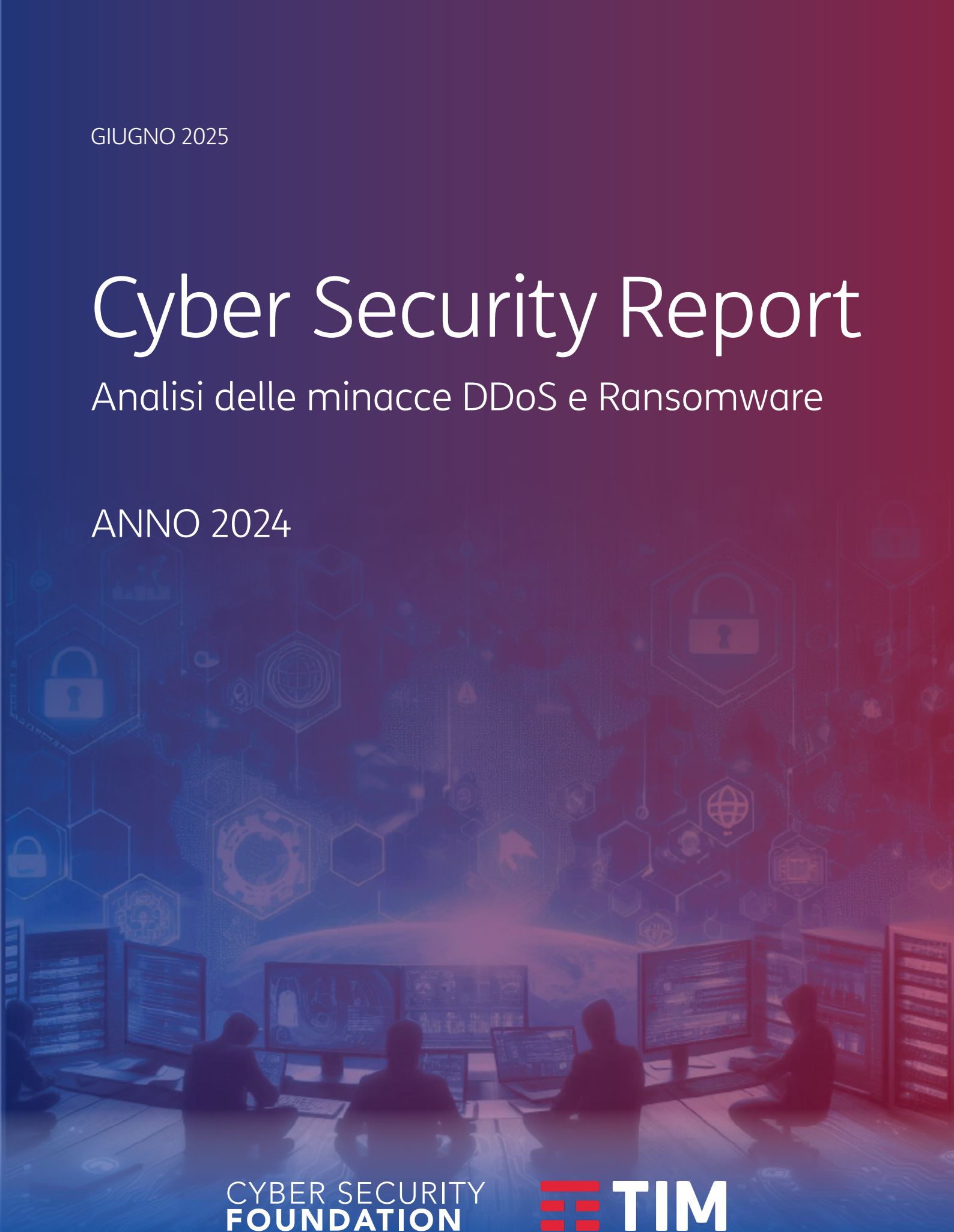
GIUGNO 2025

Cyber Security Report

Analisi delle minacce DDoS e Ransomware

ANNO 2024



CYBER SECURITY FOUNDATION

TIM

Executive Summary

1) Questo rapporto

L'espansione della digitalizzazione aumenta la superficie esposta alle minacce cyber, che oggi coinvolgono indistintamente istituzioni, imprese e cittadini. Nessun sistema può dirsi completamente sicuro, ma è possibile costruire infrastrutture resilienti, a partire da una maggiore conoscenza di questo fenomeno in forte crescita. Per questo, la Fondazione Italiana sulla Cyber Security che ha la mission di approfondire e diffondere la cultura sulla sicurezza cibernetica in Italia e TIM, che svolge un'azione quotidiana per prevenire e mitigare gli incidenti informatici attraverso i suoi CyberSOC e altre realtà del Gruppo come Telsy e TS-Way, hanno deciso di dare vita a questo rapporto che è articolato su quattro ambiti di osservazione specifici:

- Principali attacchi: osservazione degli eventi cyber più rilevanti dell'anno, con focus su attacchi DDoS e Ransomware, basata sui dati operativi raccolti da TIM.
- Analisi settoriale: analisi degli attacchi per settore, con particolare attenzione al mondo aziendale, produttivo e istituzionale, per identificare gli ambiti più colpiti e le principali direttrici di minaccia.
- Elementi normativi: panoramica sulle strategie e sulle iniziative normative in ambito europeo e comunitario, che guidano il rafforzamento della difesa cibernetica dell'Unione e dei paesi membri come l'Italia.
- Tecnologie emergenti: focus sulle innovazioni tecnologiche che stanno trasformando il panorama della cybersecurity, sia dal punto di vista delle difese sia degli attacchi.

2) Principali Attacchi

La prima parte del rapporto si concentra sugli eventi di sicurezza rilevati nel corso del 2024 dai team di difesa cibernetica di TIM, in particolare dal Security Operation Center e dalle unità di Threat Intelligence. L'obiettivo è distinguere tra semplici minacce e attacchi veri e propri, valorizzando il ruolo della prevenzione e del monitoraggio continuo.

2.1. DDoS

Un attacco di tipo DOS «Denial of Service» rientra tra le minacce alla disponibilità degli asset/servizi digitali, colpendo server, siti web e infrastrutture con enormi volumi di traffico, generando un sovraccarico che impedisce la normale erogazione dei servizi. Questi possono essere condotti anche sfruttando reti di dispositivi compromessi o utenti ignari, di cui l'attaccante è in grado di prendere il controllo. L'obiettivo è saturare le risorse del target fino a renderlo inutilizzabile. Nonostante la dinamica degli attacchi sia nota, la loro rilevazione resta complessa: possono svilupparsi lentamente e a ondate, provenire da più aree geografiche o nascondersi dietro traffico apparentemente legittimo. Alcuni attacchi colpiscono persino i sistemi di monitoraggio. Inoltre, l'uso dell'intelligenza artificiale da parte degli attaccanti li rende ancora più sofisticati e difficili da intercettare.

Di seguito si riportano le informazioni più significative del 2024, rilevate grazie al presidio diretto delle reti dei SOC del Gruppo TIM.

Gli attacchi DDoS crescono di nuovo a livelli del periodo della pandemia

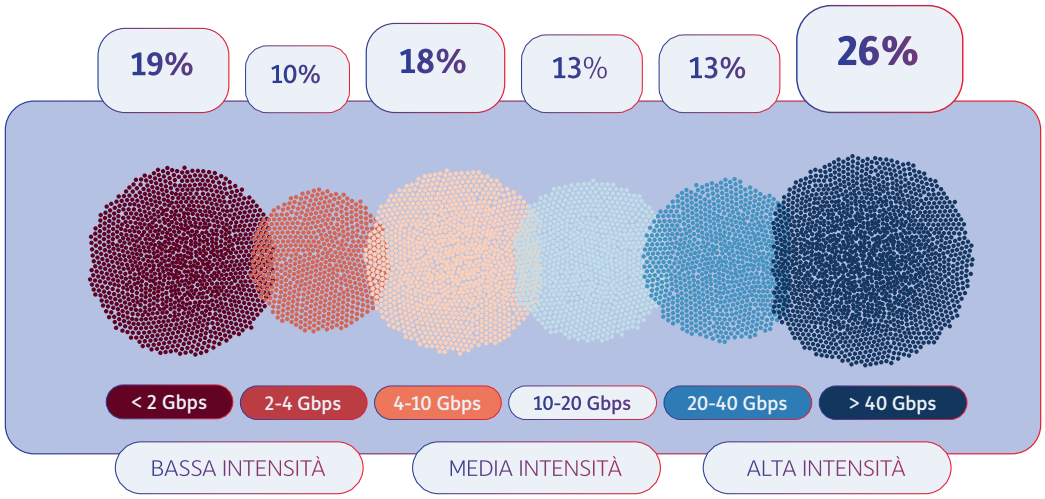
Il 2024 ha registrato una forte intensità in termini di eventi DDoS con un aumento del 36% rispetto al 2023: in media, circa 560 casi per mese con due momenti di picco ed una progressiva diminuzione nell'ultimo trimestre dell'anno. Da agosto 2023 a dicembre 2024 emerge una media di 580 casi per mese, con un picco di 765 eventi che si colloca a livelli simili a quelli del periodo pandemico. Le motivazioni dietro l'intensificarsi degli attacchi DDoS non sono solo di tipo finanziario, ma anche di natura geopolitica, legate al conflitto in Ucraina ed a quello nella striscia di Gaza che ha contribuito al peggioramento del quadro complessivo.

Si affermano nuove tecnologie e tecniche di attacco

Nel biennio 2023–2024 si è osservato un incremento delle minacce DDoS con l'adozione di tecniche sempre più sofisticate: attacchi iper-volumetrici, capaci di generare centinaia di milioni di richieste al secondo; utilizzo di vettori distribuiti, inclusi dispositivi IoT compromessi e macchine virtuali (VM/VPS),che generano traffico fino a 5.000 volte superiore rispetto a un singolo device; attacchi multi-target, che colpiscono simultaneamente siti web, reti, dispositivi e infrastrutture della medesima organizzazione, rendendo inefficaci molte difese tradizionali. Gli attacchi si sono evoluti anche a livello applicativo. Vengono rilevati sempre più spesso attacchi diretti a interfacce Web e API, difficili da identificare a causa del traffico cifrato. Alcuni attacchi si indirizzano verso i DNS, che sovraccaricati di richieste massive bloccano la risoluzione degli indirizzi web. Vengono utilizzate tecniche di elusione avanzate, come IP dinamici e header HTTP manipolati, in modo da mascherare il traffico malevolo. Questi diverse modalità e tecniche di attacco rendono sempre più complessa la rilevazione tempestiva e l'attivazione di contromisure efficaci.

Aumenta la classe di intensità dell'attacco

Nel 2024 sono stati rilevati circa 6.700 eventi DDoS, un volume paragonabile a quello del secondo lockdown pandemico, ma radicalmente differente in termini di intensità. Nel 2024, gli eventi con intensità inferiore ai 10 Gbps sono stati il 47% del totale, mentre nel 2021 erano l'80%. Al contrario, gli attacchi superiori a 20 Gbps sono passati dal 5% (2021) al 39% nel 2024, con un picco del 26% oltre i 40 Gbps, oggi la fascia più rilevante (ogni 10 eventi, 4 sono di alta intensità). Seppure gli attacchi a più bassa intensità non siano meno pericolosi (perché in grado di mimetizzarsi con il traffico legittimo), questo cambiamento evidenzia un netto aumento della capacità offensiva degli attaccanti, imponendo un adeguamento delle contromisure difensive.



Un secondo parametro fondamentale: la durata dell'attacco

Il livello d'intensità va esaminato insieme alla durata dell'evento. Un evento DDoS può avere durate differenti, minuti, ore e addirittura giorni. La durata media di un evento DDoS nel 2024 è stata di circa 39 minuti. Le categorie degli attacchi molto lunghi, oltre le 24 ore, diminuiscono rispetto al 2023 e risultano molto esigue e quindi episodiche, ma sono in crescita, con un peso significativo per il loro impatto, gli eventi DDoS sia tra i 30 min e le 2 ore, sia inferiori alle 24, perché connesse a maggiore disponibilità di banda larga e uso di tecnologie innovative quali AI e Cloud.

Distribuzione degli attacchi DDoS sui settori

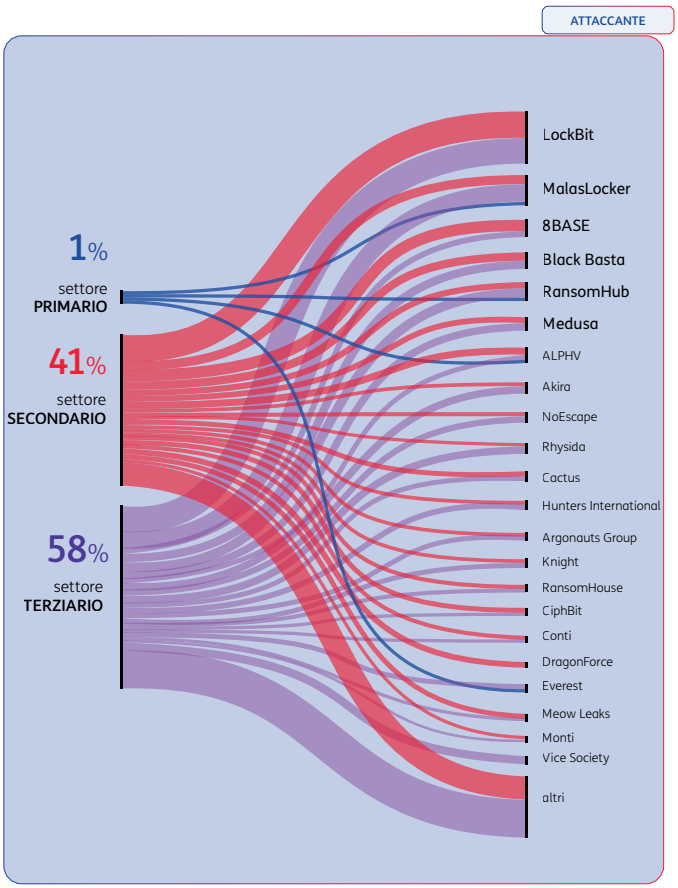
La maggior parte degli eventi che sono stati registrati nel 2024 si è indirizzata verso gli "Home Users" (famiglie e individui), che rappresentano un target molto più ampio da raggiungere, mentre poco meno di un quarto si è rivolto verso organizzazioni pubbliche o private. La Pubblica Amministrazione è il settore con la maggiore crescita di eventi DDoS tra il 2023 ed il 2024, dal 1% al 42% del totale dei

casi rivolti verso i settori. Diminuisce invece la quota di eventi indirizzati contro i servizi professionali (dal 36% al 17%), che restano però il target principale tra le imprese. Altri settori che presentano una quota in aumento rispetto al 2023 sono: il Settore finanziario (dal 3% al 14%), la Difesa (dal 4% al 6%) e il settore dei Media (dall'1% al 2%).

Gli attacchi DDoS verso le imprese possono avere diverse motivazioni: ragioni opportunistiche, atti di vandalismo digitale, concorrenza sleale, movimenti di attivismo politico, dimostrazioni di potere da parte di gruppi hacker, ma il gran volume di eventi che hanno interessato il settore istituzionale nel 2024 suggerisce una probabile correlazione con il contesto geopolitico.

2.2. Ransomware e Malware

Analizzare il fenomeno ransomware è complesso a causa della difficoltà nella raccolta dei dati e nella denuncia degli attacchi. Questo porta a discrepanze nei dati raccolti, rendendo difficile una visione completa del fenomeno. Il Paese più colpito nel 2024 a livello globale sono gli Stati Uniti: degli oltre 5.200, circa un attacco su due si è indirizzato verso imprese statunitensi. L'Italia, con 146 casi, si colloca al quinto posto nella classifica mondiale ed al secondo in quella dell'UE, dietro alla Germania. Tra i Paesi Europei non UE, il Regno Unito è il Paese più colpito con 262 casi.



Nel triennio 2022-2024, la maggior parte degli attacchi ransomware denunciati si è indirizzata verso il settore dei servizi (58% degli eventi totali), ma il settore in assoluto più colpito è quello manifatturiero che ha attirato il 26% degli attacchi.

Focalizzando l'osservazione solo sul 2024, i gruppi di attaccanti che hanno minacciato l'Italia con ransomware sono stati 42.

I più attivi sono stati RansomHub, Lockbit, 8BASE e Black Basta. La diffusione del modello Ransom as a Service (RaaS), un modello di business del crimine informatico in cui una banda vende il proprio codice ransomware ad altri hacker contribuisce alla crescita di questi gruppi.

Una campagna di diffusione di malware rappresenta un'azione concertata che ha l'obiettivo di propagare software malevolo, conosciuto come malware (MALicious softWARE), attraverso una serie di canali per compromettere sistemi informatici, reti e dispositivi, utilizzando sistemi differenti (virus, worm, trojan, spyware ecc.), ciascuno con modalità operative specifiche.

Nel 2024, le campagne di malware in Italia (168) hanno mirato a compromettere sistemi informatici attraverso varie tecniche, sfruttando vulnerabilità dei sistemi o attraverso tecniche di ingegneria sociale, che puntano ad adescare degli utenti per sottrarre le loro password o informazioni riservate. Le principali minacce sono venute da Remote Access Trojan, che si installano in un computer, in un dispositivo mobile o in un apparato ed aprono un varco che permette a degli attaccanti di poter controllare la macchina infetta a distanza.

3) Cybersecurity e regolamentazione nell'UE: un quadro in evoluzione

In questo quadro di forte minaccia, che colpisce imprese e catene di fornitura senza considerare i confini nazionali, è opportuno approntare dei sistemi di difesa comuni, a partire dallo scambio di informazioni e dalla definizione di prassi condivise. È per questo che l'Unione Europea ha avviato da tempo un processo per la costruzione di un sistema di difesa cibernetica comune che nel contesto geopolitico attuale rappresenta una condizione abilitante per la sovranità tecnologica e la competitività dell'economia digitale. SI tratta di una sfida complessa, che deve fare i conti con innovazioni tecnologiche continue (5G, Cloud, Intelligenza Artificiale), fattori geopolitici variabili (nel recente passato: la Brexit, oggi i mutamenti nelle relazioni politiche e commerciali), emergenze inattese (pandemia), nuove modalità di consumo e di lavoro, cambiamenti nella sensibilità sociale verso alcuni temi (protezione dei dati). Tutti questi fattori cambiano continuamente il quadro e definiscono nuovi spazi in cui le minacce cyber possono introdursi.

A questa complessità l'UE risponde adeguando costantemente le policy di cybersecurity e le norme che vigilano sulla protezione dello spazio digitale.

Nel corso del 2024 è entrata in vigore la NIS2 che ha esteso il numero di settori ed imprese che devono implementare specifiche misure di sicurezza e hanno l'obbligo di segnalare incidenti cyber. Oltre alla NIS2, nel 2024 sono state introdotte altre novità:

- il Cybersecurity Act (CSA), che fissa un quadro comune in UE, rafforzando il ruolo dell'Agenzia europea per la cybersecurity ENISA definendo norme comuni tra i Paesi Membri
- il Cyber Resilience Act (CRA), che definisce i requisiti di cybersecurity per prodotti dotati di componenti digitali (ad esempio, strumenti medicali e giocattoli smart).

A queste novità principali si aggiungono:

- la Direttiva CER: per la protezione delle infrastrutture critiche.
- il Regolamento EUid: per una gestione sovrana e sicura delle identità digitali.
- DORA: per la resilienza operativa digitale degli attori del settore finanziario.

La costruzione del cyberspazio europeo come ambiente sicuro e regolato è oggi un elemento cardine della politica industriale dell'Unione. Tuttavia, la complessità e la stratificazione normativa pongono anche sfide di armonizzazione, implementazione efficace e inclusione delle PMI, che necessitano di strumenti e supporto per non rimanere escluse dalla trasformazione. In questo contesto, l'Italia - tramite l'ACN e gli operatori privati più strutturati – può giocare un ruolo da protagonista nel trasformare la compliance in leva di competitività e fiducia digitale.

4) Nuovi fronti tecnici di attenzione: minacce e opportunità

4.1. AI e Cybersecurity

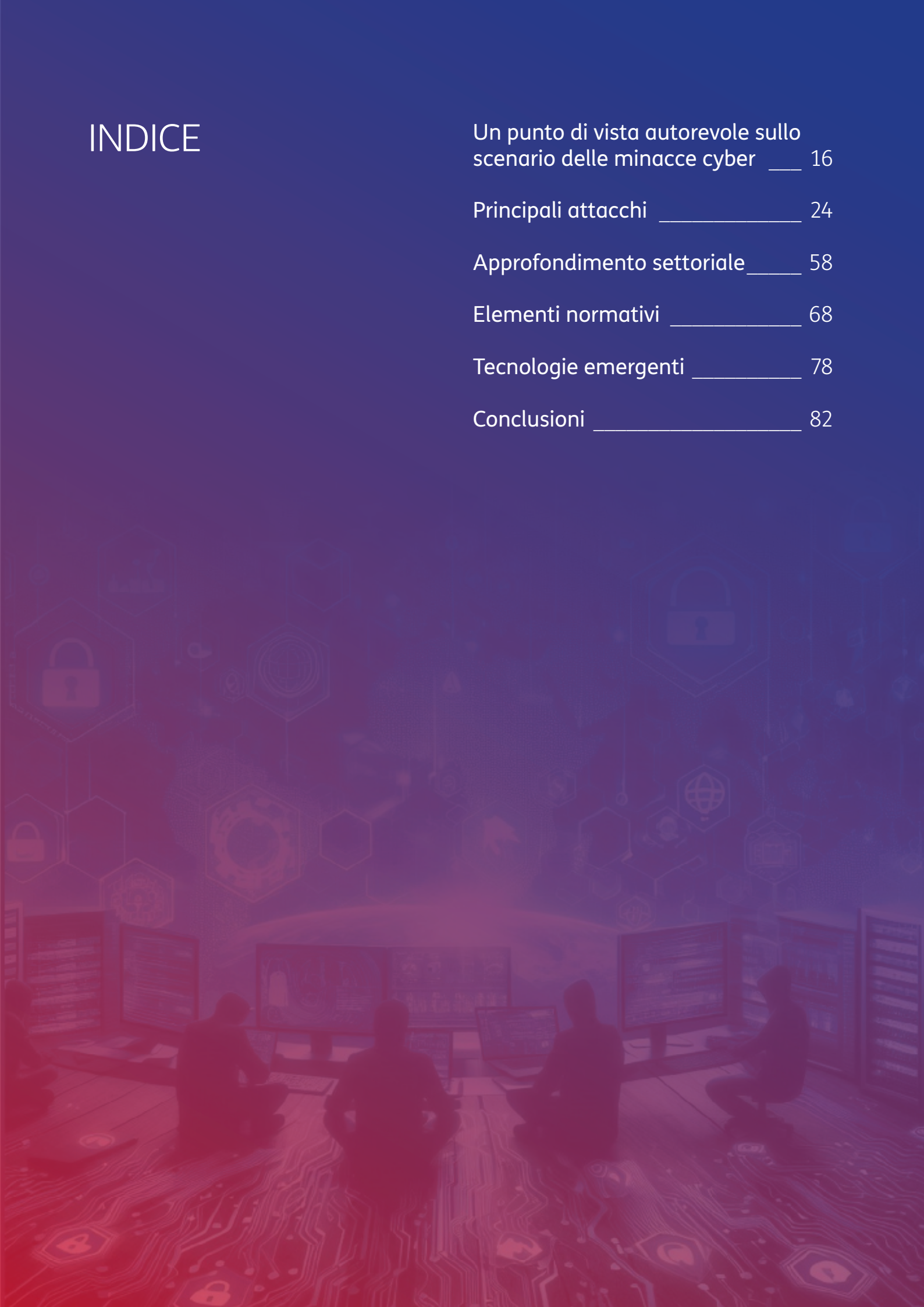
L'intelligenza artificiale (IA) sta diventando un fattore chiave nella cybersecurity, agendo contemporaneamente come strumento di difesa avanzata e come leva offensiva nelle mani degli attaccanti. Le tecnologie e soluzioni di cybersecurity basate su IA possono supportare e migliorare la prevenzione e il rilevamento delle minacce grazie a capacità predittive e di adattamento, potenziare l'apprendimento dei comportamenti degli utenti e dei sistemi, permettendo di distinguere attività legittime da quelle anomale, accelerare i processi di risposta agli incidenti, l'analisi dei dati, la protezione delle reti e l'individuazione delle vulnerabilità. Al contempo l'IA sta abilitando anche l'evoluzione delle tecniche cybercriminali. La IA generativa viene oramai utilizzata tramite strumenti alternativi come WormGPT e FraudGPT, per scopi malevoli (scrittura di malware, phishing evoluto, sviluppo exploit, recononnaissance avanzata con uso di deep fake).

L'IA può quindi amplificare il potenziale distruttivo degli attacchi informatici, abbassando le barriere tecniche all'ingresso e rendendo le campagne malevole più sofisticate, credibili e difficili da intercettare. Le organizzazioni e le istituzioni sono chiamate a fronteggiare l'uso antagonista e malevolo dell'IA con altrettanto sviluppo tecnologico degli strumenti e processi di difesa, sempre nel rispetto delle normative di riferimento (GDPR e AI Act).

4.2. Quantum Technology

Le tecnologie quantistiche stanno emergendo come la nuova frontiera nella trasformazione digitale, con potenziali applicazioni sia nelle soluzioni difensive, sia offensive in ambito cybersecurity, grazie alla loro straordinaria capacità di calcolo e gestione di sistemi complessi. Come per le tecnologie di IA, anche nel quantum computing si innestano sia profili di minacce potenziali sia opportunità per migliorare i presidi di difesa. Tra le minacce potenziali si annoverano le capacità del quantum computing nel rendere vulnerabili in tempi ridotti gli attuali algoritmi crittografici. In risposta a questo rischio, sia gli USA sia l'UE si sono mosse con programmi strategici che puntano all'adozione della crittografia quantistica in modo da rendere resiliente le infrastrutture di crittografia con la maggiore penetrazione del quantum computing prevista nei prossimi anni. Infatti le tecnologie quantistiche aprono nuove possibilità per rafforzare la sicurezza e le difese non solo nel campo della crittografia, ma anche nel settore dei microprocessori per applicazioni dedicate alla cybersecurity basate su tecnologie quantistiche. In questa prospettiva, Telsy ha sviluppato un Secure Microchip, una micro-piattaforma programmabile e sicura by design che utilizza algoritmi PQC per garantire una difesa anche contro avversari quantistici, selezionato tra le migliori innovazioni tecnologiche dal GSMA. Il quantum computing rappresenta quindi una discontinuità tecnologica destinata a ridefinire i paradigmi della cybersecurity. Mentre pone serie minacce alle infrastrutture crittografiche attuali, offre al contempo strumenti inediti per rafforzare la sicurezza delle informazioni più sensibili, rendendo prioritario l'avvio di strategie di transizione verso modelli quantum-resilient.

INDICE



Un nuovo rapporto sulla cybersecurity

TIM è uno dei maggiori operatori di telecomunicazioni europei e questa posizione ci offre una prospettiva unica sul panorama delle minacce alla sicurezza informatica. Nell'ultimo anno, i nostri CyberSOC hanno analizzato quotidianamente molteplici eventi di sicurezza per prevenire possibili incidenti o mitigarne gli effetti. Un'incessante attività quotidiana che ci impegna giorno e notte a protezione delle nostre infrastrutture di rete, delle piattaforme cloud, dei sistemi di servizio, dei nostri clienti.

Nel Gruppo TIM sono presenti diversi attori che si coordinano tra di loro per far fronte alle minacce informatiche: la sicurezza di rete, il SOC, l'attività di Telsy e di TS-Way. **Dal nostro osservatorio privilegiato possiamo quindi offrire una vista unica e non replicabile sull'entità del fenomeno degli attacchi informatici in Italia,** osservare ed analizzare le caratteristiche degli attacchi sferrati, evidenziare le dinamiche e gli aspetti specificamente legati al contesto italiano, monitorare i trend delle minacce e dei gruppi criminali attivi.

