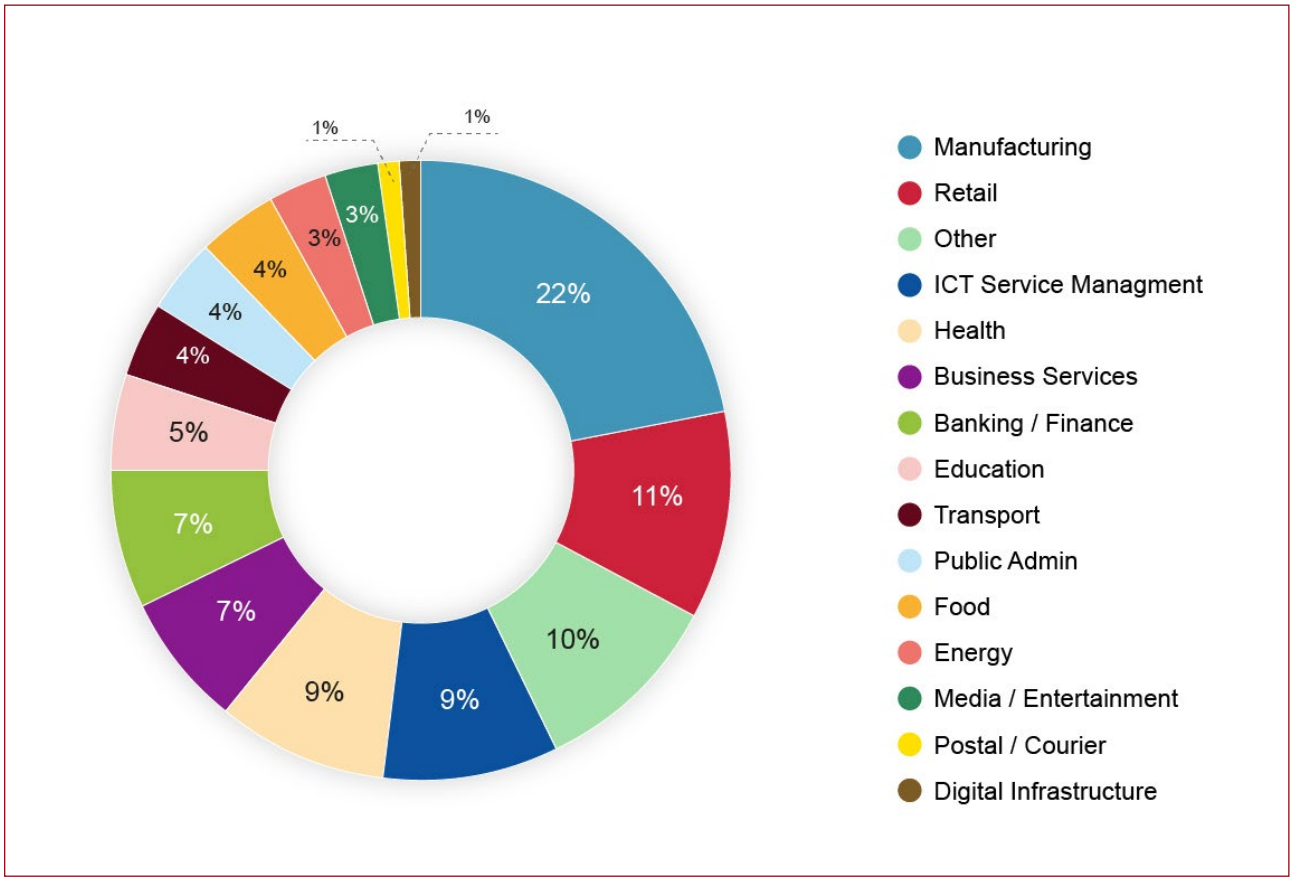
Fonte 4

Nell'analisi dei primi 20 threat actor "attivi" durante il periodo di riferimento, emerge nuovamente la tendenza degli attori a essere spesso sector-agnostic, ovvero distribuiti trasversalmente su molteplici settori. Analogamente al 2023, i gruppi di hacktivisti attivi continuano a privilegiare in particolare la pubblica amministrazione e il settore transport.

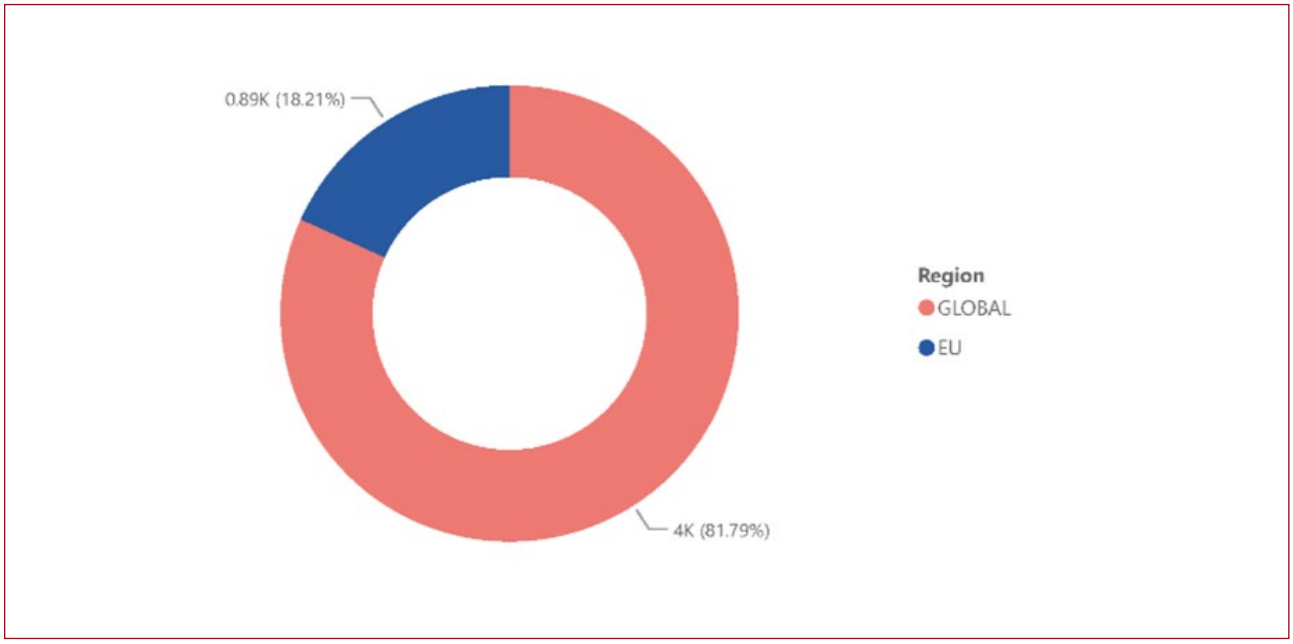
Altre analisi, partendo da quelle pubblicate nel marzo 2023, forniscono un'analisi dettagliata degli eventi cyber più rilevanti registrati tra gennaio 2021 e ottobre 2022, con un focus specifico sui segmenti aviazione, marittimo, ferroviario e stradale.

La distribuzione degli eventi evidenzia che la maggioranza degli attacchi si concentra su ransomware (38%) e violazioni di dati (30%), seguiti da malware (17%), attacchi Distributed Denial of Service (DDoS) e Ransom Denial of Service (RDoS) (16%), campagne di phishing e spear phishing (10%) e attacchi alla supply chain (10%).

