Assintel Cyber Report 2023

Estratto

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Powered by:

mediatech

HACKMANAC

Swascan
TINEXTA GROUP

Sommario

EXECUTIVE SUMMARY

Con il dipanarsi pervasivo della transizione digitale, la cybersecurity è ormai diventata un tema dominante per ogni organizzazione, perché - indipendentemente dalle sue dimensioni – può rappresentare un bersaglio facilmente accessibile ai cyber criminali. Il patrimonio di dati, le operazioni, il marchio, la reputazione e i canali sono potenzialmente a rischio, e non parliamo solo aspetti tecnologici ma anche di fattori umani. In questo panorama, sempre più complesso, c'è un target più fragile di cui dobbiamo occuparci: sono le micro, piccole e medie aziende, che spesso non hanno risorse e cultura per considerare la cybersecurity come un investimento a protezione del proprio business. Ed è su questo fronte che diventa essenziale il ruolo delle associazioni di settore, così come avviene con il Cyber Think Tank di Assintel, che monitora regolarmente il contesto e ne dà evidenza in report periodici come il presente.

I dati consuntivi del 2023 mostrano che gli attacchi sono aumentati in modo costante: **+184%** a livello global con un totale di **7.068 attacchi** individuati. Nel 61% dei casi sono arrivati dal Dark Web, geograficamente sono aumentati del 50% in America e del 27% in Europa.

Il settore manifatturiero è stato il più colpito, passando dal 5% al 16% degli attacchi totali nel 2023, seguito dal settore professionale/scientifico/tecnico, ICT, sanitario e finanziario/assicurativo.

Le tecniche più utilizzate per i cyber attacchi sono il malware, che ha raggiunto il 70% del totale. Quasi un quarto degli attacchi ha avuto impatti critici, mentre il 67% ha avuto impatti gravi. Questo indica un aumento significativo degli attacchi con conseguenze economiche, legali o reputazionali catastrofiche per le vittime.

Il furto di Dati e il Ransomware sono in costante crescita con **4965 attacchi** nel mondo, dominati dalle gang LockBit, CLOP, PLAY, Alphv/BlackCat e 8BASE. L'Italia si colloca al sesto posto nella classifica, dominata dagli Stati Uniti (2261 attacchi), con 149 attacchi. È interessante notare la progressione del secondo semestre dello scorso anno: il numero di vittime è aumentato del 62% rispetto al trimestre precedente, e le PMI - in particolare le piccole e micro aziende - si sono confermate il target preferito dai Criminal Hacker, rappresentando l'80% delle vittime.

EVOLUZIONE DEI CYBER ATTACCHI NEL 2023

Da quando si è accesa un'attenzione crescente sulla cyber sicurezza, sta emergendo un panorama di attacchi e vulnerabilità sempre più nutrito e variegato, in cui gioca un ruolo decisamente robusto il dark Web. Per questo motivo il presente Report l'ha incluso nel suo campione di analisi, fotografando un impressionante aumento del **184%** di cyber attacchi nel 2023, corrispondenti a **7.068 eventi**.

Di questi, l'aspetto più preoccupante è che **4.289 incidenti**, pari al **61%** del totale, proviene esclusivamente da fonti del **Dark Web**, senza la possibilità di rintracciarne alcun riscontro nel Clear Web.

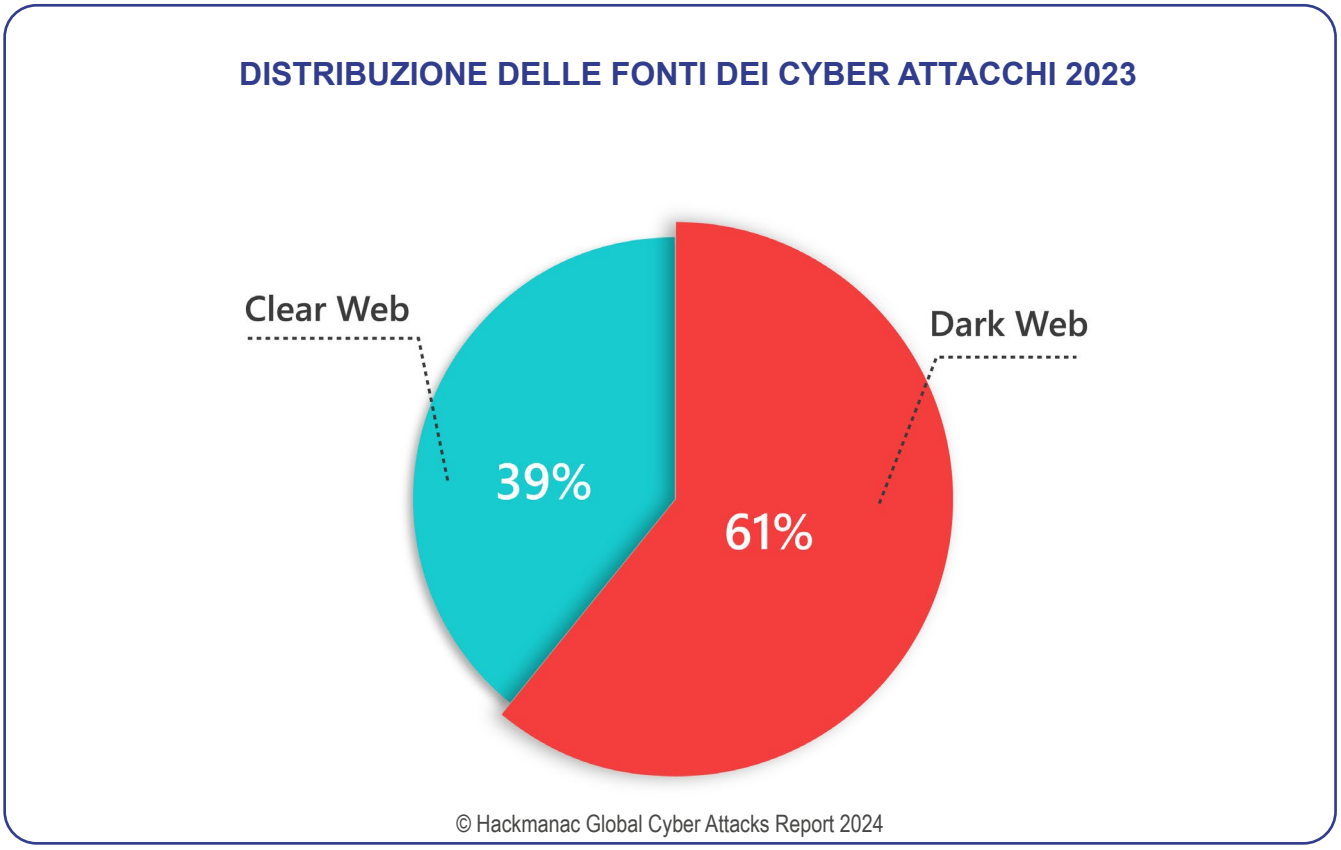

Figura 1: Distribuzione delle fonti dei cyber attacchi nel 2023

Questo sottolinea l'importanza di raccogliere informazioni sugli attacchi avvenuti anche tramite fonti non convenzionali.

Anche la media mensile è aumentata considerevolmente e nel 2023 raggiunge i **589 attacchi** (**406** solo per quanto riguarda gli incidenti collezionati dal Dark Web).