Gli attacchi colpiscono cittadini ed imprese, famiglie, enti ed istituzioni. Tutti i settori rappresentano indistintamente un obiettivo degli attacchi informatici. Alcuni sono degli obiettivi più sensibili per ragioni intrinseche e strutturali, altri lo diventano per motivi opportunistici, come ad esempio un livello di difesa che viene percepito più debole dagli attaccanti. **Questo ci ha spinto a dedicare una parte della nostra analisi all'osservazione dei settori**, al fine di individuare dei possibili ambiti di criticità, per stimolare anche una maggiore consapevolezza del sistema.

La nostra visione è che quanto più forte è il sistema, tanto più efficace è la difesa che possiamo mettere in campo. Un concetto che è anche alla base del sistema di cyber difesa europeo. Per questo **cerchiamo di offrire una sintesi di come sta evolvendo il contesto normativo ed istituzionale**, evidenziando come si sta intervenendo per aumentare le difese e cosa si sta operando a livello europeo per contrastare gli attacchi sempre crescenti.

Crediamo fermamente nel potenziale del mondo digitale. È il nostro mercato e la nostra missione. Ma **lo sviluppo tecnologico deve garantire allo stesso tempo innovazione e sicurezza.** Solo un sistema affidabile può darci la possibilità di vivere pienamente il presente ed il futuro digitale, attraverso servizi che semplificano e arricchiscono la vita quotidiana.

In questa visione rientra anche la necessità di aumentare la consapevolezza di tutti sulla protezione dalle minacce informatiche e **questo rapporto rappresenta un contributo a diffondere una "cultura della cybersecurity"**, rivolgendosi non solo ai professionisti del settore, ma soprattutto ai non esperti, che vogliono farsi un'idea più precisa dell'evoluzione dello scenario della sicurezza informatica; per questo abbiamo fatto ricorso a schemi e infografiche, in modo da semplificare un tema molto complesso che riguarda tutti noi da vicino.

La nostra **visione** è che quanto **più forte è il sistema**, tanto **più efficace è la difesa** che possiamo mettere in campo e per questo **bisogna aumentare la consapevolezza** di tutti

Come leggere il rapporto

Una struttura in 4 parti

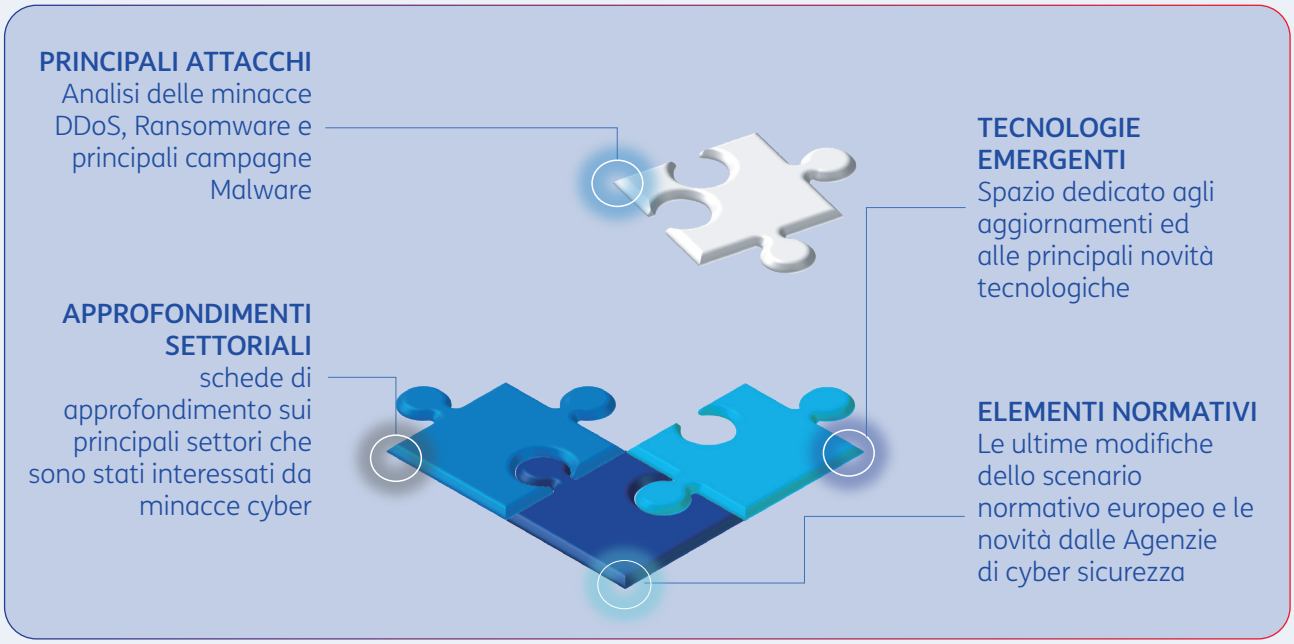
Il rapporto è organizzato su quattro principali aree di approfondimento e monitoraggio continuo:

PRINCIPALI ATTACCHI: in questa sezione vengono analizzate le principali evidenze raccolte nel corso dell'anno, basandosi sui dati provenienti in larga parte dall'attività svolta, in particolare riferiti ad eventi DDoS, (Distributed Denial of Service), Ransomware e Malware.

APPROFONDIMENTO SETTORIALE: la maggior parte degli attacchi informatici rilevati si rivolge al mondo consumer, costituito da famiglie e individui. Tuttavia, gli attacchi più dirompenti sono diretti verso il mondo delle aziende, dei settori produttivi e delle istituzioni, che rappresentano il fulcro della nostra attenzione. In questa sezione si fornisce un'analisi dei dati per ambiti di attacco, individuando i settori e gli attori istituzionali più colpiti, cercando di delineare le principali direttrici di attacco.

ELEMENTI NORMATIVI: il sistema di difesa cibernetico nazionale si basa sulle strategie e sulle normative definite a livello europeo. In questa sezione viene offerta una sintesi delle attività e delle iniziative in corso nell'Unione Europea.

TECNOLOGIE EMERGENTI: il contesto della cybersecurity è in continua evoluzione, influenzato soprattutto dalle innovazioni tecnologiche che possono rapidamente modificare le regole del settore. In questa sezione vengono aperti approfondimenti sulle novità dello scenario, sia in termini di difese sia di attacchi.



Un punto di vista autorevole sullo scenario delle minacce cyber

Il direttore del servizio Operazioni dell'Agenzia per la Cybersicurezza Nazionale, Gianluca Galasso, ci introduce ai rischi di oggi e di domani e fa il punto sulle evoluzioni attese del quadro normativo

Considerando il Rapporto prodotto dalla Fondazione Italiana sulla Cybersecurity in collaborazione con TIM sugli attacchi DDoS e Ransomware, **quali sono le considerazioni che emergono sul panorama attuale della cybersecurity in Italia**, inclusi i trend emergenti e le vulnerabilità critiche? Inoltre, quale contributo specifico vede nella **partnership tra i Soggetti privati e l'ACN nella prevenzione e nel contrasto** di queste minacce e nel migliorare la resilienza delle infrastrutture del sistema paese?

Il nostro Paese è sempre più frequentemente vittima di attacchi cyber di diversa natura; i numeri che emergono dalle attività operative dell'Agenzia per la Cybersicurezza Nazionale sono in costante crescita e pongono l'Italia sempre ai primi posti tra i paesi più bersagliati a livello europeo ed a livello globale, insieme ai paesi maggiormente prosperi. In buona sostanza possiamo tranquillamente affermare che le economie più forti, caratterizzate da un elevato livello di digitalizzazione, attraggono maggiormente le attenzioni dei cyber criminali mossi ai fini di lucro. Inoltre, la complessa situazione geopolitica in atto sicuramente produce un aumento delle fenomenologie cyber con scopi anche diversi dal solo vantaggio economico diretto.

Ransomware ed attacchi DDoS, in primis, tengono costantemente impegnati i team di incident response dell'Agenzia. I primi, sempre più sofisticati, minacciano prevalentemente gli operatori privati, in particolare quelli operanti nel manufatturiero, mentre gli attacchi DDoS, sicuramente meno dirompenti rispetto ai primi e legati prevalentemente al contesto geopolitico in atto, hanno comunque assunto in tempi recenti profili maggiormente aggressivi. Emerge, inoltre, una sempre maggiore sofisticatezza nelle campagne di spear-phishing, spesso abilitate da applicazioni di intelligenza artificiale per sviluppare complesse manovre di attacco che hanno come obiettivo le persone, prima dei sistemi, sfruttandone le debolezze (password inadeguate, comportamenti errati nell'uso di dispositivi, disattenzioni). Questo quadro di situazione è destinato a perdurare nel tempo, per cui l'obiettivo che tutto l'ecosistema cibernetico nazionale si deve porre è quello di rendere le infrastrutture digitali sempre più resilienti alle diverse forme di minaccia, adottando soluzioni organizzative e tecnologiche che riducano al minimo gli impatti degli attacchi cibernetici.

A tal fine, l'Agenzia si è da subito impegnata per sviluppare quelle capacità tecnico-operative necessarie per individuare ed anticipare le minacce cyber che gravano sul Paese a vantaggio degli operatori pubblici e di quelli privati, con particolare riguardo alle infrastrutture critiche, così come ha anche sviluppato una piena capacità di intervento in caso di incidente, in particolare a supporto degli erogatori di servizi più critici.

Per tale ragione sono state avviate nel corso dei primi due anni di attività dell'Agenzia alcune importanti iniziative che vedono il diretto coinvolgimento degli operatori privati, allo stesso tempo originatori di informazioni tecnico operative e fruitori di informazioni arricchite dalla stessa Agenzia. Faccio riferimento in particolare alla capacità denominata HyperSoc, una piattaforma di scambio dati relativi ad eventi malevoli in fase di sviluppo con il supporto di alcuni operatori privati, oggi già operativa in una versione baseline, alla quale hanno aderito alcune importanti realtà nazionali. Tale strumento, che vedrà nel corso del 2025 nuove implementazioni tecniche e l'apertura ad numero sempre maggiore di partecipanti, sicuramente rappresenta un esempio importante di collaborazione pubblico-privato sul quale l'Agenzia ripone, a ragione, molte aspettative.

02 INTELLIGENZA ARTIFICIALE E CYBERSECURITY

L'intelligenza artificiale (AI) sta rivoluzionando molti settori, inclusa la cybersecurity. Come possono le tecnologie e le capacità avanzate dell'AI, applicate ai presidi di sicurezza, sostenere le organizzazioni nell'implementazione di misure di sicurezza proattive e reattive, come il rilevamento delle anomalie, la risposta automatica agli incidenti e la previsione delle minacce? Inoltre, quali ritiene siano **i principali rischi** che le organizzazioni dovranno fronteggiare con l'evoluzione delle tecniche di attacco AI-based, utilizzando algoritmi avanzati di machine learning per identificare vulnerabilità ed exploit, e quali ambiti dovrebbero essere maggiormente monitorati per mitigare tali rischi?

L'utilizzo dell'AI per rafforzare la propria postura di sicurezza non è del tutto una novità; esistono infatti diverse soluzioni in commercio già da diversi anni che sfruttano alcune applicazioni di intelligenza artificiale di tipo "narrow", ad esempio per l'analisi dei malware o l'individuazione di anomalie nel traffico di rete. Tuttavia, le recenti innovazioni tecnologiche in questo campo stanno espandendo enormemente le possibili applicazioni dell'AI.

In particolare, oltre ai modelli di AI tipicamente utilizzati a supporto del lavoro degli analisti di primo livello, possono trovare spazio anche i modelli generativi, quali ausilio alla risoluzione di molteplici compiti attraverso una semplice interfaccia testuale, rendendo di fatto molto più accessibile tale tecnologia. Questo senza dubbio avrà un notevole impatto nella gestione operativa delle attività di cybersicurezza proattive e reattive. Infatti, grazie alle nuove applicazioni di AI è possibile, tra l'altro, fornire ad un analista dettagli rispetto ad un allarme, suggerimenti sulle azioni da svolgere per rispondere ad un incidente, una descrizione testuale delle funzionalità di un codice o un sistema automatizzato per la produzione e l'analisi della reportistica. L'ausilio di queste nuove tecnologie permetterà pertanto di migliorare ed automatizzare le attività degli analisti, soprattutto di fronte a grandi quantità di dati da analizzare e correlazioni da eseguire, a beneficio della postura cyber delle infrastrutture IT da proteggere.

In questo scenario è tuttavia importante curare la formazione degli analisti al fine di evitare, nel tempo, la perdita delle competenze tecniche necessarie per comprendere e, se del caso, validare i risultati forniti dalle macchine.

D'altro canto, l'IA è allo stesso tempo un potente strumento in grado di aumentare le capacità degli attaccanti. Ciò è già una realtà, come testimoniato dalle evidenze che iniziano ad emergere in alcuni contesti operativi e dal fatto che nel framework Mitre ATT&CK, tassonomia utilizzata a livello globale per descrive le tattiche e le tecniche utilizzate durante un attacco cyber, sia stato incluso di recente anche l'utilizzo dell'IA per l'ottenimento di capacità offensive. Diversi studi evidenziano come l'IA avrà un ruolo di amplificatore per la minaccia cyber, non solo in termini di sofisticatezza, ma anche in termini di quantità di minacce generate; ciò significa che la nuova tecnologia abiliterà minacce più sofisticate ed in numero superiore alle attuali. Gli strumenti di attacco dotati di IA potranno essere proficuamente utilizzati da attaccanti in possesso di minori capacità tecniche rispetto a quelle necessarie per condurre attacchi "convenzionali"; ciò significa che operatori che oggi possiedono capacità elementari e che pertanto sono incapaci di compiere azioni offensive importanti, avranno la possibilità eseguire attacchi

più complessi con un impatto più rilevante sulle loro vittime. Basti pensare alla facilità con cui è già oggi possibile accedere a strumenti per la creazione di contenuti multimediali falsi, i cosiddetti "deepfake", utilizzati largamente non solo per diffondere disinformazione, ma anche per realizzare sofisticati e pericolosissimi attacchi con tecniche di phishing.

Per adattarsi a questi cambiamenti in termini di sofisticatezze e magnitudine delle minacce, è necessario migliorare le proprie attività di resilienza adottando strumenti abilitati a loro volta da applicazioni di AI, per rendere più efficaci le proprie attività di risposta e di resilienza. L'adozione di queste nuove tecnologie, ad esempio quelle cosiddette di GenAI SOC, permetterà di sopravvivere ai problemi sempre pressanti dovuti alla complessità crescente dei Security Operation Center, alla cronica carenza di personale tecnico specializzato, ai volumi sempre crescenti di "alert" sui sistemi ed alla complessità delle analisi che richiedono sempre più tempo e competenze.

03 LE EVOLUZIONI DEL QUADRO NORMATIVO

Il nuovo quadro normativo comunitario e nazionale in materia di cybersecurity, caratterizzato da direttive come la NIS2, i regolamenti DORA e AI Act, il PSNC ecc., pone nuove sfide e opportunità per le organizzazioni italiane. **In che modo queste normative possono supportare le organizzazioni a migliorare la maturità della propria postura e dei presidi di sicurezza informatica?**

Il nuovo quadro normativo comunitario e nazionale in materia di cybersecurity mira a rafforzare la resilienza e la sicurezza informatica a livello nazionale ed europeo, stabilendo standard più elevati e un approccio integrato alla gestione dei rischi cyber. L'obiettivo comune è quello di rispondere alla rapida evoluzione del panorama tecnologico e alla crescente complessità delle minacce cibernetiche avendo come comun denominatore quello dell'analisi e della gestione del rischio (valutazione dei rischi, pianificazione e implementazione di opportune misure di sicurezza, monitoraggio continuo e risposta agli incidenti). Comprendere e gestire tali aspetti è una responsabilità che nessun soggetto può permettersi di ignorare, poiché garantisce un continuo miglioramento della propria postura di sicurezza informatica e deve essere intesa come una priorità strategica.

Le opportunità da considerare pongono dunque le basi per una **gestione a 360 gradi del rischio informatico in cui governance, policy e procedure non vanno a sostenere solamente la piena conformità normativa, ma rafforzano l'intera infrastruttura** del soggetto che sarà così sempre più in grado di proteggere i propri dati e informazioni, garantire la continuità operativa anche in caso di attacco informatico e salvaguardare la propria reputazione.

Tali aspetti, ovviamente, prescindono dalle dimensioni di un'organizzazione e coinvolgono allo stesso modo anche le PMI. Le aziende minori, che dispongono di risorse limitate, devono affrontare importanti sfide nell'adeguarsi a normative complesse. Tuttavia, per garantire che anche le PMI possano trarre vantaggio da questo quadro normativo, è essenziale un supporto mirato dal Sistema Paese, che includa formazione, incentivi finanziari e strumenti di conformità accessibili.

04 LE SFIDE DEI PROSSIMI ANNI

Alla luce della «Strategia Nazionale di Cybersicurezza 2022 – 2026», quali **sono gli ambiti e le sfide principali che l'ACN dovrà affrontare nei prossimi anni?** Qual è il suo punto di vista su come le organizzazioni private, comprese quelle che erogano servizi essenziali, possono cooperare in modo efficace per garantire la sicurezza del sistema paese? In particolare, quali **strategie di collaborazione** ritiene possano essere adottate per mitigare le minacce cyber e proteggere le infrastrutture critiche da attacchi e violazioni della sicurezza?

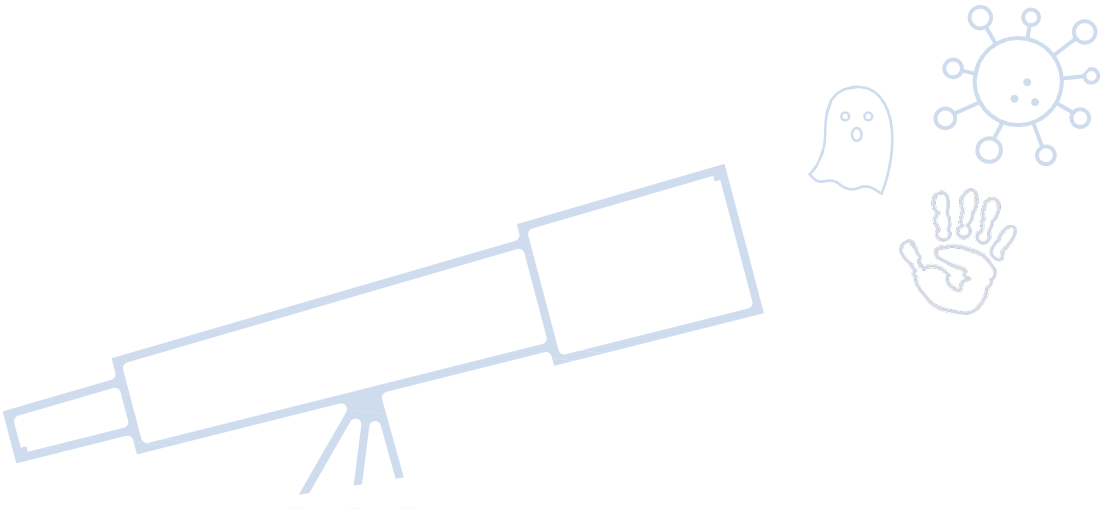
La digitalizzazione, motore delle funzioni e dei servizi essenziali dello Stato, rende la cybersicurezza un obiettivo di fondamentale importanza per la tutela degli interessi nazionali nello spazio cibernetico. Ad essa è strettamente connessa una velocissima evoluzione tecnologica che, oltre agli aspetti innovativi, comporta nuovi rischi per la sicurezza a cui non sempre corrisponde un adeguato grado di consapevolezza da parte della società. L'Agenzia con la **Strategia Nazionale di Cybersicurezza 2022-2026** ha perciò impostato un piano volto a pianificare, coordinare e attuare una serie di misure tese a rendere il Paese più sicuro e resiliente, che mira ad affrontare le seguenti sfide:

- assicurare una **transizione digitale cyber** resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo;
- anticipare l'**evoluzione della minaccia** cyber;
- prevenire e gestire le **crisi cibernetiche**;
- garantire **autonomia strategica** nazionale ed europea nel settore del digitale.

Per affrontare al meglio tali aspetti, sono stati individuati **tre obiettivi fondamentali** in cui vengono raggruppate per aree tematiche le misure funzionali ad assicurare la concreta attuazione della Strategia:

- **PROTEZIONE** – proteggere gli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, in cui si innestano normative, misure, strumenti e controlli necessari ad abilitare la transizione digitale del Paese.
- **RISPOSTA** – impiegare elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta associati alle minacce, agli incidenti e alle crisi cyber nazionali, attivando tutti quei processi che coinvolgono l'intero ecosistema di cybersicurezza nazionale.
- **SVILUPPO** – sviluppare in maniere sicura delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

L'Agenzia con la Strategia Nazionale di Cybersicurezza 2022-2026 ha perciò impostato un piano volto a pianificare, coordinare e attuare una serie di misure tese a rendere il Paese più sicuro e resiliente



Nell'ambito dell'obiettivo "Risposta" trovano spazio i programmi denominati "servizi cyber nazionali", che l'Agenzia sta sviluppando con il fine di potenziare le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione delle minacce cyber. È in questo contesto che si innestano **HyperSOC, ISAC Italia e la rete nazionale di ISAC** dove, tramite il rafforzamento della Partnership Pubblico-Privato, le organizzazioni possono collaborare in sinergia con ACN per individuare precocemente eventuali pattern di attacco complessi che potrebbero rappresentare minacce emergenti di interesse nonché rafforzare la capacità di prevenire, identificare, mitigare e contrastare i rischi informatici attraverso analisi di contesto basate sulle peculiarità del proprio settore.

L'approccio adottato è quello di una comunicazione bidirezionale tra tutti gli attori coinvolti, in modo tale che i dati scambiati possano diventare informazioni validate, analizzate e arricchite così da poter potenziare il proprio livello di consapevolezza situazionale. La protezione delle infrastrutture critiche nazionali dalla minaccia cyber non risulta dunque una sfida individuale, quanto piuttosto una responsabilità collettiva dove la creazione di un ecosistema di fiducia parte proprio dalla condivisione di conoscenze sui rischi informatici. La cybersicurezza è un problema di rischi e come tale va affrontato insieme.

Nell'ambito dell'obiettivo "Risposta" trovano spazio i programmi denominati "servizi cyber nazionali", che l'Agenzia sta sviluppando con il fine di potenziare le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione delle minacce cyber

PRIMA PARTE

Principali attacchi

Man mano che la digitalizzazione si estende a più attività, interessando tutti gli ambiti della nostra vita, si amplia l'area di esposizione a minacce provenienti dal mondo cibernetico e questo riguarda tutti: istituzioni, imprese, enti, comuni cittadini. L'unica certezza è che tutti siamo potenzialmente soggetti a subire gli effetti di un attacco cyber: blocco delle attività, impossibilità di accedere a computer, server, siti o altre risorse informatiche, sottrazione di dati ed informazioni, siano esse sensibili o meno. Costruire un sistema sicuro al 100% è impossibile, ma costruire un sistema resiliente si può, partendo dalla maggiore conoscenza del modo in cui avvengono questi eventi. In questa prima parte ci focalizziamo sugli eventi che i gruppi di difesa cibernetica del Gruppo TIM hanno rilevato nel corso dell'ultimo anno. Parliamo di eventi perché non sempre le minacce che ci arrivano si traducono in attacchi e incidenti.
L'attività di prevenzione, difesa e contrasto svolta dai team del Gruppo, in particolare quelli operanti nel Security Operation Center (SOC) e quelli impegnati in attività preventiva di Threat Intelligence, è fondamentale.

Gli attacchi

Come li classifichiamo?

I primi problemi che si incontrano quando si entra nel mondo della cybersecurity riguardano innanzitutto la comprensione di cosa stiamo osservando. La complessità del tema è resa ancora più accentuata dal numero di punti di vista che possiamo assumere, ciascuno dei quali può utilizzare tassonomie differenti, ciascuna ha il suo scopo.

Ad esempio, una delle più diffuse è la **tassonomia MITRE ATT&CK**, con l'obiettivo di costituire una base conoscitiva comune.
Per questo distingue il campo di osservazione in tre «domini»: Enterprise (reti d'impresa e cloud), Mobile e Sistemi di Controllo Industriale. Per ciascuno di questi individua le tattiche (le motivazioni), le modalità (le tecniche messe in campo) nonché le varianti e le procedure che alcuni avversari possono attuare (sub-techniques). La mappa è in continua evoluzione. Ad esempio, per il segmento Enterprise, tra aprile 2024 e febbraio 2025 le tattiche sono rimaste invariate (14), le tecniche sono di una unità (da 202 a 203) mentre sono si sono incrementate le varianti (da 435 a 453).

Un altro riferimento è costituito dalla **tassonomia VERIS** (Vocabulary for Event Recording and Incident Sharing) che si concentra invece sugli incidenti di sicurezza. Questa tassonomia è stata sviluppata da un gruppo di esperti incaricati dalla Commissione Europea allo scopo di creare un linguaggio comune per descrivere che cosa si verifica in un attacco e individua 4 prospettive: chi è dietro un incidente (Actors), quali metodi utilizza (Actions), quali dispositivi attacca (Assets) e come sono stati colpiti (Attributes).

A sua volta, ciascuno di questi ambiti è declinato in un numero di opzioni possibili in modo da definire un framework comune per descrivere gli eventi registrati.

Per i nostri **obiettivi**, che cercano di fornire una vista degli attacchi cyber privilegiando una **più facile comprensione del fenomeno**, adotteremo la **classificazione dell'ENISA**

Le tassonomie descritte hanno un enorme valore per gli esperti del settore, ma risultano troppo complesse per chi ha meno competenze. Per questo seguiremo l'**approccio dell'ENISA, l'Agenzia Europea di Cybersecurity**, che nei suoi rapporti annuali individua 8 principali categorie di minacce e che risulta più immediato e comprensibile.

Le principali minacce cyber

L'ENISA, l'agenzia della cybersecurity europea, nell'ambito dello European Threat Landscape, individua 8 tipi di attacchi cyber, ossia di eventi consapevoli diretti a penetrare le maglie di difesa di organizzazioni, aziende e privati per finalità differenti.

Attacchi DOS e DDoS
(Distributed Denial Of Service)

Attacco che mira a rendere inutilizzabile una risorsa/servizio sovraccaricando i componenti delle infrastrutture di rete

Minacce ai Dati

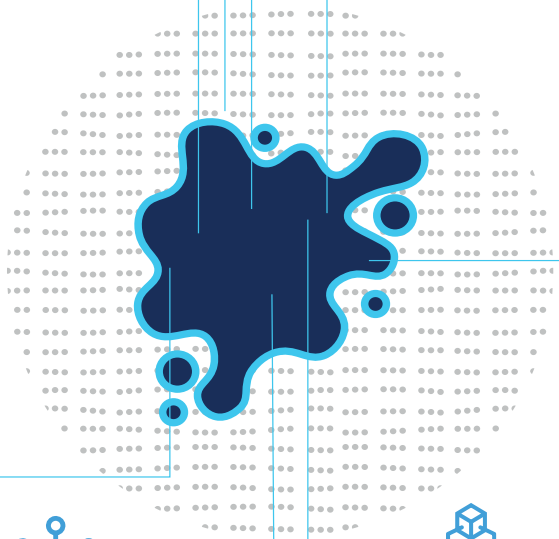
Accesso non autorizzato ai dati per sottrazione, divulgazione e manipolazione. Spesso combinato con ransomware e attacchi DDoS

Ransomware

L'attacco mira a penetrare nei sistemi (reti, computer, cloud, ecc.), prendere il controllo delle risorse (dati, asset, ecc.) cifrando e nella maggior parte dei casi esfiltrando i dati al fine di chiedere un riscatto

Malware

Software o firmware che esegue un processo non autorizzato con impatto negativo sull'integrità o sulla disponibilità o sul funzionamento di un sistema.



Minacce di ingegneria sociale

Comprende un'ampia gamma di attività che sfruttano l'errore con l'obiettivo di ottenere l'accesso a informazioni o servizi.