RANSOMWARE - EU

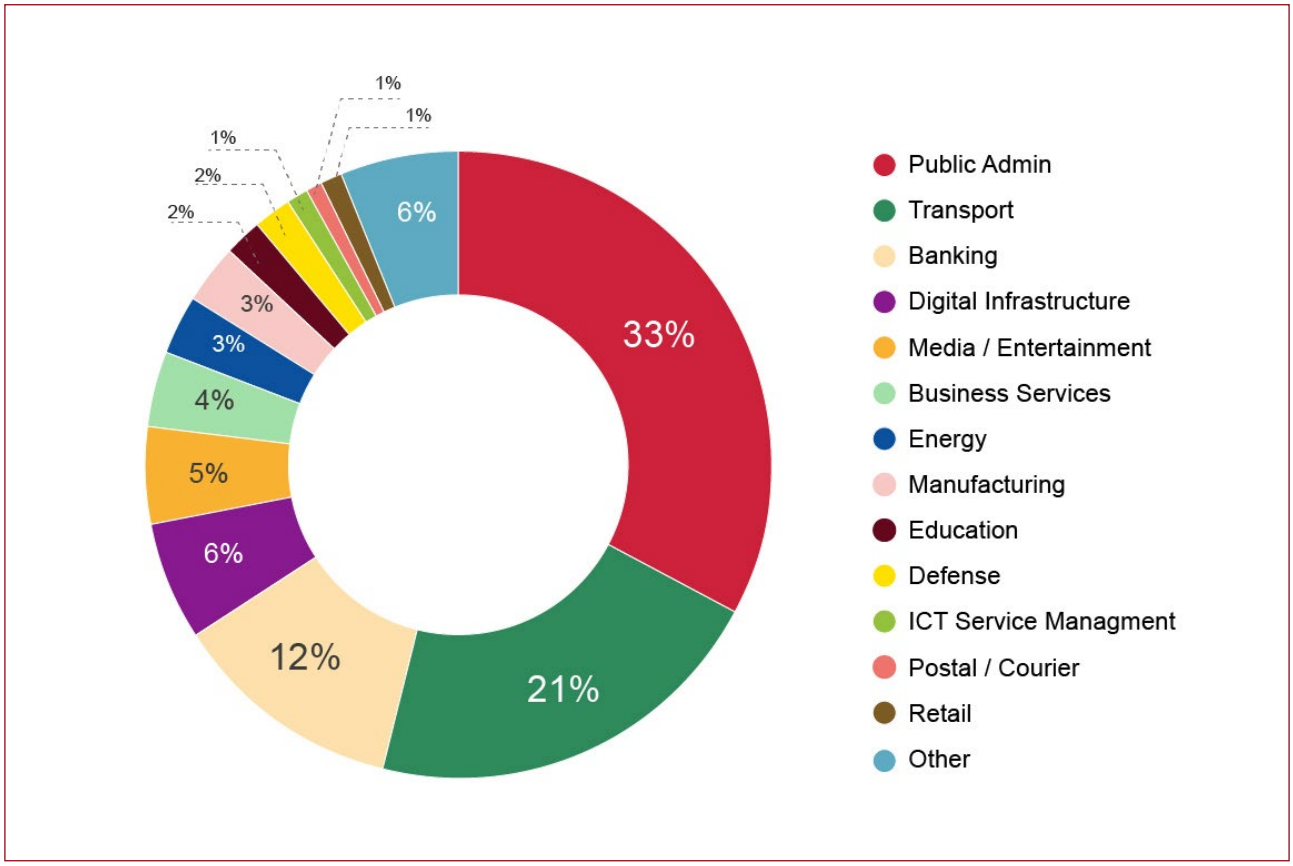


Fonte 4

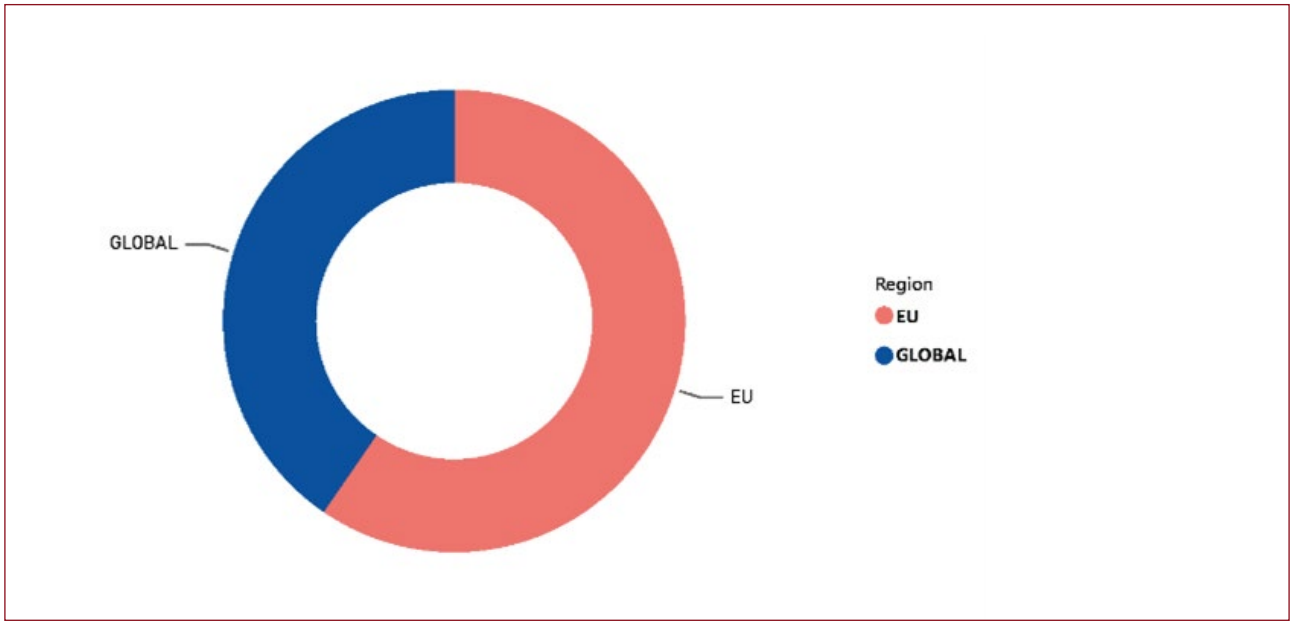


Fonte 4

DDOS - EU



Fonte 4



Fonte 4

ITALIA

Il settore della Logistica e dei Trasporti ha registrato una crescita significativa negli investimenti in cybersecurity, superando la media nazionale. Nel 2024, questo comparto ha visto un aumento della spesa di oltre il 25%. Questa accelerazione è stata in parte stimolata dalla Direttiva NIS2, che ha imposto nuovi obblighi e ha spinto le aziende a rafforzare le proprie difese. Sebbene non siano disponibili cifre monetarie specifiche per gli investimenti del settore trasporti nel biennio 2024-2025 , la percentuale di crescita elevata denota una chiara prioritarizzazione della sicurezza informatica. Il 53,8% delle aziende ha già pianificato investimenti in cybersecurity per il biennio 2025-2026 , indicando una tendenza positiva e una consapevolezza crescente.

La Direttiva NIS2 agisce come un catalizzatore primario per gli investimenti. La sua introduzione ha creato un legame diretto tra la pressione normativa e l'aumento della spesa in sicurezza. Tuttavia, la crescita, pur essendo notevole, potrebbe non essere sufficiente a colmare il divario di sicurezza esistente, considerando la vulnerabilità elevata del settore trasporti e la posizione dell'Italia nel G7. L'assenza di dati monetari specifici per il settore impedisce un confronto diretto con la dimensione complessiva del mercato, suggerendo che anche una percentuale di crescita elevata potrebbe tradursi in un investimento assoluto ancora relativamente modesto per un'infrastruttura così critica.

Confronto con la Media Nazionale e Altri Settori Critici

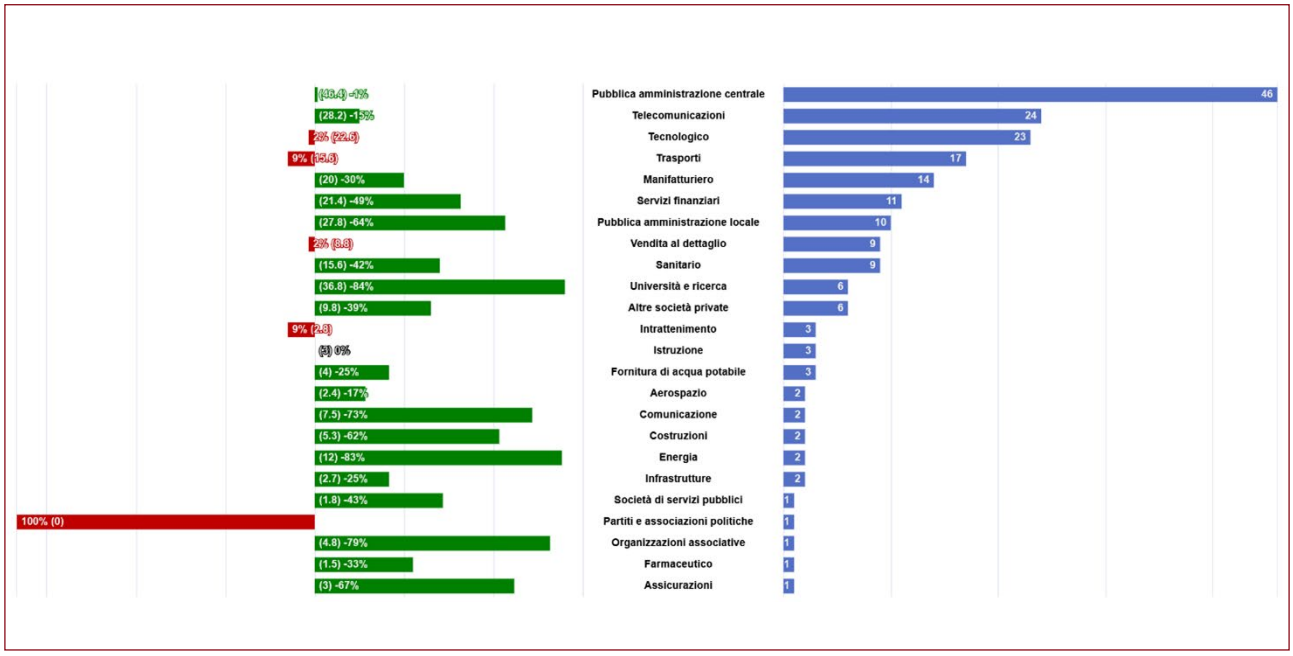
La crescita del 25% negli investimenti in cybersecurity nel settore trasporti nel 2024 supera significativamente la media nazionale del 15%. Altri settori che hanno registrato una crescita importante includono i Servizi (+24%), la Finanza e la Pubblica Amministrazione, quest'ultima beneficiando anche degli investimenti dell'Agenzia per la Cybersicurezza Nazionale (ACN). Questa dinamica riflette una risposta settoriale al profilo di rischio elevato e agli obblighi normativi. I settori direttamente interessati dalla NIS2, in particolare quelli classificati come "essenziali" come i trasporti, stanno reagendo con maggiore aggressività alle minacce percepite e alle nuove regolamentazioni rispetto al mercato generale. Questo potrebbe portare a un riequilibrio graduale della postura di cybersecurity nelle infrastrutture critiche nazionali, ma evidenzia anche potenziali disparità con settori meno regolamentati o meno consapevoli.