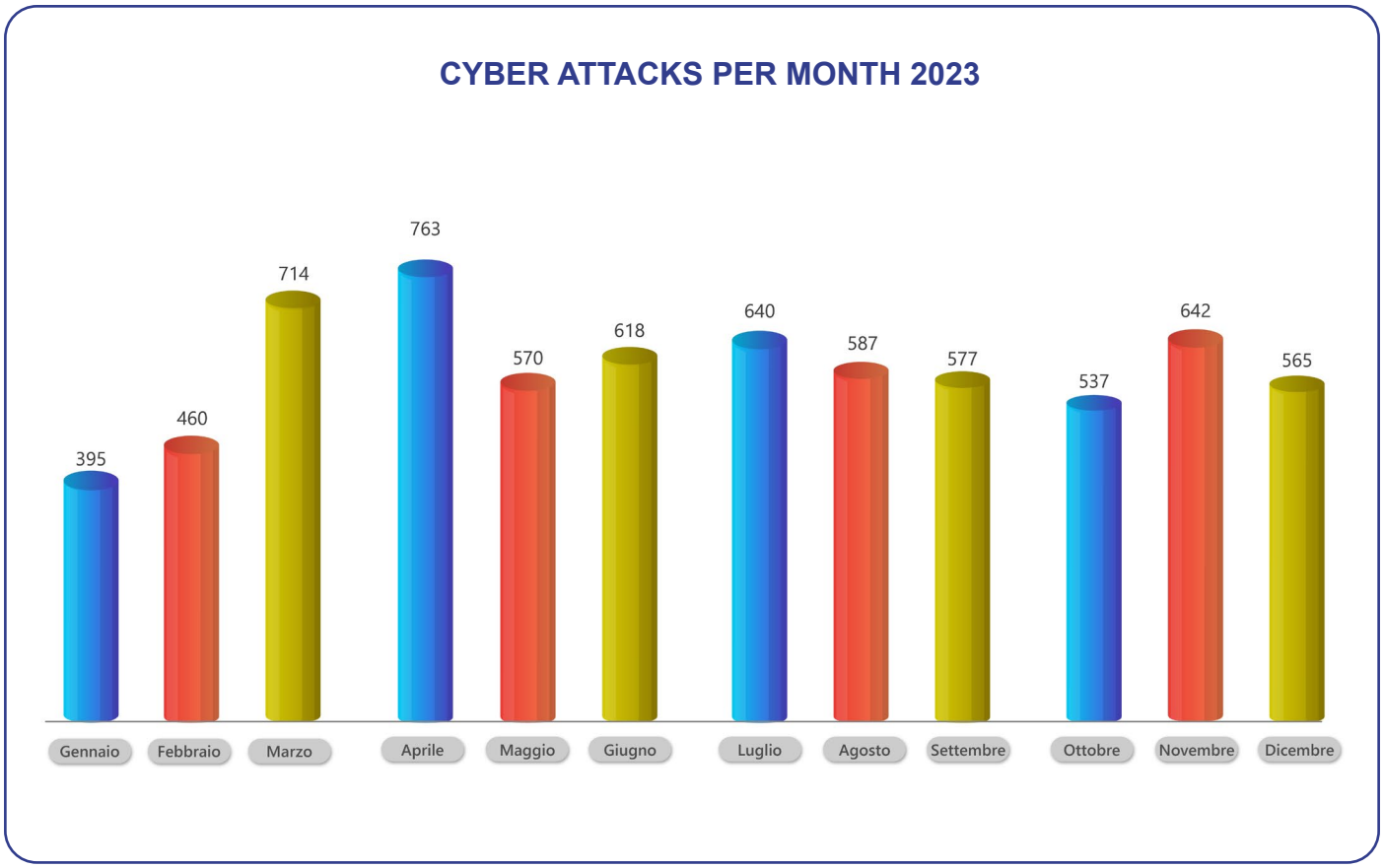

Figura 2: Cyber attacchi per mese nel 2023

Storicamente l'andamento dei cyber attacchi nel corso dell'anno mostra di frequente un picco in primavera: nel 2023 **aprile** è il mese con il numero maggiore di attacchi, **763** in totale.

A seguire marzo (**714**), novembre (**642**), luglio (**640**) e giugno (**618**).

Gennaio e febbraio sono invece i mesi in cui abbiamo riscontrato meno attività criminali (rispettivamente **395** e **460** cyber attacchi).

GLI ATTACANTI

Le varie tipologie di attaccanti che utilizziamo nella nostra classificazione rappresentano anche la principale motivazione degli incidenti.

Il **Cybercrime** è da anni la principale minaccia, considerando anche che, tra gli attacchi di pubblico dominio, alcune categorie come **Espionage** e **Information Warfare** sono sottorappresentate rispetto al reale numero di incidenti che avvengono in questi ambiti.

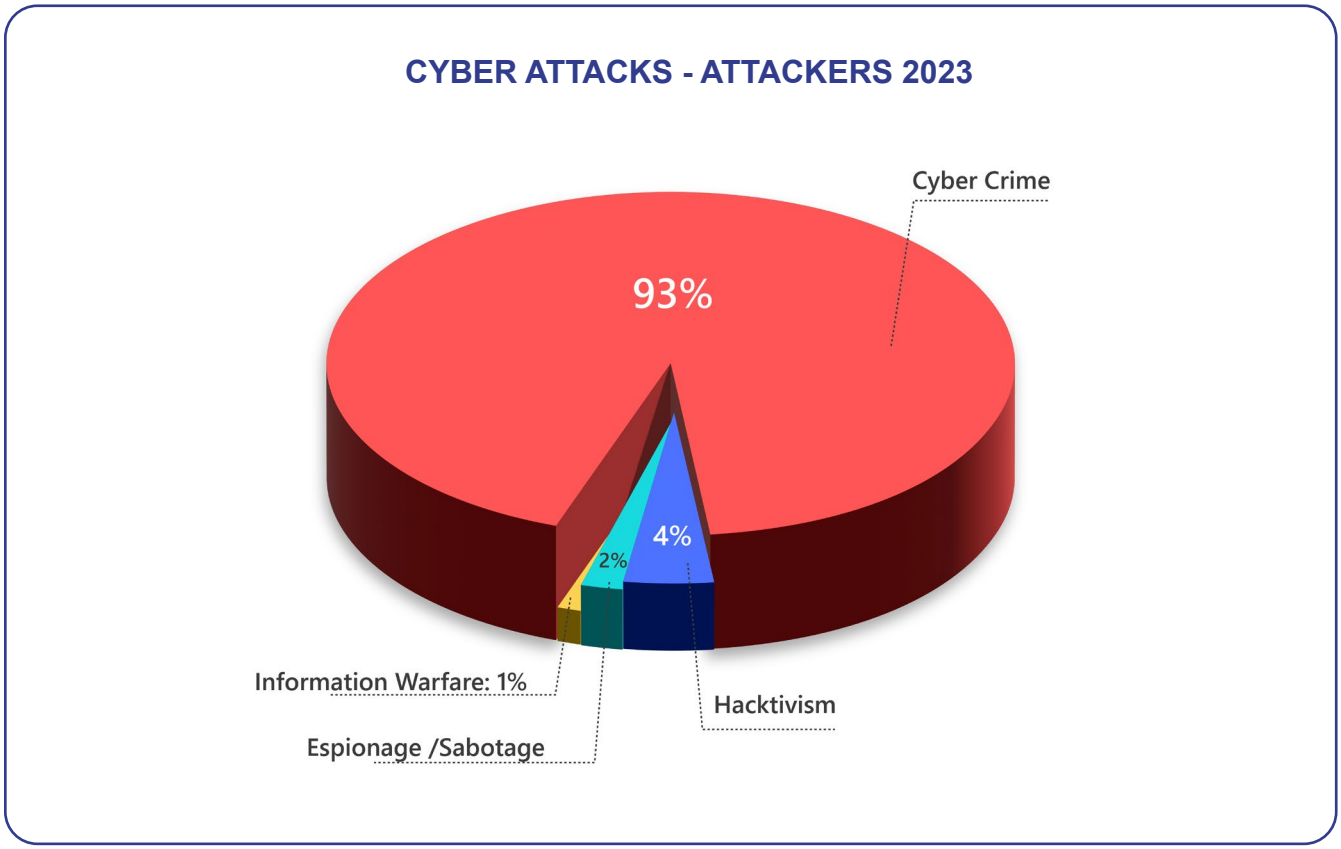

Figura 3: Distribuzione attaccanti nel 2023

Nel 2023 il fenomeno del cybercrime, che negli anni precedenti è cresciuto in maniera continua, raggiunge il **93%** degli attacchi totali, mentre gli incidenti noti legati a fenomeni di **Espionage / Sabotage** e **Information Warfare** (rispettivamente **2%** e **1%**), sembrano in discesa rispetto all'anno precedente.