Minacce alle reti e ad Internet

Incidenti in cui si verifica un'interruzione intenzionale o non intenzionale dell'accesso ad internet o delle comunicazioni elettroniche

Attacchi alle catene di fornitura

Un attacco che prende di mira il rapporto tra le organizzazioni e i loro fornitori (es. penetra la rete di un'azienda per esfiltrare dati all'azienda cliente)

Manipolazione Informazione

Imprese e privati presi di mira da campagne di disinformazione prevalentemente finalizzate a screditarne la reputazione o creare incertezza, tra cui rientrano i casi di FIMI (Foreign Information Manipulation and Interference).

Attacchi **DDOS**

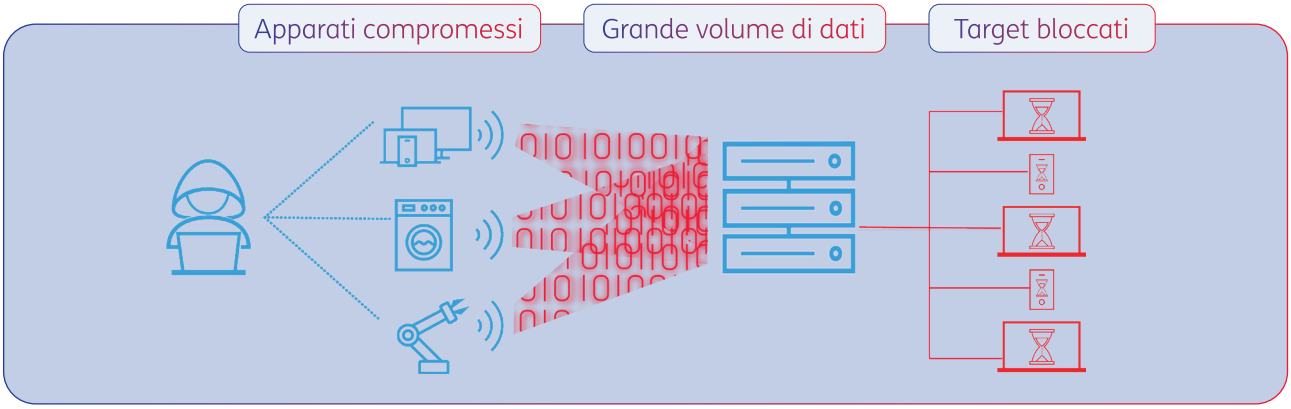
Un attacco di tipo DOS «Denial of Service» rientra tra le minacce alla disponibilità di un asset/servizio. In questo rapporto ci concentreremo sugli attacchi di tipo volumetrico in cui un attaccante è in grado di attivare un importante volume di traffico verso una risorsa di rete, un sito web o un server sovraccaricandolo ed impedendogli di fornire il servizio. Questo viene fatto anche attivando dispositivi ed apparati di persone ignare di cui l'attaccante è in grado di prendere il controllo. L'attacco proviene quindi da più direzioni e per questo è definito «distribuito».

Un utente che vuole utilizzare un sistema sotto attacco DDoS, accedere a dati o altre risorse rilevanti si trova nell'impossibilità di farlo perché l'enorme flusso di dati (oppure, nel caso di eventi DDoS non volumetrici, il numero di richieste) ne paralizza la funzionalità. L'effetto è simile a quello che si verifica quando si prova ad acquistare un biglietto per un evento particolarmente richiesto ed il sistema non risponde. Questo succede perché il traffico inonda il target da colpire oltre la capacità che ha la risorsa colpita (un server, un sito, ecc.) di gestire questo improvviso afflusso.

Nonostante sia chiaro il modo in cui avviene l'aggressione, l'ENISA evidenzia che non è sempre facile individuarlo per una serie di motivi:

- Gli attacchi possono iniziare lentamente o procedere ad ondate senza un chiaro inizio/fine rendendo difficile distinguere eventi diversi.
- Un attacco può colpire più siti da uno stesso indirizzo IP complicando la valutazione dell'obiettivo e della durata dell'attacco.
- Gli attacchi possono provenire da più aree geografiche.
- Anche i sistemi di monitoraggio possono essere colpiti, rendendo più difficile la rilevazione.

Inoltre, emergono sempre nuove casistiche: con l'intelligenza artificiale (IA) gli attaccanti possono orchestrare e mascherare gli assalti. I SOC del Gruppo TIM lavorano sulla rete e sono quindi in grado di rilevare e intervenire prima che gli attacchi si manifestino concretamente. Di seguito vengono forniti i dati di questa attività di monitoraggio, prevenzione e contrasto.



Attacchi DDOS
Sintesi **2024**

Gli attacchi DDoS crescono di nuovo a livelli pandemia

+36%

Eventi DDoS 2024 vs 2023

Il 2024 registra una forte intensità di attacchi DDoS per volume, intensità, durata e severità. Ad alimentare questo fenomeno contribuiscono i conflitti in corso, ma anche nuove tecniche di attacco

>20Gbps

4 ogni 10 eventi hanno una potenza superiore a 20 Gbps

I settori più colpiti da eventi DDoS

Istituzioni
Servizi professionali
Settore finanziario
Telecomunicazioni
Difesa

oltre il 25%

degli eventi sono gravi con potenza massima e durata superiore alle due ore

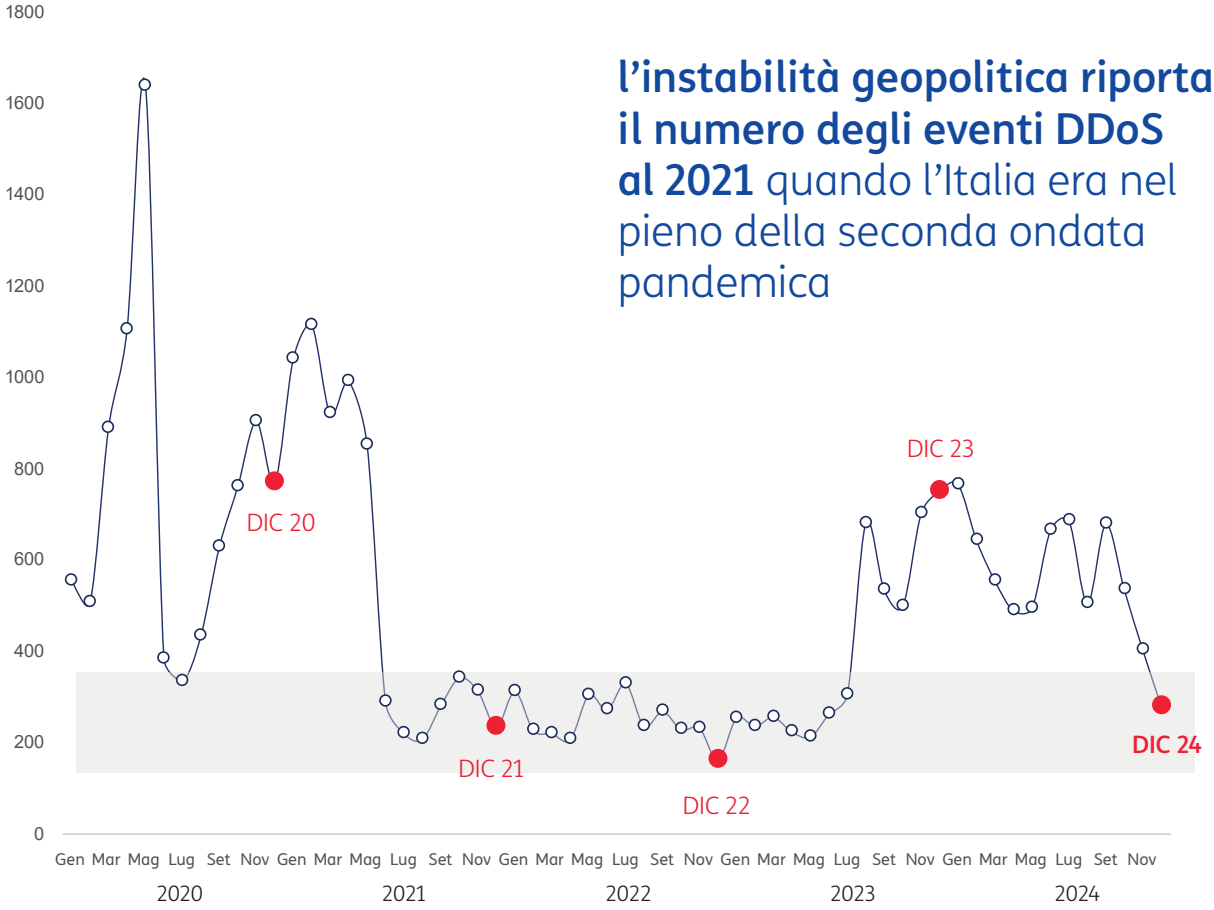
x4 la severità rispetto al 2020 (gli eventi gravi erano il 6% del totale)

Attacchi DDOS
2024: un anno **intenso**

Il 2024 ha registrato una forte intensità in termini di eventi DDoS: in media, circa 560 casi per mese con due momenti di picco ed una progressiva diminuzione nell'ultimo trimestre dell'anno. Osservando la dinamica degli eventi in un quadro più ampio (2020-2024), si individuano tre periodi distinti di lunghezza simile:

- gennaio 2020 - agosto 2021, con una media di circa 725 eventi al mese e due picchi di 1.600 e 1.100 casi. La grande intensità di questo periodo, con il Paese alle prese con i lockdown, si spiega con l'ampliamento della superficie d'attacco (lavoro a distanza, didattica online, ecc.).
- settembre 2021 - luglio 2023, a bassa intensità, con una media di circa 260 eventi al mese.
- agosto 2023 - dicembre 2024, con una media di 580 casi per mese, con un picco di 765 eventi che si colloca a livelli simili a quelli del periodo pandemico a causa della instabilità del quadro geopolitico.

Eventi DDoS in Italia rilevati dal SOC di TIM anni 2020-2024



l'instabilità geopolitica riporta il numero degli eventi DDoS al 2021 quando l'Italia era nel pieno della seconda ondata pandemica

Il boom degli attacchi DDOS
1) l'influenza dei **conflitti**

La diffusione di nuove tecniche di attacco DDoS aumenta la potenza degli eventi di questo tipo, come potrà essere osservato più avanti nel rapporto. Tuttavia, a queste cause "interne" si aggiungono anche altre motivazioni legate al contesto, come ad esempio i lockdown nel 2020-2021 e le tensioni geopolitiche degli ultimi mesi.

In effetti, un attacco DDoS ha molteplici motivazioni (economiche, ideologiche, personali) e può anche essere utilizzato come strumento di cyber-warfare nella cosiddetta guerra ibrida per provocare danni economici, interruzioni ad infrastrutture e servizi essenziali di potenziali avversari, dare una dimostrazione di forza.

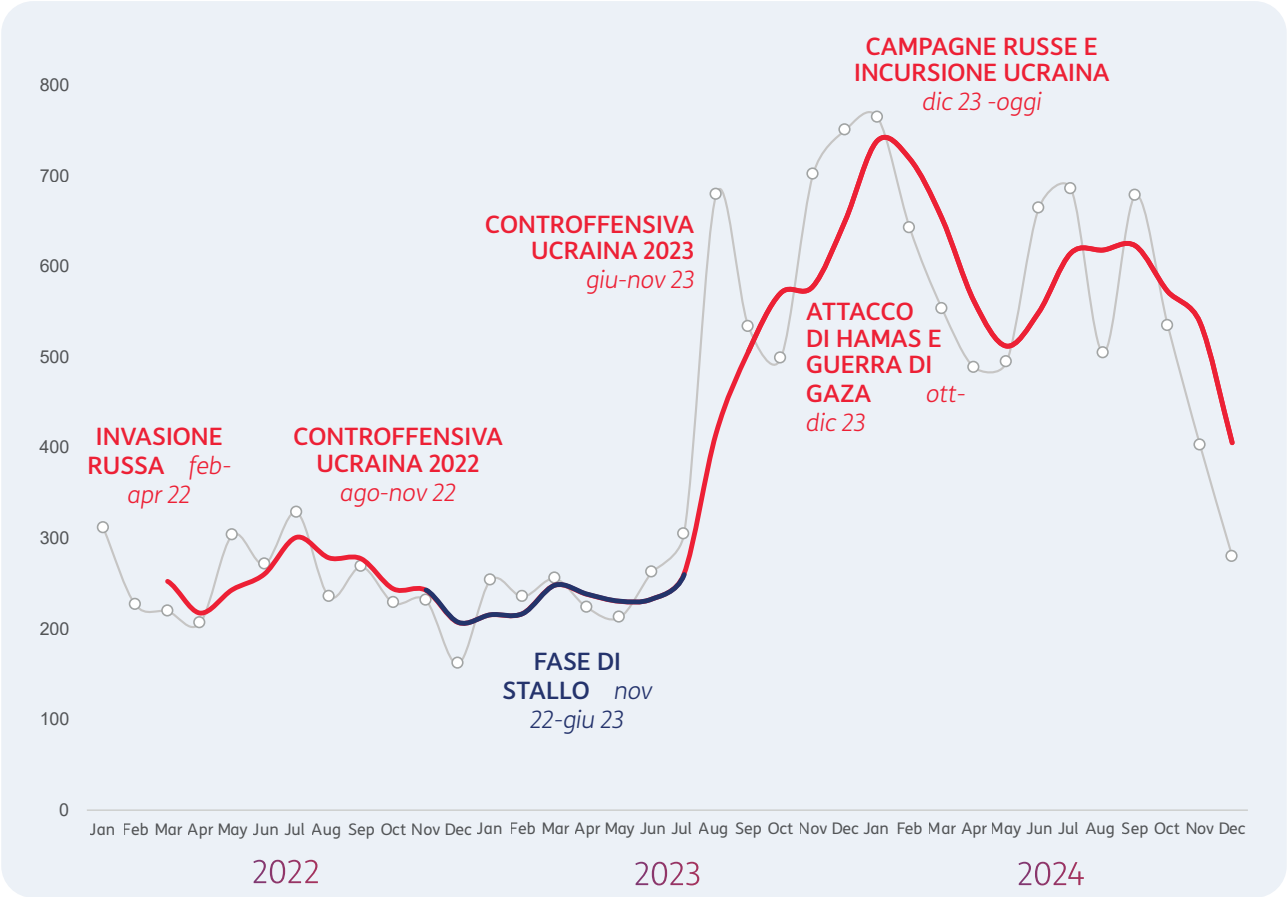
La crescita degli eventi DDoS degli ultimi mesi si lega sicuramente ai conflitti presenti in questo periodo e va a colpire i Paesi europei per le posizioni di sostegno espresse rispetto ai belligeranti. Nel 2022 e nella prima metà del 2023, gli eventi DDoS mostrano una dinamica contenuta per poi esplodere a partire da agosto, in cui si registra una prima impennata che si ripete tra novembre e gennaio 2024 in un momento in cui si intensifica il conflitto russo-ucraino e scoppia quello tra Israele ed Hamas. Da questo punto di vista, il fenomeno degli eventi DDoS può assomigliare ad un termometro che misura la stabilità geopolitica. Anche ENISA evidenzia una crescita degli incidenti DDoS che nel periodo di osservazione luglio 2023-giugno 2024 raddoppiano in termini di incidenza rispetto a tutti gli eventi registrati: dal 21% passano al 41% del totale.

Attacchi DDoS in forte aumento anche come conseguenza dei conflitti in atto

GLI ATTACCHI DDoS, UN'ARMA DI CYBERWARFARE

Le motivazioni dietro gli attacchi DDoS non sono solo di tipo finanziario ma anche di natura geopolitica. Il conflitto in Ucraina ha visto il ritorno degli attivisti con motivazioni politiche e si è registrato un ulteriore peggioramento a causa del conflitto nella striscia di Gaza.

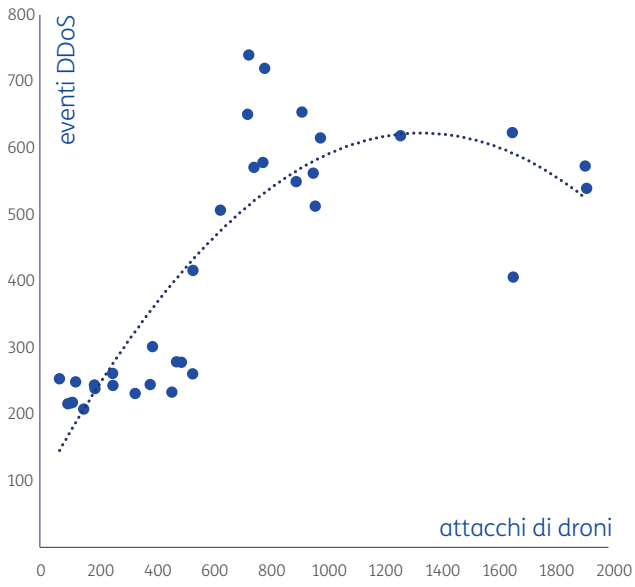
ATTACCHI DDoS IN ITALIA RILEVATI DAL SOC DI TIM
in relazione alle fasi dei conflitti in atto – anni 2023-2024



Fasi Conflitto Russo-Ucraino https://en.wikipedia.org/wiki/Timeline_of_the_Russian_invasion_of_Ukraine#

Abbiamo provato a mettere in relazione l'evoluzione degli eventi DDoS dal 2022 al 2024 e i dati raccolti da ACLED (ONG indipendente senza scopo di lucro) sul conflitto russo-ucraino, in particolare gli attacchi realizzati con droni, che hanno rappresentato una escalation tecnologica a partire dalla metà del 2023.

Pur con molte cautele, si osserva una correlazione empirica tra le due serie. Anche questo può avvalorare la tesi di una matrice geopolitica dietro l'impennata degli attacchi registrata tra la metà del 2023 ed il 2024.



fonte dati: ACLED.
I dati relativi agli attacchi tramite droni sono stati estratti da ACLED Armed Conflict Location & Event Data. I dati sono stati estratti dal database "Ukraine & Black Sea" reperibile al link https://acleddata.com/ukraine-conflict-monitor/#data (aggiornamento dati 28 febbraio 2025, media mobile 3 mesi)

Il boom degli attacchi DDoS
2) nuove tecnologie e **tecniche di attacco**

Nel corso del 2023 e del 2024 sono cresciute anche minacce portate utilizzando altre tecniche. Un esempio sono gli attacchi DDoS di tipo iper-volumetrico che indirizzano decine e a volta centinaia di milioni di richieste al secondo a delle applicazioni impedendone la funzionalità. Da questo punto di vista gli attaccanti possono sfruttare l'allargamento dei vettori di attacco potenziali, ossia apparati compromessi di cui si impossessano e che contribuiscono ad alimentare le richieste o il traffico. Sono stati rilevati attacchi lanciati da sistemi IoT ma anche da Server Privati Virtuali (VPS) o – più in generale – da Macchine Virtuali (VM), che generano un traffico 5.000 volte maggiore grazie alle risorse computazionali e alla larghezza di banda a disposizione.
L'utilizzo combinato di più vettori di attacco rende più difficile i meccanismi di difesa tradizionali e permette anche di colpire diversi livelli di rete ed elementi all'interno dell'infrastruttura di un'organizzazione, agendo contemporaneamente sul sito web, sulla rete/infrastruttura, sui dispositivi per infliggere il massimo danno possibile.

Un'altra evoluzione sono gli attacchi UDP che colpiscono il protocollo di rete che permette lo scambio di pacchetti TCP e l'interazione tra i sistemi. Anche in questo caso la gran mole di richieste impedisce al protocollo UDP di funzionare in modo efficace. Infine sono stati rilevati diversi attacchi a livello applicativo che prendono di mira siti Web e punti di accesso API, i protocolli che permettono alle applicazioni di interagire in modo automatico tra loro. Poiché questo tipo di traffico è crittografato, il rilevamento di attività malevole che imitano richieste legittime diventa complesso. A tutto questo si aggiunge l'uso di tecniche di evasione come indirizzi IP dinamici, intestazioni http casuali, ed altro. Infine, ci sono gli attacchi a livello di DNS, il sistema che «traduce» gli indirizzi IP da numeri (es. 192.158.X.YY) a indirizzi comprensibili (www.nomedifantasia.com). Il server DNS è investito da un numero richieste di inoltramento che non riesce a verificare e si blocca.

Attacchi ipervolumetrici

Attacchi che permettono di aumentare la potenza di attacco (nell'ordine dei Terabit/sec) a volte utilizzando più vettori

Attacchi da botnet VM/VPS

Attacchi lanciati da macchine virtuali (VM) o server privati virtuali (VPS) che generano un traffico 5000 volte più alto di un solo dispositivo

Attacchi multivettore

Combinazione di più vettori di attacco all'interno di un'unica campagna per rendere più difficile i meccanismi di difesa tradizionali

Attacchi a livello applicativo

Prendono di mira sempre più siti Web e interfacce di gestione (API gateway), imitando richieste legittime e rendendo difficile l'identificazione

Il volume degli eventi DDoS quasi 5 eventi al giorno di **intensità elevatissima**

UN PARAMETRO RILEVANTE: LA CLASSE D'INTENSITÀ DELL'ATTACCO

Se il numero di eventi DDoS registrati in media nel 2024 si colloca a livelli paragonabili a quelli del secondo lockdown pandemico, cambiano completamente le caratteristiche.

Uno dei parametri rilevati è l'intensità: tanto più questa è alta, tanto più elevata è la capacità aggressiva che viene messa in campo dagli attaccanti. Questo non significa che gli attacchi più deboli siano meno pericolosi, dal momento che sono in grado di mimetizzarsi con il traffico legittimo, diventano più difficili da rilevare e possono quindi andare a segno in modo più subdolo. Nella nostra analisi suddividiamo gli eventi in 6 classi di intensità: i primi tre gruppi arrivano fino a 10 Gigabit per secondo (Gbps) mentre gli ultimi due raccolgono i casi dai 20 Gbps a crescere. Il modo in cui l'intensità varia nel tempo mostra con i fatti come le nuove tecniche di attacco stiano cambiando il panorama degli attacchi DDoS.

CIRCA 6700 EVENTI NEL CORSO DEL 2024, IN PREVALENZA A BASSA INTENSITÀ

Nel 2024, il 47% dei circa 6.700 eventi registrati (+36% rispetto al 2023) ha avuto un'intensità inferiore ai 10 Gbps. Sebbene quasi la metà degli eventi sia a bassa intensità, il loro peso sul totale dei casi registrati è in progressiva diminuzione.

Fino al 2021, gli eventi a bassa intensità rappresentavano almeno l'80% del totale, mentre quelli con flussi superiori ai 20 Gbps erano circa il 5%. Nel 2023, gli eventi a bassa intensità erano già scesi al 56% del totale e quelli di portata superiore ai 20 Gbps erano saliti al 30%. Nel 2024, il peso dei casi di intensità superiore ai 20 Gbps raggiunge quasi il 39% dei casi. In particolare, l'ultima classe, quella con eventi di intensità superiore ai 40 Gbps diventa quella dal peso più significativo (26%).

MA GLI ATTACCHI AD ELEVATISSIMA INTENSITÀ SONO CIRCA 5 AL GIORNO, UN VALORE MOLTO RILEVANTE

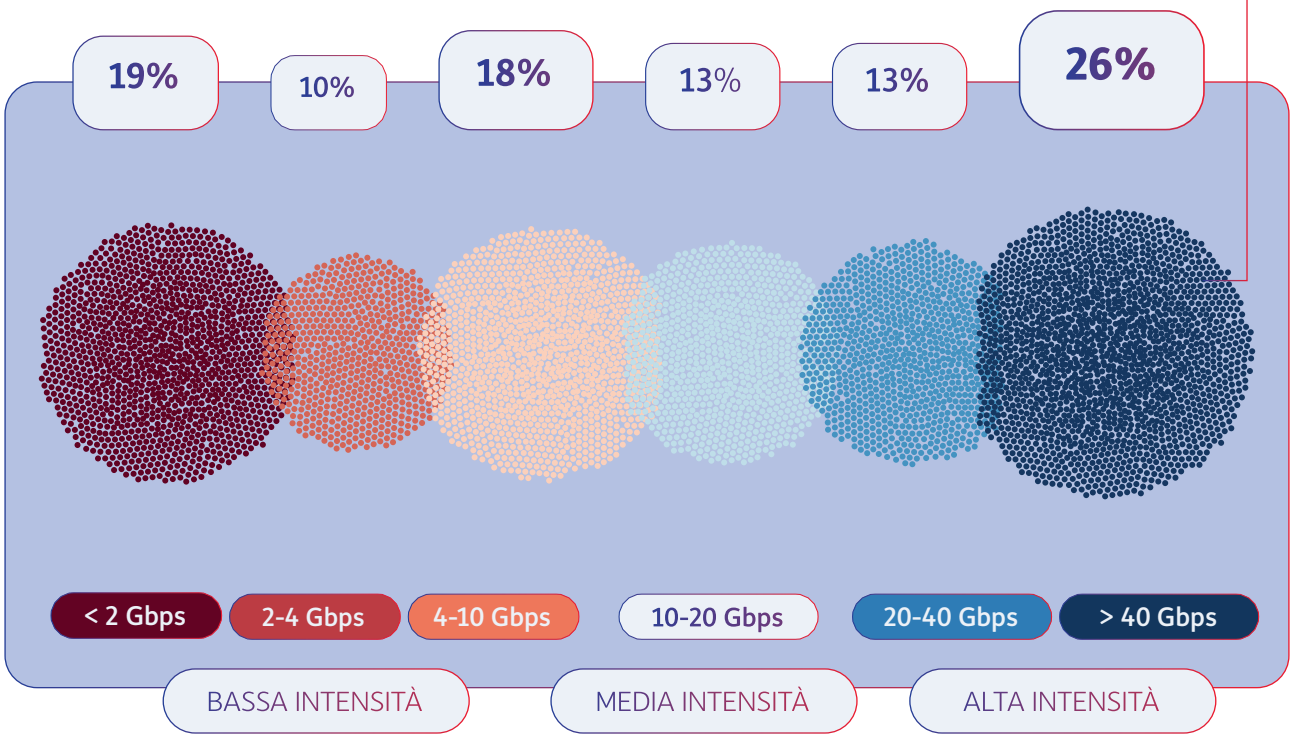
Questo significa che ogni giorno registriamo in media 18-19 eventi, di cui circa 7 con intensità superiori a 20 Gbps e 5 che superano i 40 Gbps, ossia circa 1 ogni 4.

Il volume degli eventi DDoS
ripartizione per **intensità**

Questo grafico rappresenta gli eventi di tipo DDoS che sono stati rilevati dal Security Operation Center di TIM nel corso **del 2024**.

Sono circa 6.700 e li abbiamo rappresentati in modo da evidenziare il diverso livello di intensità. **A sinistra**, in toni rosso- arancio **gli eventi meno intensi**, con una potenza inferiore ai 10 Gbps. **A destra**, in gradazioni di blu, **gli eventi più intensi**, superiori ai 20 Gbps.