Il settore dei Trasporti e della Logistica in Italia ha visto una crescita degli attacchi, rappresentando il 7,3% di tutti gli attacchi nel 2024. Un aspetto particolarmente allarmante è che un quarto degli incidenti cyber globali nel settore Trasporti e Logistica ha avuto come obiettivo aziende italiane. Questo rende il comparto italiano dei trasporti e della logistica una "vittima preferenziale". A livello globale, il settore Trasporti e Logistica ha registrato un calo del 7% degli attacchi rispetto al 2023 , rendendo la proporzione italiana ancora più sorprendente. La combinazione di una quota sproporzionata di attac-

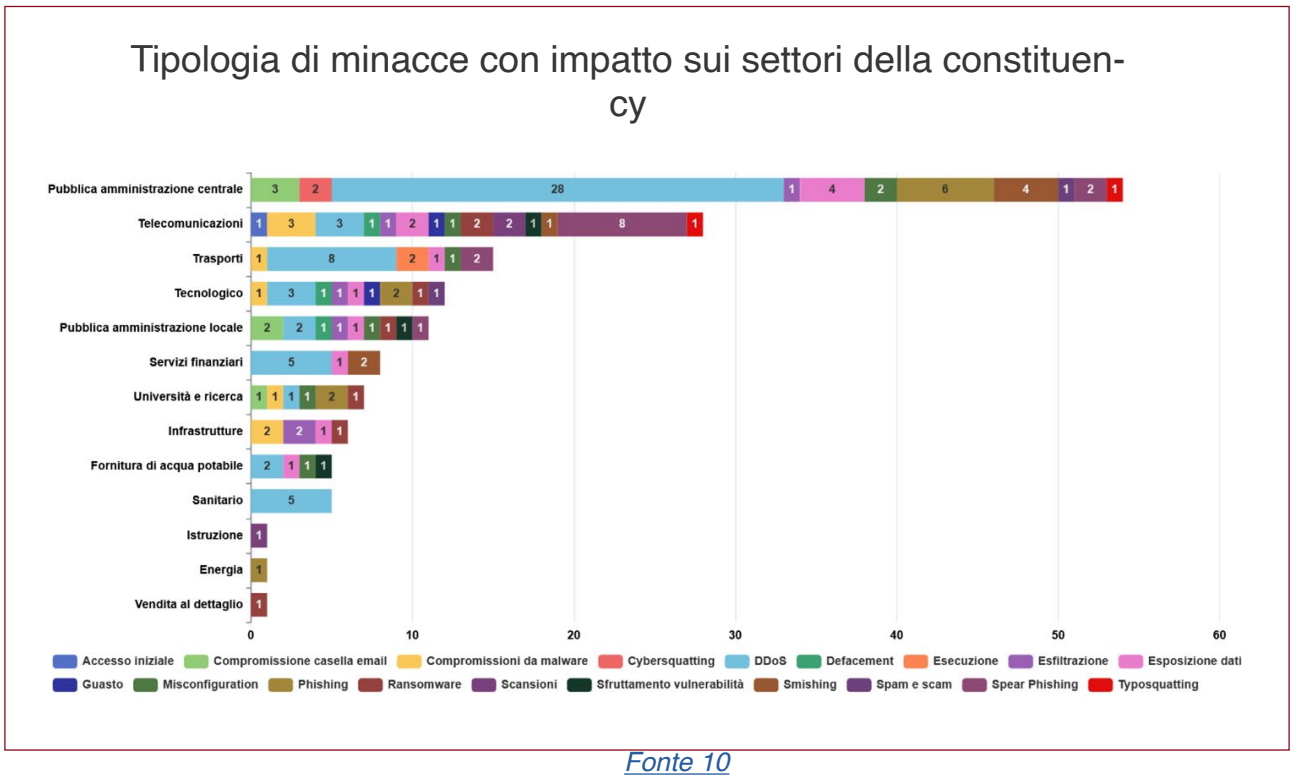
chi globali subiti dall'Italia e il fatto che un quarto degli attacchi al settore trasporti a livello mondiale colpisca entità italiane dipinge un quadro dell'Italia, e in particolare del suo settore trasporti, come un bersaglio altamente attraente e vulnerabile per i cybercriminali.

Di seguito gli attacchi in Italia nel Q1 2025:

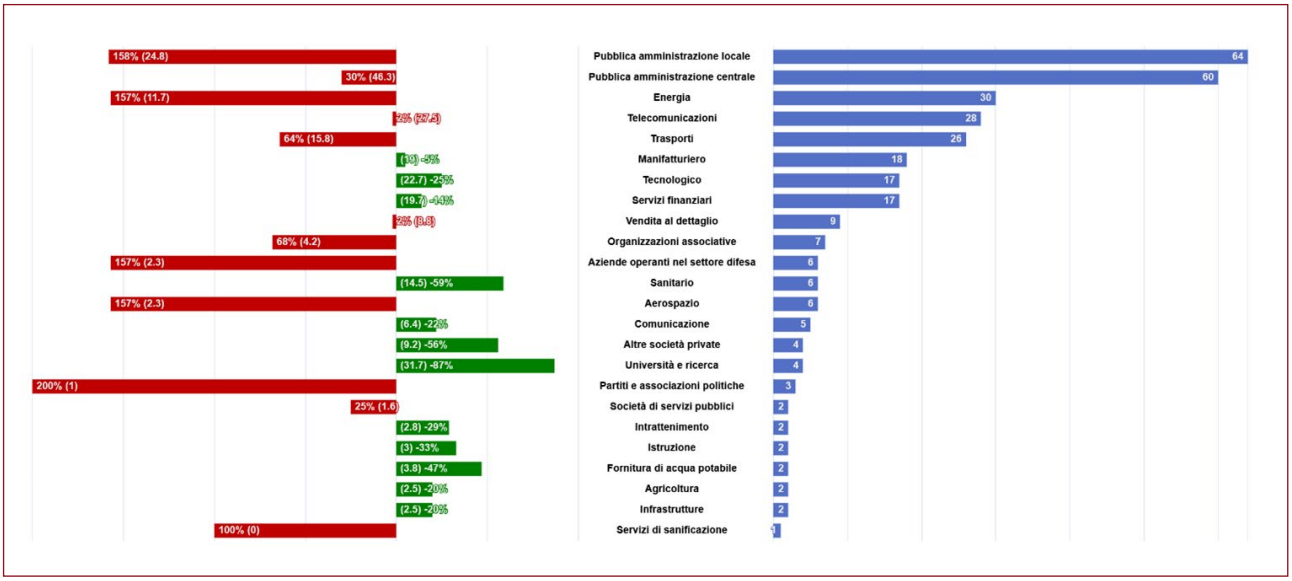
GENNAIO 2025



Fonte 10

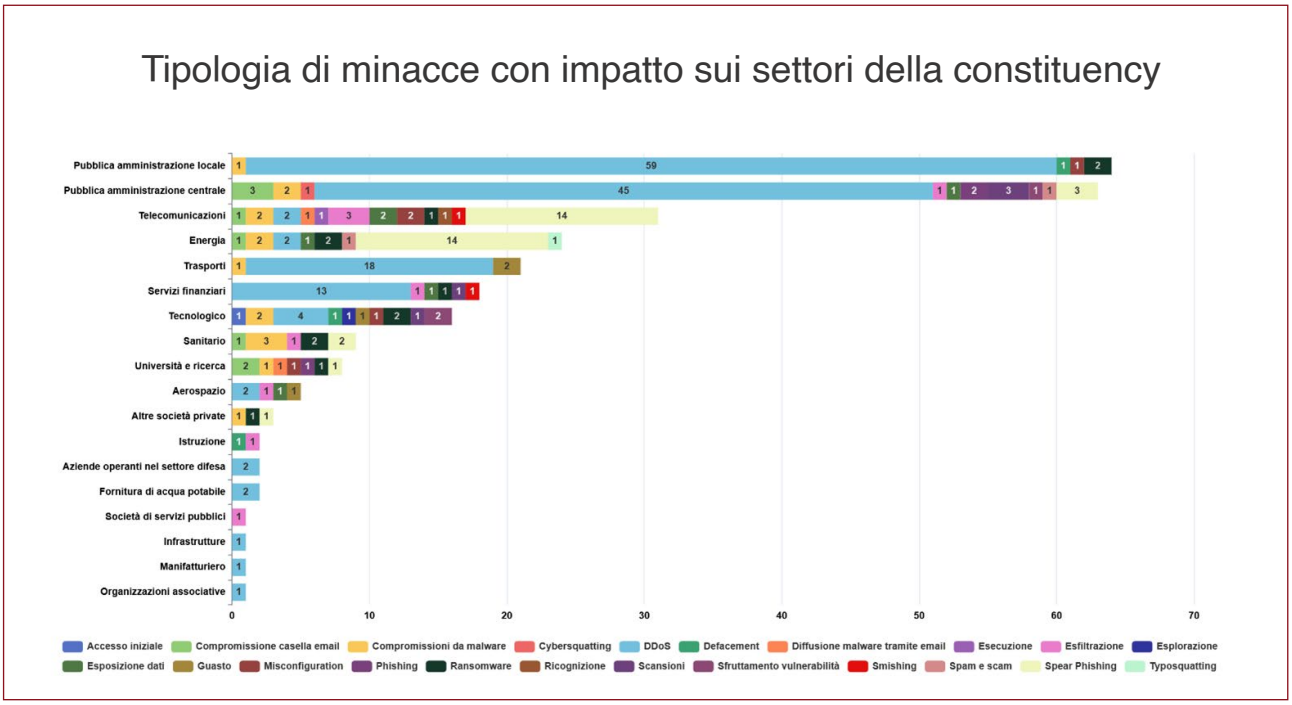


Fonte 10

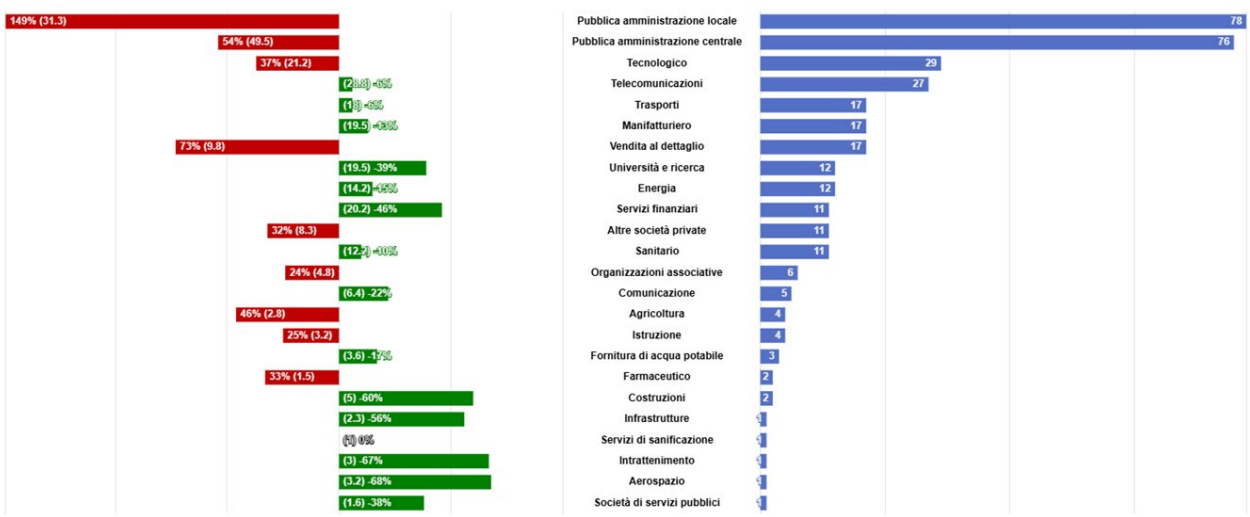


Fonte 11

A febbraio, le campagne offensive sono state indirizzate contro siti web della pubblica amministrazione, nonché di aziende operanti nei settori dei trasporti e dei servizi finanziari. Tali azioni sono state impiegate come mezzo per ottenere visibilità mediatica e amplificare il messaggio propagandistico delle rivendicazioni. A conferma di ciò, dei 181 attacchi DDoS rilevati nel periodo, solo il 3% ha determinato disservizi, che si sono rivelati comunque di carattere temporaneo (tipicamente circa un'ora di irraggiungibilità della risorsa attaccata).



Fonte 11

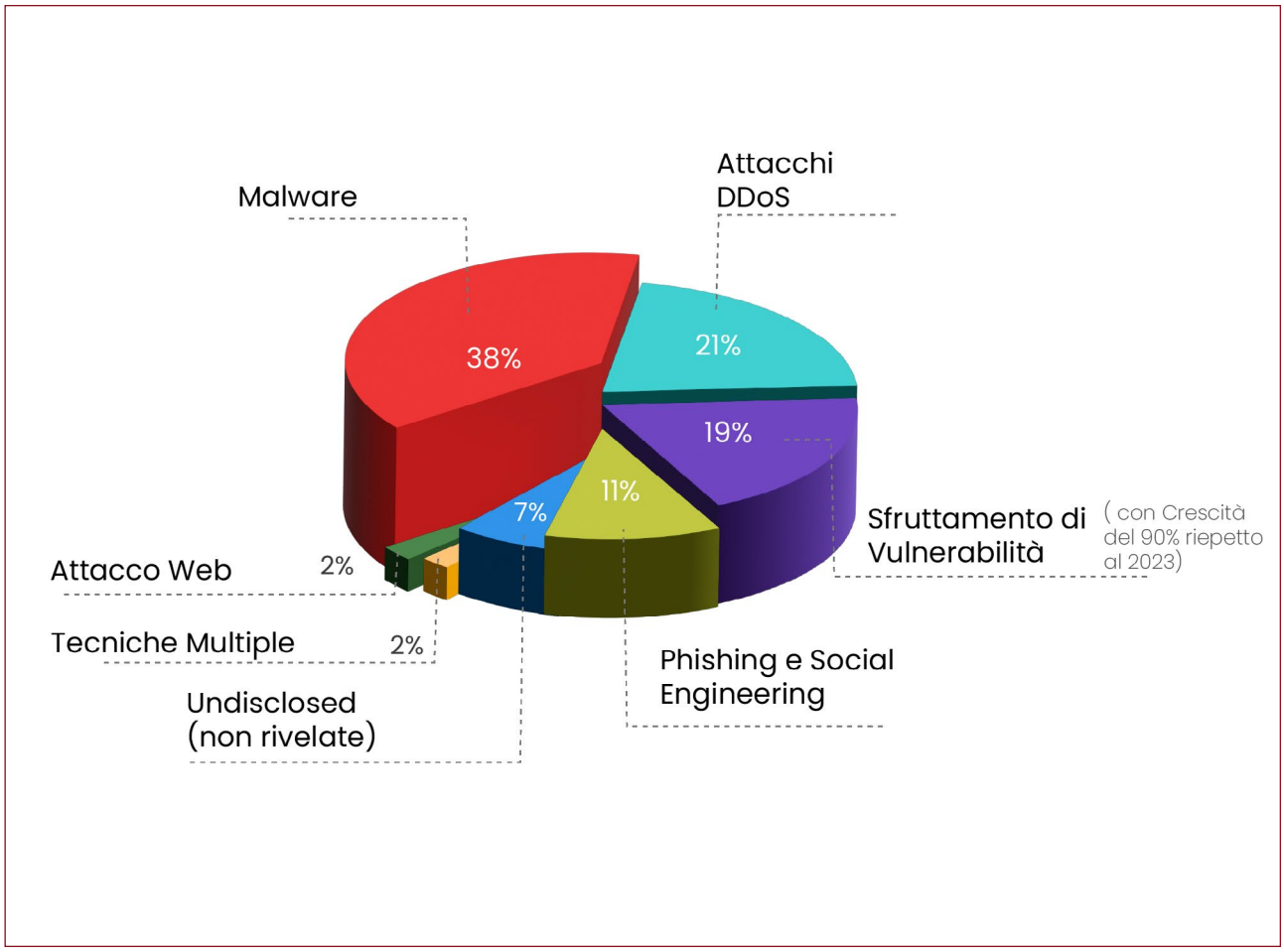


Fonte 12

Tipologia di minacce con impatto sui settori della constituency

Fonte 12

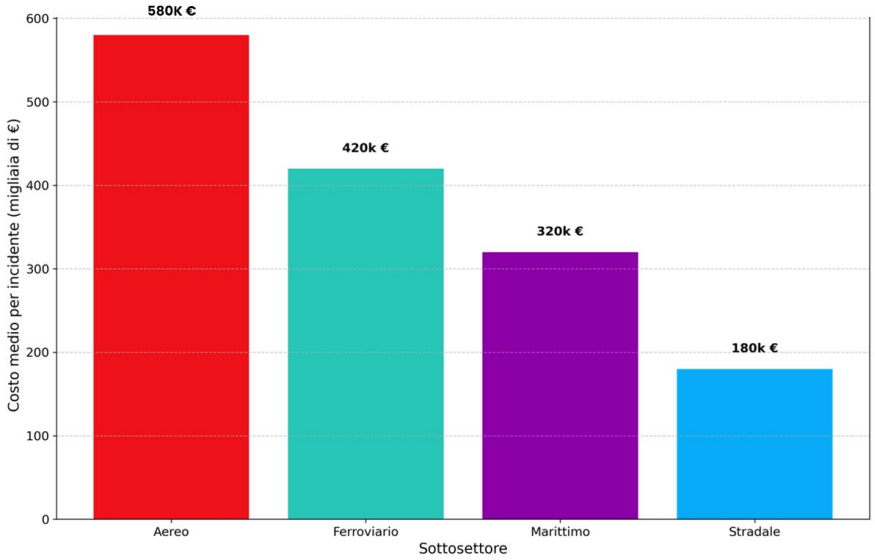
Tecniche di Attacco più Diffuse nel Settore Trasporti Italiano



Danni e impatti economici degli attacchi cyber: Costi diretti e indiretti

Da analisi di report di settore emerge che il trasporto aereo registra il costo medio più elevato per incidente (580.000 euro), seguito dal ferroviario (420.000 euro), dal marittimo (320.000 euro) e dallo stradale (180.000 euro). Questa distribuzione riflette sia la criticità dei sistemi coinvolti sia il potenziale impatto economico delle interruzioni di servizio.