Cresce leggermente invece il fenomeno **Hacktivism**, passando dal 3% al **4%**.

LE VITTIME

Andando ad analizzare le vittime principali dei cyber attacchi, il settore **Manufacturing** è in assoluto il più preso di mira oltre che quello che mostra la crescita più rapida: si passa, infatti, dal 5% del totale degli attacchi nel 2022 al **16%** nel 2023.

Questa è una novità rispetto agli anni precedenti dove "Multiple Targets" era la categoria con il più alto numero di incidenti.

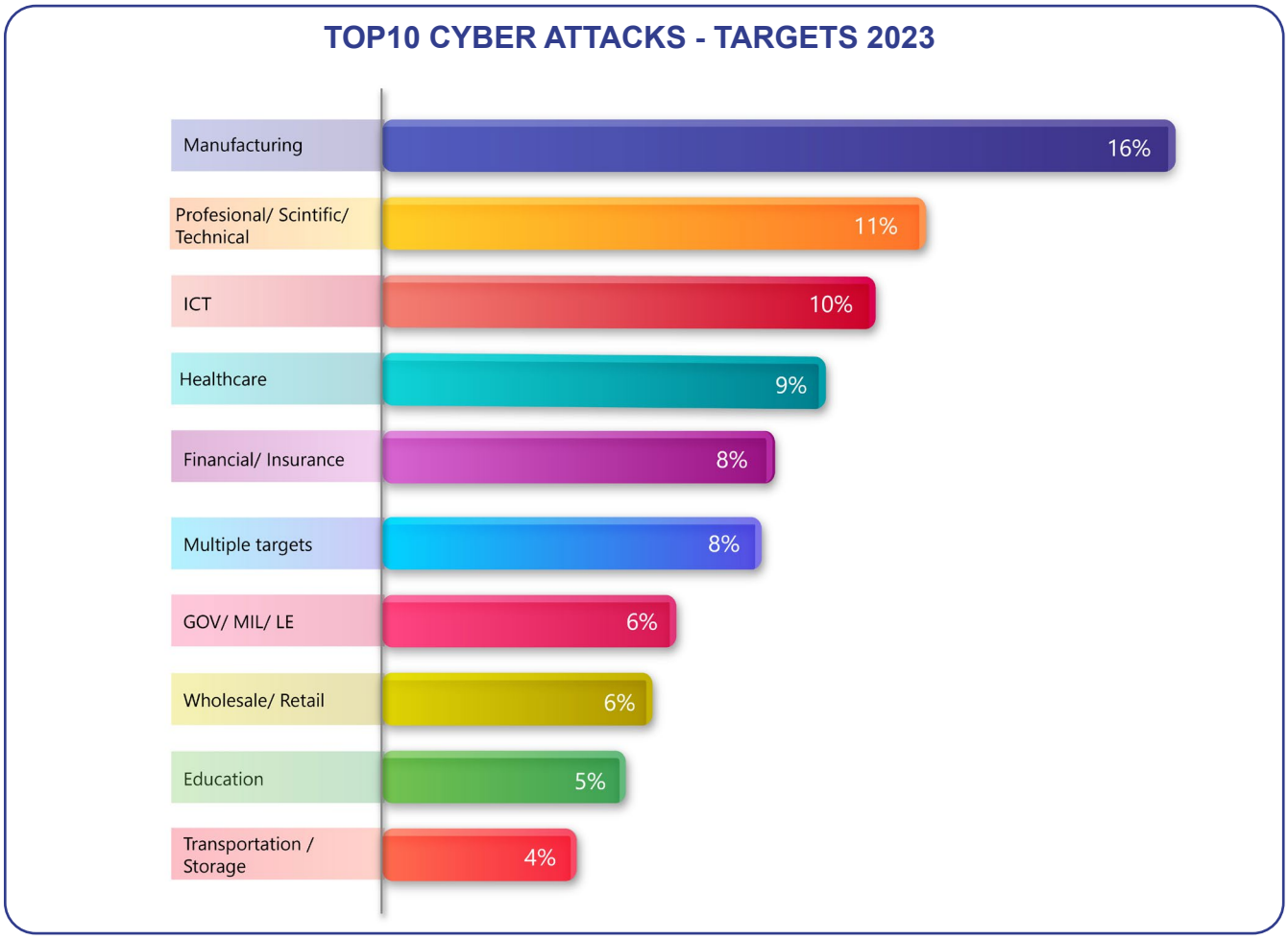

Figura 4: Distribuzione delle prime 10 categorie di vittime nel 2023

Nel 2023 questa categoria viene invece presa di mira solo nell'**8%** dei casi (rispetto al 21% del 2022) e, per la prima volta, figura solo al sesto posto tra le prime 10 categorie merceologiche delle vittime.

Un altro settore in notevole crescita e al secondo posto tra i settori maggiormente presi di mira è **Professional / Scientific / Technical**, che passa dal 3% all'**11%** degli attacchi totali.

A seguire **ICT** (**10%**), **Healthcare** (**9%**) e **Financial / Insurance** (**8%**).

LA GEOGRAFIA DELLE VITTIME

Nel 2023 tornano a crescere le vittime sul territorio americano che, dopo la flessione degli anni precedenti, si erano attestate al 37% nel 2022.