Ogni **10** eventi,
4 sono ad **alta intensità**

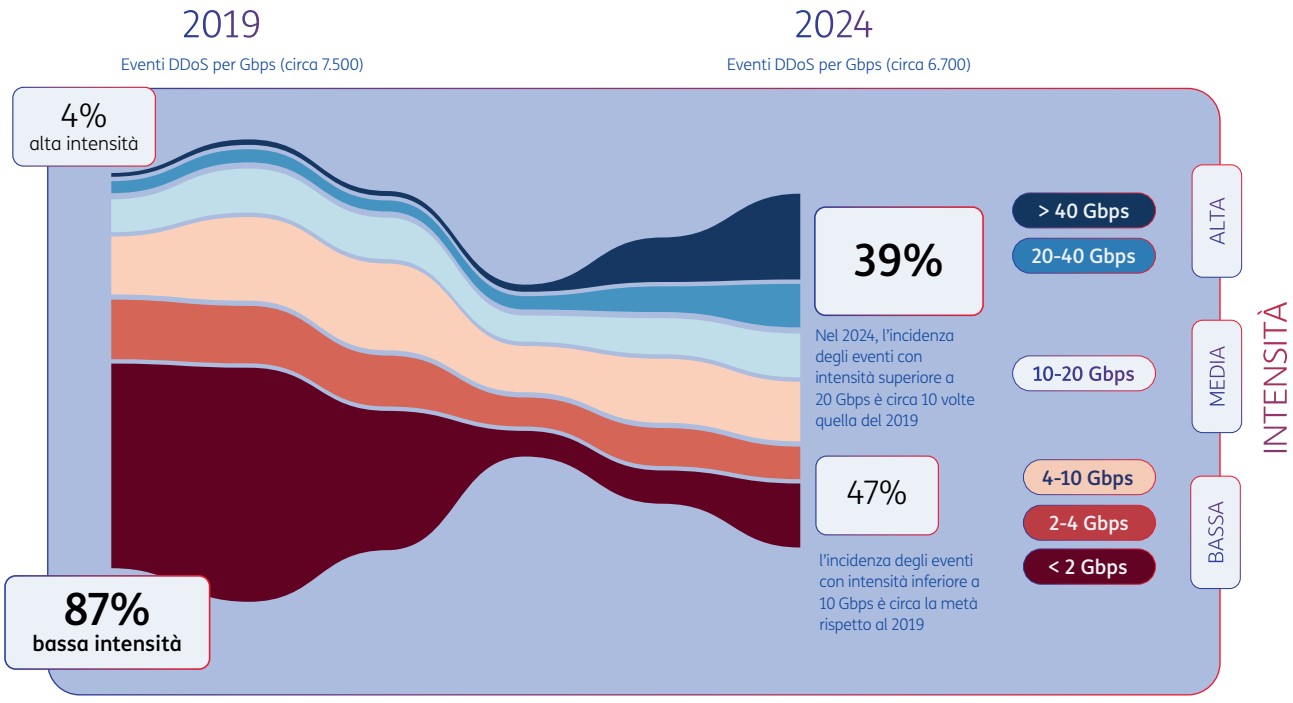


Nel 2024 rispetto al 2023 raddoppia il peso degli eventi ad alta **intensità**

Il fenomeno degli eventi DDoS ad alta intensità si osserva meglio considerando la serie storica di tutti i casi registrati a partire dal 2019, ripartiti per classe di intensità.

Il confronto mostra chiaramente uno spostamento progressivo delle proporzioni della distribuzione: mentre nel 2019 e negli anni successivi era molto elevato il peso degli eventi a bassa intensità (intorno all'87%), negli ultimi anni tende ad aumentare l'incidenza di quelli ad alta intensità, che rappresentano oggi circa il 40% del totale. Inoltre, nel 2024 gli eventi si polarizzano nelle due classi estreme dove sono raccolti gli eventi di maggiore e di minore intensità. Anche questo è una spia di come si stia modificando il panorama degli attacchi DDoS.

Eventi DDoS in Italia per livello di intensità: 2019 vs 2024



All'origine di questa intensa crescita ci sono diversi fattori: la diminuzione del costo dei servizi di DDoS a pagamento per Gigabit al secondo offerto, una maggiore presenza di botnet sfruttabili per scopi illeciti, un certo ritardo nell'adozione dei servizi di anti-spoofing e la forte accentuazione degli attacchi dovuta al peggioramento del contesto geopolitico.

Picchi di Attacco: la banda massima **utilizzata**

LA DIMENSIONE DI BANDA DI ATTACCO

Un'altra caratteristica degli eventi, connessa a sua volta all'intensità dell'attacco, è la capacità di banda utilizzata.

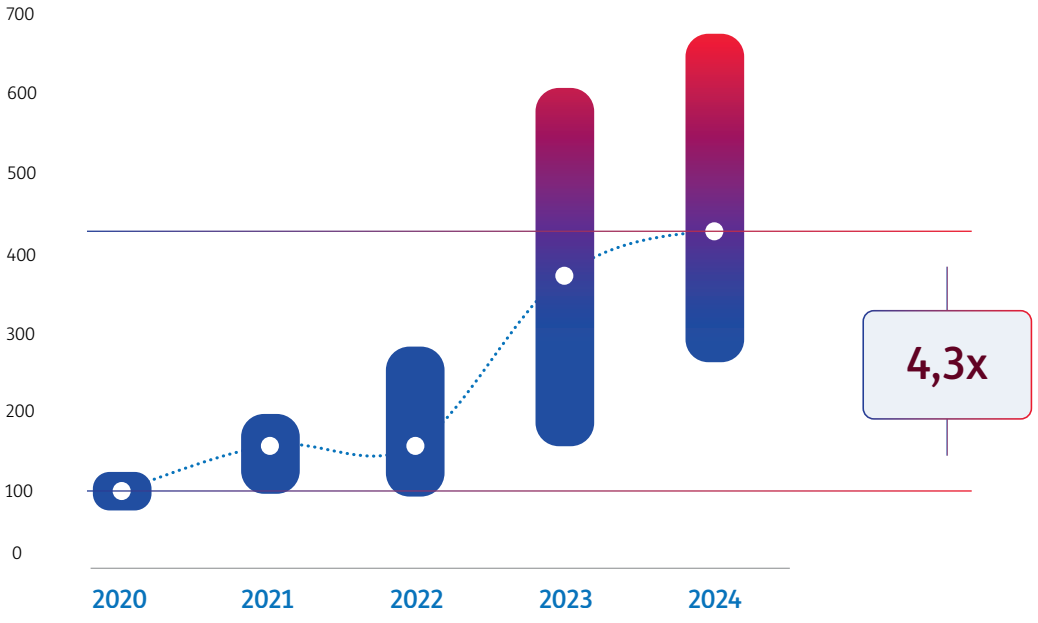
In questo caso riportiamo i picchi massimi raggiunti da un singolo attacco nel corso di un periodo temporale, tipicamente un mese o un trimestre.

Nel corso del 2024, ed in particolare nel primo trimestre dell'anno, si è registrato anche un significativo incremento della banda massima utilizzata da un singolo attacco ed anche questo è un elemento che differenzia il tipo di attacchi che abbiamo registrato nel 2024 rispetto a quelli del 2020.

Considerando i picchi massimi raggiunti da un singolo evento nel corso di un mese, si osserva che questo valore aumenta nel tempo. Ad esempio, se nel 2020 la media dei picchi registrati in ogni mese dell'anno è pari a 100, nel 2024 lo stesso valore cresce a 4,3. Aumenta anche la banda dell'attacco più significativo registrato nel 2024 (circa 6,6 volte il massimo assoluto del 2020) e si allarga la forbice tra il picco massimo ed il picco minimo dell'anno. Se quindi il volume di eventi registrati nel 2020 resta ancora ineguagliato, la potenza aumenta sensibilmente nel corso del tempo con forti oscillazioni da un mese all'altro.

Max Dimensione in banda eventi DDoS (Gbps)

Numeri indice (100= media 2020)



Aumenta la dimensione di banda utilizzata per attacchi DDoS.

Tra il 2020 ed il 2024, la media degli attacchi più significativi aumenta di oltre 4 volte

Attacchi di lunga durata: i 40 minuti che **scottano**

UN SECONDO PARAMETRO FONDAMENTALE: LA DURATA DELL'ATTACCO

Il livello d'intensità va esaminato insieme alla durata dell'evento. Un evento DDoS può avere durate differenti, minuti, ore e addirittura giorni. Nella maggior parte dei casi l'evento si svolge in un tempo relativamente breve, ma sta aumentando la durata del fenomeno.

Nella nostra classificazione distinguiamo gli eventi brevissimi (al di sotto dei 10 minuti), brevi (tra 10 e 30 minuti, attacchi di durata media che vanno da 30 a 120 minuti e attacchi di durata lunga (da 120 minuti a 24 ore) e molto lunga (superiori alle 24 ore).

9 ATTACCHI DDoS SU 10 HANNO UNA DURATA INFERIORE AI 30 MINUTI

Attacchi brevi e brevissimi.
Gli eventi di durata breve e brevissima rappresentano il 90% dei casi rilevati nel corso del 2024 e questa quota è in crescita: nel 2022 rappresentavano circa l'85%. I casi brevi (tra 10 e 30 minuti) sono all'incirca la metà degli eventi registrati.

Attacchi con durata superiore alle 2 ore.
Le categorie degli attacchi lunghi risultano ancora molto esigue e quindi episodiche, ma sono in crescita perché connesse a maggiore disponibilità di banda larga e uso di tecnologie innovative (IA, Cloud), nuove modalità di attacco. Tra gli attacchi superiori ai 30 minuti, la numerosità diminuisce all'aumentare della durata. Il primo gruppo di attacchi lunghi, che include i casi che hanno una durata tra 2 e 24 ore, sono stati quasi 170 (in crescita di 10 unità rispetto al 2023). Si dimezzano invece gli attacchi superiori al giorno: da 22 a 11, valori comunque molto ridotti.

Complessivamente, resta invariato il peso degli attacchi di durata superiore alle due ore rispetto al totale (all'incirca il 4% del totale).

GLI EVENTI DDoS CON DURATA SUPERIORE ALLE 2 ORE HANNO UN PESO IN MINUTI PARI AL 57% DEL TOTALE

La prospettiva cambia se trasformiamo i casi in minuti, prendendo a riferimento la mediana di ciascun intervallo temporale come durata di ogni evento DDoS*. In questo caso, i circa 180 eventi con una lunghezza temporale di 2 ore e più hanno un «peso» pari all'incirca al 57% del numero totale di eventi (nel 2023 erano il 65%). * Per gli eventi di durata superiore alle 24 ore sono stati considerati 1441 minuti, pari a 24 ore + 1 minuto.

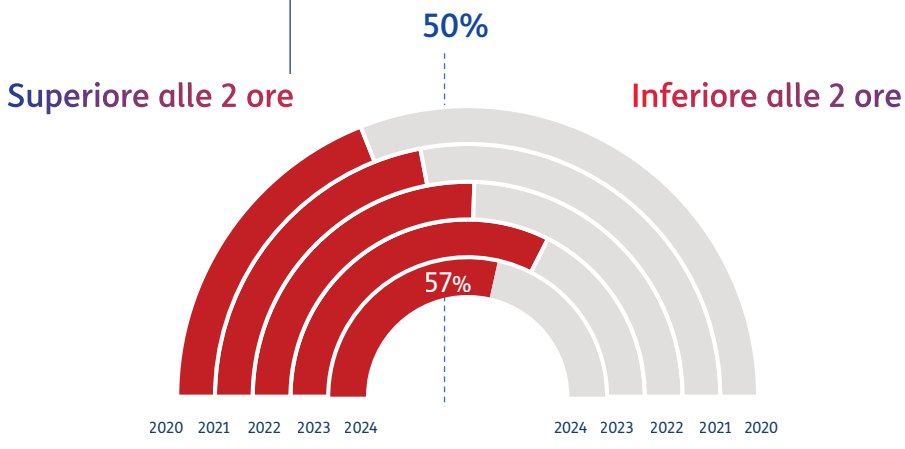
La **durata media** di un evento DDoS nel 2024 è stata di circa **39 minuti**.

L'EVOLUZIONE DELLA DURATA
Degli attacchi negli ultimi 5 anni

Attacchi Brevi

> 10 min	2.866	+59%
10 - 30 min	3.198	+21%
30 - 120 min	454	+52%
120 min - 24 h	169	+6%
> 24 h	11	-50%

Attacchi Lunghi



Peso in minuti degli attacchi (%)

Analisi effettuata considerando la durata mediana per ogni singolo segmento.
Per l'ultima classe sono stati considerati attacchi di durata di 1441 minuti, pari a 24 ore + 1 minuto

Diminuiscono gli eventi di durata superiore alle due ore

Il peso complessivo in termini di minuti di attacco scende sotto al 60%

Severità degli eventi: maggiore **potenza** e **durata**

LA MAPPA DELLA SEVERITÀ È UNO STRUMENTO UTILE PER OSSERVARE LA TRASFORMAZIONE DEGLI ATTACCHI DDoS

Abbiamo osservato che gli eventi DDoS stanno mostrando una importante trasformazione: la maggior parte dei casi è ancora per lo più di intensità bassa e di durata breve se non brevissima, ma le nuove tecniche stanno portando ad un cambiamento nell'intensità e nella durata.

Naturalmente queste sono le principali evidenze di cui abbiamo dato conto. Gli eventi registrati nel corso del tempo presentano una grande varietà di tecniche e di modalità, possono cambiare le finalità, gli obiettivi ed anche le risorse e gli asset su cui si concentrano le aggressioni.

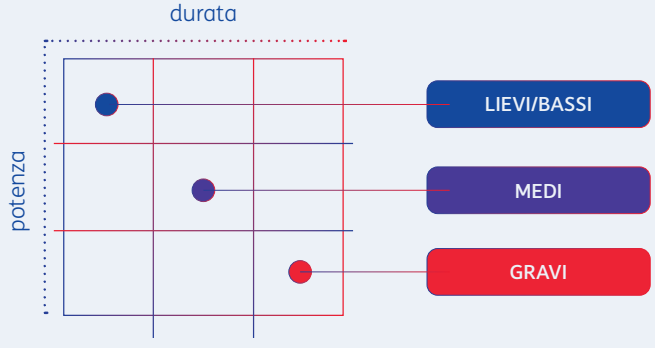
Anche gli effetti causati possono concorrere a differenziare gli eventi. Tuttavia, rimanendo solo alle variabili di intensità e durata, possiamo rappresentare questa trasformazione nella mappa della severità degli attacchi che incrocia queste due caratteristiche ed evidenzia uno spazio dove possiamo individuare diverse aree di riferimento (attacchi lievi, bassi, medi e gravi) ed al contempo permettono di visualizzare la crescita del fenomeno, la tendenza e la direzione in cui si si stanno orientando gli attacchi.

L'analisi storica dei dati raccolti a partire dal 2019 evidenzia che il baricentro si sposta da un'area di severità lieve/bassa ad una più intermedia a causa dell'aumento della potenza e della durata degli attacchi DDoS.

Tuttavia, tende a diminuire la durata media e questo cambia leggermente la dinamica di variazione del baricentro che era stata registrata negli ultimi anni.

LA MAPPA DELLA SEVERITÀ

L'incrocio delle due variabili definisce uno spazio dove possiamo collocare ogni attacco in funzione della durata e della potenza ed effettuare alcune analisi sull'evoluzione degli eventi nel tempo

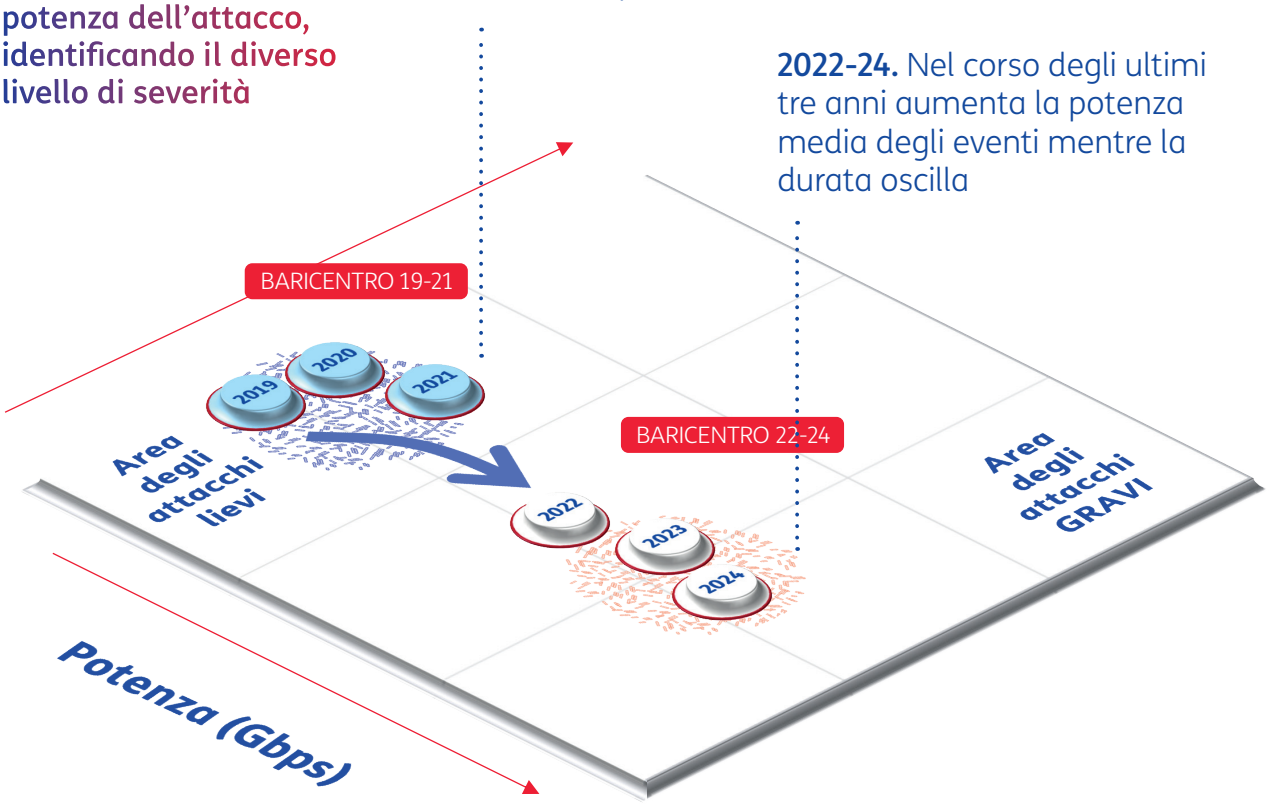


LA MAPPA DELLE SEVERITÀ
2023 vs 2024

Gli eventi DDoS si possono classificare in base alla durata ed alla potenza dell'attacco, identificando il diverso livello di severità

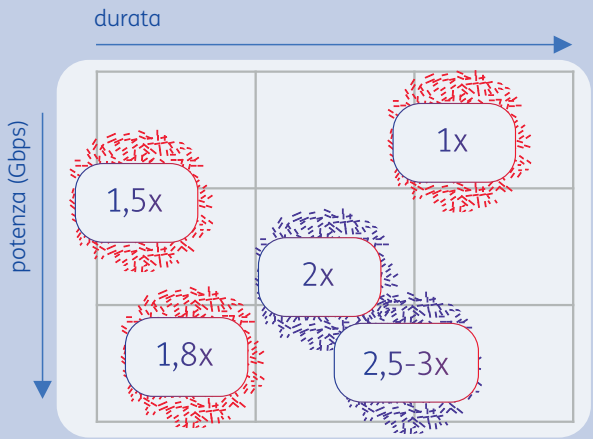
2019-2021. Dal 2019 al 2021 la maggior parte degli eventi DDoS presenta una bassa intensità (tra 2 e 4 Gbps) ed una durata inferiore ai 30 minuti

2022-24. Nel corso degli ultimi tre anni aumenta la potenza media degli eventi mentre la durata oscilla



2023 VS 2024

Come cambia il peso delle singole aree di severità:



Quanto osservato mostra che tra il 2023 ed il 2024, aumentano il numero di fenomeni di elevata potenza e breve durata (quasi 2 volte) mentre non cambiano sostanzialmente gli eventi di bassa intensità e lunga durata. La crescita più significativa si registra nell'area degli eventi ad alta intensità e durata intermedia (2-3X)

L'aumento della severità, aumenta la necessità **di mitigazione**

GLI EVENTI DELLA MASSIMA SEVERITÀ SONO AUMENTATI DI QUATTRO VOLTE IN QUATTRO ANNI

Lo spostamento del baricentro verso un'area intermedia è una naturale conseguenza dei trend che abbiamo osservato e che si manifestano in modo più compiuto quando andiamo a considerare l'andamento degli attacchi con la massima severità nel corso degli ultimi anni. Nel 2020, prendendo in considerazione tutti gli attacchi che rientrano nell'area della severità che consideriamo grave, rappresentavano il 6% del totale. Nel 2022 la loro incidenza era diventata del 12%, raddoppiando il peso relativo in due anni. Nel 2024 questa quota è si è portata al 26%.

Detto in altre parole, gli eventi di massima severità sono aumentati di oltre quattro volte in quattro anni.

Nello stesso arco temporale sono più che raddoppiati gli eventi di severità media che hanno raggiunto una quota del 22% del totale. Gli eventi DDoS di severità media e alta rappresentano nel complesso quasi la metà del totale (erano il 16% nel 2020

QUESTO RICHIEDE UN MAGGIORE IMPEGNO IN TERMINI DI PREVENZIONE E MITIGAZIONE

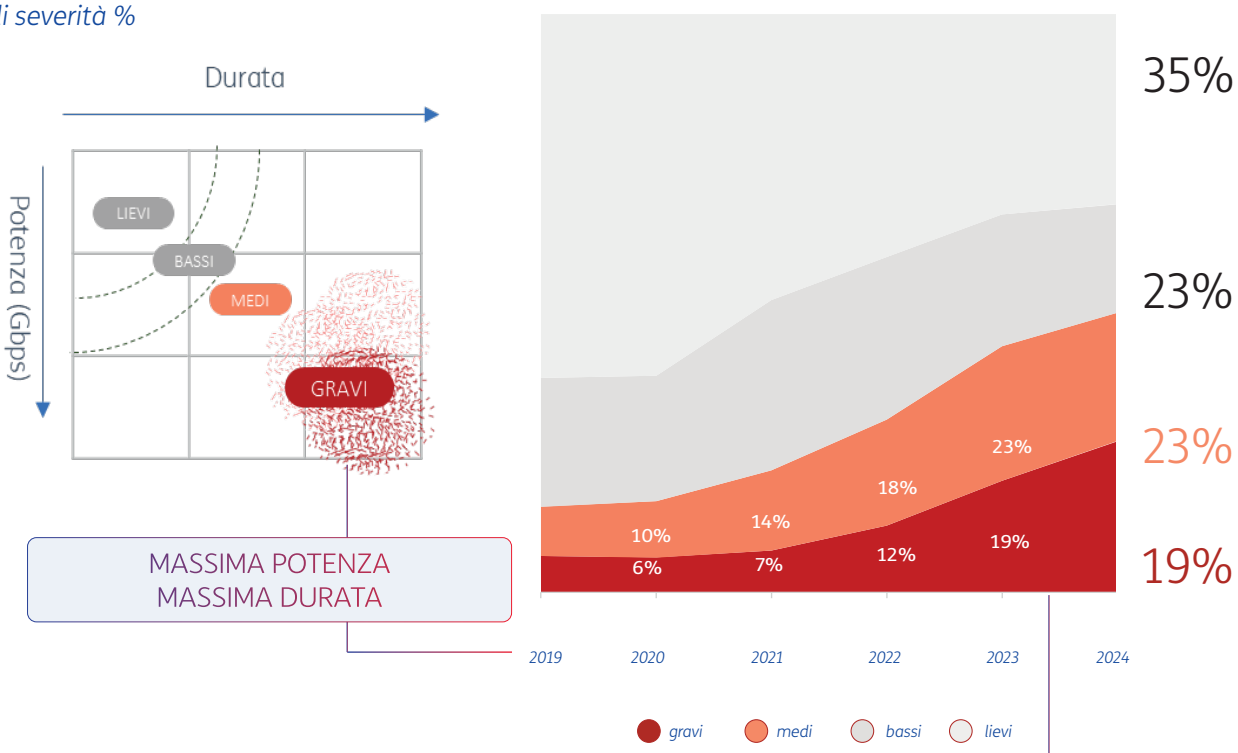
All'aumentare delle capacità di attacco deve fare fronte una corrispondente attenzione alla capacità di difesa. La continua trasformazione dei tentativi di attacco cyber, inclusi quindi quelli DDoS, impone un costante aggiornamento delle tecnologie e dei sistemi di prevenzione, identificazione, mitigazione e contrasto, al fine di assicurare la protezione e la continuità delle attività delle imprese, delle PA e anche dei singoli cittadini.

La crescente potenza degli eventi DDoS nel corso di questi ultimi mesi ha richiesto una sempre più intensa attività di mitigazione per garantire un perimetro di difesa di protezione di pari livello rispetto all'aumento e all'intensità degli attacchi. In effetti, gli interventi di mitigazione del 2024 sono oltre tre volte quelli del 2020.

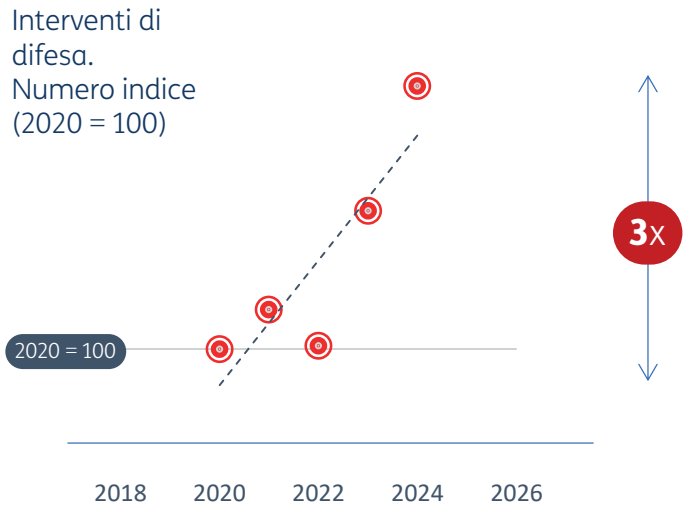
LE FASI DI UN PROCESSO DI MITIGAZIONE

GLI ATTACCHI GRAVI SONO TRIPLICATI RISPETTO AL 2020
(alti e altissimi) - 2023

Attacchi per livello di severità %



AUMENTA IL BISOGNO DI INTERVENTO



A fronte dell'intensità degli attacchi, la necessità di intervento è più che triplicata rispetto al 2020

Attacchi DDoS strategie **opportunistiche**

Gli attacchi DDoS colpiscono tutti indistintamente per creare danni e confusione, soprattutto quando vengono lanciati con finalità non estorsive. Del resto, alcuni segmenti vengono attaccati più di altri semplicemente perché ci si rende conto che alcuni «pezzi» del sistema possono essere colpiti più facilmente e attraverso questa azione si indebolisce tutto il sistema. La strategia di attacco è quindi spesso di tipo opportunistico e può variare nel tempo in base a numerosi fattori connessi alle caratteristiche del sistema, alle circostanze e alle opportunità derivanti dalle innovazioni tecniche.

QUASI 8 EVENTI OGNI 10 RILEVATI SI INDIRIZZANO VERSO GLI "HOME USERS"

Distinguiamo i tentativi di attacco DDoS rivolti alle famiglie (ossia ai privati nell'ambito di attività non professionali) e quelli rivolti alle organizzazioni, come imprese e istituzioni. Circa 3 su 4 eventi DDoS che sono stati rilevati nel 2024 si è indirizzato verso gli "Home Users", famiglie e singoli individui. Questa quota, nel quinquennio 2020-2024, mostra diverse oscillazioni attorno ad un valore medio del 78% del totale.

Gli eventi DDoS rivolti verso imprese ed istituzioni costituiscono il 23% del totale dei casi registrati nel 2024.