Costo medio per incidente cyber per sottosettore dei trasporti (2024)



I principali costi diretti includono:

- **Ripristino dei sistemi:** Costi associati al recupero dei dati e al ripristino delle operazioni
- **Indagini forensi:** Spese per l'analisi dell'incidente e l'identificazione delle vulnerabilità
- **Pagamento di riscatti**
- **Sanzioni normative:** Penalità per il mancato rispetto delle normative sulla protezione dei dati e sulla sicurezza informatica

Gli attacchi informatici comportano anche significativi costi indiretti, spesso più difficili da quantificare ma non meno impattanti:

- **Interruzione del servizio**
- **Danni reputazionali:** Perdita di fiducia da parte di clienti e partner commerciali
- **Perdita di produttività:** Tempo e risorse dedicate alla gestione dell'incidente anziché alle normali operazioni
- **Aumento dei premi assicurativi:** Incremento dei costi delle polizze cyber a seguito di incidenti.

Rischi specifici per il settore Trasporti

Rischi comuni a tutti i sottosettori

Vulnerabilità della supply chain

La supply chain del settore trasporti è particolarmente complessa e coinvolge numerosi attori, ciascuno con potenziali vulnerabilità:

- **Fornitori di software e hardware:** secondo il whitepaper “Verso la NIS2” del Gruppo TIM (2024), il 62% delle organizzazioni colpite da ransomware ha riferito che l’infezione era originata da un partner o fornitore.
- **Sistemi di terze parti:** l’integrazione con sistemi esterni (prenotazioni, pagamenti, tracking) aumenta la superficie di attacco.
- **Componenti hardware:** molti sistemi critici utilizzano componenti commerciali di largo consumo (COTS) non progettati con la cybersecurity come priorità.

Il report ENISA (dicembre 2024) evidenzia che gli attacchi alla supply chain sono aumentati del 42% nel 2024 rispetto all’anno precedente, con il settore dei trasporti tra i più colpiti.

Obsolescenza tecnologica

Secondo alcune analisi, l’obsolescenza delle infrastrutture è indicata dal 73% dei CISO come uno dei principali fattori di impatto sul rischio cyber. Nel settore trasporti, questo problema è particolarmente acuto:

- **Sistemi legacy:** molte infrastrutture di trasporto utilizzano sistemi operativi e software obsoleti, non più supportati dai produttori.
- **Ciclo di vita esteso:** i mezzi di trasporto (navi, treni, aerei) hanno cicli di vita molto lunghi, spesso decenni, durante i quali i sistemi di bordo diventano progressivamente più vulnerabili.
- **Difficoltà di aggiornamento:** l’aggiornamento dei sistemi critici richiede spesso fermi operativi costosi e complessi.

Convergenza IT/OT

La crescente integrazione tra sistemi IT (Information Technology) e OT (Operational Technology) nel settore dei trasporti – stradale, ferroviario e marittimo – rappresenta una delle sfide più complesse in ambito cybersecurity:

- **Sistemi OT non progettati per la sicurezza:** molte tecnologie di controllo (es. SCADA, sistemi di bordo, segnalamento ferroviario o marittimo) privilegiano disponibilità e funzionalità, trascurando la sicurezza.
- **Protocolli proprietari e legacy:** l'uso di protocolli non standardizzati ostacola l'integrazione di misure di sicurezza efficaci.
- **Monitoraggio limitato:** spesso manca una piena visibilità sugli eventi di sicurezza nei sistemi OT.

Nel contesto dei trasporti, è fondamentale adottare standard e framework specifici, tra cui:

» **IEC 62443:** sicurezza dei sistemi di automazione industriale, applicabile ai sistemi di controllo nei trasporti ferroviari e intelligenti.

» **ISO/SAE 21434:** Cybersecurity engineering per veicoli stradali connessi e autonomi.

» **UNECE WP.29 – R155**: regolamento ONU sulla gestione della cybersecurity nei veicoli stradali.

» **IMO 2021 (MSC.428(98))**: obbligo di gestione del rischio cyber nei sistemi di bordo delle navi commerciali a partire dal 2021.

» **MITRE ATT&CK for ICS**: Framework per l'identificazione delle tecniche di attacco nei sistemi OT critici, inclusi quelli ferroviari e marittimi.

Fattore umano

Come dimostrano report di settore, il fattore umano è indicato dal 75% dei CISO come il principale elemento di impatto sul rischio cyber:

- **Personale operativo non formato:** gli operatori dei sistemi di trasporto spesso non hanno una formazione adeguata in materia di cybersecurity.
- **Social engineering:** gli attacchi di phishing e social engineering rappresentano uno dei principali vettori di ingresso per attacchi più complessi.
- **Insider threat:** il personale interno con accesso privilegiato può rappresentare una minaccia significativa, intenzionale o non intenzionale.

Rischi emergenti

Intelligenza Artificiale

Dalle analisi effettuate risulta che il 33% dei CISO ritiene che l'adozione spontanea di soluzioni di AI da parte del business generi un alto impatto nell'esposizione al rischio cyber:

- **Attacchi potenziati da AI:** l'intelligenza artificiale viene utilizzata per rendere più sofisticati gli attacchi, ad esempio generando phishing più convincenti o automatizzando la ricerca di vulnerabilità.
- **Manipolazione dei sistemi AI:** i sistemi di trasporto che utilizzano AI per ottimizzare operazioni o per la guida autonoma possono essere ingannati attraverso tecniche di adversarial machine learning.
- **Shadow AI:** l'adozione non governata di strumenti di AI all'interno delle organizzazioni crea nuove vulnerabilità.

IoT e edge computing

La proliferazione di dispositivi IoT nel settore trasporti crea nuove superfici di attacco:

- **Sensori non sicuri:** molti sensori IoT utilizzati per monitorare infrastrutture di trasporto hanno capacità di sicurezza limitate.
- **Gateway edge:** i dispositivi edge che aggregano dati da sensori IoT possono rappresentare punti di ingresso per attacchi più profondi.
- **Gestione delle credenziali:** la gestione delle credenziali per migliaia di dispositivi IoT rappresenta una sfida significativa.

5G e connettività avanzata

L'adozione di tecnologie 5G nel settore trasporti introduce nuovi rischi:

- **Network slicing:** la segmentazione virtuale delle reti 5G, se non correttamente implementata, può consentire la propagazione di attacchi tra segmenti.
- **Maggiore superficie di attacco:** la maggiore densità di dispositivi connessi e l'architettura distribuita del 5G aumentano la superficie di attacco.
- **Dipendenza da infrastrutture critiche:** la dipendenza da infrastrutture 5G per operazioni critiche crea nuovi single points of failure.

Normative e investimenti in cybersecurity

Quadro normativo europeo: la Direttiva NIS2

La Direttiva NIS2 (Network and Information Security 2), entrata in vigore il 18 ottobre 2024, rappresenta il principale riferimento normativo per la cybersecurity nel settore dei trasporti a livello europeo. Questo provvedimento, che sostituisce e amplia la precedente Direttiva NIS del 2016, introduce requisiti di sicurezza più rigorosi con l'obiettivo di potenziare la resilienza e la protezione delle reti e delle informazioni che garantiscono il funzionamento di servizi essenziali.

Impatto sul settore Trasporti

Il settore dei trasporti è esplicitamente identificato come critico all'interno della Direttiva NIS2, che copre:

- **Trasporto aereo:** compagnie aeree, aeroporti, sistemi di controllo del traffico aereo.
- **Trasporto ferroviario:** operatori ferroviari, gestori dell'infrastruttura.
- **Trasporto marittimo e vie navigabili:** compagnie di navigazione, porti, sistemi di gestione del traffico marittimo.
- **Trasporto stradale:** operatori di sistemi di trasporto intelligenti, gestori di infrastrutture stradali.

Secondo la Direttiva, le organizzazioni del settore trasporti devono:

1. Implementare misure di gestione del rischio cyber proporzionate al livello di rischio.
2. Notificare incidenti significativi alle autorità competenti entro 24 ore dall'identificazione.
3. Garantire la continuità operativa attraverso piani di disaster recovery e business continuity.
4. Proteggere le supply chain valutando i rischi di sicurezza dei fornitori.
5. Designare responsabili per la gestione della sicurezza informatica.