Nel 2023 l'**America** viene invece impattata per il **50% degli attacchi.**

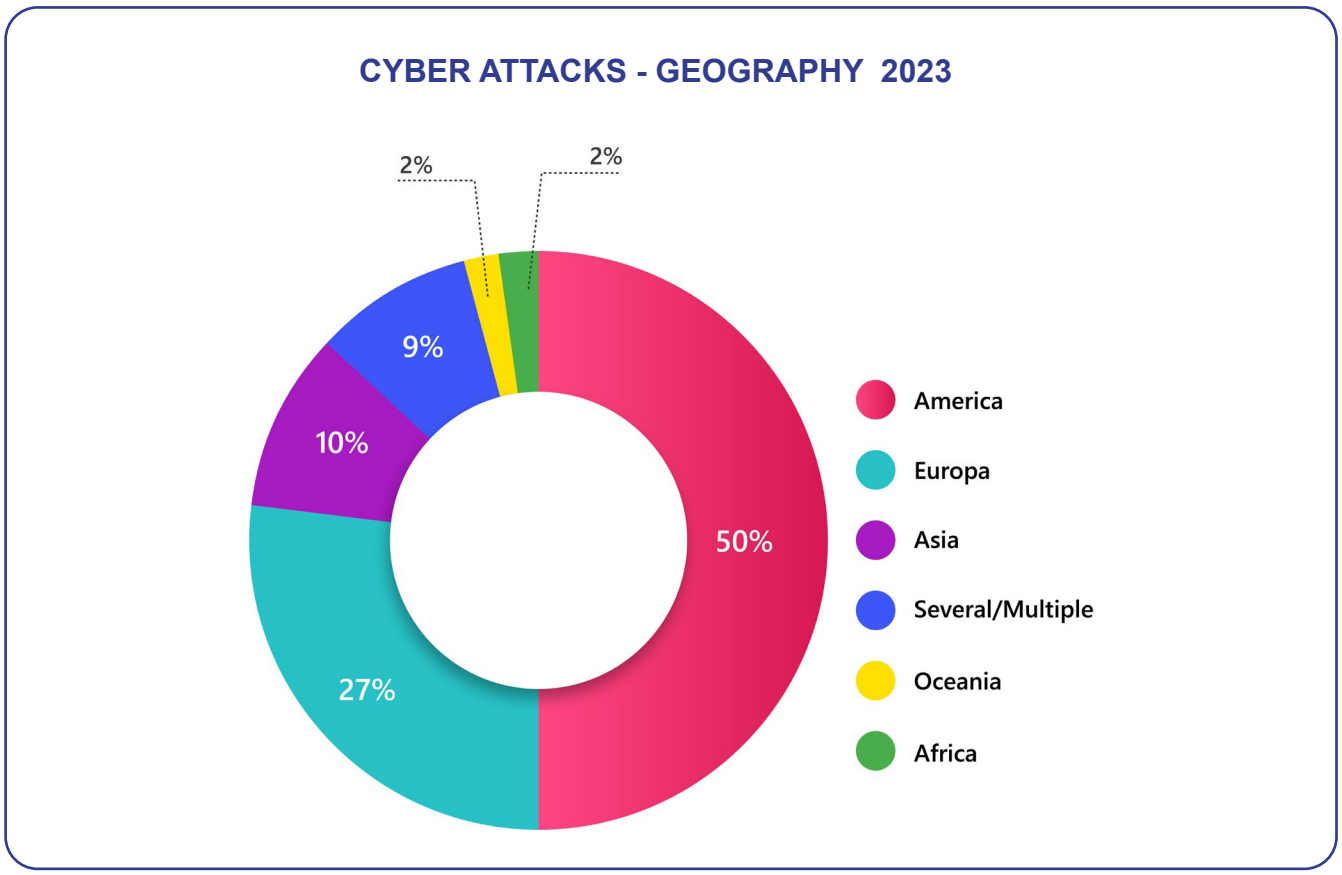

Figura 5: Distribuzione delle vittime per continente nel 2023

L'incremento degli attacchi americani non avviene però a discapito di quelli verso l'**Europa** che continuano a salire passando dal 24% nel 2022 al **27%**, quasi un terzo del totale degli incidenti.

In aumento anche gli attacchi verso **Asia**, cresciuti dall'8% al **10%**, e **Africa**, da una quota sostanzialmente irrisoria nel 2022 al **2%** del totale degli eventi classificati nel 2023.

Restano sostanzialmente invariate le quote di **Oceania** (**2%**), mentre scendono considerevolmente gli attacchi verso bersagli situati in località **multiple**, passando dal 29% nel 2022 al **9%**, a riprova del fatto che nel 2023 gli attacchi sono più mirati.

LE TECNICHE DI ATTACCO

Non è un segreto che da diversi anni il **Malware** spicca tra le tecniche di attacco più utilizzate dai cyber criminali, anche grazie alla notevole "resa" dei ransomware per gli attaccanti.

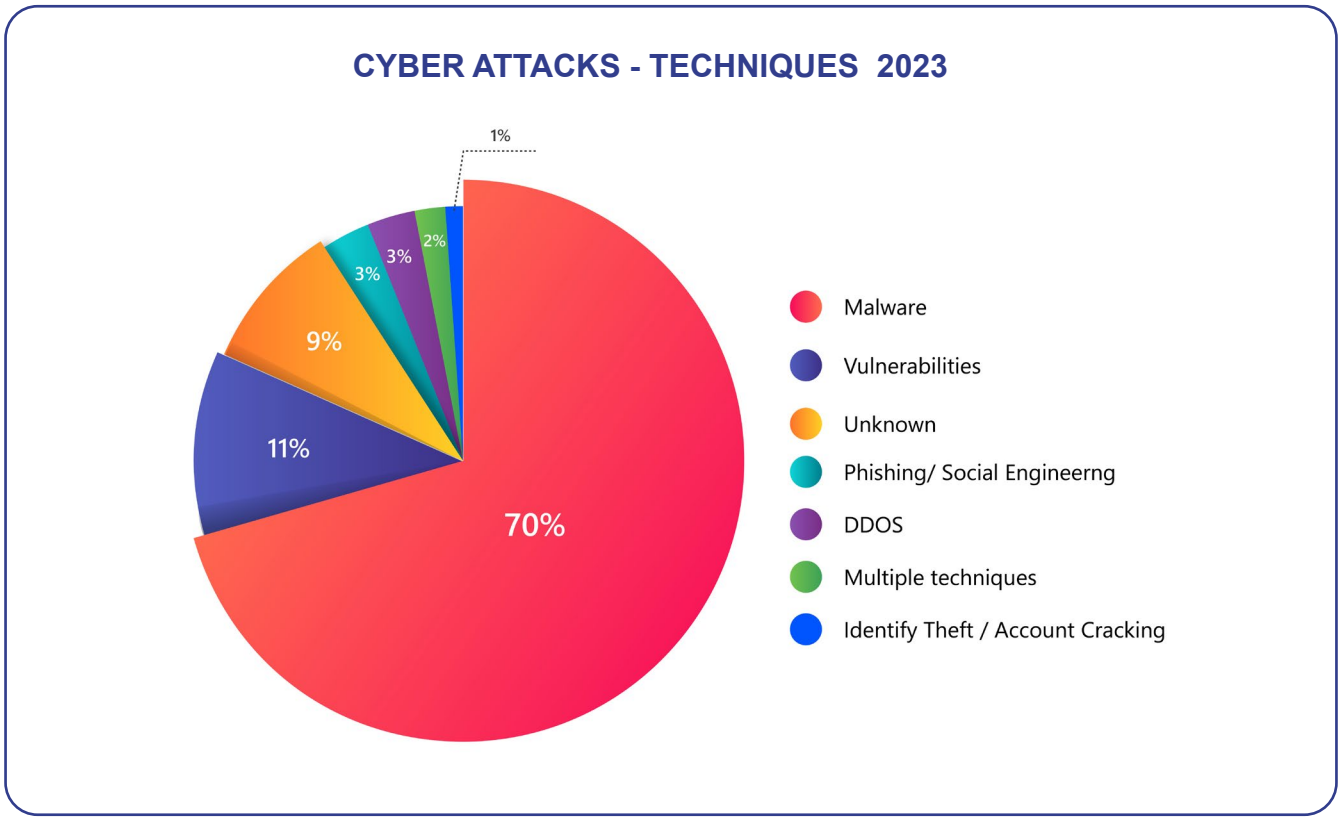

Figura 6: Distribuzione delle tecniche di attacco nel 2023

Ma nel 2023 il ricorso a questa tecnica aumenta pericolosamente, arrivando quasi a raddoppiare e toccando il **70%** del totale degli attacchi (rispetto al 37% nel 2022), indice che i cyber criminali fanno sempre più affidamento sull'impiego di codice malevolo.

Seguono lo **sfruttamento delle vulnerabilità** (**11%**), in leggero calo rispetto all'anno scorso, e le tecniche sconosciute (**9%**), in netta diminuzione rispetto al 24% del 2022, un ulteriore segnale che gli attaccanti prediligono a questo punto tecniche più affidabili e consolidate.