IL SETTORE ISTITUZIONALE REGISTRA LA MAGGIOR CRESCITA DI EVENTI DDoS. TRA LE IMPRESE, IL SETTORE DEI SERVIZI PROFESSIONALI È QUELLO PIÙ SOTTO TIRO

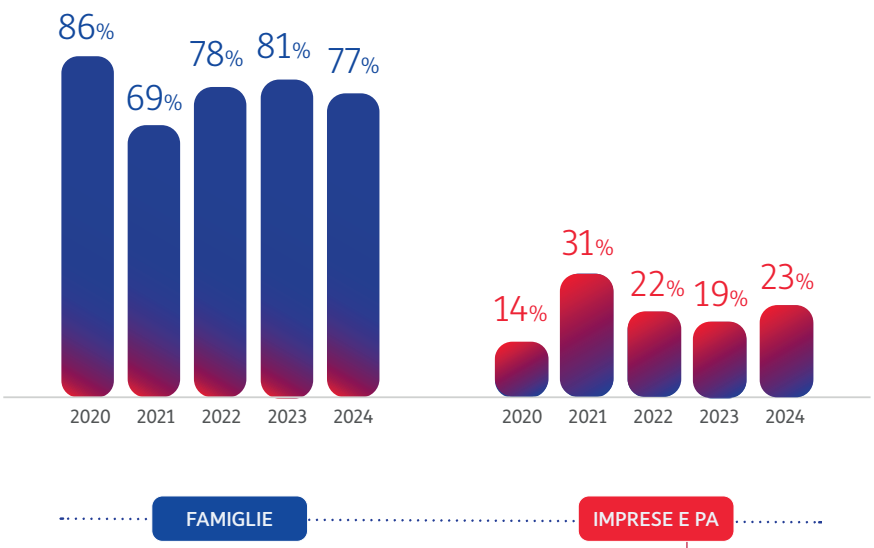
È chiaro che il gran volume di eventi indirizzati verso il target "Home Users" non consente di osservare con chiarezza le dinamiche che interessano gli altri target. Escludendo questa componente, si osserva un significativo aumento degli eventi DDoS verso la Pubblica Amministrazione (PA) centrale e locale, con una crescita dal 1 al 42% del totale dei casi non "Home Users". Parallelamente, il settore finanziario registra un incremento dal 3 al 14%, mentre la difesa passa dal 4 al 6% e i media dall'1 al 2%. Al contrario, i servizi professionali mostrano un trend in diminuzione passando dal 36 al 17% degli eventi DDoS, pur rimanendo un target di interesse per gli aggressori. I servizi professionali sono il target più colpito nel 2024 se si escludono gli obiettivi istituzionali, seguiti dal settore finanziario e delle telecomunicazioni.

Questo cambiamento nei trend degli attacchi suggerisce alcune considerazioni. Da un lato l'evoluzione del contesto geopolitico mette sotto tiro obiettivi che sono considerati rappresentativi del Paese, rendendoli bersagli preferenziali per gli attacchi DDoS. Dall'altro, l'evoluzione delle direttrici di attacco dei cybercriminali diventa sempre più diversificata e non sempre prevedibile e questo aumenta la necessità per le organizzazioni di adottare misure di sicurezza sempre più avanzate e efficaci per proteggere le proprie infrastrutture digitali.

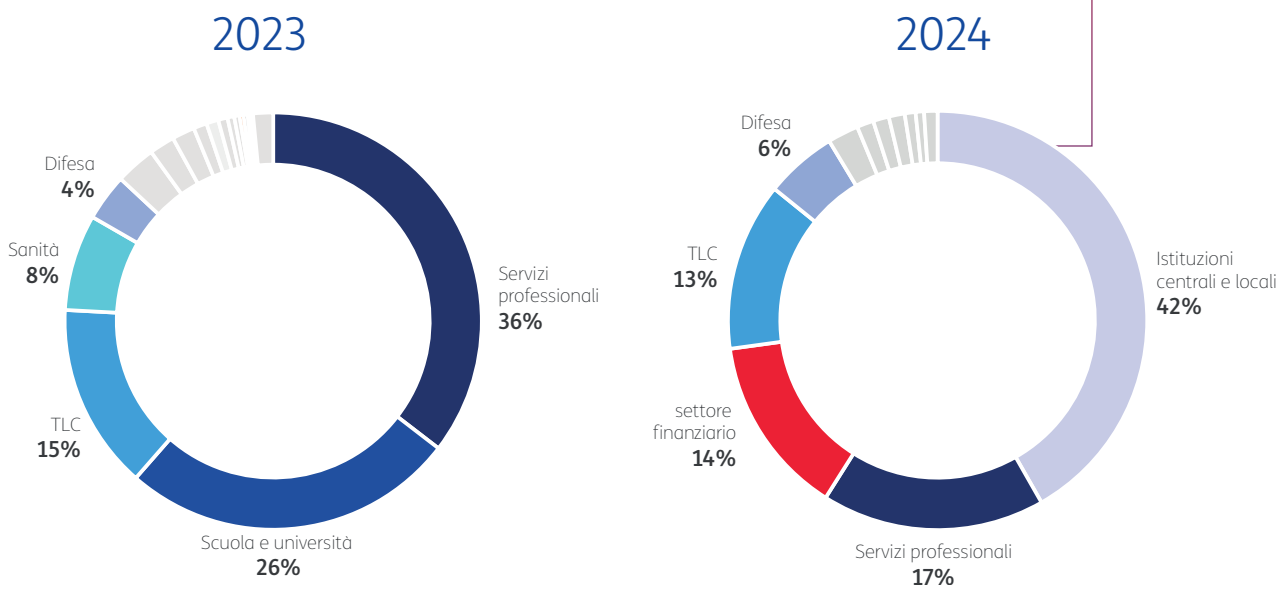
NEL 2024 GLI EVENTI CHE RIGUARDANO IMPRESE E PA RAPPRESENTANO POCO PIÙ DEL 20%
del totale

Gli attacchi DDoS possono avere diverse motivazioni: ragioni opportunistiche, atti di vandalismo digitale, concorrenza sleale, movimenti di attivismo politico, dimostrazioni di potere da parte di gruppi hacker. Il gran volume di eventi che ha interessato il settore istituzionale nel 2024 suggerisce una possibile correlazione con il contesto geopolitico.

% eventi DDoS verso famiglie e imprese



Ripartizione eventi DDoS verso imprese per settore



Attacchi
RANSOMWARE

Negli ultimi anni il ransomware è diventato uno dei tipi di attacco più diffusi, colpendo organizzazioni di tutte le dimensioni in tutto il mondo. Tecnicamente, è la situazione in cui gli attaccanti prendono il controllo degli asset di un obiettivo e richiedono un riscatto in cambio del ripristino della situazione.

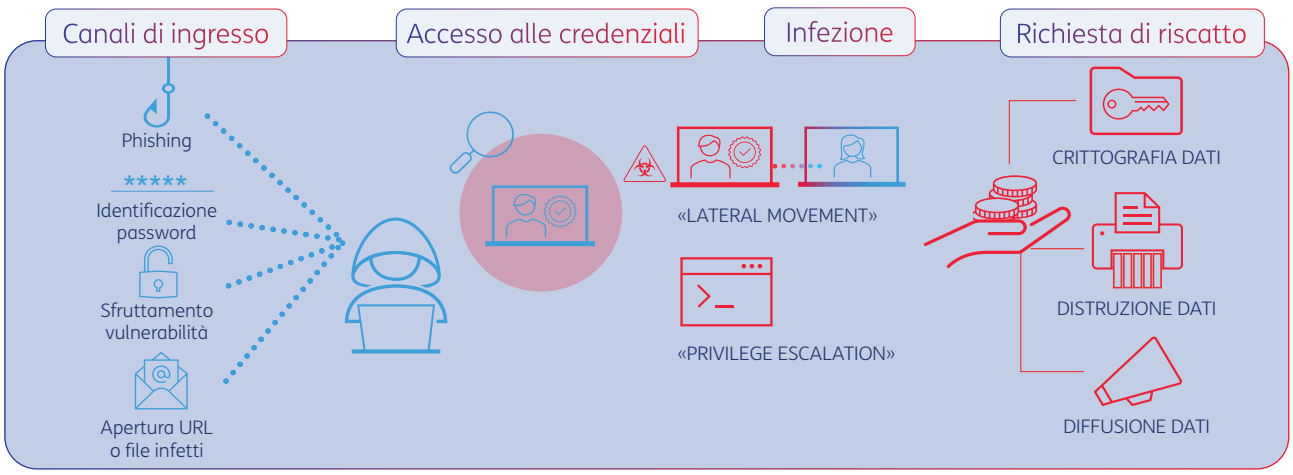
I Gruppi Ransomware più strutturati attivano modelli definiti «a doppia estorsione»: per mettere pressione alle vittime si ricorre al blocco/distruzione delle risorse, nonché ad un'esfiltrazione preventiva di dati ed informazioni che, se diffuse online, creano danni di vario tipo (penali, legali, di concorrenza...).

Ad aumentare i volumi contribuisce anche il ransomware-as-a-service, una modalità in cui questo tipo di attacco viene messo sul mercato ed offerto come un qualunque altro servizio.

Un attacco ransomware segue diverse fasi:

- lo sfruttamento di debolezze di un sistema (phishing, identificazione di password deboli, vulnerabilità, apertura di URL o file infetti) permette all'attaccante di penetrare nelle reti e di muoversi liberamente all'interno dell'ambiente, ad esempio, spostandosi su altri computer o entrando negli account con maggiori privilegi.
- Una volta identificati i punti deboli, si mette in atto la minaccia, avvertendo il soggetto attaccato della compromissione dei suoi sistemi, bloccando l'accesso alla risorsa digitale colpita con conseguente richiesta di riscatto.

Di seguito riportiamo i dati rilevati dal nostro sistema di Threat Monitoring nel corso dell'anno. I valori non rappresentano la diffusione completa del fenomeno, ma solo la parte che diventa visibile. Purtroppo, nonostante le raccomandazioni contrarie delle Autorità, gli attori colpiti cedono alle richieste di riscatto e questo non agevola la raccolta delle informazioni. Molte informazioni sono desunte dalle rivendicazioni dei Gruppi Ransomware.



Attacchi RANSOMWARE
Sintesi **2024**

Nel 2024 sono state registrate oltre 5.200 rivendicazioni ransomware a livello globale, in crescita del 12% rispetto allo scorso anno e la metà del totale è indirizzata verso gli Stati Uniti.

146

Attacchi ransomware rivendicati verso l'Italia (circa il 3% del totale mondiale)

I settori più colpiti da attacchi Ransomware

Manifatturiero
Servizi professionali
Settore tecnologico
Commercio

L'Italia è il secondo paese in UE per attacchi ransomware

dietro alla Germania (168). Allargando all'intera Europa, il Regno Unito è il Paese più colpito (262)

42 **Attaccanti attivi** in Italia nel corso del 2024

RansomHub, Lockbit e Black Basta i gruppi più attivi nel nostro Paese

Le regioni più interessate dal ransomware sono la **Lombardia, il Lazio, l'Emilia-Romagna e il Piemonte**.

Attacchi Ransomware: l'Italia è il secondo Paese UE **per numero di attacchi**

IL RANSOMWARE È UN FENOMENO DIFFICILE DA MONITORARE

Effettuare un'analisi del fenomeno ransomware è particolarmente complesso per una serie di motivi:

- innanzitutto c'è una difficoltà intrinseca nella raccolta dei dati perché non sempre all'attacco segue la denuncia del soggetto colpito nonostante le raccomandazioni e gli obblighi che vanno via via definendosi per far fronte a questo fenomeno.

- In altri casi, la denuncia avviene tardivamente e non sempre si riesce a fare affidamento sulle rivendicazioni dei gruppi criminali.

Questo conduce a discrepanze tra i dati raccolti e aumenta la percezione di trovarsi di fronte un fenomeno di cui vediamo una sola parte senza avere una vista completa della sua interezza. Un effetto «punta d'iceberg» che è tipicamente connaturato ad altri fenomeni criminosi o illegali.

OLTRE 5.200 RANSOMWARE NEL 2024, SOPRATTUTTO DIRETTI VERSO GLI USA. IN ITALIA 146 EVENTI (IL 2,8% DEL TOTALE)

Il sistema di monitoraggio effettuato dalla Threat Intelligence del Gruppo TIM ha permesso di rilevare oltre 5.200 attacchi di tipo ransomware a livello globale nel corso del 2024, di cui 146 hanno riguardato l'Italia, in calo rispetto al 2023 (176 eventi registrati).

Il Paese più soggetto ad attacchi di tipo Ransomware sono gli Stati Uniti, contro cui si sono indirizzati quasi 2.650 colpi. In pratica, quasi un attacco su due ha riguardato imprese statunitensi. L'Italia si colloca al quinto posto nella classifica dei Paesi interessati da questi eventi, appena dietro alla Germania e davanti a Francia, Brasile e India.

Se consideriamo l'Unione Europea nel suo complesso, gli attacchi ransomware nel 2024 sono stati 835, ossia all'incirca il 16% del totale. Complessivamente, nell'arco degli ultimi tre anni osservati, abbiamo rilevato 389 casi, una quota pari al 18% di quelli indirizzati ai Paesi dell'Unione Europea.

> Il monitoraggio effettuato **A LIVELLO GLOBALE** ha permesso di rilevare **OLTRE 5.200 ATTACCHI DI TIPO RANSOMWARE**

Focalizzando l'attenzione sui gruppi che portano minacce ransomware, in base alle rivendicazioni ne sono stati identificati con certezza 88, di cui 42 attivi in Italia.

IL VOLUME DEGLI ATTACCHI RANSOMWARE
in Italia, UE e USA

88
avversari
a livello Global

42
attivi
in Italia

STATI UNITI

Sono il Paese più colpito da attacchi ransomware rivendicati

2.640
attacchi

51%
del totale

UNIONE EUROPEA

Rappresenta il secondo bersaglio a livello mondiale

867
attacchi

16%
del totale

ITALIA

Il secondo paese UE per attacchi ransomware complessivi

146
attacchi

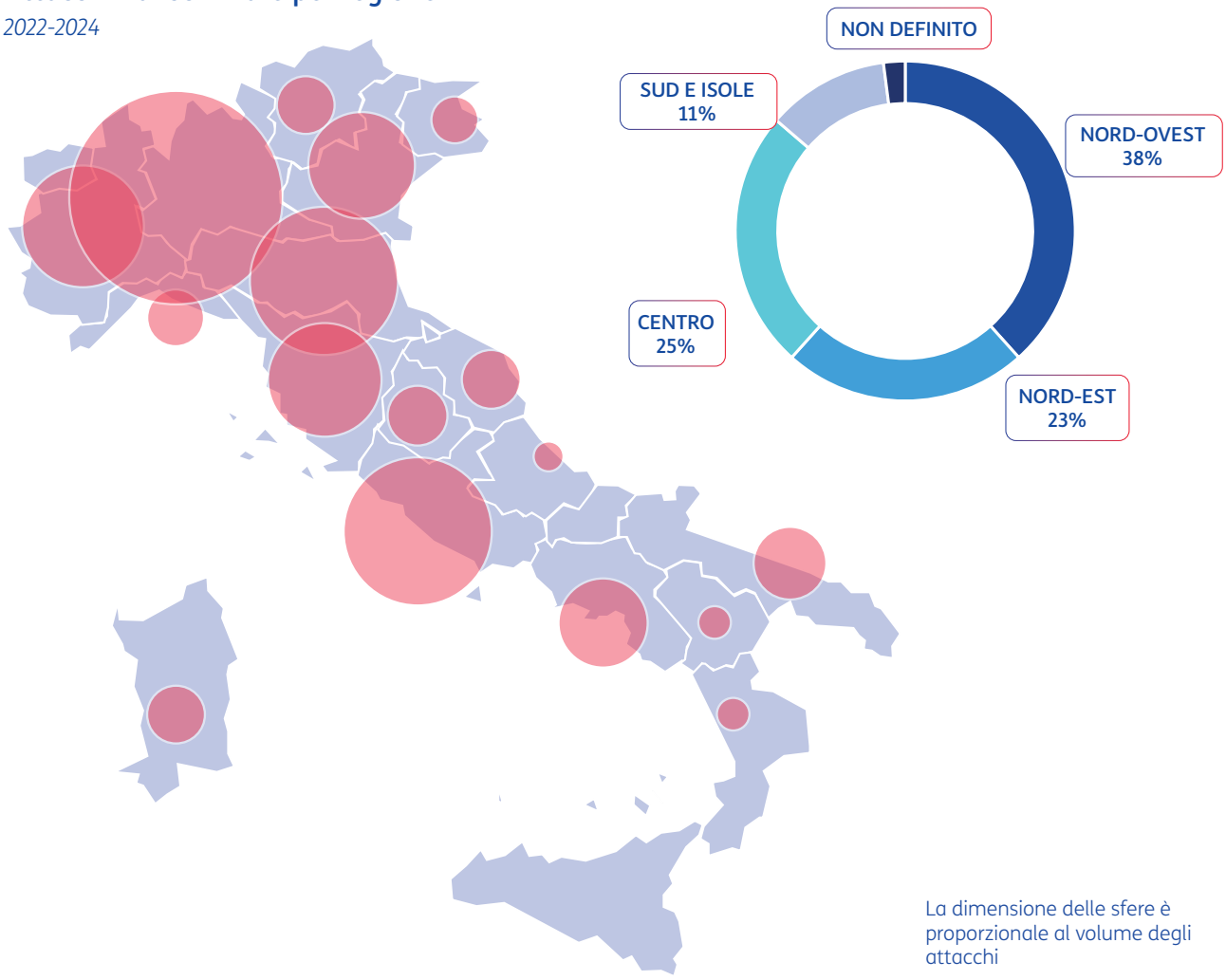
~3%
del totale

Attacchi Ransomware:
Il Nord-Ovest
il più bersagliato

A partire dai dati raccolti sui ransomware è possibile dare conto delle differenze a livello geografico che si evidenziano per il nostro Paese. Emerge con forza una maggiore esposizione al fenomeno da parte delle regioni del Nord-Ovest del nostro Paese (38% dei ransomware del 2024), mentre Sud e Isole rappresentano una quota molto più ridotta (all'incirca 11% del totale). La Lombardia è la regione con il maggior numero di eventi nel 2024 (40) seguita da Lazio, Emilia-Romagna e Piemonte. Non risultano eventi in Molise e Sicilia. La particolare natura dei ransomware non permette di valutare a pieno se queste differenze dipendano solo dalla diversa struttura produttiva di queste aree o anche da una diversa attenzione a denunciare il fenomeno.

Attacchi Ransomware per regione

2022-2024



La dimensione delle sfere è proporzionale al volume degli attacchi

I settori più sotto tiro: servizi professionali e **manifatturiero**

Nessun settore è immune, ma si possono evidenziare alcune specificità quando si analizza l'impatto degli attacchi ransomware nei diversi ambiti del nostro sistema economico.

In particolare, il settore terziario appare più soggetto ad attrarre attacchi ransomware, mentre il settore secondario appare meno esposto.

Ripartizione attacchi per settore

% totale degli eventi rilevati nel triennio

1%

IL PRIMARIO SI MANTIENE ANCORA IN SECONDA FILA

41%

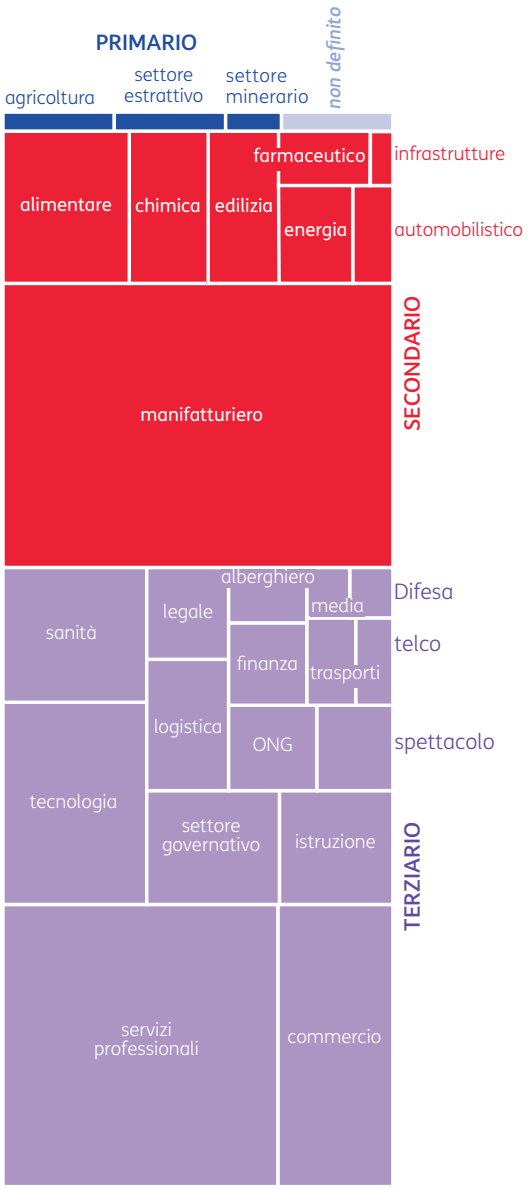
IL SECONDARIO PRESENTA ATTACCHI PIÙ CONCENTRATI (VERSO LA MANIFATTURA)

Verso il secondario si indirizzano all'incirca il 41% degli eventi ransomware nel triennio 2022-24 (39% nel 2024) e in questo settore si inserisce il comparto più colpito in assoluto: le imprese del manifatturiero sono state oggetto di circa il 26% degli attacchi ransomware nel triennio, con una incidenza in crescita nel 2024 (la quota del comparto arriva al 30%).

58%

IL TERZIARIO È PIÙ COLPITO DA ATTACCHI RANSOMWARE

Il terziario è il settore più colpito soprattutto perché comprende comparti che gestiscono informazioni molto sensibili come ad esempio le informazioni bancarie o assicurative o i dati medici. Più l'informazione è preziosa, più diventa un target appetibile per un ransomware. Inoltre, la presenza di reti commerciali ampie con filiali, uffici e partner, aumenta la superficie di attacco Nel triennio 2022-2024 circa il 58% degli eventi ha riguardato il settore terziario, con una incidenza lievemente più alta nel 2024 (59%). Il settore più colpito è quello dei servizi professionali, con una quota media del 18% nel triennio (e del 22% circa nel 2024).



L'attività dei gruppi attaccanti: l'importanza del **RaaS**

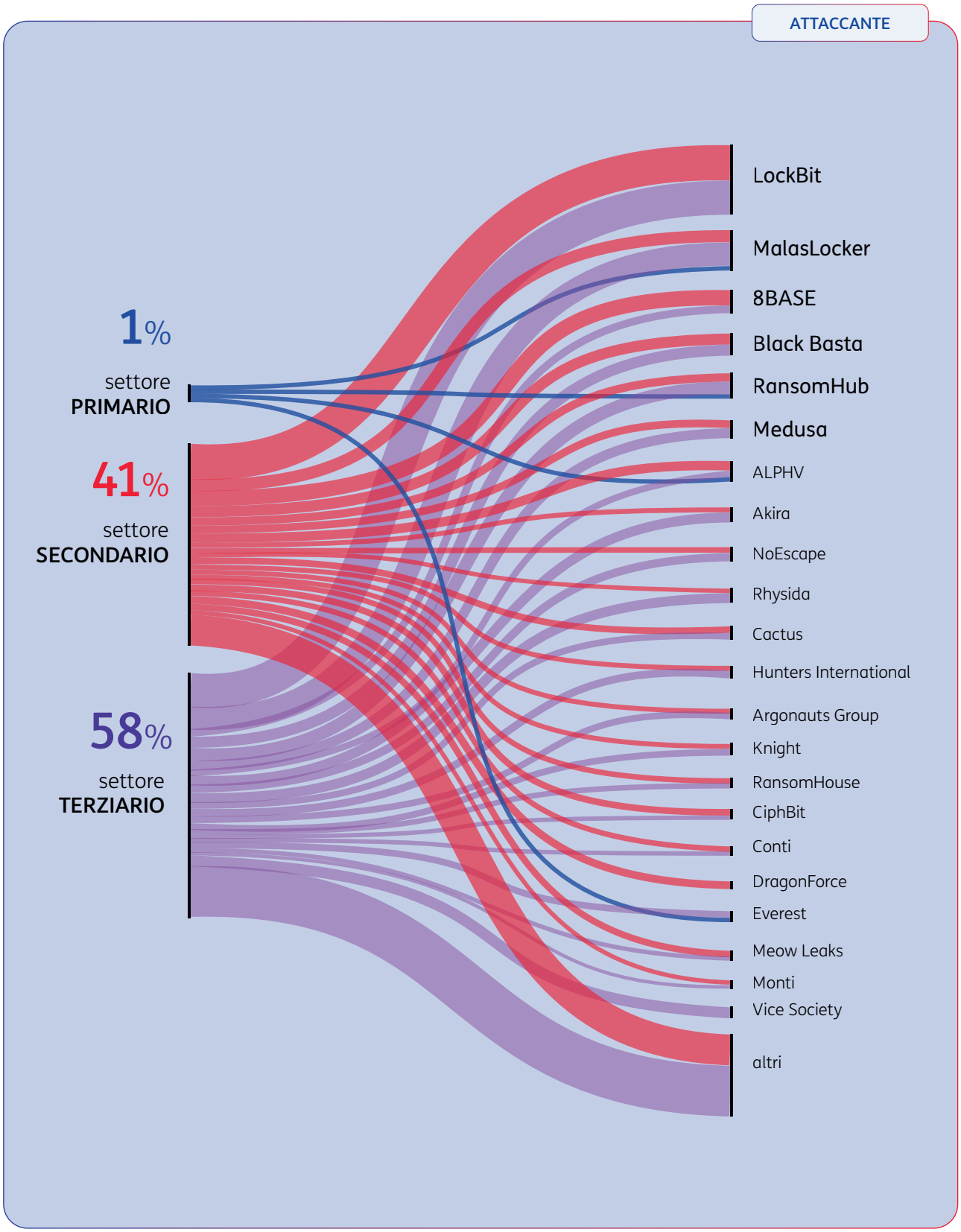
Nel corso del 2024 sono stati identificati 42 gruppi di attaccanti che hanno portato delle minacce ransomware in Italia, su un totale di 88 avversari censiti a livello globale. Tra i gruppi che hanno rivendicato attacchi ransomware in Italia nel 2024, i più attivi sono stati RansomHub (18 casi), Lockbit (12 casi), 8BASE (11 casi) e Black Basta (10 casi).

Nel triennio 2022-2024, Lockbit è responsabile del 21% dei casi rilevati, seguito da MalasLocker (9%) e Black Basta, 8BASE e RansomHub (con quote attorno al 5%). Lo sviluppo temporale delle attività di questi avversari mostra delle differenze significative. Lockbit mostra rivendicazioni per tutto il periodo di osservazione, con un'attività più intensa nel corso del 2022-2023 ed un'attenuazione dell'attività nel corso del 2024. L'attività di Malaslocker appare concentrata nel mese di maggio 2023. Black Basta, 8BASE e RansomHub sono invece più attivi nel corso del biennio 2023-2024. Queste azioni appaiono guidate spesso da ragioni di opportunità e pertanto non si individuano delle specializzazioni su settori o comparti. Tuttavia, in base alle rivendicazioni raccolte, mentre Lockbit e Black Basta distribuiscono le loro azioni abbastanza equamente tra tutti i settori, 8BASE appare più sbilanciato verso il secondario (80% dei ransomware tra il 2022 ed il 2024), mentre al contrario RansomHub è più orientato verso attacchi al settore terziario. Tuttavia, nel valutare questi risultati bisogna anche considerare che negli ultimi anni la crescita di alcuni gruppi si deve anche alla diffusione di modelli di Ransom as a Service RaaS, un modello di business del crimine informatico in cui una banda vende il proprio codice ransomware ad altri hacker, con il quale a loro volta mettono in atto attacchi ransomware. È chiaro che, tanto più un gruppo lancia soluzioni di Raas, tanto più questo aumenta il suo peso nelle classifiche. Secondo un rapporto del 2022 di Zscaler è emerso che 8 delle 11 varianti di ransomware più attive erano varianti RaaS.

COME FUNZIONA IL MODELLO RAAS

Il RaaS funziona alla stregua di legittimi modelli di business di Software-as-a-Service. Gli sviluppatori di ransomware (operatori RaaS), realizzano strumenti e infrastrutture ransomware e confezionano un kit RaaS che vendono ad altri hacker, detti affiliati RaaS. È facile capire perché il modello RaaS sia così popolare presso i criminali informatici. Infatti, abbassa il livello di conoscenze necessarie per darsi al crimine informatico, consentendo di effettuare attacchi informatici anche ad attori di minacce con competenze tecniche limitate. Il RaaS, inoltre, è reciprocamente vantaggioso: gli hacker possono trarre profitto dall'estorsione evitando di sviluppare malware e gli sviluppatori di ransomware possono aumentare i profitti senza dover attaccare manualmente le reti. I kit RaaS sono pubblicizzati sui forum del dark web dove alcuni operatori di ransomware reclutano attivamente nuovi affiliati. Una volta acquisito il kit, gli affiliati possono contare su un servizio di assistenza e in alcuni casi anche su servizi accessori (forum di assistenza, servizi di scrittura delle richieste di riscatto, assistenza nelle trattative, ecc.). Il modello di business può essere differente: dall'abbonamento mensile al servizio fino alla partecipazione agli utili (quota parte del riscatto).