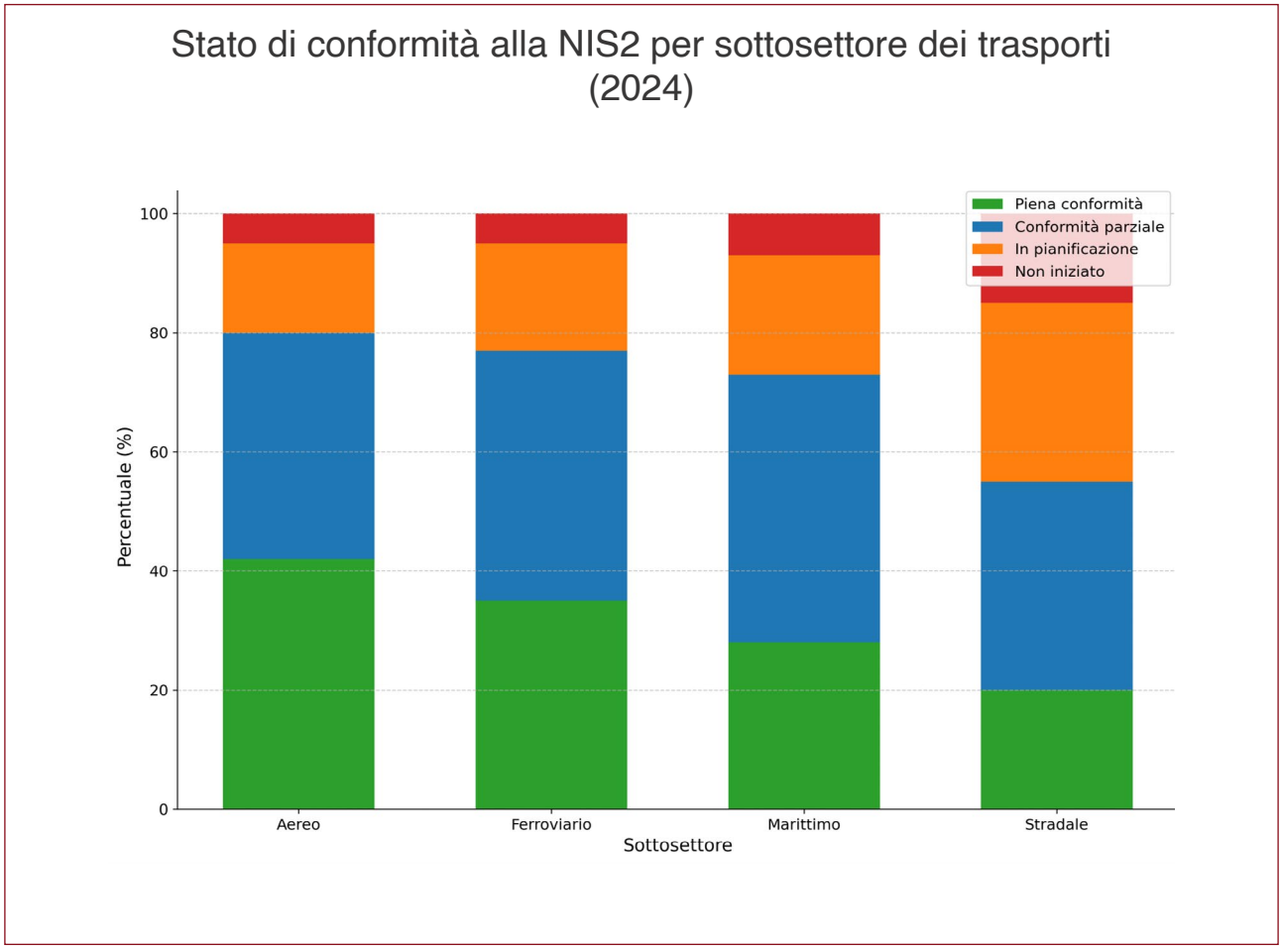
Recepimento in Italia: il Decreto Legislativo 138/2024

L'Italia ha recepito la Direttiva NIS2 con il Decreto Legislativo 138/2024, pubblicato in Gazzetta Ufficiale il 16 ottobre 2024. Il decreto stabilisce:

- **Agenzia per la Cybersicurezza Nazionale (ACN)** come autorità nazionale competente

- **Obbligo di registrazione** alla piattaforma ACN entro il 28 febbraio 2025 per le aziende del settore trasporti
- **Sanzioni fino a 10 milioni di euro** o al 2% del fatturato globale annuo per le violazioni più gravi
- **Requisiti specifici per i diversi sottosettori** del trasporto, con particolare attenzione alle infrastrutture critiche

La Figura illustra lo stato di conformità alla NIS2 per i diversi sottosettori del trasporto in Italia nel 2024.



Il trasporto aereo mostra il livello più alto di piena conformità (42%), seguito dal ferroviario (35%), dal marittimo (28%) e dallo stradale (20%). Questa distribuzione riflette i diversi livelli di maturità cyber dei vari sottosettori, con il trasporto stradale che presenta la percentuale più alta di organizzazioni che non hanno ancora iniziato il percorso di adeguamento (15%).

Trend di investimento in Italia

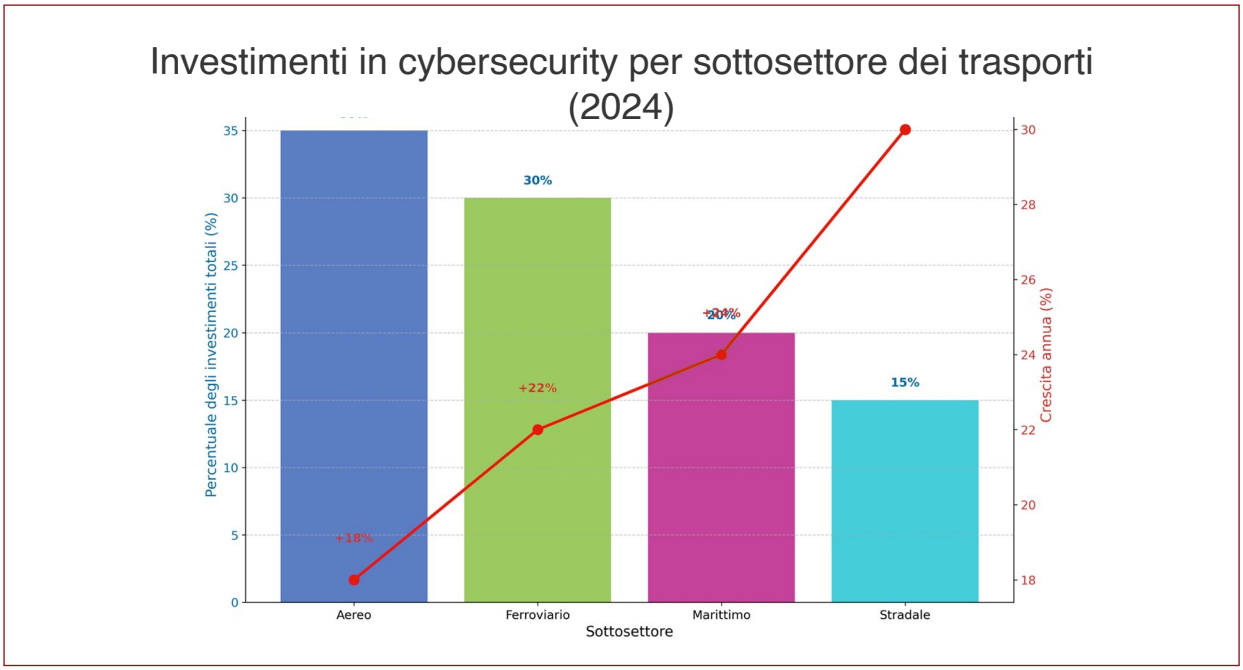
Secondo l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, nel 2024 il settore Logistica e trasporti ha registrato una crescita degli investimenti in cybersecurity del 25%, superiore alla media nazionale del 15%. Questo incremento è in parte attribuibile alla spinta normativa della direttiva NIS2.

I principali ambiti di investimento includono:

1. **Tecnologie di protezione:** sistemi di rilevamento e prevenzione delle intrusioni, firewall di nuova generazione.
2. **Servizi di monitoraggio:** security Operation Center (SOC), threat intelligence.
3. **Formazione del personale:** programmi di sensibilizzazione e training specifici.
4. **Consulenza normativa:** supporto per l'adeguamento alla NIS2.

Differenze tra sottosettori

Gli investimenti in cybersecurity variano significativamente tra i diversi sottosettori del trasporto, come illustrato nella Figura.



Il trasporto aereo è il sottosettore con i maggiori investimenti (35% del totale), seguito dal ferroviario (30%), dal marittimo (20%) e dallo stradale (15%). Tuttavia, è interessante notare che il trasporto stradale, pur avendo la quota minore di investimenti, presenta il tasso di crescita più elevato (+30% nel 2024), riflettendo la crescente consapevolezza delle vulnerabilità in questo ambito e la necessità di colmare il gap di maturità cyber.

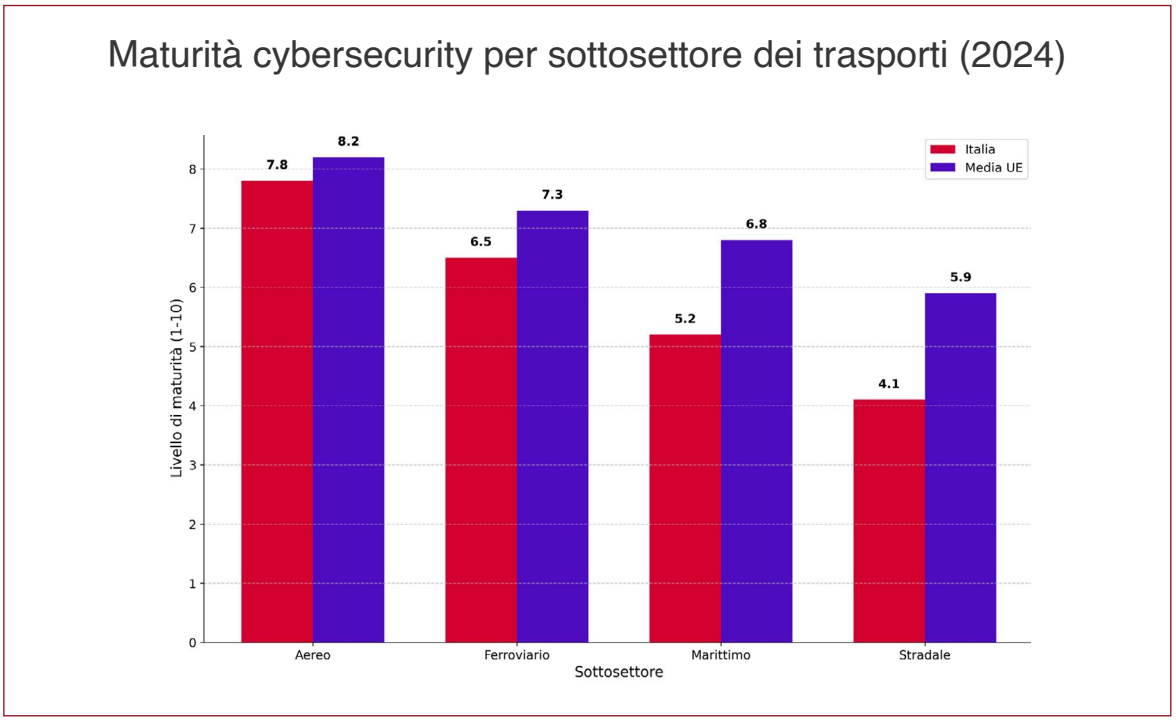
Confronto internazionale

Nonostante la crescita degli investimenti, l'Italia continua ad essere all'ultimo posto tra i membri del G7 nel rapporto tra spesa in cybersecurity e PIL, con un valore ancora lontano da quello degli Stati Uniti e dal Regno Unito:

1. **Stati Uniti:** 0,66% del PIL investito in cybersecurity
2. **Regno Unito:** 0,33% del PIL
3. **Germania:** 0,28% del PIL
4. **Francia:** 0,25% del PIL
5. **Italia:** 0,14% del PIL

Questo gap è particolarmente evidente nel settore dei trasporti, dove gli investimenti in cybersecurity in Italia rappresentano circa lo 0,8% del budget IT totale, contro una media europea del 1,5%.

La Figura illustra il livello di maturità cybersecurity per sottosettore dei trasporti, confrontando l'Italia con la media UE.



In tutti i sottosettori, l'Italia presenta un livello di maturità inferiore alla media UE, con il gap più significativo nel trasporto marittimo (5,2 vs 6,8 su una scala 1-10) e nel trasporto stradale (4,1 vs 5,9). Questo divario evidenzia la necessità di maggiori investimenti e di un approccio più strutturato alla cybersecurity nel settore trasporti in Italia.

Strategie di mitigazione e best practice

Approccio basato sul rischio

Le organizzazioni del settore trasporti stanno adottando un approccio basato sul rischio per l'implementazione della NIS2:

1. **Valutazione del rischio:** identificazione e prioritizzazione dei rischi cyber specifici per il sottosettore.
2. **Implementazione di controlli:** adozione di misure di sicurezza proporzionate al livello di rischio.
3. **Monitoraggio continuo:** valutazione regolare dell'efficacia delle misure implementate.

Collaborazione pubblico-privato

La collaborazione tra settore pubblico e privato è fondamentale per migliorare la resilienza cyber del settore trasporti:

- **Information Sharing and Analysis Center (ISAC):** piattaforme per la condivisione di informazioni sulle minacce.
- **Esercitazioni congiunte:** simulazioni di attacchi cyber per testare la preparazione.
- **Partenariati per la ricerca:** collaborazioni per lo sviluppo di nuove tecnologie di sicurezza.

Formazione e sensibilizzazione

La formazione del personale è un elemento chiave della strategia di cybersecurity nel settore trasporti:

- **Programmi di sensibilizzazione:** campagne per aumentare la consapevolezza sui rischi cyber.
- **Formazione tecnica:** training specifico per il personale IT e OT.
- **Simulazioni di Phishing / Vishing:** è ormai essenziale includere simulazioni di vishing nei test di sicurezza, poiché l'uso dell'intelligenza artificiale per clonare voci rende gli attacchi telefonici sempre più realistici e pericolosi. I cybercriminali possono imitare dirigenti o colleghi con brevi audio reperiti online, sfruttando fiducia e urgenza per ottenere bonifici o credenziali. Valutare la risposta dei dipendenti a queste minacce è oggi cruciale per misurare la resilienza contro le forme più evolute di social engineering.

Conclusioni

L’analisi della cybersecurity nel settore trasporti evidenzia un panorama di minacce in rapida evoluzione, con un incremento significativo sia nella frequenza che nella sofisticazione degli attacchi. La crescente digitalizzazione e interconnessione dei sistemi di trasporto, unita alla loro criticità strategica, li rende obiettivi particolarmente appetibili per diverse categorie di attaccanti, dalle organizzazioni criminali ai gruppi con possibili motivazioni geopolitiche. Il ransomware si conferma la minaccia predominante (38%), seguito dagli attacchi DDoS (24%) e dal phishing (18%).

Gli investimenti in cybersecurity nel settore trasporti sono in crescita (+25% nel 2024), ma l’Italia presenta ancora un gap significativo rispetto alla media europea, con un livello di maturità cyber inferiore in tutti i sottosettori, particolarmente evidente nel trasporto marittimo e stradale.

Prospettive future

Il quadro normativo sulla cybersecurity nel settore trasporti è destinato a evolversi ulteriormente, con possibili revisioni della NIS2 basate sull'esperienza di implementazione e l'introduzione di regolamenti dedicati ai singoli sottosettori del trasporto.

Le tecnologie emergenti come l'Intelligenza Artificiale, l'IoT e il 5G stanno plasmando il futuro della cybersecurity nel settore trasporti, introducendo nuove opportunità ma anche nuove sfide. L'adozione di modelli di sicurezza basati sul principio "zero trust" e lo sviluppo di soluzioni quantum-safe rappresentano trend significativi per il futuro.

Si prevede che gli investimenti in cybersecurity nel settore trasporti continueranno a crescere, con un tasso di crescita annuo composto (CAGR) stimato al 18-20% per il periodo 2025-2030, e un focus crescente su soluzioni proattive e predittive.

In conclusione, la cybersecurity nel settore trasporti richiede un approccio olistico, che integri tecnologie, processi e persone, e una collaborazione stretta tra settore pubblico e privato per garantire la resilienza di queste infrastrutture critiche per l'economia e la società.

Cyber Framework Maticmind

Il Cyber Framework Maticmind si allinea alla Direttiva NIS2 attraverso un modello integrato che anticipa minacce emergenti, riduce rischi con analisi proporzionate, promuove la sicurezza “by design”, implementa tecnologie avanzate (EDR, SIEM, zero trust) e rafforza la resilienza tramite monitoraggio continuo e risposta rapida agli incidenti.

Questo approccio trasforma la compliance normativa in vantaggio strategico, garantendo continuità operativa, mitigazione degli impatti economici degli attacchi e una governance cyber dinamica.

Predittiva – Anticipare

Monitoraggio costante del panorama delle minacce tramite Cyber Threat Intelligence e tecniche OSINT, per identificare rischi emergenti prima che si manifestino.

Preventiva – Prevenire

Valutazione e gestione del rischio tecnologico, umano, organizzativo e compliance, per rafforzare la postura di sicurezza e ridurre la probabilità di incidenti.

Progettuale – Costruire Sicuro

Integrazione della sicurezza nei processi di design e architettura, secondo principi di “secure by design” e “security by resilience”, per garantire sistemi resilienti.

Produttiva – Implementare Soluzioni

Adozione e gestione di tecnologie di difesa (firewall, EDR, IAM, SIEM) che trasformano le strategie in protezione operativa e misurabile.

Proattiva – Reagire e Migliorare

Monitoraggio continuo, risposta agli incidenti e analisi forense: la sicurezza come processo dinamico e adattivo, guidato dal miglioramento continuo.

Una Cyber Acies

Cinque centri di competenza, un’unica forza cyber

1

Centro strategico per l’analisi e gestione del rischio cyber: governance, compliance, modelli di maturità, supply chain security posture.

- Offensive Security
- Consulting Services (CisoasaService, PM,..)
- Governance, Risk e Compliance
- Social Engineerinf Simulation
- Risk Assessment
- Maturity Model checkup
- Supply Chain Security Posture
- Cyber Academy

3

Esecuzione ed implementazione di progetti complessi di sicurezza: infrastrutture, cloud, OT/IoT, application security e integrazione di soluzioni cyber.

- Infrastructure & Network Security Management
- Cyber Resiliency e Data Protection
- Microsoft, Fortinet & CISCO Competence Center
- Cloud Security By Design
- Application Security SSDLC
- OT & IoT Security Management
- Security System Integration and Monitoring

5

Progetti speciali e sperimentazione: architetture avanzate, droni, AI, cyber-physical systems, prototipi e soluzioni non convenzionali.

- Architetture avanzate multi-layer e ibride
- Sistemi di comando e controllo per droni e UAV
- Integrazione AI in contesti cyber e sicurezza industriale
- Progetti su ambienti cyber-physical / smart infrastructure
- Soluzioni sperimentali
- Cyber testbed per ambienti OT e industriali
- Soluzioni cyber per difesa e protezione civile
- Soluzioni sperimentali edge & fog computing.

2

Continuità operativa e sicurezza in tempo reale assicurata da presidio operativo che integra SOC H24, con le capacità tecniche del TAC e il controllo infrastrutturale del NOC. Garantisce un monitoraggio continuo, una risposta tempestiva agli incidenti e un supporto tecnico evoluto.