Diminuisce inoltre il ricorso a **Phishing / Social Engineering** (dal 12% al **3%**), **DDoS** (dal 4% al **3%**), **tecniche multiple** (dal 7% al **2%**), I**dentity Theft / Account Cracking** (dal 3% all'**1%**).

I Web attack, che già negli anni precedenti rappresentavano una minima parte degli attacchi totali, continuano la loro decrescita e raggiungono a questo punto quota zero.

GLI IMPATTI

Oltre a svolgere un'analisi statistica degli incidenti avvenuti, abbiamo introdotto una stima dei loro impatti, elemento essenziale per comprendere quanto gli attacchi analizzati siano stati concretamente incisivi.

L'algoritmo con cui effettuiamo questa valutazione assegna uno score di "severity" agli impatti osservati, in termini di ricadute economiche, tecnologiche e di reputazione.

Per raggruppare in modo sintetico i diversi livelli di gravità degli attacchi abbiamo definito 4 classi di severity: Low, Medium, High e Critical.

Nel 2023 gli attacchi con impatti gravi o gravissimi sono il **91%**, la percentuale più alta degli ultimi 7 anni, un dato francamente molto preoccupante.

Quasi un quarto degli attacchi (**24%**) hanno avuto impatti **critici,** una quota impressionante considerando che le ripercussioni per le vittime di attacchi di questa natura in termini economici, legali o reputazionali sono spesso catastrofiche.

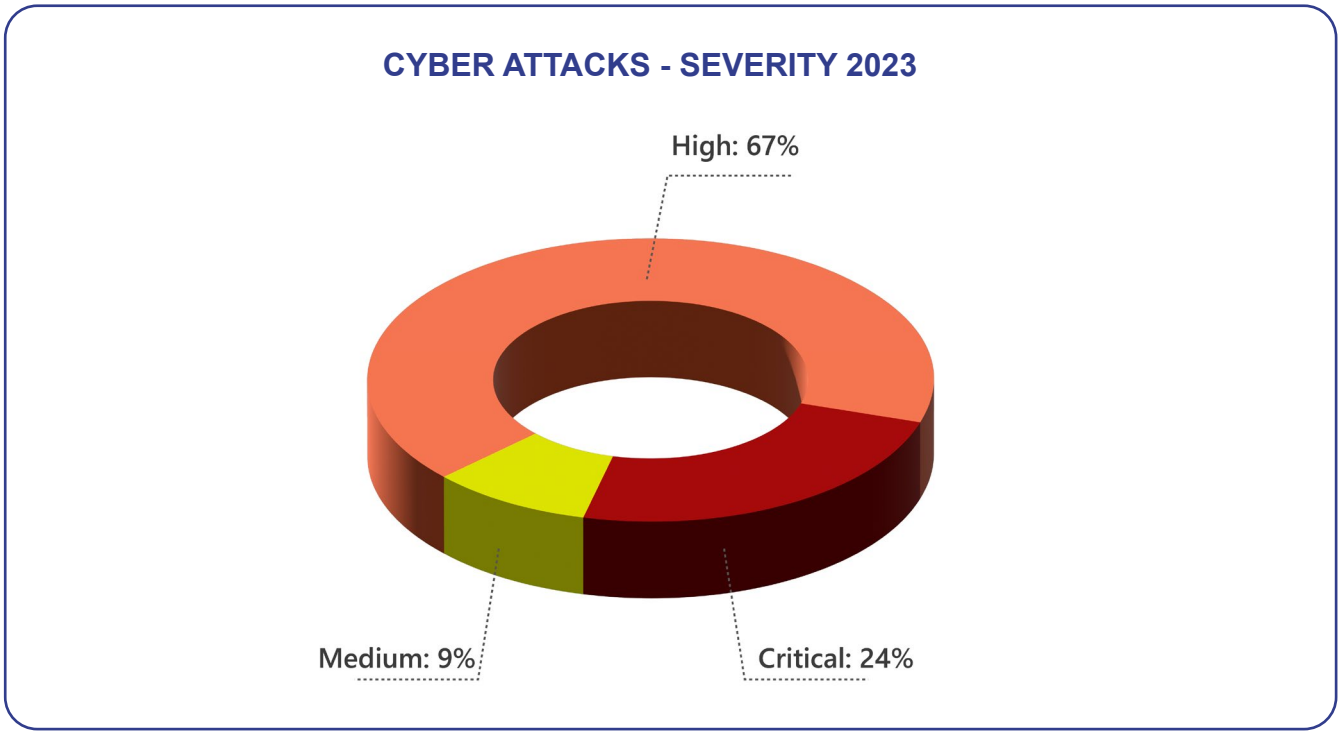

Figura 7: Distribuzione delle severity degli attacchi nel 2023

Anche gli attacchi con **impatti gravi** crescono considerevolmente, passando dal 44% nel 2022 al **67%**.

Diminuiscono invece quelli con **impatti medi** (dal 19% al **9%**), mentre restano a quota zero quelli con impatti classificati come "Low".

LA PROSPETTIVA RANSOMWARE

Il ransomware, una forma di attacco informatico sempre più diffusa e sofisticata, rappresenta un grave pericolo per individui, aziende e intere comunità digitali. Questo tipo di minaccia si è evoluto nel corso degli anni, diventando uno strumento di estorsione altamente efficace per i criminali informatici. Esploriamo le ragioni per cui il ransomware è considerato così pericoloso, analizzando le sue implicazioni tecniche, finanziarie e sociali. In primo luogo, il ransomware colpisce indiscriminatamente, prendendo di mira sia le grandi imprese che gli utenti individuali. La sua capacità di infiltrarsi nei sistemi informatici attraverso varie vie, come email di phishing, siti web compromessi o vulnerabilità di software, lo rende una minaccia onnipresente. Una volta che il ransomware infetta un dispositivo o una rete, cripta i file crittografandoli, rendendoli inaccessibili agli utenti legittimi. Questo processo di crittografia è spesso rapido e quasi indistinguibile, lasciando le vittime senza alcuna possibilità di prevenzione o difesa.

La natura silenziosa e subdola del ransomware aggiunge un ulteriore livello di pericolo. Molte varianti avanzate possono rimanere latenti all'interno di un sistema per lunghi periodi di tempo, studiando il comportamento dell'utente e dei processi di rete per massimizzare l'impatto dell'attacco. Questa capacità di mimetizzazione rende estremamente difficile per le soluzioni di sicurezza tradizionali rilevare e mitigare il ransomware in modo tempestivo, consentendo agli attaccanti di infliggere danni significativi prima di essere scoperti. Un'altra ragione per cui il ransomware è così pericoloso è la sua natura finanziaria. Gli attacchi ransomware sono spesso condotti da gruppi criminali organizzati che cercano un profitto rapido e considerevole. Le richieste di riscatto possono variare da centinaia a milioni di dollari, a seconda della dimensione e della natura critica dell'organizzazione colpita. Questo ha un impatto finanziario devastante sulle vittime, che devono affrontare non solo il costo del riscatto stesso, ma anche le perdite legate alla sospensione delle attività, al recupero dei dati e alla riparazione dei sistemi compromessi.