DISTRIBUZIONE DEGLI ATTACCHI
per settore industriale e per attaccante



Campagne
MALWARE

Una campagna di diffusione di malware rappresenta un'azione concertata che ha l'obiettivo di propagare software malevolo, conosciuto come malware (MALicious softWARE), attraverso una serie di canali per compromettere sistemi informatici, reti e dispositivi, utilizzando sistemi differenti (virus, worm, trojan, spyware ecc.), ciascuno con modalità operative specifiche.

Frequentemente, queste campagne sfruttano le vulnerabilità dei sistemi oppure si avvalgono di tecniche di ingegneria sociale, allegati di posta elettronica infetti, siti web compromessi, link corrotti per diffondere il malware. Gli scopi con cui vengono lanciate delle campagne di Malware sono diversi, tra cui:

- acquisire accesso non autorizzato ai dispositivi in modo da potervi esercitare il controllo,
- sottrarre informazioni riservate (password, accessi ai conti bancari, ecc.),
- distribuire spam o condurre altre attività malevole attraverso i dispositivi compromessi e sotto controllo,
- criptare o danneggiare i file degli utenti, talvolta richiedendo un riscatto per il loro recupero (ransomware).

Questo tipo di attacchi può essere lanciato a livello globale oppure può colpire determinati target (Settori, Paesi).

Quelli più attivi in Italia nel corso del 2024 appartengono alle seguenti categorie:

- **Keylogger:** malware progettato per registrare segretamente le sequenze di tasti effettuate su un computer o un dispositivo mobile
- **RAT:** Remote Access Trojan che si installano in un computer, in un dispositivo mobile o in un apparato ed aprono un varco che permette a degli attaccanti di poter controllare la macchina infetta a distanza
- **Infostealer:** malware che infettano computer ed apparati per rubare dati o informazioni
- **Downloader:** progettati per scaricare ed installare software malevoli. Aprono la strada ad altri Malware
- **Loader:** software che carica altri malware in memoria.
- **Trojan Bancari:** progettati specificatamente per sottrarre credenziali di accesso ed informazioni sensibili relative all'online banking e comprometterne gli account
- **Compromised website:** questa categoria indica che sono stati utilizzati siti web compromessi per distribuire o eseguire attacchi.

Campagne MALWARE
Sintesi **2024**

168

campagne malware

dirette verso
il nostro Paese
e contrastate
nel 2024

In maggiore evidenza in Italia i Malware di tipo RAT Remote Access Threath

sistemi che si installano furtivamente e permettono il controllo a distanza del dispositivo

circa il **40%**

delle campagne malware dirette verso l'Italia sono collegate a **Agent Tesla** e **GuLoader**

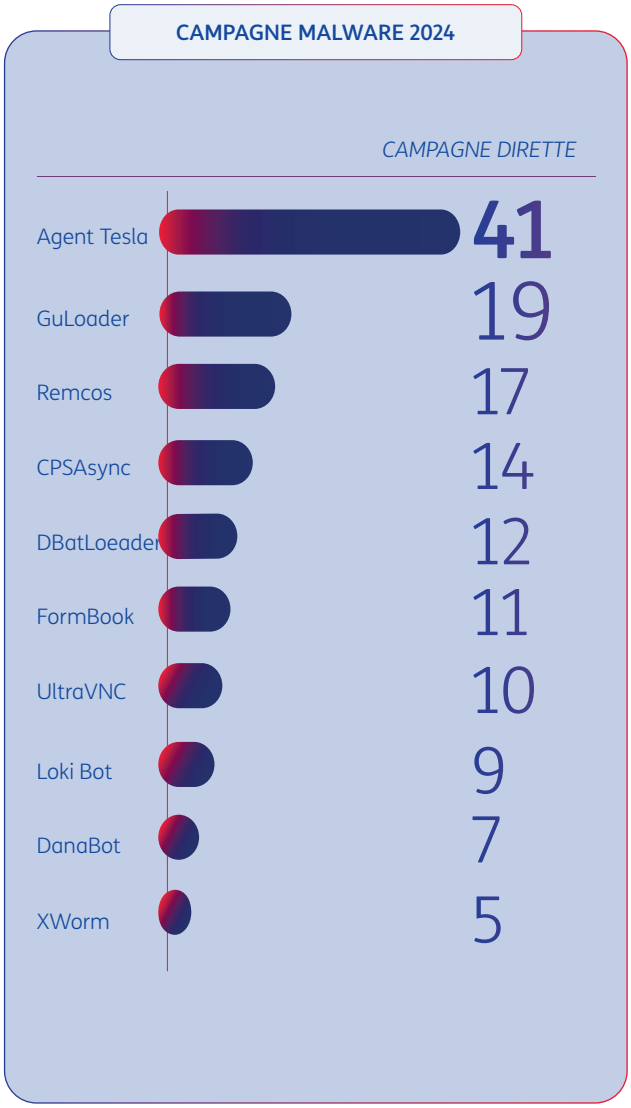
Campagne Malware: oltre 160 campagne dirette **verso l'Italia**

Le campagne malware possono essere sia globali che mirate a specifici paesi, e la differenza risiede principalmente nel loro obiettivo e nella loro portata. Le Campagne di Malware Globali sono lanciate indiscriminatamente con l'obiettivo di colpire più soggetti possibili. Spesso, tali azioni hanno l'intento di preparare il terreno ad altra attività malevole (ad esempio, creare una rete estesa di macchine compromesse da cui lanciare degli attacchi di DDoS).

Le campagne mirate puntano ad attaccare un determinato target sia per motivi di opportunità (specifiche vulnerabilità), sia per colpire deliberatamente un Paese (ad esempio, azioni che vengono lanciate con motivazioni politiche o di cyberwarfare).

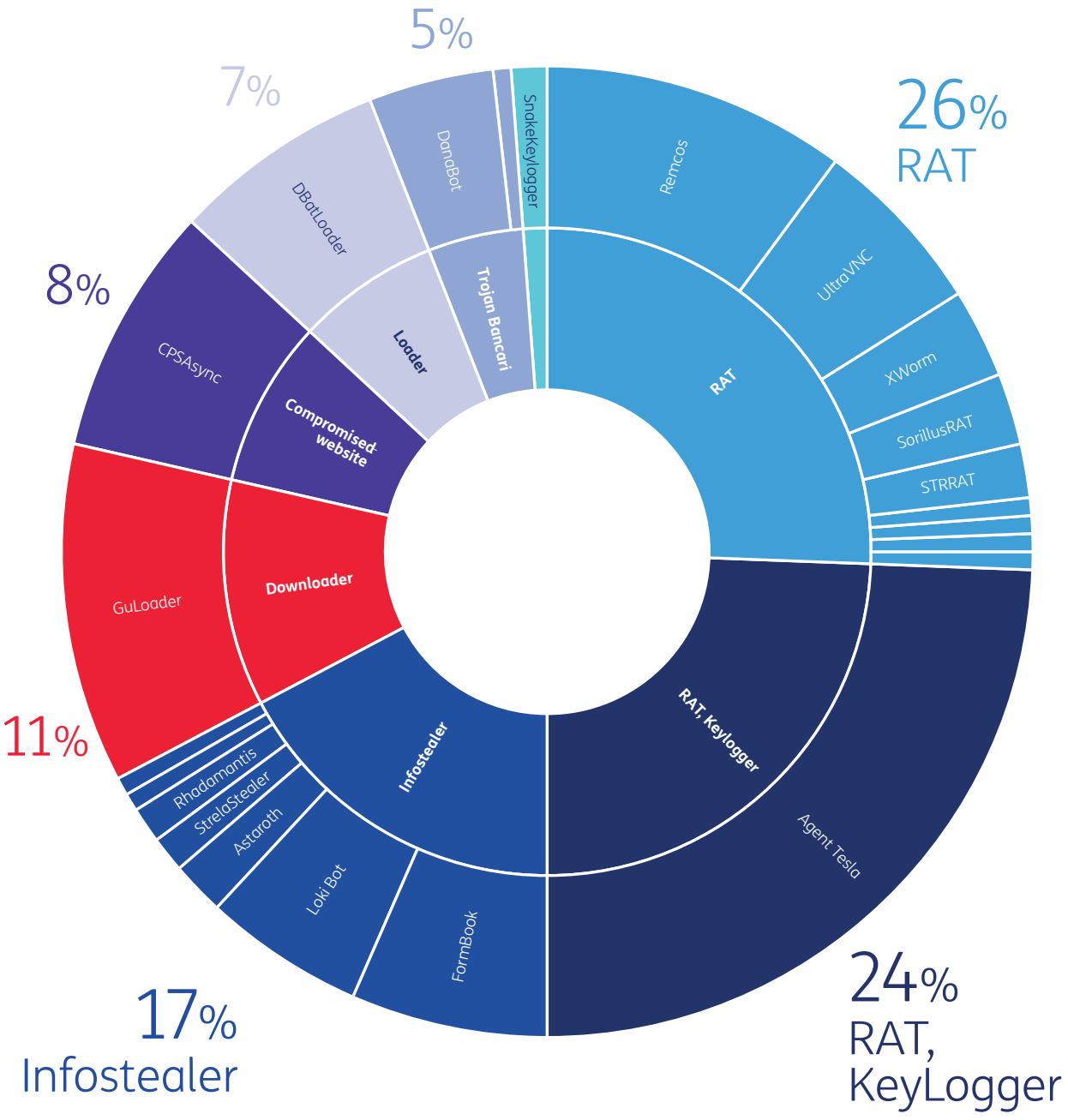
Nel corso del 2024 sono state identificate e contrastate 168 campagne di Malware.

Le principali minacce malware nel 2024 sono state portate da AgentTesla (41 campagne) e GuLoader (82 campagne). Queste due minacce rappresentano il 36% di tutte le campagne malware lanciate direttamente verso il nostro Paese.



CAMPAGNE MALWARE
per tipologia

Nel 2024, poco più di una campagna malware ogni quattro è di tipo RAT (26%), senza considerare Agent Tesla che ha delle caratteristiche ambivalenti (RAT e Keylogger) e ha un'incidenza del 24%. Seguono gli infostealer (17%) e i downloader (11%).



SECONDA PARTE

Approfondimenti settoriali

Una gran parte degli attacchi informatici che rileviamo si indirizza verso il mondo consumer, costituito da famiglie e individui. Tuttavia gli attacchi più dirompenti si orientano verso il mondo delle aziende, dei settori produttivi, delle istituzioni che sono il target più appetibile e rappresentano il cuore della nostra osservazione.
Gli attacchi a questi target sono più sofisticati e hanno delle importanti ripercussioni. In generale, arresto della produzione, costi di ripristino, perdita di dati, danni reputazionali e conseguenze sul posizionamento di mercato. Per enti, aziende di pubblico servizio ed istituzioni il blocco dell'attività ha effetti anche sulla vita quotidiana dei cittadini fino addirittura a compromettere la sicurezza nazionale. In questa sezione effettuiamo una «lettura» dei dati in nostro possesso per ambiti di attacco. La conoscenza è uno degli ingredienti alla base della sicurezza cibernetica e approfondire quanto avviene nel mondo ciber rappresenta il primo passo per definire delle strategie di difesa che possano aumentare il livello di protezione e la resilienza dei sistemi.

il livello di esposizione
una vista **d'insieme**

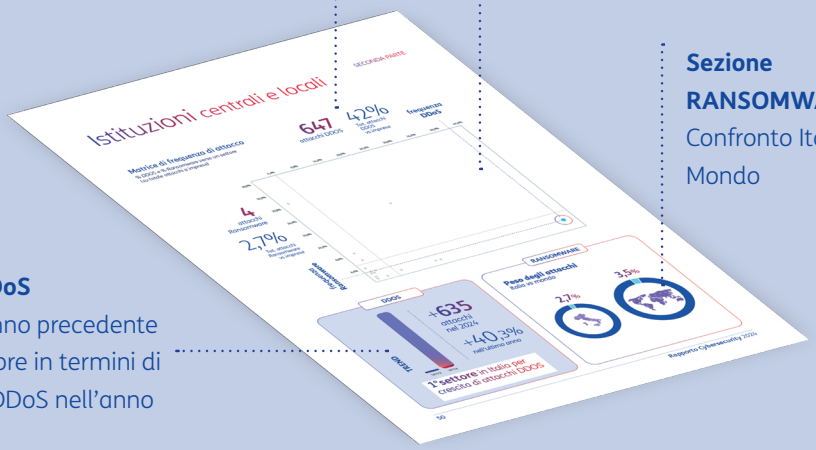
Nella scheda di sintesi riportiamo le informazioni rilevanti per ciascuno dei settori esaminati in merito alle tipologie di attacco DDoS e Ransomware.
Come abbiamo visto, alcuni settori appaiono in generale più esposti mentre altri sembrano essere colpiti in funzione delle opportunità che possono venirsi a creare, specifiche vulnerabilità, campagne mirate. A tale proposito può essere utile monitorare quanto avviene in un settore rispetto agli altri ed evidenziare gli andamenti degli attacchi nel corso del tempo.
Un altro dato che può emergere è una difformità tra quanto osservato a livello nazionale ed internazionale. Specie per i settori tipicamente più esposti, questa difformità può essere una spia di una specifica debolezza o al contrario una maggiore capacità di difesa di un settore rispetto alla media internazionale.

LE SCHEDE SETTORE

Le schede settore sono ripartite in quattro sezioni: una più generale di sintesi, una dedicata al DDoS, una al Ransomware e una vista d'insieme sulle frequenza d'attacco

VOLUMI TOTALI
Numero di attacchi di tipo DDoS e Ransomware

MATRICE frequenza d'attacco
Posizionamento del settore rispetto alle minacce DDoS e Ransomware



Sezione RANSOMWARE
Confronto Italia vs Mondo

Sezione ATTACCHI DDoS
Andamento attacchi vs anno precedente e posizionamento del settore in termini di variazione degli attacchi DDoS nell'anno

Istituzioni centrali e locali

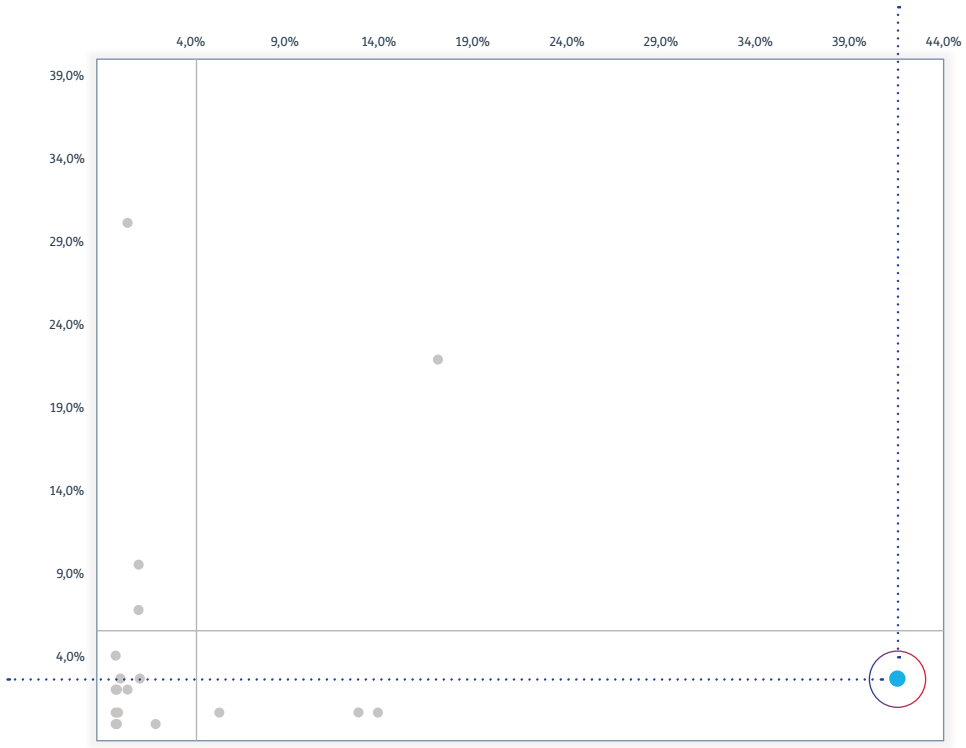
Matrice di frequenza di attacco

DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

647 *eventi DDoS*

42% *degli eventi DDoS vs imprese*

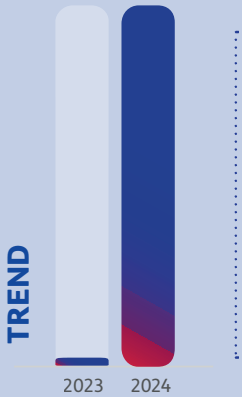
frequenza DDoS



4 *attacchi Ransomware*

2,7% *degli attacchi Ransomware vs imprese*

DDOS



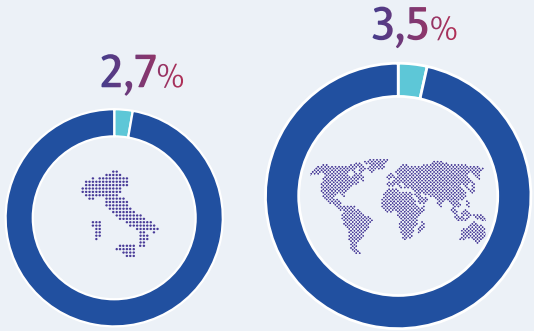
+635 *eventi nel 2024*

+40,3% *nell'ultimo anno*

1°settore in Italia per crescita di eventi DDoS

RANSOMWARE

Peso degli attacchi
Italia vs mondo



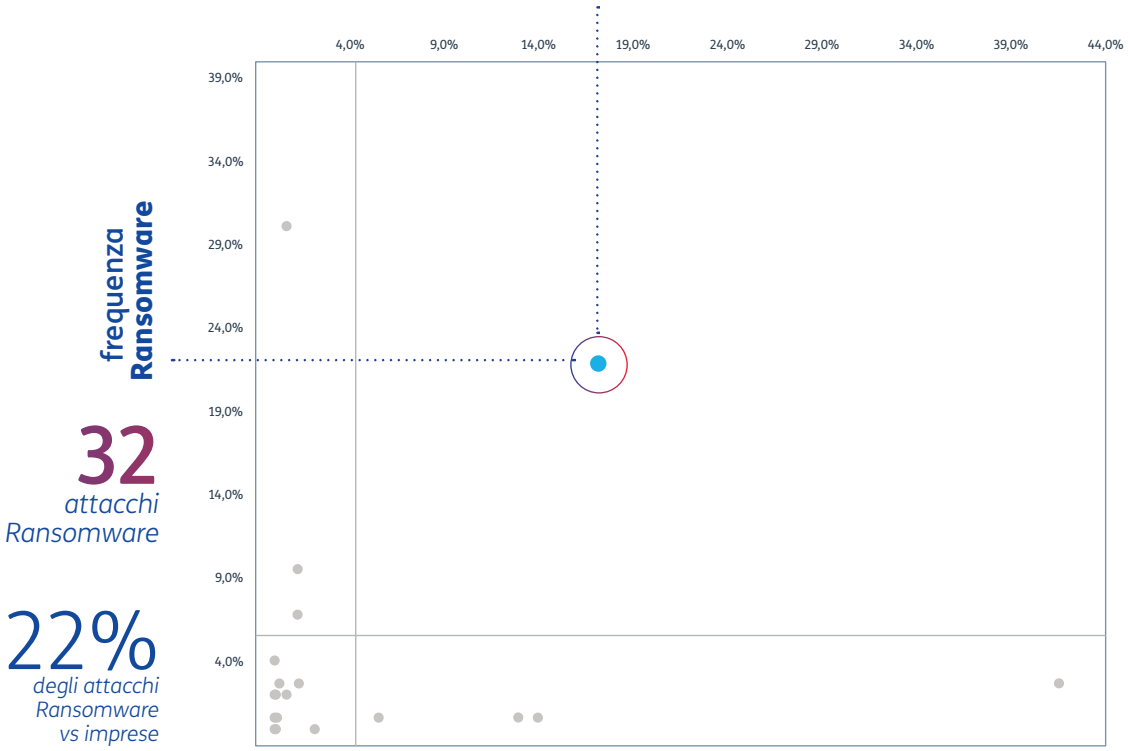
Servizi professionali

Matrice di frequenza di attacco

DDoS e Ransomware verso un settore
(quota % su totale attacchi a imprese)

267
eventi DDoS

17%
degli eventi DDoS vs imprese



32
attacchi Ransomware

22%
degli attacchi Ransomware vs imprese

DDOS

TREND

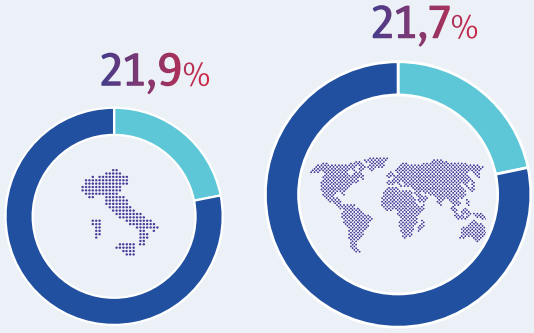
-75
eventi nel 2024

-19,3%
nell'ultimo anno

penultimo settore in Italia per **contrazione** di eventi DDoS

RANSOMWARE

Peso degli attacchi
Italia vs mondo



Settore finanziario

Matrice di frequenza di attacco

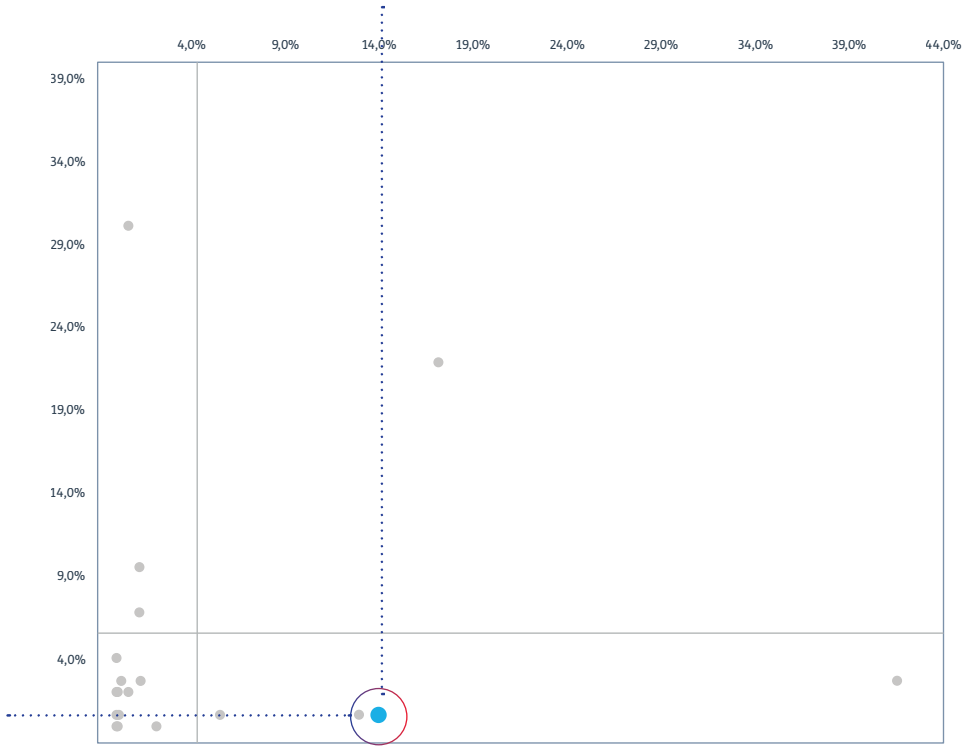
DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

217 *eventi DDoS*

14% *degli eventi DDoS vs imprese*

1 *attacchi Ransomware*

0,7% *degli attacchi Ransomware vs imprese*



DDOS

TREND

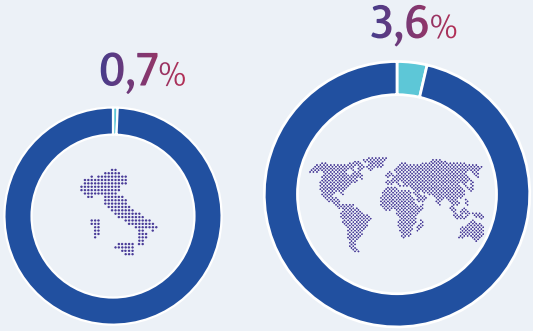
+187 *eventi nel 2024*

+10,8% *nell'ultimo anno*

2°settore in Italia per crescita di eventi DDoS

RANSOMWARE

Peso degli attacchi
Italia vs mondo



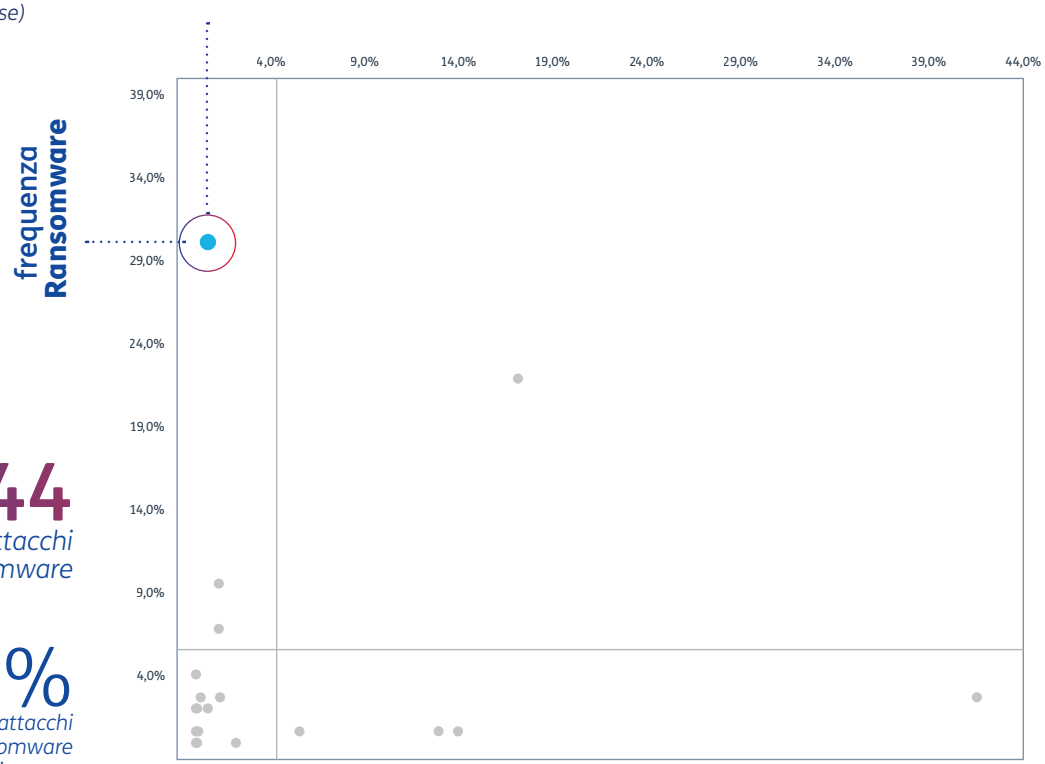
Manifatturiero

Matrice di frequenza di attacco

DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

10 *eventi DDoS*

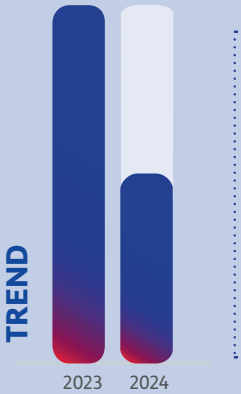
0,6% *degli eventi DDoS vs imprese*



44 *attacchi Ransomware*

30% *degli attacchi Ransomware vs imprese*

DDOS



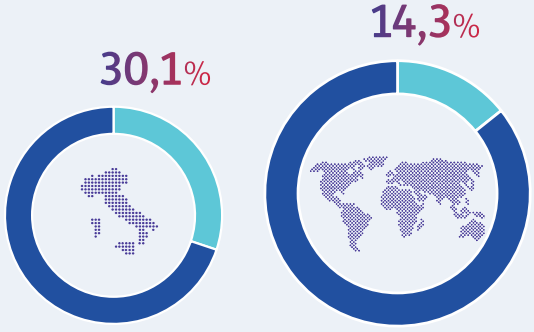
-9 *eventi nel 2024*

-1,4% *nell'ultimo anno*

diminuzione di eventi DDoS nell'ultimo anno

RANSOMWARE

Peso degli attacchi
Italia vs mondo



Commercio

Matrice di frequenza di attacco

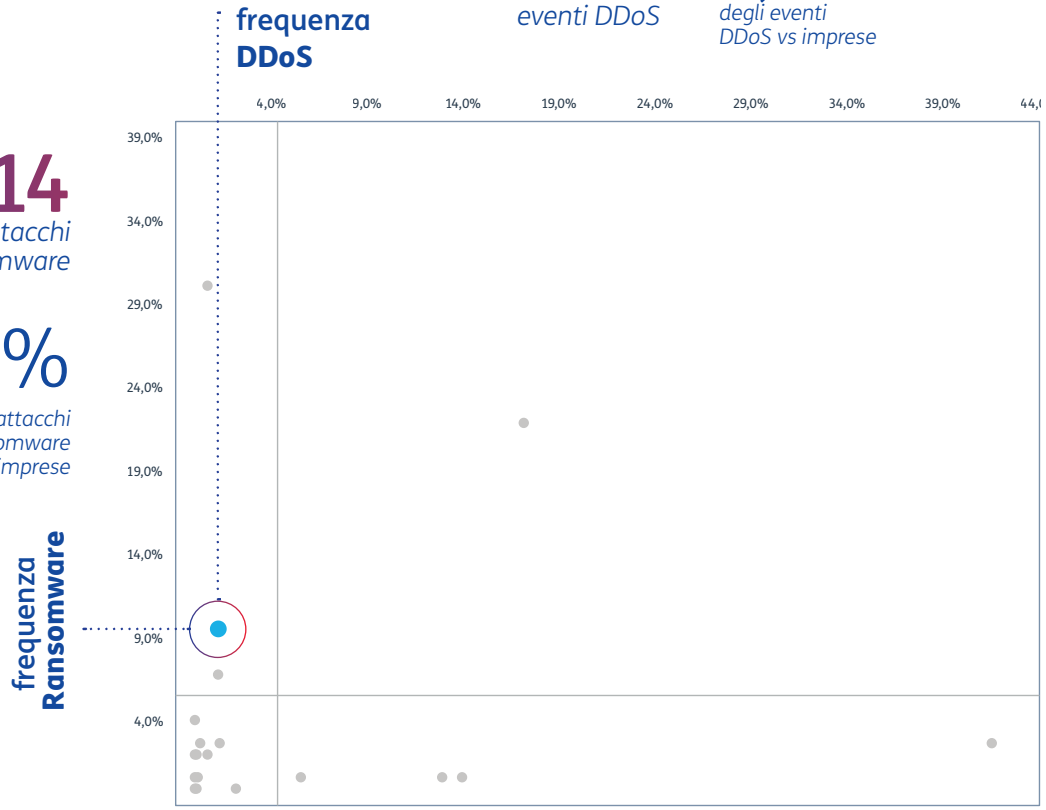
DDoS e Ransomware verso un settore (quota % su totale attacchi a imprese)