- **SOC (Security Operation Center)**
  - SOC H24
  - Cyber Threat Intelligence
  - Malware Analysis
- **SOS (SECURITY OPERATION SERVICES)**
  - Crisis Management
  - IncidentResponse & Digital Forensic Analysis
- **TAC (Technical Assistance Center)**
  - Gestione di ticket e supporto tecnico avanzato
  - Assistenza su soluzioni proprietarie e terze parti
  - Troubleshooting di sicurezza e infrastruttura
  - Supporto su incidenti tecnici e configurazioni complesse
- **NOC (Network Operation Center)**
  - Monitoraggio infrastrutturale H24
  - Supervisione performance di rete, cloud e sistemi
  - Gestione allarmi e segnalazioni
  - Coordinamento tecnico con il SOC in caso di anomalie

4

Gestione e integrazione di soluzioni proprietarie e tecnologie di terze parti: piattaforme EDR, firewall, IAM, SIEM, DLP.

- Piattaforma Twin4Cyber
- Cyber Range
- WiseView - Risk Management Platform
- SIEM/SOAR
- EDR/XDR/NDR
- Identity & Access Management (IAM/PAM)
- NGFW
- Data Loss Prevention

Bibliografia

Fonti primarie

Maticmind – Business Unit Cyber. Evidenze operative e intelligence raccolte tramite le seguenti strutture interne:

- Offensive Security Team
- Cyber Threat Intelligence Team
- Cyber Defence Center (SOC H24)
- Incident Response Management Team
- Twin4Cyber Platform
- Cyber Projects Hub e Innovation Lab

Fonti secondarie

1. Anitec-Assinform (2024). Il Digitale in Italia 2024 – Rapporto sull'evoluzione del digitale nel Paese. Milano: Confindustria Digitale.
2. Clusit (2024). Rapporto Clusit 2024 sulla sicurezza ICT in Italia. Milano: Clusit.
3. ENISA (2023). Cybersecurity Threat Landscape for the Transport Sector - March 2023. Atene: European Union Agency for Cybersecurity (ENISA).
4. ENISA (2024). ENISA Threat Landscape 2024. Atene: European Union Agency for Cybersecurity (ENISA).
5. Gruppo TIM (2024). Verso la NIS2 – Linee guida per la cybersecurity nelle infrastrutture critiche. Roma: TIM S.p.A.
6. IBM Security X-Force (2024). Threat Intelligence Index 2024. Armonk (NY): IBM Corporation.
7. Kaspersky (2024). Kaspersky Security Bulletin 2024. Mosca: Kaspersky Lab.
8. Osservatorio Cybersecurity & Data Protection del Politecnico di Milano (2025). Rapporto 2025 sulla sicurezza informatica in Italia. Milano: Politecnico di Milano.
9. Decreto Legislativo 138/2024. Attuazione della Direttiva (UE) 2022/2555 (NIS2). Roma: Gazzetta Ufficiale della Repubblica Italiana.
10. Agenzia per la Cybersicurezza Nazionale. (Gennaio 2025). Operational Summary - gennaio 2025.
11. Agenzia per la Cybersicurezza Nazionale. (Febbraio 2025). Operational Summary - febbraio 2025.
12. Agenzia per la Cybersicurezza Nazionale. (Marzo 2025). Operational Summary - marzo 2025.
13. Anitec-Assinform. (2025). Osservatorio Trimestrale del settore ICT: Schede dati.
14. Limone, E. (2023). Cyber-AntiSec 2023: Rapporto di sicurezza.
15. Marlink. (2024). 2025 Global Maritime Cyber Threat Report H2 2024.
16. SecurityScorecard Inc. (2024). The Cyber Risk Landscape of the Global Aviation Industry.
17. SOCRadar. (2024). Global Logistics & Transportation Industry Threat Landscape Report.

Disclaimer

Il presente report è stato elaborato utilizzando esclusivamente fonti di informazioni open source (OSINT) e dati pubblicamente accessibili. Le informazioni contenute in questo documento riflettono lo stato dell'arte al momento della sua redazione.

L'azienda che ha commissionato la creazione di questo report è esonerata da qualsiasi responsabilità riguardante:

- L'accuratezza, completezza o validità delle informazioni presentate
- Eventuali errori od omissioni nei dati analizzati
- Qualsiasi danno diretto o indiretto derivante dall'utilizzo delle informazioni contenute
- L'interpretazione dei dati e delle analisi presentate

Le conclusioni e le raccomandazioni fornite nel report sono basate sulle evidenze disponibili al momento della ricerca e non costituiscono garanzia di risultati futuri. Il panorama delle minacce cyber è in continua evoluzione, pertanto le informazioni potrebbero diventare obsolete rapidamente.

Questo documento è stato creato con l'unico scopo di fornire una panoramica generale sullo stato della cybersecurity nel settore trasporti e non deve essere considerato come consulenza professionale o legale.

L'azienda che ha commissionato il report declina ogni responsabilità per:

- Decisioni operative o strategiche prese sulla base delle informazioni contenute
- Eventuali conseguenze derivanti dall'implementazione delle raccomandazioni suggerite
- L'uso improprio delle informazioni presentate

Si raccomanda vivamente ai lettori di consultare esperti del settore prima di intraprendere azioni basate sul contenuto di questo report.

MATICMIND®

MAKES IT EASY

www.maticmind.it

info@maticmind.it

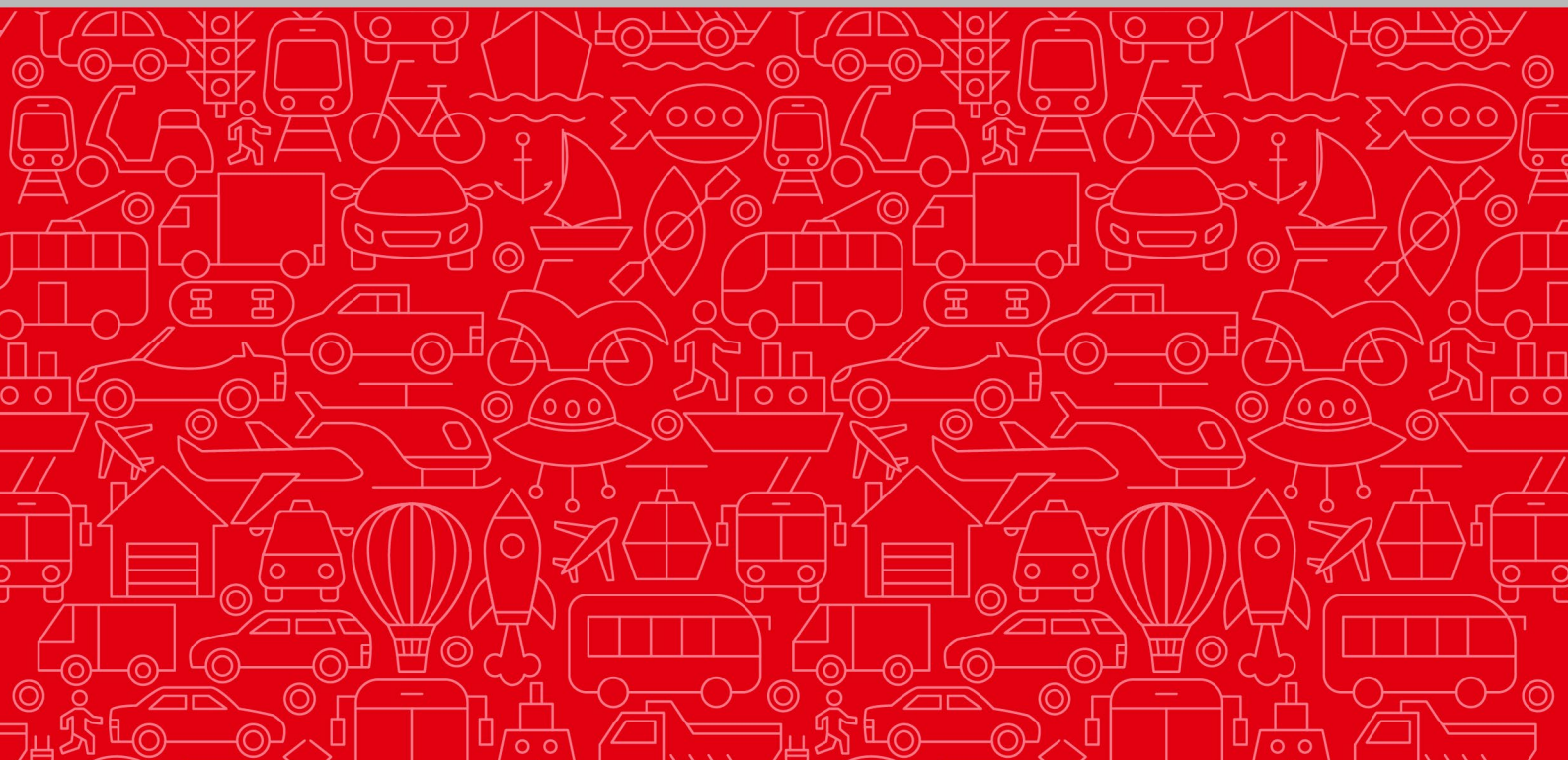
ISO 9001 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification

ISO 20000 BUREAU VERITAS Certification

ISO 45001 BUREAU VERITAS Certification

ISO 14001 BUREAU VERITAS Certification

ISO 14064-1 BUREAU VERITAS Certification

BU CyberSecurity