Inoltre, il ransomware può avere gravi implicazioni per la sicurezza nazionale e la stabilità economica. Settori cruciali come la sanità, le infrastrutture critiche e le istituzioni governative sono spesso bersagliati da attacchi ransomware, mettendo a rischio la vita e il benessere dei cittadini e la continuità delle operazioni vitali. Inoltre, le aziende colpite possono subire danni reputazionali significativi, perdendo la fiducia dei clienti e degli investitori e danneggiando l'intera economia. Da un punto di vista sociale, il ransomware mina la fiducia nell'ambiente digitale e alimenta il timore e l'insicurezza tra gli utenti. Le persone possono sentirsi impotenti di fronte alla minaccia del ransomware, temendo di perdere i propri dati personali o finanziari in qualsiasi momento. Questo può portare a comportamenti difensivi, come l'evitare di utilizzare determinati servizi online o condividere informazioni sensibili, limitando così l'innovazione e lo sviluppo nell'ambiente digitale. Inoltre, il ransomware può essere utilizzato come arma geopolitica e strumento di guerra cibernetica. Stati nazione e gruppi sponsorizzati dallo stato possono sfruttare il ransomware per destabilizzare economie rivali, compromettere la sicurezza nazionale o raggiungere obiettivi geopolitici. Questo solleva preoccupazioni riguardo alla cyber-deterrenza e alla necessità di una cooperazione internazionale più stretta per affrontare le minacce cibernetiche transnazionali.

IL 2023 IN SINTESI

Attacchi totali registrati

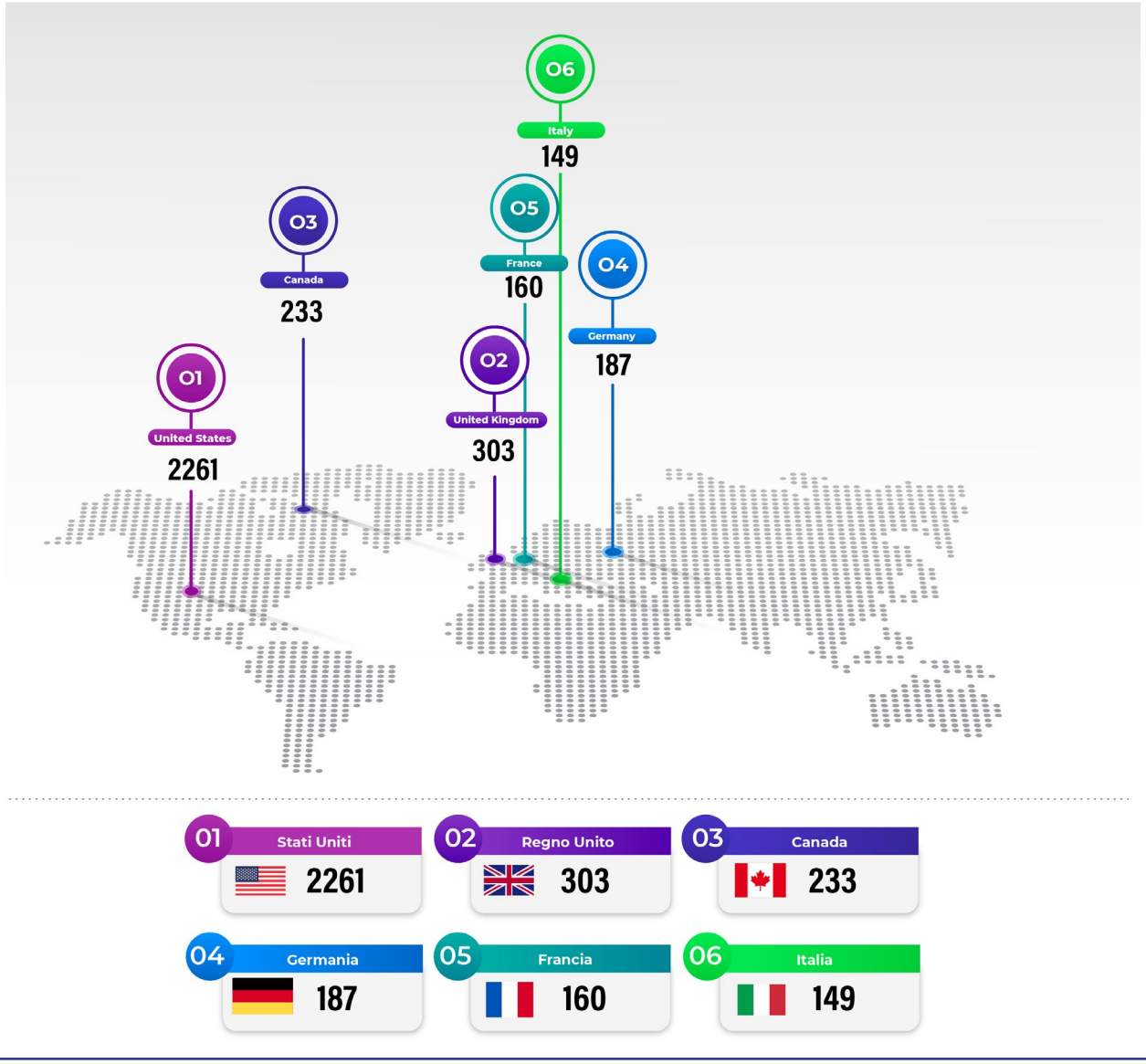

Figura 8: Distribuzione geografica

Nord America

Stati Uniti (2261 attacchi):

Gli Stati Uniti rimangono il principale bersaglio degli attacchi ransomware, con un numero estremamente elevato di incidenti segnalati. Questo riflette la grande dimensione dell'economia digitale statunitense e la presenza diffusa di aziende di varie dimensioni e settori, che sono spesso obiettivi primari per i criminali informatici.

Canada (233 attacchi):

Il Canada è stato anch'esso colpito da un numero considerevole di attacchi ransomware nel corso del 2023. Anche se meno colpito rispetto agli Stati Uniti e al Regno Unito, il fatto che i tre principali anglofoni siano sul podio delle vittime, riflette una certa "target selection" da parte dei Criminal Hacker.

Europa

Regno Unito (303 attacchi):

Anche il Regno Unito ha subito un numero significativo di attacchi ransomware, sebbene in misura molto minore rispetto agli Stati Uniti.

Germania (187 attacchi):

La Germania, come altri paesi europei, ha subito una quantità considerevole di attacchi ransomware nel corso del 2023.

Francia (160 attacchi):

Anche la Francia ha registrato un numero significativo di attacchi ransomware, sebbene inferiore rispetto ai primi tre paesi elencati.

Italia (149 attacchi):

L'Italia ha registrato un numero relativamente basso di attacchi ransomware rispetto agli altri paesi elencati. Tuttavia, è importante notare che il numero di attacchi nel secondo semestre (H2) è significativamente aumentato rispetto al primo semestre e secondo trimestre (61 vs 81), indicando un aumento della minaccia del ransomware nel corso dell'anno.