19 *eventi DDoS*

1,2% *degli eventi DDoS vs imprese*

14 *attacchi Ransomware*

9,6% *degli attacchi Ransomware vs imprese*



DDOS

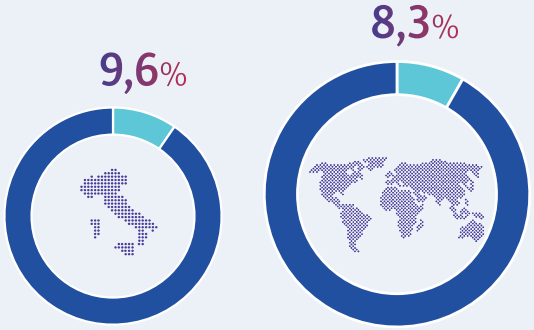
8° settore in Italia *per eventi DDoS nel 2024*

insieme al settore tecnologico

*per il Commercio, non è possibile dare evidenza del trend di crescita dell'ultimo anno poiché – a causa di una revisione delle categorie - non sono disponibili i dati relativi al 2023

RANSOMWARE

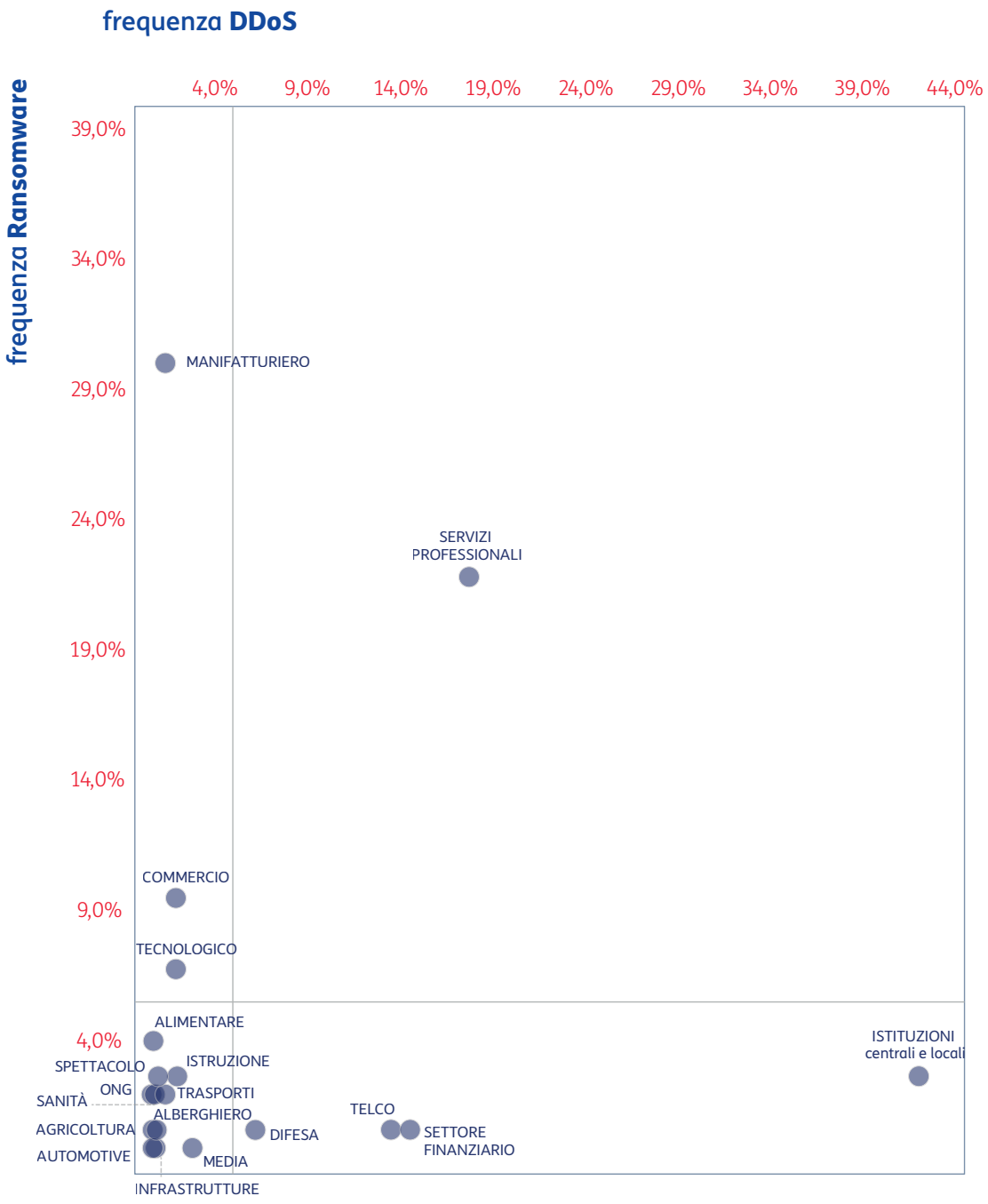
Peso degli attacchi
Italia vs mondo



Il peso degli attacchi in **tutti i settori** monitorati

Matrice di frequenza di attacco

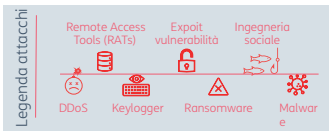
DDoS e Ransomware verso un settore
(quota % su totale attacchi a imprese)



PRINCIPALI ATTACCANTI PER TIPOLOGIA 2022-2024

SECONDA PARTE

State Sponsored



LAZARUS GROUP

ORIGINE:
Corea del Nord, 2009

ALIAS:
Dark Seoul, Hidden Cobra, Unit 121, APT 38, PLUTONIUM, TAG-71, Andariel

FINALITÀ:
Finanziamento della propria attività e del Governo nordcoreano

TECNICHE DI ATTACCO

CNE (Computer Network Exploitation): Spionaggio

CNA (Computer Network Attack): distruzione o manomissione di sistemi informatici.

- *Manipolazione account e token di accesso;*
- *acquisizione di Infrastruttura (domini, server, servizi web);*
- *esecuzione automatica all'avvio o all'autenticazione;*
- *intercettazione dati (traffico di rete, protocolli web, app);*
- *gestione dati e archiviazione.*

TARGET

Ampio range di settori; predilezione per gli attacchi alla supply chain che consente di raggiungere una vasta platea di vittime

SCARCRUFT

ORIGINE:
Corea del Nord, 2016

ALIAS:
Kimsuki, KONNI, Sector05, APT 37, Velvet Chollima, Thallium, Geumseong121, Red Eyes, Reaper

FINALITÀ:
Intelligence al servizio del Reconnaissance General Bureau, Difesa nord-coreana

TECNICHE DI ATTACCO

CNE (Computer Network Exploitation): Spionaggio

- *Manipolazione account e token di accesso;*
- *esecuzione automatica all'avvio o all'autenticazione;*
- *sfruttamento vulnerabilità nei protocolli web;*
- *cattura audio;*
- *uso interpreti di comandi o linguaggi di scripting (shell Windows, Visual Basic, Python) per eseguire operazioni dannose.*

TARGET

Obiettivi di alto profilo in Asia, USA, Europa e Russia, con predilezione per la Corea del Sud

NONAME057

ORIGINE:
Russia, 2022

FINALITÀ:
Hacktivismo filorusso; interruzione siti web ritenuti ostili alla Russia e favorevoli all'Ucraina

TECNICHE DI ATTACCO

CNA (Computer Network Attack): distruzione o manomissione di sistemi informatici.

- *Dettagli specifici sulle tecniche utilizzate per questi attacchi non sono disponibili pubblicamente. In generale, ricorso ad attacchi DDoS massicci.*

TARGET

Realtà private e pubbliche dei Paesi che sostengono l'Ucraina e contro la NATO. Canale Telegram dedicato per la rivendicazione degli attacchi.

PRINCIPALI ATTACCANTI PER TIPOLOGIA 2022-2024
Ransomware

LOCKBIT TEAM

ORIGINE:
Russia, 2019

FINALITÀ:
RaaS (Ransomware-as-a-Service)

autofinanziamento

TECNICHE DI ATTACCO

- *Furto di credenziali;*
- *elusione dei sistemi di debug e di analisi di codice e auto-diffusione;*
- *adattamento alle configurazioni specifiche dell'architettura aziendale delle vittime;*
- *cifratura dei dati con richiesta di riscatto*

TARGET

Ampio range di settori, senza un target specifico

MALASLOCKER TEAM

ORIGINE:
Area geografica sconosciuta, 2023

FINALITÀ:
Hacktivismo;

Finanziamento organizzazioni no-profit

TECNICHE DI ATTACCO

- *Sfruttamento vulnerabilità con metodo di encryption insolito: uso di algoritmi particolari*
- *nota con istruzioni dettagliate su come effettuare la donazione – senza specificare l'importo - e fornire la ricevuta*

TARGET

Vari settori, molto colpiti target italiani

BLACK BASTA TEAM

ORIGINE:
Russia, 2022

FINALITÀ:
RaaS (Ransomware-as-a-Service)

autofinanziamento

TECNICHE DI ATTACCO

- *Uso interpreti di comandi o linguaggi di scripting (PowerShell, Windows Command Shell) per eseguire operazioni dannose;*
- *creazione di processi per eseguire codice dannoso in background e mantenere l'accesso persistente al sistema;*
- *cifratura dei dati con richiesta di riscatto;*
- *elusione dei sistemi di debug e di analisi di codice;*
- *modifica aspetto di siti web e app interne.*

TARGET

Obiettivi di diversi settori anche critici, in prevalenza in ambito sanitario

TERZA PARTE

Elementi normativi

Come abbiamo più volte richiamato, la difesa nello spazio cibernetico richiede una forte collaborazione. La condivisione di informazioni e la definizione di prassi comuni rappresentano un modo molto efficace di contrastare le minacce provenienti dai diversi attori che a vario titolo portano delle minacce cyber a cittadini, imprese e stati nazionali.

Come nota la Commissione Europea «in un ambiente connesso, un incidente di sicurezza informatica in un prodotto può colpire un'intera organizzazione, o un'intera catena di fornitura, propagandosi spesso oltre i confini».

Per strutturare risposte coordinate a livello europeo, l'UE ha cercato di strutturare una cornice di riferimento comune, modulando sia la produzione normativa, sia le iniziative più operative – dalla certificazione degli apparati, ai processi di risposta alle aggressioni - per favorire un processo di convergenza tra i sistemi di cybersicurezza nazionali, così come effettuato in altri campi di interesse comune.

Per questo motivo, è fondamentale monitorare l'evoluzione del contesto normativo che rappresenta uno dei fattori di stimolo della strategia di difesa nazionale.

Cybersecurity in UE
assetti e **regole**

La protezione dello spazio digitale europeo è un fattore fondamentale per permettere la realizzazione di un'economia digitale compiuta. Si tratta di un obiettivo altamente complesso che interseca diversi aspetti fondamentali:

- **gli sviluppi tecnologici,** che procedono ad una elevatissima velocità e richiedono un costante adeguamento delle policy di protezione: il 5G, lo sviluppo delle piattaforme Cloud, l'Intelligenza Artificiale, aprono nuovi punti di attenzione con la necessità di definire nuove soluzioni.
- **Le evoluzioni del quadro geopolitico**, che comportano la revisione dei perimetri di ciber-difesa, adeguandoli alle nuove situazioni e la revisione dei protocolli comuni e degli accordi: la Brexit ha richiesto negoziati per gestire il passaggio da un quadro di difesa comune europeo ad una situazione più fluida.
- **I cambiamenti nei modelli di consumo**, come ad esempio la progressiva diffusione dei sistemi di pagamento elettronici, effettuata mediante API (application programming interface) soluzioni che facilitano l'interscambio automatizzato di informazioni tra apparati e sistemi. Questo da un lato agevola il pagamento, ma allarga la catena degli intermediari e richiede un adeguamento della disciplina in materia per normare i casi di frodi e di sottrazione di informazioni sensibili.
- **Le nuove sensibilità sociali,** che sollecitano una maggiore attenzione all'uso dei dati ed alla diffusione al di fuori del perimetro europeo, in modo da assicurare che il trattamento e la gestione sia in linea con i principi ed i valori UE.
- **I fenomeni congiunturali,** spesso imprevedibili, come ad esempio la diffusione del Covid, che ha avuto anche la conseguenza di accelerare il processo di digitalizzazione della società, con il lavoro agile, l'insegnamento a distanza, il boom dell'e-Commerce aprendo nuovi fronti da analizzare e difendere per assicurare un contesto più sicuro.

Questi ed altri fenomeni richiedono una costante revisione del quadro regolamentare. Provando a sintetizzare, per far fronte a questi cambiamenti, lo sviluppo normativo in materia di cybersecurity ha prodotto diverse normative, tra cui le principali sono:

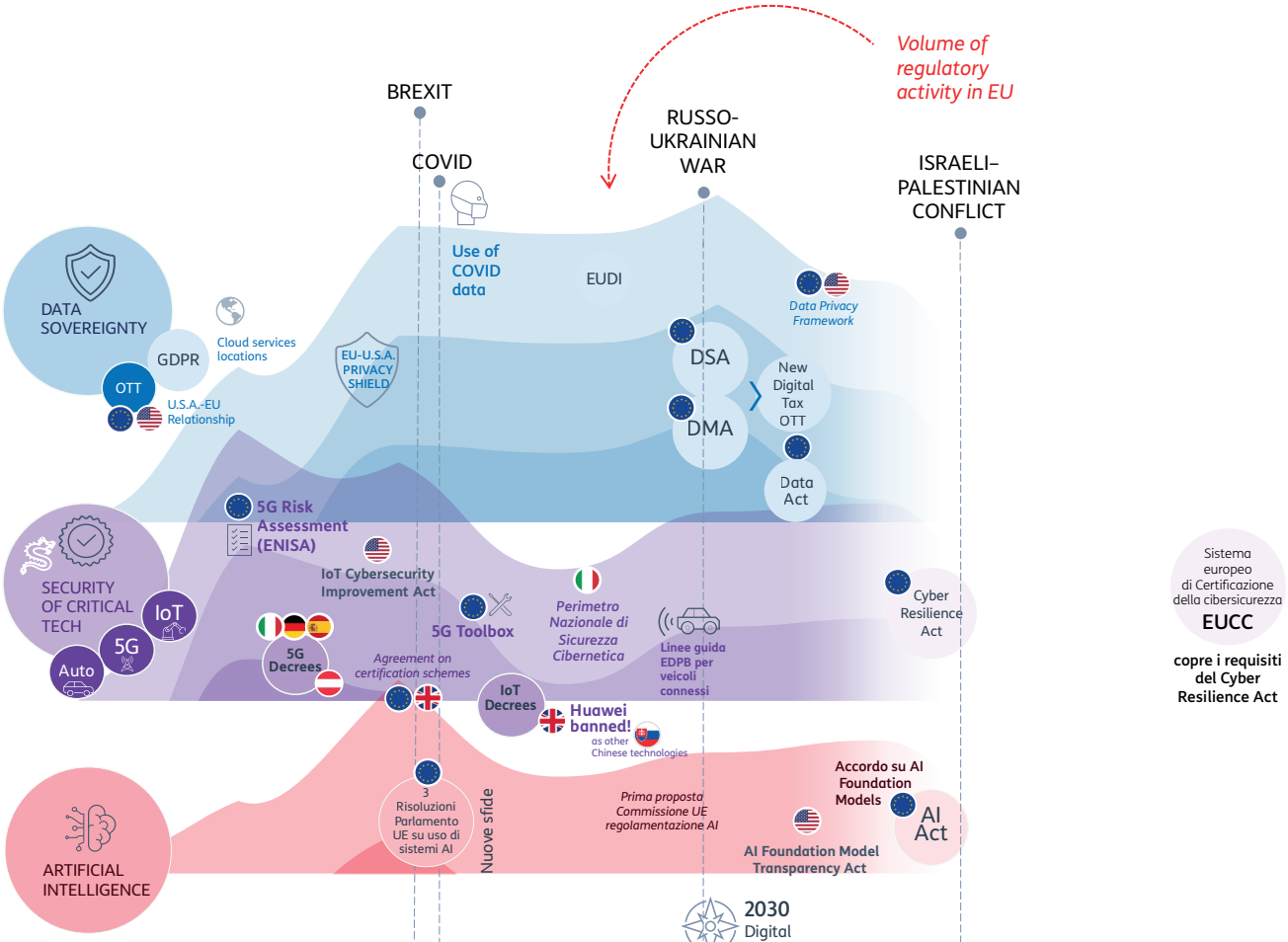
- La Direttiva NIS (2016)
- La strategia sulla Cybersecurity (2017)
- Il Cybersecurity Act - CSA (2019)
- La raccomandazione UE sulla cybersecurity delle reti 5G
- La nuova strategia sulla cybersecurity (2020)
- La Direttiva CER (2022)
- La Direttiva NIS 2 (2022, pubblicata 2023)
- Il Cyber Resilience Act – CRA (2024)

Il primo schema di certificazione redatto a livello UE in base al CSA è stato quello che ha definito dei criteri comuni (EUCC - Common Criteria). Sono oggi in discussione gli schemi di certificazione per la cybersecurity di

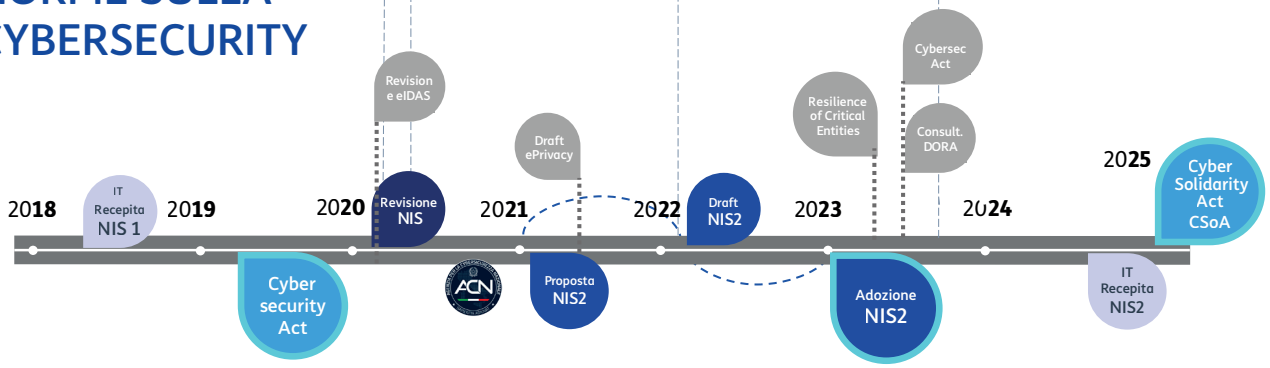
- Servizi Cloud (EUCS)
- Reti 5G (EU5G)

SI prevede che i prossimi schemi riguarderanno i Managed Services (inseriti recentemente nell'ambito del CSA) e i portafogli di identità digitale (in ottemperanza alle richieste del Regolamento europeo sull'identità digitale, EUid). A questi atti più generali, si aggiungono normative specifiche verticali per ambiti di attività più critici (come quello dell'offerta di servizi finanziari e di pagamento, interessati dall'evoluzione della normativa Digital Operational Resilience Act o DORA).

EVOLUZIONE QUADRO NORMATIVO UE



LE TAPPE DELLE NORME SULLA CYBERSECURITY



Fonte: Cullen International, notizie di stampa

Dalla NIS alla NIS2: Un cambiamento **fondamentale**

Le prime misure europee trasversali a tutela della sicurezza in ambito ICT risalgono alla Direttiva del Parlamento europeo e del Consiglio del 6 luglio 2016, misura legislativa congiunta che si pone l'obiettivo di innalzare la cooperazione tra gli Stati membri e creare un primo livello di armonizzazione in materia di sicurezza cibernetica: la **NIS**: (Network and Information Security).

La Direttiva ha giocato un ruolo fondamentale nell'accrescere la consapevolezza sui rischi relativi alla cybersecurity e ha costituito una guida per gli Stati Membri:

- definendo **requisiti minimi di sicurezza** per gli "operatori di servizi essenziali" (OSE) e i "fornitori di servizi digitali" (DSP – digital services providers) in settori considerati strategici (ad esempio l'energia, i trasporti, la sanità, le infrastrutture digitali (i.e. IXP, DNS, TLD));

- introducendo **obblighi di segnalazione** degli incidenti, di adozione di misure di prevenzione e di designazione di autorità nazionali competenti come oggi l'ACN in Italia.

Convertita in Decreto Legge in Italia nel 2018, il suo percorso si è intrecciato a quello di altre misure normative volte a creare un contesto di tutela degli utilizzatori dei servizi di comunicazione elettronica.

Nel 2018 il **Codice Europeo per le Comunicazioni Elettroniche** (CCEE), recepito in Italia nel 2021, ha ampliato le misure di sicurezza delle reti e i servizi di comunicazione elettronica presenti nel precedente framework.

Lo scenario evolve così rapidamente, con uno scambio di dati sempre più intenso nello spazio cibernetico – anche a seguito della pandemia - che nel 2020 si è già avviata una revisione della normativa e **nel 2022 tutte le norme sulla sicurezza vengono ricondotte alla NIS** ed i relativi articoli del CCEE vengono abrogati.

Il 27 Dicembre 2022 è stata pubblicata nella Gazzetta Ufficiale della UE la Direttiva 2022/2555 (NIS2), che sostituisce la precedente. La NIS2 mira a realizzare due importanti obiettivi:

1. **Aumento del livello di resilienza informatica** degli attori, pubblici e privati, anche ampliando il campo di applicazione.

2. **Miglioramento del livello collettivo di consapevolezza e capacità di gestione** e risposta delle minacce informatiche.

La Commissione ha deciso di mantenere lo strumento legislativo della Direttiva adottando il principio di armonizzazione minima per garantire sufficiente flessibilità nella trasposizione delle norme a livello nazionale.

Fornitori di Hardware e Software rimangono fuori dall'ambito di applicazione della NIS. La Commissione sta intervenendo normando questo ed altri aspetti attraverso diversi strumenti, come ad esempio la certificazione EUCC, il nuovo regolamento sui prodotti connessi Cyber Resilience Act (CRA) o il Regolamento europeo sull'Intelligenza Artificiale (AI Act), il Digital Operational Resilience Act (DORA) - relativo alla resilienza operativa digitale del settore finanziario, e la Direttiva Critical Entities Resilience (CER), relativa alla resilienza cyber dei soggetti considerati critici.

Nel 2024 entra in vigore la NIS2

Direttiva NIS2

La Direttiva NIS 1 individuava due categorie di soggetti, Operatori di servizi essenziali (OSE) e Fornitori di servizi digitali (FSD), a cui erano imposti due ordini di obblighi:

- **Misure di sicurezza** – adozione di misure di sicurezza commisurate al rischio e volte alla prevenzione e minimizzazione dell'impatto degli incidenti di sicurezza (con alcune misure più dettagliate nel contesto dei FSD).
- **Segnalazione incidenti** – notifica senza indebito ritardo alle autorità competenti o al CSIRT di incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati (in base al numero di utenti interessati, durata e diffusione geografica).

Agli Stati membri, nel recepirla a livello nazionale, la Direttiva NIS 1 richiedeva invece:

- l'adozione di una **strategia nazionale** in materia di sicurezza cibernetica con obiettivi strategici, priorità, politiche adeguate e misure di regolamentazione a livello nazionale;
- **cooperazione internazionale** e collaborazione con l'ENISA (European Network and Information Security Agency) attraverso meccanismi individuati;
- **designazione di autorità nazionali competenti**, di punti di contatto e del CSIRT (Computer Security Incident Response Team), responsabili della sicurezza e del monitoraggio degli incidenti a livello nazionale.

La Direttiva **NIS 2** rafforza gli obblighi già presenti all'interno della Direttiva NIS 1, superando la classificazione in OES e DSP e **riclassificando le entità soggette alla regolamentazione in "essenziali" e "importanti"**. Tra le entità essenziali rientrano le "infrastrutture digitali" (ECN, ECS, cloud, data centre, CDN, etc.)

- **NUOVE Misure di sicurezza –** mantenimento di un approccio "multirischio" nell'adozione di misure di sicurezza tecniche, operative e organizzative adeguate e proporzionate per (i) gestire i rischi per la sicurezza dei sistemi di rete e di informazione che tali soggetti utilizzano per le loro operazioni o per la fornitura dei loro servizi e (ii) prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi. La NIS 2 prevede un elenco minimo delle misure di sicurezza da implementare.