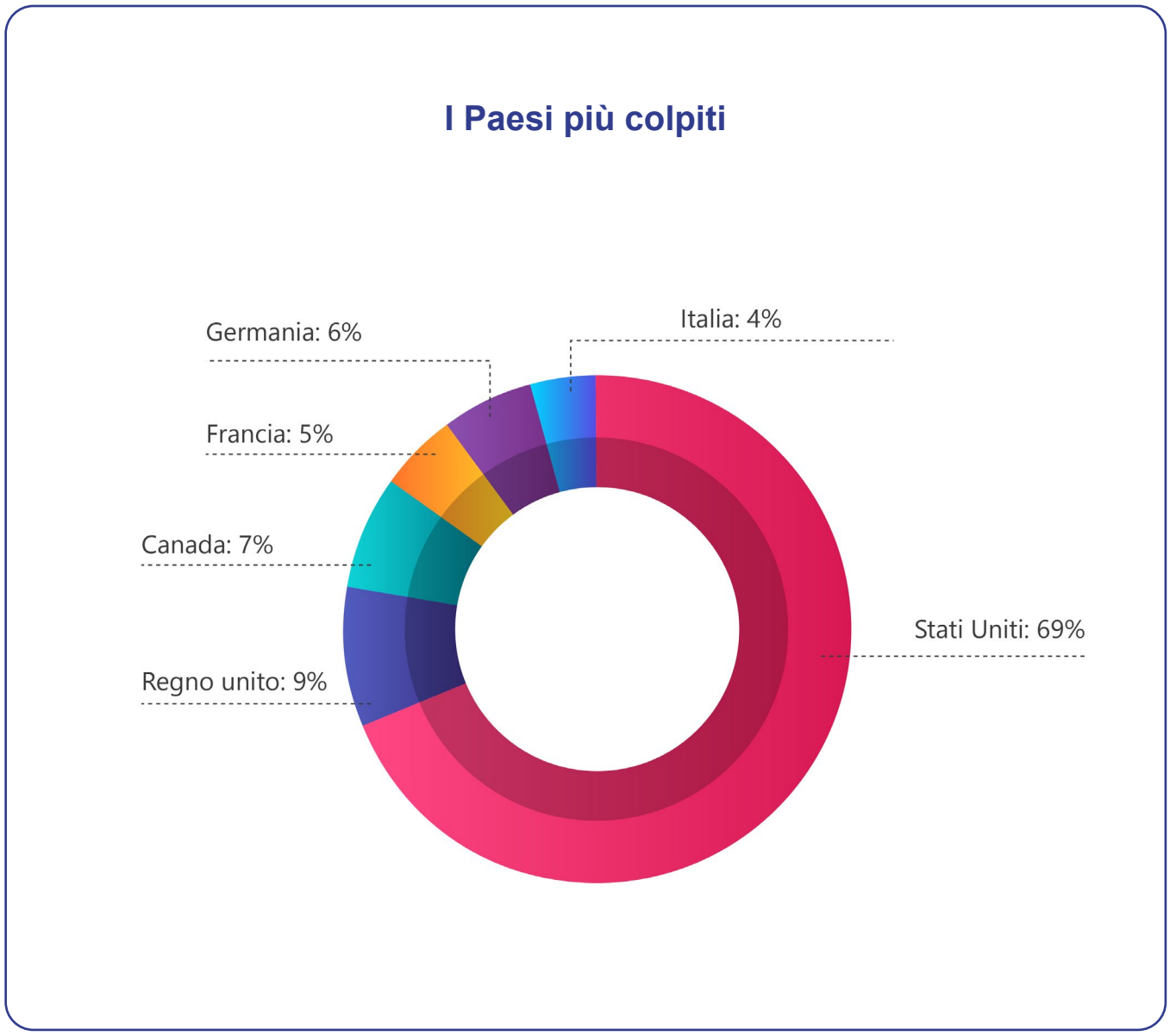

Figura 9: I paesi più colpiti

I SETTORI PRESI DI MIRA

L'analisi delle percentuali di attacchi ransomware nei vari settori durante il primo e il secondo semestre (H1 e H2) del 2023 offre interessanti spunti riguardo alle tendenze e ai cambiamenti nelle strategie degli attaccanti. Vediamo cosa ci dicono i dati:

Primo Semestre (H1):

1. **Servizi (45.5%):** Nel primo semestre, il settore dei servizi ha subito la percentuale più elevata di attacchi ransomware. Questo potrebbe essere attribuito alla vasta gamma di aziende e organizzazioni che rientrano in questa categoria, rendendola un bersaglio attraente per i criminali informatici. Le aziende dei servizi spesso gestiscono una grande quantità di dati sensibili dei clienti, rendendole obiettivi appetibili per estorsioni finanziarie.
2. **Manufacturing (15%):** Il settore manifatturiero è risultato essere il secondo più colpito nel primo semestre. Le aziende manifatturiere possono avere sistemi informatici complessi e interconnessi che, se compromessi, possono causare interruzioni significative nella produzione e nelle operazioni aziendali. Questo li rende un obiettivo desiderabile per i criminali informatici che cercano di ottenere un vantaggio finanziario attraverso l'estorsione di riscatti.
3. **Technology (7%):** Nonostante il settore tecnologico sia spesso associato a competenze avanzate in materia di sicurezza informatica, è stato comunque bersagliato da una percentuale significativa di attacchi ransomware nel primo semestre. Questo potrebbe indicare che anche le aziende tecnologiche, pur avendo competenze interne per gestire la sicurezza informatica, possono essere vulnerabili a minacce sofisticate.
4. **Finance (5%):** Il settore finanziario, noto per gestire dati altamente sensibili e transazioni finanziarie, è stato colpito dal 5% degli attacchi ransomware nel primo semestre. Questo sottolinea l'importanza cruciale per le istituzioni finanziarie di mantenere sistemi di sicurezza informatica robusti e resilienti per proteggere i propri dati e quelli dei clienti.
5. **Construction (4%):** Anche se in misura minore rispetto ad altri settori, il settore delle costruzioni ha comunque registrato un numero significativo di attacchi ransomware nel primo semestre. Le aziende di costruzioni possono gestire una vasta gamma di dati, inclusi piani di progettazione, informazioni finanziarie e dati dei fornitori, che possono essere obiettivi attraenti per i criminali informatici.

Secondo Semestre (H2):

1. **Manufacturing (20%):** Nel secondo semestre, il settore manifatturiero ha mostrato un aumento significativo nella percentuale di attacchi ransomware, diventando il settore più colpito. Questo cambiamento potrebbe essere attribuito a una varietà di fattori, tra cui l'aumento della dipendenza dalle tecnologie digitali nel settore manifatturiero e l'evoluzione delle tattiche degli attaccanti per sfruttare le vulnerabilità presenti.

2. **Servizi (21%):** Nonostante una leggera diminuzione rispetto al primo semestre, il settore dei servizi rimane uno dei più colpiti nel secondo semestre. Questo potrebbe riflettere la continua attrattiva delle aziende dei servizi come obiettivi per i criminali informatici, data la quantità di dati sensibili che gestiscono e la loro esposizione agli attacchi tramite e-mail di phishing e altre tecniche.

3. **Healthcare (11%):** Il settore sanitario è emerso come un nuovo obiettivo significativo nel secondo semestre, con una percentuale del 11% degli attacchi ransomware. Questo è preoccupante, considerando la natura altamente sensibile dei dati sanitari e il ruolo vitale che svolge il settore sanitario nel garantire la salute e il benessere della popolazione.

4. **Technology (9%):** Anche nel secondo semestre, il settore tecnologico è rimasto vulnerabile agli attacchi ransomware, sebbene con una percentuale leggermente inferiore rispetto al primo semestre. Questo sottolinea l'importanza per le aziende tecnologiche di continuare a investire nella sicurezza informatica e nell'aggiornamento delle proprie difese contro le minacce cibernetiche.

5. **Utilities (6%):** Il settore delle utilities, responsabile della fornitura di servizi essenziali come energia elettrica, acqua e gas, ha subito una percentuale significativa di attacchi ransomware nel secondo semestre. Questo solleva preoccupazioni riguardo alla sicurezza delle infrastrutture critiche e alla necessità di proteggere questi servizi vitali da potenziali minacce informatiche.

In conclusione, l'analisi delle percentuali di attacchi ransomware nei vari settori durante il primo e il secondo semestre del 2023 evidenzia la continua e crescente minaccia che questa forma di attacco rappresenta per un'ampia gamma di settori industriali. È essenziale che le aziende adottino una strategia di sicurezza informatica solida e aggiornata per proteggere i propri dati e le proprie operazioni dagli attacchi ransomware.

DIMENSIONE AZIENDALE: SPICCANO LE PMI

Le piccole e medie imprese (PMI) hanno subito un impatto sproporzionato dagli attacchi ransomware durante tutto il 2023, rappresentando una percentuale che si è mantenuta costantemente elevata, oscillando tra il 77% e l'80%.

Questo fenomeno può essere attribuito a diversi fattori. In primo luogo, molte PMI possono non avere le risorse finanziarie o umane necessarie per investire in soluzioni di sicurezza informatica avanzate o per implementare procedure di gestione dei rischi efficaci.

Di conseguenza, possono essere più vulnerabili agli attacchi ransomware e meno in grado di recuperare rapidamente dai danni causati. Inoltre, le PMI spesso gestiscono una vasta gamma di dati sensibili, tra cui informazioni finanziarie dei clienti, dati dei dipendenti e proprietà intellettuale, rendendole obiettivi attraenti per i criminali informatici in cerca di estorsioni finanziarie. Questo sottolinea l'importanza cruciale per le PMI di adottare misure proattive per proteggere i propri sistemi e dati, inclusa la formazione del personale sulla consapevolezza della sicurezza informatica.

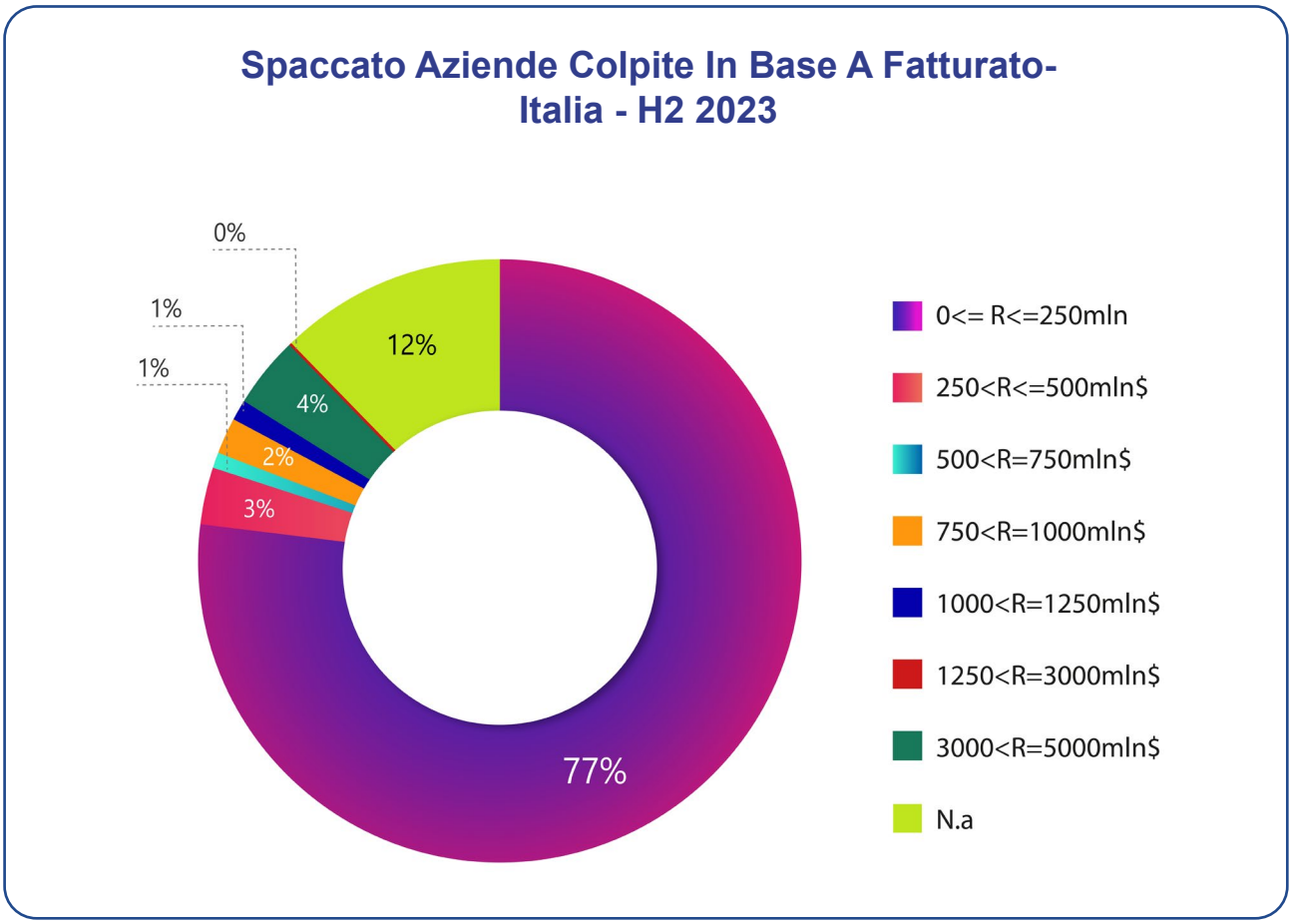

Figura 10: Spaccato Aziende Colpite In Base A Fatturato

DISCLAIMER & DATA COLLECTION NOTICE

La ricerca svolta dal Cyber Think Tank Assintel è basata su dati ottenuti tramite tecnologie proprietarie.

Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e Assintel si riserva la prerogativa di aggiornamento periodico.

Fonti di terze parti sono citate a seconda dei casi. Assintel non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione.

La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente.

Né Assintel né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.

Il presente rapporto è stato redatto esclusivamente dalle aziende parte del Cyber Think Tank Assintel.

Le informazioni raccolte e presentate in questo documento – in riferimento agli attacchi ransomware - rappresentano solo la parte "in chiaro" dell'intera situazione, poiché sono state prese in considerazione esclusivamente entità colpite da attacchi di ransomware che, avendo rifiutato di pagare il riscatto, hanno subito la pubblicazione dei propri dati su siti di data leak.

Si sottolinea che il numero riportato nel presente rapporto riflette un trend generale basato sulle informazioni disponibili. Tuttavia, è fondamentale comprendere che tale dato rappresenta solamente la punta dell'iceberg, in quanto il numero reale di vittime potrebbe essere significativamente superiore, considerando un fattore moltiplicativo n volte più grande.

Assintel non può garantire l'esattezza o la completezza delle informazioni fornite nel rapporto, poiché tali dati sono soggetti a cambiamenti e possono essere influenzati da vari fattori esterni. Gli utenti sono pertanto invitati a considerare attentamente il contesto e la complessità della situazione prima di trarre conclusioni definitive o prendere decisioni basate su queste informazioni.

Si declina ogni responsabilità per eventuali conseguenze derivanti dall'uso delle informazioni contenute nel presente rapporto. Assintel si impegna a mantenere la massima riservatezza e professionalità nelle proprie attività di analisi e fornisce questo rapporto a scopo informativo senza assumersi alcuna responsabilità legale o di altro genere.

Analysis by:

Hackmanac
Mediatech
Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

www.assintel.it
segreteria@assintel.it

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

CYBER
Think Tank
ASSINTEL

Assintel è l'associazione nazionale delle imprese ICT e rappresenta le aziende dell'ecosistema tecnologico e digitale italiano.

Aderisce a Confcommercio – Imprese per l'Italia, entro cui è punto di riferimento per la valorizzazione del Digitale, sia a livello di mercato sia di politiche istituzionali.

L'associazione è un vero business network per l'ecosistema ICT, capace di creare relazioni, sinergie e opportunità concrete per le aziende socie su tutto il territorio nazionale, negli ambiti tecnologici più innovativi e nei diversi settori economici, dagli operatori globali alle PMI e alle startup.