- **NUOVA Segnalazione incidenti –** rafforzamento degli obblighi di segnalazione e notifica di "incidenti significativi" alle autorità competenti e al CSIRT secondo uno schema a più fasi con tempistiche predefinite (ridotte a 24 ore dalla conoscenza per l'invio di un "early warning", seguito dalla notifica inziale entro 72 ore ed una analisi dettagliata dell'incidente entro 1 mese). Ove opportuno, viene prevista la notifica senza indebito ritardo degli incidenti significativi anche nei confronti dei destinatari dei servizi stessi.

Anche le prescrizioni rivolte agli Stati membri sono rafforzate, rispetto sia alla previsione di misure di vigilanza e esecuzione a cui sottoporre i soggetti essenziali e importanti (es. audit mirati e ispezioni), sia a nuovi obblighi di condivisione delle informazioni.

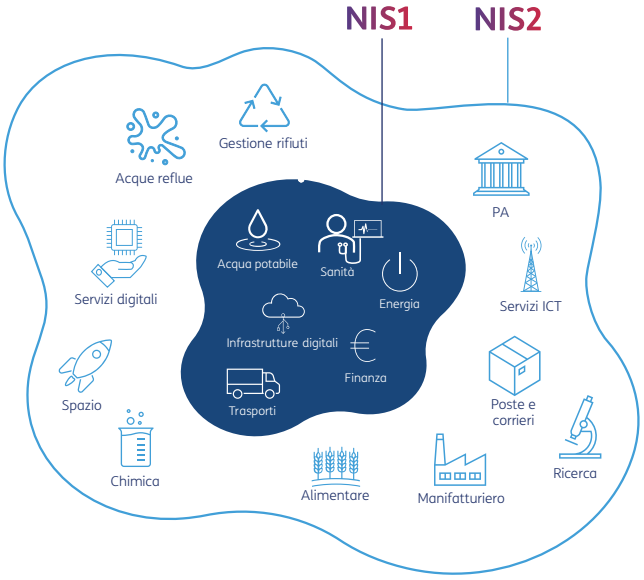
La direttiva NIS2 è stata pubblicata nella Gazzetta ufficiale dell'Unione europea nel dicembre 2022 ed è entrata in vigore il 16/01/2023. Gli Stati membri avevano 21 mesi di tempo dall'entrata in vigore della direttiva per recepire le disposizioni nel loro diritto nazionale (data effettiva: 18/10/2024) ma ad oggi soltanto Italia, Belgio, Croazia, Grecia, Lituania, Romania, Slovacchia e Ungheria hanno completato l'iter di trasposizione.

LA NIS 2:
perimetro, settori e scala

I criteri per la definizione degli enti sottoposti a normativa dalla NIS1 hanno portato a differenze ed incongruenze nelle scelte operate dai diversi Paesi Membri. Per superare l'incertezza e fare maggiore chiarezza, è stato definito un diverso criterio, classificando in soggetti in entità essenziali ed entità importanti in base all'appartenenza a settori altamente critici (rispetto a settori critici) ed alla dimensione dell'azienda

PERIMETRO ESTESO

NIS2 amplia il perimetro della NIS1 introducendo nuove misure con il fine di rendere tutto il sistema economico europeo più resiliente agli attacchi esterni.



CLASSIFICAZIONE DI SOGGETTI E SETTORI

SOGLIA DIMENSIONALE

	DIPENDENTI	FATTURATO	SETTORI **ALTAMENTE CRITICI**	ALTRI SETTORI **CRITICI**
Grandi imprese	**250+**	M€ **50+**	Entità **Essenziali**	Entità **Importanti**
Medie imprese	**50-249**	M€ **10-50**	Entità **Importanti**	Entità **Importanti**
Piccole imprese	**< 50**	M€ **<10**	*Coinvolte solo se rientrano nei settori definiti critici dalla NIS2*	
Micro imprese	**< 10**	M€ **≤2**		

Attività 2024:

Cyber Resilience Act (CRA)

Il Cyber Resilience Act (CRA), finalizzato a definire i requisiti di cybersecurity per prodotti dotati di componenti digitali, è entrato in vigore il 10/12/2024.

Questo regolamento si applica a diverse tipologie di prodotti dotati di componenti hardware o sistemi software, dagli strumenti medicali ai giocattoli intelligenti, che possono essere violati e utilizzati per penetrare in sistemi connessi aggirando le protezioni di sicurezza. Il regolamento prevede che i prodotti siano ripartiti in due diverse classi a seconda della diversa criticità e del livello di rischio. Inoltre, sono stati fissati quattro obiettivi specifici:

- garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali sin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita;
- garantire un quadro coerente in materia di cibersicurezza, agevolando la conformità per i produttori di hardware e software;
- migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali, e
- consentire alle aziende e ai consumatori di utilizzare in modo sicuro i prodotti con elementi digitali.

Il CRA è un regolamento orizzontale, finalizzato a garantire un livello minimo di sicurezza per tutti i prodotti hardware e software circolanti in UE e interagisce con tutte le altre normative verticali specifiche (NIS2, sistemi IoT, ecc.).

Il 11/12/2024 la Commissione europea ha costituito un gruppo di esperti per assistere e consigliare la Commissione su questioni rilevanti per l'attuazione del CRA.

Cyber Security Act (CSA)

Il regolamento sulla cibersicurezza è entrato in vigore il 7/01/2024 e nello specifico:

- rafforza il ruolo dell'ENISA, l'agenzia dell'UE che si occupa di sicurezza informatica;
- fornisce sostegno agli Stati membri, alle istituzioni dell'UE e alle imprese in settori chiave, compresa l'attuazione della direttiva NIS2;
- introduce un quadro di certificazione della cibersicurezza a livello dell'UE per i prodotti, i servizi e i processi TIC.

DORA

- Il regolamento DORA (Digital Operational Resilience Act) stabilisce i requisiti e gli standard tecnici per la gestione del rischio del settore finanziario, includendo anche i fornitori terzi di servizi TIC tra le entità finanziarie.
- DORA è una lex specialis della NIS2; pertanto, alle entità soggette alla DORA non si applicano le pertinenti disposizioni della NIS2 relative a misure di gestione dei rischi di cybersecurity, notificazione degli incidenti significativi, vigilanza e esecuzione.
- Gli standard tecnici previsti sono entrati in vigore il 17 gennaio 2025.

Le agenzie di Cybersecurity
Un ruolo da **protagonisti** in Europa

Gli interventi dell'Unione Europea in ambito cybersecurity puntano a superare le differenze tra Paesi Membri, realizzando un sistema unico europeo di sicurezza cibernetica resiliente e assicurando un maggiore livello di controllo dei confini digitali superando alcuni retaggi del passato, dipendenti dagli assetti istituzionali dei singoli Paesi Membri

In questo contesto, l'Agenzia di Cybersecurity Europea, l'ENISA assume un ruolo centrale basato su quattro cardini:

- Cybersecurity Policy: l'ENISA è un centro nevralgico di competenze e supporta lo sviluppo della politica dell'UE in materia di cybersecurity.
- Cooperazione Operativa. Sostiene il coordinamento tra i diversi sistemi di sicurezza informatica europei e facilita una risposta rapida negli incidenti su larga scala da parte della rete degli CSIRT e in CyCLONe, la rete europea per la gestione delle crisi informatiche
- Soluzioni affidabili. Presidia la certificazione del livello di sicurezza degli apparati, evitando la proliferazione di sistemi nazionali basati su standard differenti tra loro.
- Sviluppo della capacità. Promuove la circolazione delle informazioni, la formazione, la diffusione di best practice che aiuta i Paesi Membri a valutare il livello di maturità del proprio sistema di ciberdifesa.

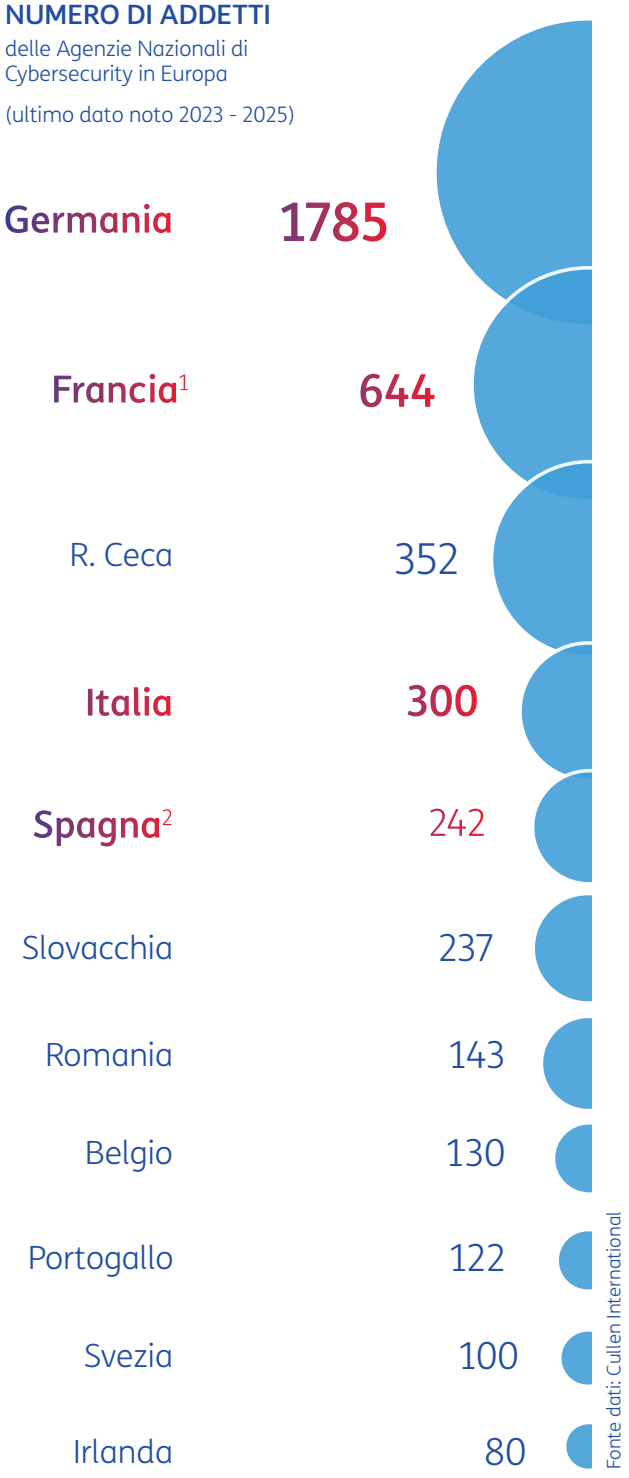
In altri termini, l'ENISA svolge un ruolo di riferimento strategico, politico, tecnico ed operativo per le diverse strutture di cybersecurity nazionali, che a loro volta rappresentano per ciascun Paese il punto di riferimento per assicurare un ambiente digitale sicuro e resiliente. Le direttive impongono che tali strutture debbano essere "adeguatamente dotate di personale per garantire la disponibilità continuativa" e - operando sul campo per garantire la sicurezza cibernetica dei principali Paesi europei - devono ospitare lo CSIRT, l'unità tecnica che ha il compito di monitorare e rispondere agli incidenti che interessano le infrastrutture critiche a livello nazionale.

Possiamo renderci conto della complessa e fitta rete di attività che interessano le Agenzie osservando il quadro di attività della ACN, l'Agenzia Nazionale di Cybersecurity che in Italia, svolge - tra gli altri - i seguenti compiti:

- Autorità competente NIS e punto di contatto unico
- Autorità per l'integrità delle reti di telecomunicazione
- Presidia il perimetro di Sicurezza Nazionale Cibernetica
- Qualifica le infrastrutture e i servizi cloud per la Pubblica Amministrazione
- Centro di Valutazione e Certificazione Nazionale (CVCN)
- CSIRT Italia
- Nucleo per la Cybersicurezza (NCS)
- Centro Nazionale di Coordinamento Italiano (NCC-IT) e supporta il Centro europeo di competenza in cybersecurity

LE CYBER AGENZIE EUROPEE: PERSONALE

NUMERO DI ADDETTI
delle Agenzie Nazionali di Cybersecurity in Europa
(ultimo dato noto 2023 - 2025)



Personale delle Agenzie Nazionali di Cybersecurity

In Italia, l'Agenzia Nazionale di Cybersecurity ha attualmente una dotazione di circa 300 unità, che a pieno organico dovrebbe arrivare a circa 800 unità, un numero di risorse in linea con la Francia, che nel 2022 aveva una dotazione di poco meno di 800 unità operanti nell'ANSSI (circa 650 FTE nel 2024).

In Europa, il Paese con il maggior numero di risorse è la Germania: il BSI (Bundesamt für Sicherheit in der Informationstechnik) poteva contare all'incirca su 1700 persone ad inizio 2024. Secondo fonti di stampa, il personale dell'Agenzia Nazionale Spagnola per la Sicurezza Informatica è stimato tra 200 e 250 persone.

Budget delle Agenzie Nazionali di Cybersecurity

Per quanto riguarda i budget, la situazione è meno chiara perché le informazioni non sono sempre disponibili e le risorse possono essere allocate tra diverse entità. Sulla base dei dati disponibili, l'agenzia tedesca BSI ha il budget più elevato, stimato in circa 240 milioni di euro, mentre l'ANSSI in Francia ha a disposizione circa 80 milioni. Non sono disponibili dati aggiornati per la Spagna (secondo i dati del 2022, tuttavia, il budget per dipendente era il più elevato tra quelli noti). Nei Paesi Bassi, il budget è aumentato a causa del consolidamento di diverse strutture.

1 FTE

2 dato stimato

Per ragioni di sicurezza nazionale, le informazioni sul numero di risorse impiegate nell'Agenzia nazionale di Cyber Security nel **Regno Unito** non sono pubblici. L'ultimo dato disponibile (2019) riportava più di 1000 addetti.

QUARTA PARTE

Tecnologie emergenti

Il settore della cybersecurity non è mai fermo. I cambiamenti dello scenario geopolitco, il lancio di nuove soluzioni tecnologiche e servizi, l'individuazione di nuove falle e vulnerabilità nei sistemi, rappresentano fattori che alimentano continuamente nuove tecniche di attacco e aprono fronti inattesi di minaccia.

È per questo che occorre monitorare con costanza il panorama e tenere sotto controllo gli sviluppi in atto, cercando di anticipare il più possibile le mosse di avversari che dal punto di vista tecnologico sono spesso un passo più avanti dei difendenti più evoluti.
L'obiettivo di questa sezione è quello di fornire alcune novità che emergono dallo scenario della cybersecurity, sia in termini di minacce, sia di soluzioni di difesa, prevenzione e contrasto.

Nuovi fronti d'attenzione tecniche: **uso dell'AI**

In questa fase globale di trasformazione digitale l'impatto dell'intelligenza artificiale (IA) diventa sempre più significativo e percepibile in ogni settore della società, incluso quello della sicurezza informatica. Grazie alla rapida evoluzione della sua capacità di apprendimento, adattamento e previsione delle minacce, l'IA è diventata uno strumento sofisticato indispensabile per proteggere le aziende e i governi dalle minacce derivanti dalle tecnologie connesse: dagli attacchi informatici, allo spam, alla manipolazione dell'informazione. Al tempo stesso, l'IA pone anche nuove sfide sul fronte degli attacchi per via della crescente accessibilità e diffusione di questo strumento ormai largamente a disposizione anche degli attaccanti.

Un esempio del duplice ruolo ricoperto dall'intelligenza artificiale nell'ambito della sicurezza informatica è rappresentato dall'IA generativa: in risposta alle barriere inserite in alcuni prodotti commerciali come ChatGPT per impedire un uso improprio della tecnologia, sono stati sviluppati **strumenti antagonisti**, come WormGPT o FraudGPT, per aggirare tali barriere e supportare i cybercriminali nella scrittura di codice malevolo o nello sviluppo di malware.

L'intelligenza artificiale generativa viene sfruttata anche nell'avvio di **campagne di phishing, creando e-mail convincenti e messaggi ingannevoli sempre più difficili da identificare** con un minor utilizzo di risorse e tempo rispetto al passato. Inoltre, gli attaccanti sono in grado di identificare in modo più efficiente gli obiettivi di alto valore e di personalizzare gli attacchi diretti al bersaglio profilato mediante **algoritmi di apprendimento automatico utilizzati per l'analisi di social media e di altri dati online.**

L'IA può potenziare il malware attraverso l'apprendimento dei comportamenti tipici dell'utente o del sistema, consentendo attacchi o esfiltrazione di dati ed evitando il rilevamento dai sistemi di sicurezza e simulando una situazione normale di attività.

Gli strumenti di ricognizione basati su IA permettono di effettuare attività d**i scansione delle reti alla ricerca di vulnerabilità,** scegliendo automaticamente l'exploit più efficace per compiere l'attacco. Grazie al processo di addestramento dell'IA si possono poi identificare e selezionare le informazioni più preziose da esfiltrare, riducendo ulteriormente le possibilità di rilevamento dai sistemi di sicurezza.

Infine, l'IA viene sfruttata dagli attaccanti per generare **deepfake** audio o video impiegati durante gli attacchi di phishing o **vishing** (phishing vocale), impersonando in modo convincente persone fidate e conferendo maggiore credibilità agli attacchi di ingegneria sociale.

Nel 2019, in una società del settore energetico del Regno Unito è stata simulata la voce dell'AD per richiedere un bonifico urgente a un fornitore con sede in Ungheria e trasferire illegalmente fondi.

A marzo 2022, i criminali informatici hanno hackerato un canale televisivo Ucraino e caricato video deepfake sui social network in cui il presidente Zelensky chiedeva la deposizione delle armi e la resa all'esercito russo.

A maggio 2022 è stato diffuso su YouTube un deepfake di Elon Musk che prometteva agli investitori di una piattaforma di trading di criptovalute rendimenti fino al 30%.

A maggio 2023, gli hacker etici di Social Proof Security hanno utilizzato il clone vocale di un corrispondente televisivo statunitense per indurre uno dei membri dello staff dell'emittente a consegnare informazioni personali sensibili.

Nuovi fronti d'attenzione tecniche: **Quantum Technology**

Le tecnologie quantistiche rappresentano un'altra frontiera della ricerca applicata. La grande potenza computazionale dei computer quantistici permette di risolvere categorie di problemi complessi in minor tempo e per questo tali tecnologie trovano applicazione laddove è necessario governare l'interazione di un numero elevato di variabili (ottimizzazione, pianificazione, simulazione ecc.). Già oggi è possibile ipotizzare diversi sviluppi delle tecnologie quantistiche, anche nel campo della cybersecurity.

MINACCE POTENZIALI

In primo luogo, la potenza di calcolo pone un tema di possibile minaccia. Le soluzioni di crittografia adottate oggi si basano su chiavi particolarmente complesse e difficili da rompere, ma non con un computer quantistico che può ottenere una soluzione in tempi brevi.

Di fronte a questa eventualità, alcuni Paesi hanno già iniziato a muoversi: il Memorandum sulla sicurezza nazionale degli USA (2022) prevede l'obiettivo di migrazione alla crittografia quantum-resistant entro il 2035. In Europa, la Commissione Europea ha lanciato il progetto Euro-QCI, Quantum Communications Infrastructure, basata sulla distribuzione di chiavi quantistiche (QKD, Quantum Key Distribution) per crittografia. Tale infrastruttura dovrebbe essere prevalentemente utilizzata per lo scambio di informazioni tra agenzie governative e autorità degli Stati membri e dell'UE.

Insieme alla Post-Quantum Cryptography (PQC), la QKD è il principale approccio adottato a livello mondiale per la transizione a sistemi crittografici quantum-resilient.

La PQC prevede il design di schemi crittografici classici particolarmente complessi e considerati resistenti anche ai computer quantistici. La QKD è un metodo di livello fisico basato sulla meccanica quantistica che fornisce sicurezza incondizionata, ovvero indipendente dal modello di calcolo considerato.

OPPORTUNITÀ DI DIFESA.

Allo stesso tempo, la potenza di calcolo rappresenta una opportunità di difesa: la fisica dei quanti consente di implementare chiavi di cifratura basate sui fotoni, come la già citata QKD, che consiste in un sistema sincrono di scambio di chiavi simmetriche per proteggere lo scambio di dati altamente sensibili (es. dati sanitari, dati finanziari ecc.). L'eventuale violazione della chiave è immediatamente rilevata da coloro che si scambiano i dati crittografati, che quindi possono interrompere lo scambio e generare una nuova chiave.

Un'altra evoluzione interessante è la Quantum Number Random Generation (QRNG), un'applicazione per la generazione di numeri casuali che sfrutta le proprietà fisiche dei fenomeni naturali che generano entropia per superare il limite degli attuali algoritmi adottati sui computer tradizionali dove la generazione avviene attraverso un innesco numerico deterministico.

Un'altra evoluzione da citare è quella dei microprocessori per applicazioni dedicate alla cybersecurity basate su tecnologie quantistiche. In questa prospettiva, Telsy ha sviluppato un Secure Microchip, una micro-piattaforma programmabile e sicura by design che utilizza algoritmi PQC per garantire una difesa anche contro avversari quantistici. Per la sua innovazione, il Secure Microchip è stato selezionato tra le migliori innovazioni tecnologiche da GSMA, l'associazione mondiale degli operatori TLC.

Conclusioni

a cura di Ivano Gabrielli

Direttore del Servizio polizia postale e delle comunicazioni

Il 2024 può essere considerato, a tutti gli effetti, un anno "zero" per la cybersecurity nel nostro Paese. Si è assistito infatti a una fase di profonda trasformazione, nella quale l'attenzione istituzionale, l'evoluzione normativa, la maturazione delle strutture operative e la crescente consapevolezza degli attori economici hanno tracciato un nuovo perimetro per la sicurezza digitale nazionale.

La minaccia cibernetica, della quale si è registrato un consistente incremento, non si limita più a colpire esclusivamente le infrastrutture critiche e sensibili, ma si manifesta sempre più come un fenomeno sistemico, trasversale e interconnesso con le dinamiche geopolitiche globali. Si rilevano attacchi continui e mirati alla pubblica amministrazione e ai settori strategici del Paese, ma è sul fronte delle piccole e medie imprese che l'impatto risulta particolarmente significativo. Le PMI, che rappresentano il 63% dell'economia italiana, si confermano infatti come l'anello debole del sistema, spesso prive delle risorse economiche e delle competenze tecniche necessarie per adottare adeguate misure di sicurezza informatica. Questo le rende obiettivi privilegiati da parte della criminalità organizzata e di gruppi ostili, che sfruttano tali vulnerabilità per condurre attacchi sempre più sofisticati.

Di fronte a questo scenario, emerge la necessità di un cambio di paradigma. La cybersecurity deve essere integrata in modo strutturale nei modelli organizzativi e produttivi delle imprese, con la stessa logica con cui in passato si è affrontato il processo di digitalizzazione o si è garantita la sicurezza fisica degli asset aziendali. La progettazione sicura dei sistemi e dei processi, secondo il principio della cybersecurity-by-design, deve diventare la norma. Le imprese, in particolare le PMI, dovranno essere accompagnate verso soluzioni sostenibili, come l'acquisto di servizi di sicurezza da remoto o l'adesione a strutture consortili settoriali in grado di offrire servizi condivisi di monitoraggio e risposta agli incidenti, attraverso SOC e CSIRT comuni. Tale approccio rappresenta una risposta concreta alla necessità di distribuire i costi e le competenze in un ecosistema produttivo frammentato ma vitale.

C'è da dire che l'Italia, la cui economia è fortemente basata sul comparto manifatturiero, presenta caratteristiche analoghe a quelle di altri Paesi europei come Francia e Germania. I dati mostrano una sostanziale coerenza con il quadro internazionale, ma ciò non può e non deve rappresentare un elemento di rassicurazione. Oltre alla crescita numerica degli attacchi, preoccupa l'elevata complessità delle offensive digitali, spesso orchestrate da organizzazioni criminali strutturate e capaci di accedere a un mercato globale della tecnologia criminale. La minaccia, dunque, non è solo più frequente, ma anche più articolata e difficile da fronteggiare con strumenti convenzionali.

Dal punto di vista operativo, si è assistito a una significativa maturazione dei processi adottati sia dalle strutture di Law Enforcement, sia a livello istituzionale, con la creazione di meccanismi più rapidi ed efficaci di risposta alle minacce informatiche, col fine di rendere il sistema nazionale più coeso, resiliente e reattivo. Proprio in questo contesto si colloca il potenziamento delle strutture territoriali della Polizia Postale: una vera e propria backbone per la prevenzione e il contrasto dei crimini informatici, a supporto delle Procure distrettuali, che permetta di integrare l'azione investigativa con un presidio tecnico continuo e qualificato.

Sul piano normativo, un ruolo decisivo è stato svolto dall'attuazione della direttiva NIS2 e dall'approvazione della Legge 28 giugno 2024, n. 90. Questi strumenti hanno ridefinito i rapporti tra i principali soggetti coinvolti nella governance della cybersicurezza, in particolare tra l'Agenzia per la Cybersicurezza Nazionale, l'autorità giudiziaria e le strutture di Law Enforcement, introducendo elementi di chiarezza, condivisione delle responsabilità e maggiore cooperazione interistituzionale. Ne è derivato un contesto normativo più strutturato, capace di sostenere una risposta organica alle minacce digitali.

Importanti progressi sono stati registrati anche nell'ambito degli strumenti investigativi, con l'adozione di tecnologie sempre più evolute, essenziali per fronteggiare attacchi sofisticati e transnazionali. Questa modernizzazione ha consentito un salto di qualità nella capacità di risposta delle forze dell'ordine, potenziando la possibilità di individuare tempestivamente le minacce, ricostruirne la provenienza e intervenire in modo mirato, pur in un contesto in cui i confini tra minaccia criminale e strategica sono sempre più sfumati.

I dati evidenziano con chiarezza come l'Italia debba prepararsi a convivere, nei prossimi anni, con un livello di rischio costantemente elevato. Non si tratta di un'eventualità, ma di una condizione strutturale che impone la definizione di un presidio permanente e interistituzionale, in grado di garantire una capacità di risposta continua, aggiornata e coordinata. In questa direzione sarà essenziale rafforzare il partenariato pubblico-privato, ponendolo come pilastro di un sistema di cybersicurezza distribuito, resiliente e sostenibile.

Il 2024 ha rappresentato quindi un punto di svolta non solo per il consolidamento delle capacità esistenti, ma per l'avvio di una nuova fase strategica per la sicurezza digitale nazionale. Le istituzioni hanno compiuto uno sforzo rilevante nella costruzione di una capacità operativa in grado di rispondere alle minacce complesse che caratterizzano l'odierno spazio cibernetico, minacce che colpiscono simultaneamente libertà individuali, servizi pubblici essenziali e asset economici di primaria importanza.

Il quadro normativo italiano si può oggi considerare all'avanguardia nel contesto europeo, ma un elemento che non può e non deve essere sottovalutato è dato dalla necessità di promuovere un investimento forte e coordinato nella formazione delle competenze, con l'introduzione di modelli formativi innovativi. È necessario che lo Stato si faccia carico di uno sforzo per la creazione di una nuova generazione di esperti in sicurezza cibernetica, formati per essere immediatamente operativi nei ruoli istituzionali e successivamente in grado di contribuire, anche nel settore privato, al rafforzamento del presidio cyber nazionale. In questa prospettiva, si delinea l'opportunità di un patto tra istituzioni e mondo economico, capace di sostenere un ciclo formativo che sia utile oggi per il pubblico, e domani per il privato, nella costruzione di un ecosistema di cybersicurezza realmente partecipato ed efficiente.

Si ringrazia l'**On. Alessandro Colucci,** Segretario di Presidenza della Camera dei Deputati e Presidente del "Intergruppo parlamentare per la Sicurezza Informatica e Tecnologica", per aver incoraggiato lo sviluppo del presente report e l'interesse dimostrato nella diffusione della consapevolezza in ambito cibernetico a livello nazionale.

Si ringraziano per i dati forniti ACLED (Armed Conflict Location & Event Data) e Cullen International.

L'immagine di copertina è stata generata con AI.

CYBER SECURITY FOUNDATION

TIM

Cyber Security Report

Analisi delle minacce DDoS e Ransomware

giugno 2025

www.gruppotim.it

www.cybersecurityfoundation.it